SECURITY AND COMPLIANCE:

ZYLAB-ONE

SEPTEMBER 2018

This document provides an overview of ZyLAB's security and compliance commitments and information specific to ZyLAB-One, including detailed responses to the Cloud Security Alliance consensus questionnaire.

ZYLAB SECURITY AND COMPLIANCE

ZyLAB delivers innovative software for fact finding missions (eDiscovery) in large or small electronic data sets related to business-critical projects of governmental agencies, law firms and companies of any size.

ZyLAB appreciates that our customers place their trust in our company every day and that we have a responsibility to manage and protect our customers' information assets in exactly the same way as we protect our own. The Management Team of ZyLAB takes this responsibility very seriously and is fully committed to comply with industry best practices in regards to information security as illustrated in our overall ISO Certification strategy.

ZYLAB DELIVERS INNOVATIVE SOFTWARE FOR FACT FINDING MISSIONS

ZYLAB SECURITY AND COMPLIANCE

INFORMATION SECURITY GOALS

Being active in the fact finding arena (eDiscovery) adds requirements for ZyLAB to not only produce secure software, but also deliver a secure SaaS platform. Customers do require a high level of security for their information being processed under ZyLAB's control.

To meet these goals, ZyLAB maintains information security policies and defined several information security goals:

- *Confidentiality*

Confidentiality of information systems ensures only authorized entities can access the system and its data. ZyLAB processes customer confidential data in its applications that needs the appropriate protection against potential security risks. ZyLAB is a trustworthy organization securing information for its customers and itself.

- *Integrity*

Integrity is all about trustworthiness of information systems. Our security measures work to prevent unauthorized alteration of information processed in services offered by ZyLAB. This supports customer satisfaction and makes ZyLAB a trustworthy business partner.

- *Availability*

Availability is the characteristic that provides the information systems to authorized users when required. This supports customer satisfaction.

ZYLAB SECURITY AND COMPLIANCE

The way ZyLAB manages information security is based on the Network Application Consortium ESA framework. To ensure a pragmatic security framework, the Risk Bow-tie methodology is integrated in the NAC ESA framework. Besides this framework, requirements from ISO27001 are integrated in the security program.

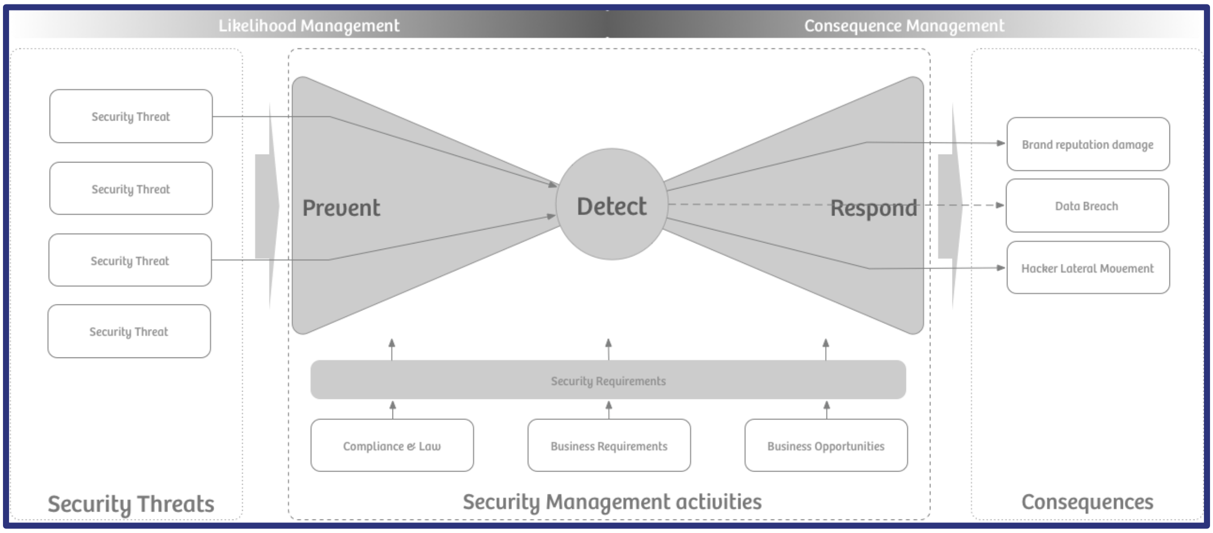


Figure 1: Security Control Framework Approach

Main goal of the information security program, and the security management activities, is to manage consequences caused by security threats for the organization. Security drivers affect the way the security activities are organized.

For details on how ZyLAB manages security for ZyLAB-One, our responses to the Cloud Security Alliance (CSA) consensus questionnaire (version 3.0.1) can be found in Appendix A.

ZYLAB SECURITY AND COMPLIANCE

CLOUD PLATFORM

The ZyLAB SaaS application is hosted in a high security Microsoft Azure Cloud. Azure Cloud meets Security policies which are determined based upon requirements from ISO27001 and the organization's threat profile. ZyLAB's information security goals are: the highest standards of physical and logical security and comply with industry standards.

More details can be found in this document and on Microsoft's website:
www.microsoft.com/en-us/trustcenter

CLOUD SECURITY ALLIANCE

The Cloud Security Alliance (CSA) is a nonprofit organization providing knowledge on securing cloud infrastructures. CSA performs ongoing research and develops resources to help companies improve cloud security. It offers the Certificate of Cloud Security Knowledge (CCSK) to prove knowledge of cloud security as well as consensus questionnaires and a cloud control matrix for securing your cloud services.

More information on the CSA can be found at
www.cloudsecurityalliance.org

SECURITY AUDITS

ZyLAB has an "agreement-to-be-audited" approach for customers wanting to audit our security by reviewing our policies, procedures or working instructions. Details on the audit process by a customer are available from your sales representative. Customer planning to perform penetration tests against our hosted environment should request this in advance. This is related to the Terms and Conditions from our service providers, as well as the fact we will assess if other customers might be affected. A penetration test request form is available via your sales representative.

ZYLAB-ONE SOLUTION - SECURITY AND COMPLIANCE

The ZyLAB-One solution is delivering a complete eDiscovery SaaS solution. ZyLAB-One's capability consists of ZyLAB Legal Processing, ZyLAB Legal Review & ZyLAB Legal Production.

Below is an overview of security and compliance information for capabilities within ZyLAB-One. Additional details are available in the CSA consensus questionnaire in Appendix A. For questions not addressed in this document, please contact your sales representative.

- *Datacenter*

The ZyLAB-One solution is hosted in Microsoft Azure Cloud. ZyLAB utilizes 2 production environments:
– *Azure EU (West Europe - NL) for EU based customers and*
– *Azure US (East) for US based customers*
No replication of data between datacenters is allowed by our policies.

- *Data encryption*

ZyLAB-One supports data encryption: At Rest – Both at Storage level as well as VM level (Azure managed Disks & Bitlocker). In transit - External endpoints use HTTPS with TLS v1.2, SHA 256-2048 bits.

- *Network Security Groups - NSG (Firewall & Security)*

NSGs are the gatekeepers of all virtual network subnets to allow/deny traffic from/to subnet and allow Customer isolation.

- *Application Gateway (Web Application Firewall)*

End-to-end SSL traffic (no offloading), URL restriction and OWASP 3.0 rule set are active on detection mode.

ZYLAB-ONE SOLUTION - SECURITY AND COMPLIANCE

- *Authentication*

Azure Active Directory (Azure AD) helps you ensure that only authorized users can access your computing environments, data, and applications. Multi Factor Authentication (MFA) is supported.

- *Vulnerability scans*

Vulnerability scanning of servers connected to the Internet is performed on a monthly basis. Vulnerabilities in server software will be updated on a regular basis via automated processes. Anti-Malware software on servers completes the security of the server infrastructure of ZyLAB-One.

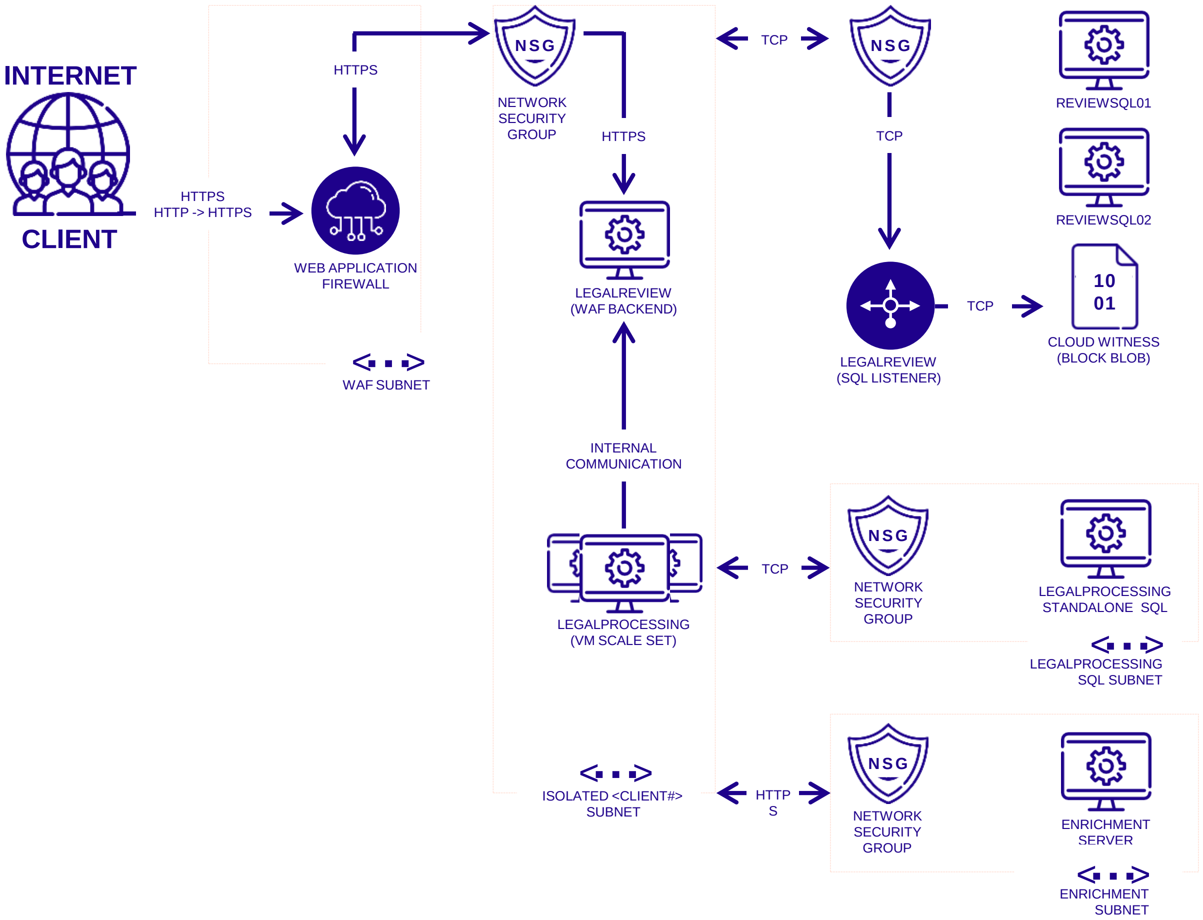
- *Product development*

ZyLAB has implemented a Secure software Development Process. Development is performed in house and no deployment is performed without automatic source code analysis and dynamic security tests. Peer reviews and static code scans are part of ZyLAB's Secure development process.

ZYLAB-ONE
SECURITY ARCHITECTURE

The image below shows the high-level architecture of ZyLAB-One, including general security measures and its layered design. As shown, all communication traveling over the internet is secured by HTTPS.

ZYLAB ONE SAAS INFRASTRUCTURE



ZYLAB-ONE CSA CONSENSUS QUESTIONNAIRE

The table below represents all questions in version 3.0.1 of the CSA questionnaire.

ZyLAB Response					
Q - ID	**QUESTION**	**YES**	**NO**	**N/A**	**COMMENT**
AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			ZyLAB follows the OWASP framework: SAMM, Top10, Testing Guides & ASVS.
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			We use Sonarqube for security static code analysis (https://www.sonarqube.org/). It is part of our CI pipeline. Those scans run on a weekly basis. Issues found are translated into Security Defects and being handled according to severity.
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?		X		ZyLAB uses automated source code analysis - Sonarqube. Security analysis is also part of code reviews.
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			ZyLAB software development is done in-house only. Azure services in use are provided by Microsoft and follow Security SDLC.
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Static and dynamic scans are part of each SaaS release (Bi-weekly). Issues are addressed according to their severity.
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			Part of ZyLAB's customer SaaS agreement
AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	X			According to ISO27001 guidelines

AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	X			According to ISO27001 guidelines
AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			Following OWASP guidelines. we validate High risk code with emphasis on input and output validation and encryption/encoding. ZyLAB follows a Secure Development Lifecycle model inspired by Microsoft. Security is assessed in Requirements, Design, Development & validation/Testing phases.
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			We follow OWASP guidelines.

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
BCR-01.1	Do you provide tenants with geographically resilient hosting options?	X			ZyLAB uses Azure as Cloud platform for hosting ZyLAB's solution
BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?		X		ZyLAB uses Azure as Cloud platform for hosting ZyLAB's solution
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		X		
BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?		X		
BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?		X		
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			Following ISO27001 standard
BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	X			Following ISO27001 standard. ZyLAB holds Business Continuity policies and plans for Operational Resilience
BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		We currently support 2 Azure geo locations: US (East) & EU (West Europe). MS Azure follows ISO27001 regarding business continuity and operational resilience.

BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			We currently support 2 Azure geo locations: US (East) & EU (West Europe). MS Azure follows ISO27001 regarding business continuity and operational resilience.
BCR-07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?		X		ZyLAB operates the Azure Cloud production environment. We have the ability to restore a tenant environment to a previous state in time.
BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		X		ZyLAB operates the Azure Cloud production environment. We do not share the VM images we use.
BCR-07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		X		ZyLAB operates the Azure Cloud production environment. We do not share the VM images we use.
BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	X			We utilize Azure Backup and Restore services for VM, Storage & DBs.
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			We currently support 2 Azure geo locations: US (East) & EU (West Europe). MS Azure follows ISO27001 regarding business continuity and operational resilience.
BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?		X		Planned in Q12019
BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		X		Planned in Q12019
BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			As described in IS27001 guidelines
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			As part of ZyLAB ISO27001 support: We hold the relevant policies for IT, HR, Operations, etc. all policies are available to all ZyLAB employees. Roles & responsibilities are well defined, including ISMS steering group, and training is provided to all ZyLAB employees.
BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	X			ZyLAB keeps daily night backups with retention of 8 days. That enables restoration of latest healthy state. More frequent backup policy can be applied upon request, to provide point in time rescue capability of short windows.
BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?		X		

BCR-11.3	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			We utilize Azure Back & Restore services as well as high availability mechanisms (redundancy).
BCR-11.4	Do you test your backup or redundancy mechanisms at least annually?	X			As stated in our Operations procedures and according to IS27001 guidelines.

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			As Described in ZyLAB's ZY_ISP109 System Acquisition, Development and Maintenance Policy as part of IS27001.
CCC-01.2	Is documentation available that describes the installation, configuration, and use of products/services/features?	X			Installation/Deployment/Configuration is described in Cloud Operations procedures and runbooks and is performed automatically by deployment scripts.
CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			As part of ZyLAB SDLC, Quality controls and activities are in place throughout the development cycle including testing automation, regression, Integration, manual testing, Security testing and acceptance.
CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	X			ZyLAB does not use outsourced software development. All ZyLAB software goes through security static code analysis and Dynamic Security testing.
CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	X			On request.
CCC-03.2	Is documentation describing known issues with certain products/services available?	X			Part of Product documentation and release notes.
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			Policies and procedures are in place to define ZyLAB SDLC, they include QA activities and testing in general as well as Security testing, verification and remediation. (following OWASP and IS27001 guidelines)
CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			Debug and test code exist in internal test environment only. All test data is auto generated and local.
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			Change Tracking solution of Operational Insights Log Analytics detects changes on the environment. Only Cloud OPS are able and allowed to install software on systems.
CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		ZyLAB holds detailed policies and procedures around production change management that describes the process, roles and responsibilities. Those are internal documents. Production changes are done only by ZyLAB Cloud Ops engineers and according to ISO27001 guidelines

ZyLAB Response					
Q - ID	**QUESTION**	**YES**	**NO**	**N/A**	**COMMENT**
DSI-01.1	Do you provide a capability to identify 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		
DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?		X		
DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?			X	
DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	X			We currently support 2 Azure geo locations: US (East) & EU (West Europe). Azure Datacenter physical locations are available in the Azure website.
DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	X			We currently support 2 Azure geo locations: US (East) & EU (West Europe). Azure Datacenter physical locations are available in the Azure website.
DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X	
DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			We currently support 2 Azure geo locations: US (East) & EU (West Europe). Tenants can choose between those 2 locations. Additional Azure locations are possible upon request and subject to additional costs
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			All data uploaded and processed in the ZyLAB system is audited/documented. All data is bound within the tenant environment (using Azure Network Security Groups (NSG) for customer/tenant isolation).
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	X			All data is bound within the tenant environment (using Azure Network Security Groups (NSG) for customer/tenant isolation). Each tenant environment resides within a single Azure geo location & physical geography location
DSI-03.1	Do you provide open encryption methodologies (3.4ES, 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			ZyLAB encrypts data in transit (HTTPS with TLS 1.2, SHA 256-2048 bits).

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			We utilize Azure Blobs which are encrypted automatically at rest. Blob transfer is done over HTTPS which is encrypted in transit.
DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	X			According to ISO27001 guidelines.
DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			According to ISO27001 guidelines. Production data only exists in the secure production environment. Access to production data is managed according to ISO27001 guidelines. (test data is auto/machine generated and does not contain customer data)
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			according to ISO27001 guidelines
DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X			
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	

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control, ZY_ISP106 Physical and Environmental Security & ZY_ISP110 Supplier Management policies.

DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
DCS-04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)?		X		As a SaaS provider, we focus on service delivery.
DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
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			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
DCS-07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	X			We currently support 2 Azure geo locations: US (East) & EU (West Europe). Tenants can choose between those 2 locations. Additional Azure locations are possible upon request and subject to additional costs
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			according to ISO27001 guidelines. As described in ZY_ISP103 asset Management, ZY_ISP104 Access Control & ZY_ISP106 Physical and Environmental Security policies.

ZyLAB Response					
Q - ID	QUESTION	YES	NO	N/A	COMMENT
EKM-01.1	Do you have key management policies binding keys to identifiable owners?	X			according to ISO27001 guidelines. As described in ZY_ISP105 Cryptography policy.
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	X			according to ISO27001 guidelines. As described in ZY_ISP105 Cryptography policy.
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	X			according to ISO27001 guidelines. As described in ZY_ISP105 Cryptography policy.
EKM-02.3	Do you maintain key management procedures?	X			according to ISO27001 guidelines. As described in ZY_ISP105 Cryptography policy.
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?			X	
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			ZyLAB uses Azure Key Vault service to manage encryption keys
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			ZyLAB encrypts At Rest – Both at Storage level as well as VM level with Azure managed Disks & Bitlocker.
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			We utilize Azure Blobs which are encrypted automatically at rest. Blob transfer is done over HTTPS which is encrypted in transit.
EKM-03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?		X		
EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			We utilize Azure key Vault service to manage encryption keys.
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			We utilize Azure key Vault service to manage encryption keys.
EKM-04.3	Do you store encryption keys in the cloud?	X			We utilize Azure key Vault service to manage encryption keys.
EKM-04.4	Do you have separate key management and key usage duties?	X			Azure Key Vault service manages keys and wrappers separately, based on the objectId properties of resources, the keys are used for.

ZyLAB Response					
Q - ID	**QUESTION**	**YES**	**NO**	**N/A**	**COMMENT**
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?		X		
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			Security & Audit solution of Operational Insights Log Analytics provides this feature.
GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		X		ZyLAB provides a SaaS solution over Azure. ZyLAB only is in charge of defining and operating the production environment including VM Images. We follow the ISO27001 and OWASP standards.
GRM-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		X		ZyLAB provides a SaaS solution over Azure. ZyLAB only is in charge of defining and operating the production environment including VM Images. We follow the ISO27001 industry standard.
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			According to ISO27001 guidelines.
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			According to ISO27001 guidelines. ZyLAB established ISMS board that governs Security within ZyLAB.
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			Upon request and according to ISO27001 guidelines.
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	X			according to ISO27001 guidelines.
GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	X			according to ISO27001 guidelines.
GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	X			according to ISO27001 guidelines.

GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			according to ISO27001 guidelines.
GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			according to ISO27001 guidelines.
GRM-06.4	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			according to ISO27001 guidelines.
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			as part of NDA, employment contract and Handbook
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			as part of NDA, employment contract and Handbook
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			according to ISO27001 guidelines.
GRM-09.1	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			according to ISO27001 guidelines. ZyLAB continuously review and maintain our security and privacy policies and procedures.
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			According to ISO27001 guidelines. We are a learning organization. We implement ISMS board that performs formal risk assessment as well as the annual ISO certification audit.
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	X			According to ISO27001 guidelines. All risk categories are taken into account. We gather inputs from continuous security testing activities, vulnerability scans, internal & external audits.
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	X			following the ISO27001 guidelines that cover organization-wide elements are the foundation of ZyLAB's security program.
GRM-11.2	Do you make available documentation of your organization-wide risk management program?	X			information on ZyLAB's Security program can be found through ZyLAB's Trust Center.

ZyLAB Response					
Q - ID	**QUESTION**	**YES**	**NO**	**N/A**	**COMMENT**
HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?		X		We follow policies and procedures manually according to ISO27001 guidelines
HRS-01.2	Is your Privacy Policy aligned with industry standards?	X			according to ISo27001 standard and GDPR requirements.
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			ZyLAB conducts background checks and verifications on all employees, contractors and other involved 3rd parties as part of ZyLAB HR security policy (and according to ISO27001 controls).
HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			ZyLAB holds an annual security awareness training and dedicated security training per role.
HRS-03.2	Do you document employee acknowledgment of training they have completed?	X			all training is tracked and documented
HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	X			Is part of the employment contract
HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			Only limited personnel can access sensitive systems and they are going through the training program.
HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	X			ZyLAB holds an annual security awareness training and dedicated security training per role.
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			Employment onboarding, change of employment and termination are part of ZyLAB's ZY_ISP102 Human Resource Security policy including the relevant procedures. (according to ISO27001 controls)
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			As described in ZyLAB's ZY_ISP102 Human Resource Security policy including the relevant procedures. (according to ISO27001 controls)
HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			Tenant data can only be accessed from a secure location by limited personnel. All mobile devices management and access control is documented in ZY_ISP103 Asset Management & ZY_ISP104 Access Control policies and related procedures. (according to ISO27001 guidelines & controls).

HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			Yearly done, also the required background checks are regular renewed.
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			As described in ZyLAB's ZY_ISP104 Access Control policy and related procedures according to ISO27001 guidelines/controls.
HRS-08.1	Do you provide documentation regarding how you may access tenant data and metadata?	X			As described in ZyLAB's ZY_ISP104 Access Control policy and related procedures according to ISO27001 guidelines/controls.
HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?		X		meta data is collected internally by the ZyLAB system.
HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			X	
HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			ZyLAB holds an annual security awareness training and dedicated security training per role. Cloud Ops members have dedicated security training program according to their role requirements.
HRS-09.1	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			ZyLAB holds an annual security awareness training and dedicated security training per role. members have dedicated security training program according to their role requirements.
HRS-10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			ZyLAB holds an annual security awareness training and dedicated security training per role. Cloud Ops members have dedicated security training program according to their role requirements.
HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	X			As illustrated in ZY_ISP 102 Human Resource Security Policy and related procedures. And through relevant security awarness training program. (according to ISO27001 guidelines/controls)
HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	X			As illustrated in ZY_ISP 102 Human Resource Security Policy and related procedures. And through relevant security awarness training program. (according to ISO27001 guidelines/controls)
HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?		X		

HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?		X		
HRS-11.3	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			Activity Logs are traced and Action Groups (OPS) are notified for each action taken on the management layer of cloud provider. Any action taken on the OS level of VMs are also traced by Change Tracking, Security & Audit and Service Map solutions of Operational Insights Log Analytics workspace. Log Analytics agents are deployed via VM extensions during the deployment, to ensure all upcoming activity is logged and analyzed.

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			We use Azure Web Application Firewall (WAF) to monitor, detect, log and deflect access to the ZyLAB system.
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			We use Azure Web Application Firewall (WAF) to monitor, detect, log and deflect access to the ZyLAB system.
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			Access management is in place. Access permissions are given or removed according to existing policies and procedures (ZY_ISP104 Access Control, ZY_ISP102 Human Resource Security).
IAM-02.2	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		
IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	X			ZyLAB is using Azure Network Security Groups (NSG)
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			According to ISO27001 guidelines as illustrated in ZY_ISP104 Access Control policy and related procedures.
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			According to ISO27001 guidelines as illustrated in ZY_ISP104 Access Control policy and related procedures.
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			some of the information is included in ZyLAB's Trust Center. Additional information can be shared through ZyLAB's security policies upon request.
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Security in Development environment: repositories, version control & tools are all deployed locally within the ZyLAB internal network and are only accessible by ZyLAB Developers. Defined roles, access and permissions are in place and systems are managed internally by ZyLAB. [ISO27001:14.2.1, 14.2.2, 14.2.6]

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			Only Cloud Operations team members have access to Production environment. Access can only be done from the internal ZyLAB Network in a secure environment. Controls are in place and follow rule of least privilege.
IAM-07.1	Do you provide multi-failure disaster recovery capability?	X			ZyLAB solution is deployed in 2 separate Azure regions (EU & US). In addition we utilize high availability on key components of ZyLAB's solution and we rely on Azure's Infrastructure disaster recovery plans and SLAs
IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?		X		
IAM-07.3	Do you have more than one provider for each service you depend on?		X		We only use Azure IaaS and services.
IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?		X		
IAM-07.5	Do you provide the tenant the ability to declare a disaster?			X	
IAM-07.6	Do you provide a tenant-triggered failover option?		X		
IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	X			Upon request and according to ISO27001 guidelines.
IAM-08.1	Do you document how you grant and approve access to tenant data?	X			As Described in the ZY_ISP104 Access Control Policy and related Procedures.
IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	X			As Described in the ZY_ISP104 Access Control Policy and related Procedures.
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			As Described in the ZY_ISP104 Access Control Policy and related Procedures.
IAM-09.2	Do you provide upon request user 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			User access is defined in the ZY_ISP104 Access Control Policy and related procedures. Tenant users are defined according to roles and assigned to Tenant only. Only ZyLAB Cloud Operations users have access to infrastructure and network. Business partners might have user access to Tenants applications.
IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	X			According to ISO27001 guidelines ZyLAB performs an annual review of users and users access

IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	X			According to ISO27001 guidelines and as described in ZY_ISP104 Access Control Policy and related procedures.
IAM-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			Upon request and according to ISO27001 guidelines.
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			According to ISO27001 guidelines and as described in ZY_ISP104 Access Control Policy and related procedures.
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			According to ISO27001 guidelines and as described in ZY_ISP104 Access Control Policy and related procedures. As well as in ZY_ISP102 Human Resource Security Policy
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard.
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	X			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard.
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard.
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			Azure B2C offers customizable policy constraints such as sign in/sign up, profile editing and password reset policies, that could be applicable to different tenants with different enforcements.
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			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard. Role based and entitlement based access to Data is managed within the ZyLAB solution

IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard.
IAM-12.7	Do you allow tenants to use third-party identity assurance services?	X			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard.
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			We use Azure B2C with 2Factor Authentication. We follow the OpenID Connect standard. Policies are defined within Azure B2C to support password and account lockout.
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?		X		ZyLAB is the only one responsible to define password and account lockouts within Azure B2C.
IAM-12.10	Do you support the ability to force password changes upon first logon?	X			As defined within ZyLAB's Azure B2C policies
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			As defined within ZyLAB's Azure B2C policies
IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	X			utility programs are restricted and limited and can only be used by Cloud Operations. Usage is monitored.
IAM-13.2	Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	X			ZyLAB uses Infrastructure-as-a-Service resources on Azure, therefore Microsoft is responsible for infrastructure security for such concerns, as a managed service provider.
IAM-13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	X			Microsoft Azure prevents these attacks to jump other hosts, by using multiple physical appliances and isolated vlans on the hypervisors.

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			Monitoring is done by Azure WAF (detection and prevention of suspicious activity) and Azure Application Insights
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			Only Cloud Operations team members can access logs from a secure location within the ZyLAB Network and office only.

IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	X			We follow the ISO27001 standard and ZyLAB controls/architecture/processes are aligned to this standard.
IVS-01.4	Are audit logs centrally stored and retained?	X			All application, audit, diagnostic, activity and event logs are sent to central log analytics workspace to be analyzed back to 90 days, as well as to a storage account that serves as log hub with the retention of 366 days.
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			ZyLAB uses Operational Management Suite product that has Security & Audit, Change Tracking, Alerting and Service Map solutions, that can trigger alerts for Action Groups. All dashboards for solutions are checked by OPS on a daily basis.
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Managed by Microsoft.
IVS-02.2	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			Managed by Microsoft.
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			Managed by Microsoft.
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			Managed by Microsoft.
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			Managed by Microsoft.
IVS-04.3	Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			Managed by Microsoft.
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			ZyLAB Software and depending technologies such as SQL Server, are installed with best practices; including the disk configuration aiming high throughput and maximum IOPS. As a SaaS provider we offer stable and high performance options as Standard and Premium packages.
IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			Managed by Microsoft.

IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	Azure Documents
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			According to ISO27001 guidelines
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			According to ISO27001 guidelines
IVS-06.4	Are all firewall access control lists documented with business justification?	X			According to ISO27001 guidelines
IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			ZyLAB uses custom images where ZyLAB software is installed as templates and applies monitoring, anti-malware, disk encryption agents via VM extensions during and/or after deployments. ZyLAB Images are updated with each release. Windows Firewall and File System rights can be changed according to release notes. Further restrictions on networking are applied by Network Security Groups as a part of the same deployment script.
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Each customer environment is segregated/isolated by Azure Network Security Groups (NSG)
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X	Only ZyLAB Cloud Operations members are creating Production or SaaS testing environments.
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			Development and Testing environments are internal in the ZyLAB network. All customer/tenant environment are in the Azure Production environment.
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			By Azure Web application Firewall (WAF). https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-overview
IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	X			By Azure Web application Firewall (WAF). https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-overview
IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	X			By Azure Web application Firewall (WAF). https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-overview. Development and Testing environments are internal in the ZyLAB network. All customer/tenant environment are in the Azure Production environment.

IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			By Azure Web application Firewall (WAF) and Azure Network Security Groups (NSG). https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-overview
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Bitlocker encrypted virtual hard drives are moved to Azure storage over https for data migration. Infrastructure and Applications are re-deployed. Data is restored from Azure Storage.
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			Each customer environment is segregated/isolated by Azure Network Security Groups (NSG). Managed by Microsoft.
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			Only ZyLAB Cloud Operations can access the virtualized production environment. 2Facotr (Azure B2C), Firewall (Azure WAF) and TLS 1.2 encrypted communication are in place. According to ISO 27001 guidelines.
IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	ZyLAB production environment does not support wireless network.
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	ZyLAB production environment does not support wireless network.
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	ZyLAB production environment does not support wireless network.
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			Network HLD and ZyLAB One topology clearly explains the subnet connectivity and allowed communications, as well as the logging and monitoring capabilities.
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			ZyLAB uses Azure basic DDoS prevention on Virtual Network and internet facing endpoint (Web Application Firewall) works with built-in OWASP 3.0 rule set to detect, which is also deployed to virtual network that has basic DDoS protection plan.

ZyLAB Response					
Q - ID	**QUESTION**	**YES**	**NO**	**N/A**	**COMMENT**
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?			X	APIs are only used for internal communication of ZyLAB Software. No APIs are currently publicly available for 3rd parties.
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			customer documents can be downloaded/produced as natives (industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).) through the ZyLAB solution
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?		X		The ZyLAB solution currently does not publish public APIs.
IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		X		The ZyLAB solution currently does not publish public APIs.
IPY-04.1	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Data import, export and service management is available to authenticated users only. Transport is encrypted using HTTPS with TLS v1.2, SHA 256-2048 bits
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			Upon request. According to ISO 27001 guidelines.
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			We use Azure IaaS & PaaS as our virtualization platform.
IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X	Managed by Microsoft.

ZyLAB Response					
Q - ID	QUESTION	YES	NO	N/A	COMMENT
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			anti-malware (also specific to mobile devices) is part of the Security awareness program in ZyLAB.
MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	X			
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?		X		
MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	X			
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?		X		

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		
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	X			
MOS-13.2	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		
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?		X		
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?		X		
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	X			
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	X			
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	X			
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?		X		
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?		X		
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	X			
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	X			
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	

MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?		X		
SEF-02.1	Do you have a documented security incident response plan?	X			According to ISO27001 guidelines as illustrated in ZY_ISP111 Management of Information Security Incidents policy and related procedures.
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?		X		ZY_ISP111 Management of Information Security Incidents policy is a generic policy applicable to all ZyLAB's customers
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			According to ISO27001 guidelines as illustrated in ZY_ISP111 Management of Information Security Incidents policy and related procedures.
SEF-02.4	Have you tested your security incident response plans in the last year?		X		We started implementing security incident response plans in Q3 2018
SEF-03.1	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	X			All relevant logs and other information sources are gathered for analysis and forensics of a security incident. As described in ZY_ISP111 Management of Information Security Incidents policy and related procedures.
SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	X			Tenants/customers are segregated/isolated to also allow monitoring on a tenant level.
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			According to ISO27001 guidelines as illustrated in ZY_ISP111 Management of Information Security Incidents policy and related procedures.
SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			According to ISO27001 guidelines as illustrated in ZY_ISP111 Management of Information Security Incidents policy and related procedures.
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			Tenants/customers are segregated/isolated allowing support of legal holds for a specific tenant.
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			According to ISO27001 guidelines as illustrated in ZY_ISP111 Management of Information Security Incidents policy and related procedures.
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	X			according to ISO27001 guidelines and upon request.

ZyLAB Response					
Q - ID	QUESTION	YES	NO	N/A	COMMENT
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			According to ISO 27001 guidelines and as described in ZY_ISP104 Access control, ZY_ISP110 Supplier Management, ZY_ISP107 Operations Security policies and related procedures.
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			According to ISO 27001 guidelines and as described in ZY_ISP111 Management of Information security Incidet policiy and related procedures.
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			ZyLAB collects Infrastructure diagnostics and use data to increase productivity of existing infrastructure.
STA-03.2	Do you provide tenants with capacity planning and use reports?	X			ZyLAB ensures that tenants receive a high quality service and no interruptions can affect tenants due to lack of capacity planning. Use reports are only provided to make billing data meaningful for the clients.
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			according to ISO 27001 guidelines
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			We rely on Azure Compliancy. See https://www.microsoft.com/en-us/trustcenter/compliance AND https://www.microsoft.com/en-us/trustcenter/common-controls-hub
STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	X			We rely on Azure Compliancy. See https://www.microsoft.com/en-us/trustcenter/compliance AND https://www.microsoft.com/en-us/trustcenter/common-controls-hub
STA-05.3	Does legal counsel review all third-party agreements?	X			As described in ZY_ISP110 Supplier Management Policy and according to ISO27001 guidelines.
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			As described in ZY_ISP110 Supplier Management Policy and according to ISO27001 guidelines.
STA-05.5	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		
STA-06.1	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	X			ZyLAB maintains appropriate relationship management with key third party suppliers and implements mechanisms in line with their relationship to the business. ZyLAB's third party management processes are reviewed annually as part of ZyLAB ongoing compliance with ISO27001.

STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			according to ISO 27001 guidelines as described in ZY_ISP107 Operation Security and ZY_ISP110 Supplier Management policies.
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			ZyLAB maintains appropriate relationship management with key third party suppliers and implements mechanisms in line with their relationship to the business. ZyLAB's third party management processes are reviewed annually as part of ZyLAB ongoing compliance with ISO27001.
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			X	
STA-07.4	Do you review all agreements, policies, and processes at least annually?	X			
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			As part of ISO27001 compliancy program.
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			We focus on the crucial partners/3rd party providers (such as Azure and ZenDesk).
STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	X			Upon request and with coordination with ZyLAB as described in ZY_ISP109 System acquisition, Development and maintenance policy.
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			Upon request and with coordination with ZyLAB as described in ZY_ISP109 System acquisition, Development and maintenance policy.

ZyLAB Response

Q - ID	QUESTION	YES	NO	N/A	COMMENT
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	X			We utilize Microsoft Antimalware for Azure Cloud Services. Details are available in ZY_ISP107 Operation Security policy & ZY_ISP103 Asset Management policy
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	X			Windows Defender and Microsoft anti-malware services are deployed via VM extensions, that ensures both agents are signatures are up to date. Any failed or late upgrade action triggers an alert to notify OPS to check consistency.
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			according to ISO 27001 and as described in ZY_ISP107 Operation Security policy

TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			according to ISO 27001 and as described in ZY_ISP109 System Acquisition, development and maintenance policy. We follow OWASP framework and use SonarQube for static code analysis and OWASP ZAP for dynamic pentests
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			Local OS layer scans are traced and reported with Security & Audit solution of Operational Insights Log Analytics
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	X			Upon request
TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	X			Updates are patched by Windows Update Management Solution of Operational Insights Log Analytics. Any manual patches can be applied through Secure Cloud OPS workstation via PSRemoting.
TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	X			Upon request. SDM contacts clients to inform about the planned critical and urgent patching operation to ensure client workloads are not affected by this operation. ZyLAB doesn't share operational time frames with clients where not necessary.
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	
TVM-03.2	Is all unauthorized mobile code prevented from executing?			X	

ZY
LAB

WWW.ZYLAB.COM