CAIQv3.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	N/A	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	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 AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Dedalus SaaS has tested the application using tool based on OWASP model guided by own security team.
		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 AWS Software Development Lifecycle, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. Refer to the AWS Overview of Security Processes for further details. That whitepaper is located here. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf Dedalus SaaS uses tools for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells, and security vulnerabilities.
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?		x		Manual source-code analysis is not employed. Automated code analysis tools are run as a part of the AWS Software Development Lifecycle
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	x			AWS implements open source software or custom code within its services. All open source software to include binary or machine-executable code from third-parties is reviewed and approved by the Open Source Group prior to implementation, and has source code that is publicly accessible. AWS service teams are prohibited from implementing code from third parties unless it has been approved through the open source review. All code developed by AWS is available for review by the applicable service team, as well as AWS Security. By its nature, open source code is available for review by the Open Source Group prior to granting authorization for use within Amazon. Dedalus SaaS use open source software or custom code within its services. Before going the adoption, there is a team that validate the implemented code.
		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, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. Refer to the AWS Overview of Security Processes for further details. That whitepaper is located here. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf Dedalus performs vulnerability scanning (SAST and DAST) of SaaS application as a part of Dedalus Software Development Life Cycle (SDLC).
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	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			AWS and Dedalus agree to a service agreement outlining the terms of service and responsibilities of both parties prior to service delivery. The requirements of Dedalus SaaS application cited will be the same of master account
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	x			AWS and Dedalus agree to a service agreement outlining the terms of service and responsibilities of both parties prior to service delivery. The requirements of Dedalus SaaS application cited will be the same of master account
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?	x			AWS data integrity controls as described in AWS SOC reports for S3, illustrates the data integrity controls maintained through all phases including transmission, storage and processing. Dedalus implements input and output integrity routines in the application and databases layer utilized within AWS environment.
		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			AWS data integrity controls as described in AWS SOC reports for S3, illustrates the data integrity controls maintained through all phases including transmission, storage and processing. Dedalus implements input and output integrity routines in the application and databases layer utilized within AWS environment.
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	x			The scope is in charge to the CSP AWS
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the	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			The scope is in charge to the CSP AWS
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	x			The scope is in charge to the CSP AWS
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	x			The scope is in charge to the CSP AWS
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	x			The scope is in charge to the CSP AWS
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	x			The scope is in charge to the CSP AWS
		AAC-02.4		Do you conduct internal audits at least annually?	x			The scope is in charge to the CSP AWS
		AAC-02.5		Do you conduct independent audits at least annually?	x			The scope is in charge to the CSP AWS
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?		x		
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	x			The scope is in charge to the CSP AWS
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	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			The scope is in charge to the CSP AWS
Business Continuity Management &	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to	Does your organization have a plan or framework for business continuity management or disaster recovery management?	x			The scope is in charge to the CSP AWS
		BCR-01.2		Do you have more than one provider for each service you depend on?	x			The scope is in charge to the CSP AWS

Operational Resilience *Business Continuity Planning*		BCR-01.1	ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you provide a disaster recovery capability?	x			Dedalus deploy SaaS on AWS placing instances and storing data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated AWS processes move data traffic away from the affected area.
		BCR-01.2		Do you monitor service continuity with upstream providers in the event of provider failure?	x			The scope is in charge to the CSP AWS
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?		x		Dedalus SaaS use publicly available mechanisms provided by AWS to report security and/or privacy events, including disasters.
		BCR-01.6		Do you provide a tenant-triggered failover option?	x			
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?		x		
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	x			The scope is in charge to the CSP AWS
Business Continuity Management & Operational Resilience	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and	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			The scope is in charge to the CSP 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			The scope is in charge to the CSP AWS
Business Continuity Management & Operational Resilience *Documentation*	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	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			The scope is in charge to the CSP AWS
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical damage anticipated and are countermeasures included in the design of physical protections?	x			The scope is in charge to the CSP AWS
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	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		
Business Continuity Management &	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	x			The scope is in charge to the CSP AWS
		BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?	x			The scope is in charge to the CSP AWS
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	x			The scope is in charge to the CSP AWS
Business Continuity Management &	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud	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, downtime tolerance, RPO and RTO etc)?	x			The scope is in charge to the CSP AWS
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	x			The scope is in charge to the CSP AWS

Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x			The scope is in charge to the CSP AWS
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical capabilities to enforce tenant data retention policies?	x			AWS maintains a retention policy applicable to AWS internal data and system components in order to continue operations of AWS business and services. Critical AWS system components, including audit evidence and logging records, are replicated across multiple Availability Zones and backups are maintained and monitored. Dedalus retain control and ownership of content stored in AWS Infrastructure and choose the appropriate data retention policy.
		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			AWS maintains a retention policy applicable to AWS internal data and system components in order to continue operations of AWS business and services. Critical AWS system components, including audit evidence and logging records, are replicated across multiple Availability Zones and backups are maintained and monitored. Dedalus maintains documented policies and procedures with data retention period compliance to GDPR requirements.
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			Dedalus implement backup and recovery of SaaS to ensure compliance with GDPR and business requirements.
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	x			Dedalus SaaS is deployed on Amazon EC2 instance and AWS automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair.
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?		x		Dedalus SaaS provides capability to restore a virtual machine to a previous configuration with AWS snapshot volume policy. Dedalus doesn't provide tenants to restore independetly a virtual machine
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?	x			Dedalus SaaS can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	x			Dedalus test backup of SaaS infrastructure annually.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	x			The scope is in charge to the CSP AWS
Change Control & Configuration Management	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	x			The scope is in charge to the CSP AWS
		CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	x			The scope is in charge to the CSP AWS
Change Control & Configuration Management *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	x			The scope is in charge to the CSP AWS
		CCC-03.2		Is documentation describing known issues with certain products/services available?	x			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	x			The scope is in charge to the CSP AWS
		CCC-03.5		Do you have controls in place to detect source code security defects for any outsourced software development activities?		x		
		CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	x			The scope is in charge to the CSP AWS
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	x			The scope is in charge to the CSP AWS
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?			x	Dedalus does not provide this level of detail of the Change Managemetn Process to customers. Dedalus notifies customers of changes to the SaaS offering in accordance with the Customer Agreement. Dedalus continuously evolves and improves existing services and frequently adds new services. If we change or discontinue any APIs, we will continue to offer the existing API for 24 months.
		CCC-05.2		Do you have policies and procedures established for managing risks with respect to change management in production environments?	x			The scope is in charge to the CSP AWS
		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 scope is in charge to the CSP AWS
Data Security & Information Lifecycle Management	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	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			The scope is in charge to the CSP AWS
		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		
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure	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			Dedalus SaaS determine the design patterns based on usage of AWS services and associated network and system components.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	x			The scope is in charge to the CSP AWS
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	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			The scope is in charge to the CSP AWS
		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			AWS APIs are available via TLS protected endpoints, which provide server authentication. Dedalus use TLS for all of interactions with AWS. AWS provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	x			Dedalus retain control and ownership of their data and implement a labeling and handling policy and procedures to meet requirements in order to ensure the security of data and objects that contain data
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		x		Dedalus use a internal standard policy to manage and label data.
		DSI-04.3		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		x		

Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	x				The scope is in charge to the CSP AWS
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	x				Dedalus has a own procedure to identify and assign the data stewardship to specific owner.
Data Security & Information Lifecycle Management	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	x				The scope is in charge to the CSP AWS
		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				The scope is in charge to the CSP AWS
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	x				The scope is in charge to the CSP 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				The scope is in charge to the CSP AWS
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	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				The scope is in charge to the CSP AWS
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Do you have a capability to use system geographic location as an authentication factor?	x				Dedalus should provide conditional user access based on IP address using IPSEC connection or AWS Security Group functionality.
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	x				The scope is in charge to the CSP AWS
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	x				The scope is in charge to the CSP AWS
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with your asset management policies and procedures?	x				The scope is in charge to the CSP AWS
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing	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				The scope is in charge to the CSP 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				The scope is in charge to the CSP AWS
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	x				The scope is in charge to the CSP AWS

Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	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			The scope is in charge to the CSP AWS
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	x			The scope is in charge to the CSP AWS
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	x			The scope is in charge to the CSP AWS
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of	Do you have a capability to allow creation of unique encryption keys per tenant?	x			The scope is in charge to the CSP AWS
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	x			The scope is in charge to the CSP AWS
		EKM-02.3		Do you maintain key management procedures?	x			The scope is in charge to the CSP AWS
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	x			Dedalus uses AWS Key Management Systems (KMS) to create and manage encryption keys lifecycle and document each stage of the lifecycle of encryption keys
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	x			The scope is in charge to the CSP AWS
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in	Do you encrypt tenant data at rest (on disk/storage) within your environment?	x			Dedalus use AWS encryption mechanism for EC2 and RDS, IPSec tunnel to VPC, KMS to create and control encryption
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	x			Dedalus use AWS encryption mechanism for EC2 and RDS, IPSec tunnel to VPC, and to create and control encryption
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	x			The scope is in charge to the CSP AWS
		EKM-03.4		Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	x			The scope is in charge to the CSP AWS
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	x			Dedalus uses AWS Key Management Systems (KMS) to create and manage encryption keys lifecycle
		EKM-04.2		Do you store encryption keys in the cloud?	x			Dedalus use AWS KMS to store encryption keys in the cloud
		EKM-04.3		Do you have separate key management and key usage duties?		x		
Governance and Risk Management *Baseline*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that	Do you have baseline security requirements for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	x			The scope is in charge to the CSP AWS
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	x			The scope is in charge to the CSP AWS
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	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			In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition, AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/ . In addition, Dedalus SaaS could choose a specific AWS region for data residency, based on specific customer requirements. Dedalus maintains documented policies and procedures with data retention period compliance to GDPR requirements.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	x			The scope is in charge to the CSP AWS
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	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 scope is in charge to the CSP AWS
Governance and Risk Management	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	x			The scope is in charge to the CSP AWS
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	x			The scope is in charge to the CSP AWS
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	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			The scope is in charge to the CSP AWS
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be 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.	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			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
		GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	x			The scope is in charge to the CSP AWS
		GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	x			The scope is in charge to the CSP AWS
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	x			The scope is in charge to the CSP AWS
Governance and Risk Management	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	x			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS

Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	x				The scope is in charge to the CSP AWS
Governance and Risk Management	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		x			
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	x				The scope is in charge to the CSP AWS
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determine the likelihood and impact of all identified risks, using qualitative and quantitative methods?	x				The scope is in charge to the CSP AWS
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	x				The scope is in charge to the CSP AWS
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	x				The scope is in charge to the CSP AWS
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?		x			Dedalus doesn't provide the Risk Management program to the customer, this document is categorized as "confidential". Dedalus Risk Management program is reviewed by internal auditors during audits for our ISO 27001 compliance.
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	x				The scope is in charge to the CSP AWS
		HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?	x				The scope is in charge to the CSP AWS
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	x				The scope is in charge to the CSP AWS
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	x				The scope is in charge to the CSP AWS
		HRS-03.2	workforce personnel user access to corporate facilities, resources, and	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				The scope is in charge to the CSP AWS
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and	Are documented policies, procedures, and guidelines in place to ensure change in employment and/or terminations?	x				The scope is in charge to the CSP AWS
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	x				The scope is in charge to the CSP AWS
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	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				The scope is in charge to the CSP AWS
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	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				The scope is in charge to the CSP AWS
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	x				The scope is in charge to the CSP AWS
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-	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				The scope is in charge to the CSP AWS
		HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	x				The scope is in charge to the CSP AWS
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and	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				The scope is in charge to the CSP AWS
		HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	x				The scope is in charge to the CSP AWS
		HRS-09.3	regular updates in organizational procedures, processes, and policies	Do you document employee acknowledgement of training they have completed?	x				The scope is in charge to the CSP AWS

		HRS-09.4	regular updates in organizational procedures, policies, and policies relating to their professional function relative to the organization.	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	x			The scope is in charge to the CSP AWS	
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	x			The scope is in charge to the CSP AWS	
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	x			The scope is in charge to the CSP AWS	
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	x			The scope is in charge to the CSP AWS	
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	x			The scope is in charge to the CSP AWS	
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	x			The scope is in charge to the CSP AWS	
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	x			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	x			The scope is in charge to the CSP AWS	
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			The scope is in charge to the CSP AWS	
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-term contracts, third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management approval, firefighter duties, etc.) • Access segmentation to sessions and data in multi-tenant system architectures by customers and non-customers • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	x			The scope is in charge to the CSP AWS	
		IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	x			The scope is in charge to the CSP AWS	
		IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multi-factor authentication?	x			The scope is in charge to the CSP AWS	
		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			
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	x			The scope is in charge to the CSP AWS	
Identity & Access Management	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also require the use of standardized	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			The scope is in charge to the CSP AWS	
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	x			The scope is in charge to the CSP AWS	
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	x			Dedalus retain the ability to manage segregations of duties of the AWS resources. Dedalus follow AWS best practices for Identity & Access Management can be found here: AWS IAM Best Practices Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	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			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Does your organization conduct third-party unauthorized access risk assessments?	x			AWS does not utilize third parties to provide services to customers, but does utilize co-location provides in limited capacity to house some AWS data centers. These controls are audited twice annually in our SOC 1/2 audits and annually in our ISO 27001/17/18 audits. There are no subcontractors authorized by AWS to access any customer-owned content that customers upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/ Dedalus does a risk assessment for third parties and it identify a data controller.	
		IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	x			AWS does not utilize third parties to provide services to customers, but does utilize co-location provides in limited capacity to house some AWS data centers. These controls are audited twice annually in our SOC 1/2 audits and annually in our ISO 27001/17/18 audits. There are no subcontractors authorized by AWS to access any customer-owned content that customers upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/ Dedalus does a risk assessment for third parties and it identify a data controller.	
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	x			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?	x			The scope is in charge to the CSP AWS	
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer data is used as part of the service and/or customer has some shared responsibility over implementation of control.	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			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	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			The scope is in charge to the CSP AWS	
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	x			The scope is in charge to the CSP AWS	
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	x			The scope is in charge to the CSP AWS	
		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			AWS 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. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001 and PCI audits. Dedalus SaaS can remediate and it will send an security update notice to all the tenants.	
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer data is used as part of the service and/or customer has some shared responsibility over implementation of control.	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			The scope is in charge to the CSP AWS	
		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			The scope is in charge to the CSP AWS	
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	x			The scope is in charge to the CSP AWS	
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	x			The scope is in charge to the CSP AWS	
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	x			The scope is in charge to the CSP AWS	
		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			Dedalus enable Policy Enforcement Point capability using a dedicated Identity Providers and establish a fine grained policies to manage permissions to AWS resources. Dedalus SaaS provide XACML policy to enforce regional legal and policy constraints in according to GDPR requirements.	
		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			The scope is in charge to the CSP AWS	
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	x			The scope is in charge to the CSP AWS	
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	x			The scope is in charge to the CSP AWS	
		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 scope is in charge to the CSP AWS	
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	x			Dedalus SaaS define password and account policies for accounts, to meet requirements of authentication framework as NIST 800-63	

		IAM-12.10		Do you support the ability to force password changes upon first logon?	x			Dedalus SaaS define password and account policies for accounts, to meet requirements of authentication framework NIST 800-63
		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			Dedalus SaaS define password and account policies for accounts, to meet requirements of authentication framework as NIST 800-63
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	x			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	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. External vulnerability assessments are conducted by an AWS approved third party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. Dedalus performs vulnerability scans penetration testing, file integrity monitoring and intrusion detection for Amazon EC2 used in SaaS application. Dedalus scan IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	x			The scope is in charge to the CSP AWS
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	x			The scope is in charge to the CSP AWS
		IVS-01.4		Are audit logs centrally stored and retained?	x			The scope is in charge to the CSP AWS
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	x			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	x			Dedalus log and alert any changes made to virtual machine images using AWS Cloud Trail feature.
		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			Dedalus log and alert any changes made to virtual machine images using AWS Cloud Trail feature.
		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			Dedalus log and alert any changes made to virtual machine images using AWS Cloud Trail feature. Dedalus take advantage of the Amazon Machine Images (AMI) to provide an image's integrity for SaaS. AWS is designed to protect the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. Dedalus use a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]). Dedalus protects data at rest using AWS encryption features.
Infrastructure & Virtualization Security *Clock*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	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			The scope is in charge to the CSP AWS
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	x			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	x			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			x	Dedalus doesn't offer IaaS to their customer.
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	x			Several network fabrics exist at Amazon, each separated by devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. Dedalus maintain information related to data flow and individual application architectures of SaaS AWS implementations.
		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		Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. 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. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, and ISO 27001. Dedalus maintain information related to data and individual architecture of SaaS application and it is also responsible for defining the security rules applied by the components offered by AWS
		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. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Dedalus maintain information related to data and individual architecture of SaaS application and it is also responsible for defining the security rules applied by the components offered by AWS
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	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			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	x			Dedalus SaaS provides separate environments for production and test processes
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			x	Dedalus doesn't offer IaaS to their customer.

		IVS-08.3		Do you logically and physically segregate production and non-production environments?	x			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	x			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
		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			Dedalus use AWS (Organization, VPC, subnet, etc) to segregate tenat and protect tenant's data.
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	x			Dedalus use AWS (Organization, VPC, subnet, etc) to segregate tenat and protect tenant's data.
Infrastructure & Virtualization Security	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-[illegible]	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	x			Dedalus use a secure, encrypted session to AWS servers using Transport Layer Security (TLS).
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	x			Dedalus use AWS (VPC, subnet, etc) to segregate production and non-production environments.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon 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).	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			The scope is in charge to the CSP AWS
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			x	Policies, procedures and mechanisms to protect AWS network environment are in place. There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.
		IVS-12.2	• The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	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	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.
		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	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall 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.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	x			Dedalus has designed a clearly architecure diagram to identify data flow and using network segmentation to segregate environmente. Internally, AWS network segmentation is aligned with the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		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 [illegible]	x			The scope is in charge to the CSP AWS
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	x			The scope is in charge to the CSP AWS
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	x			
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between [illegible]	x			Dedalus SaaS provides policies and procedures for the usage of APIs and for interoperability functionalities.
		IPY-03.2		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	x			Dedalus SaaS can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).
		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			Dedalus provides specific policies and proceucedures for the migration to and from Dedalus SaaS.
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to [illegible]	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			Dedalus use a secure, authenticathed and encrypted session to AWS servers using Transport Layer Security (TLS).
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	x			The scope is in charge to the CSP AWS
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	x			The scope is in charge to the CSP AWS
		IPY-05.2		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to [illegible]	x			Dedalus SaaS can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).
		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		

Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			x	AWS scope for mobile devices are iOS and Android based mobile phones and tablets. AWS maintains a formal mobile device policy and associated procedures. Specifically, AWS mobile devices are only allowed access to AWS corporate fabric resources and cannot access AWS production fabric where customer content is stored. AWS production fabric is separated from the corporate fabric by boundary protection devices that control the flow of information between fabrics. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. 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. Consequently, mobile devices are not relevant to AWS customer content access. Dedalus doesn't provides mobile application for this service.
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			x	See Response to MOS-01.1
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	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	See Response to MOS-01.1
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			x	See Response to MOS-01.1
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	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	See Response to MOS-01.1

Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	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		See Response to MOS-01.1
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			x		See Response to MOS-01.1
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			x		See Response to MOS-01.1
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	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		See Response to MOS-01.1
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	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		See Response to MOS-01.1

Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	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	See Response to MOS-01.1
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			x	See Response to MOS-01.1
		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	See Response to MOS-01.1
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	See Response to MOS-01.1
		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	See Response to MOS-01.1
Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			x	See Response to MOS-01.1
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			x	See Response to MOS-01.1
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			x	See Response to MOS-01.1
		MOS-16.2	and enforced through technical controls on all company devices or	Are your password policies enforced through technical controls (i.e. MDM)?			x	See Response to MOS-01.1
		MOS-16.3	devices approved for BYOD usage, and shall prohibit the changing of	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile			x	See Response to MOS-01.1
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	See Response to MOS-01.1
		MOS-17.2	backups of data, prohibit the usage of unapproved application stores,	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			x	See Response to MOS-01.1
		MOS-17.3	and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			x	See Response to MOS-01.1
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			x	See Response to MOS-01.1
		MOS-18.2	program or a company-assigned mobile device shall allow for remote	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			x	See Response to MOS-01.1
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			x	See Response to MOS-01.1
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			x	See Response to MOS-01.1
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			x	See Response to MOS-01.1
		MOS-20.2	access on a BYOD-enabled device.	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			x	See Response to MOS-01.1
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	x			The scope is in charge to the CSP AWS
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	x			The scope is in charge to the CSP AWS
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		x		
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	x			The scope is in charge to the CSP AWS
		SEF-02.4		Have you tested your security incident response plans in the last year?	x			The scope is in charge to the CSP AWS
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely	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			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	x			The scope is in charge to the CSP AWS
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	x			The scope is in charge to the CSP AWS
		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			Dedalus use AWS Organization, VPC, subnet, etc) to segregate tenat and protect tenant's data. Dedalus could choose to restore data on separate copy of server to investigative purposes.
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	x			The scope is in charge to the CSP AWS
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	x			The scope is in charge to the CSP AWS
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?			x	Dedalus tracks metrics for internal process measurements and improvements, but this level of detail is not shared with the customer and categorized ad "confidential". Any data breaches will be communicated to the data controller according to the GDPR policies.

Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	x			Dedalus SaaS inspect all accounts and analize the associated risks. Each third parties contractor must be conformed and identified as a data controller.
		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-privilege access for all personnel within your supply chain?	x			The scope is in charge to the CSP AWS
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	x			The scope is in charge to the CSP AWS
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with	Do you collect capacity and use data for all relevant components of your cloud service offering?	x			The scope is in charge to the CSP AWS
		STA-03.2		Do you provide tenants with capacity planning and use reports?	x			Dedalus for SaaS offering provide capacity planning for infrastructure sizing and use AWS report to monitor the consumption of resources.
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	x			The scope is in charge to the CSP AWS
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	x			The scope is in charge to the CSP AWS
		STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	x			The scope is in charge to the CSP AWS
		STA-05.3		Does legal counsel review all third-party agreements?	x			The scope is in charge to the CSP AWS
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	x			The scope is in charge to the CSP AWS
		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			Dedalus in the backup policies take the advantage of Amazon S3 and Glacier services that are designed to reduce the likelihood of data loss and provide durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website.
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	x			Dedalus SaaS could choose a specific AWS region to store data based on specific customer requirements.
		STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?	x			Dedalus SaaS could choose a specific AWS region to store data based on specific customer requirements.
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	x			Dedalus SaaS could choose a specific AWS region to store data based on specific customer requirements.
		STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		x		
		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			Dedalus SaaS monitor environments through AWS services (CloudWatch, etc) and application specific logs to detect privacy breaches. Dedalus SaaS follows the European laws regarding privacy according to the timing requirements (GDPR). For specific project the timing should be reduced in according to each tenants.
		STA-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		x		
		STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		x		
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	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			The scope is in charge to the CSP AWS
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	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			The scope is in charge to the CSP 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			AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/ Dedalus monitors the performaces for each subcontractors where each of them need to be conformed and identified as a data controller.
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	x			AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/ Dedalus monitors the performaces for each subcontractors where each of them need to be conformed and identified as a data controller.
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	x			The scope is in charge to the CSP AWS
		STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	x			The scope is in charge to the CSP AWS
		STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?	x			The scope is in charge to the CSP AWS
		STA-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	x			Dedalus provide isolated environment for each customer
		STA-07.8		Do you review all service level agreements at least annually?	x			The scope is in charge to the CSP AWS

Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?		x		AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/ Dedalus monitors the performaces for each subcontractors where each of them need to be conformed and identified as a data controller.
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?		x		AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/ Dedalus monitors the performaces for each subcontractors where each of them need to be conformed and identified as a data controller.
Supply Chain Management, Transparency, and	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party	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			The scope is in charge to the CSP AWS
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	x			The scope is in charge to the CSP AWS
Threat and Vulnerability Management *Anti-Virus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	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			The scope is in charge to the CSP AWS
		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			The scope is in charge to the CSP AWS
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	x			The scope is in charge to the CSP AWS
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	x			Dedalus retain control of guest operating systems, software and applications and performs regulary vulnerability scans and patching of their systems. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	x			Dedalus retain control of guest operating systems, software and applications and performs regulary vulnerability scans and patching of their systems. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?			x	
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	x			AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. Dedalus performs vulnerability scans penetration testing, file integrity monitoring and intrusion detection for Amazon EC2 used in SaaS application. Dedalus is responsible for maintaining the application of patches to Amazon instances.
		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			Dedalus provides the result of vulnerability scan to his customer. AWS Services terms are available at https://aws.amazon.com/service-terms/
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	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	Dedalus doesn't provide mobile code to be installed on mobile device, because provide a web application. AWS allows customers to manage client and mobile applications to their own requirements.
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			x	Dedalus doesn't provide mobile code to be installed on mobile device, because provide a web application. AWS allows customers to manage client and mobile applications to their own requirements.