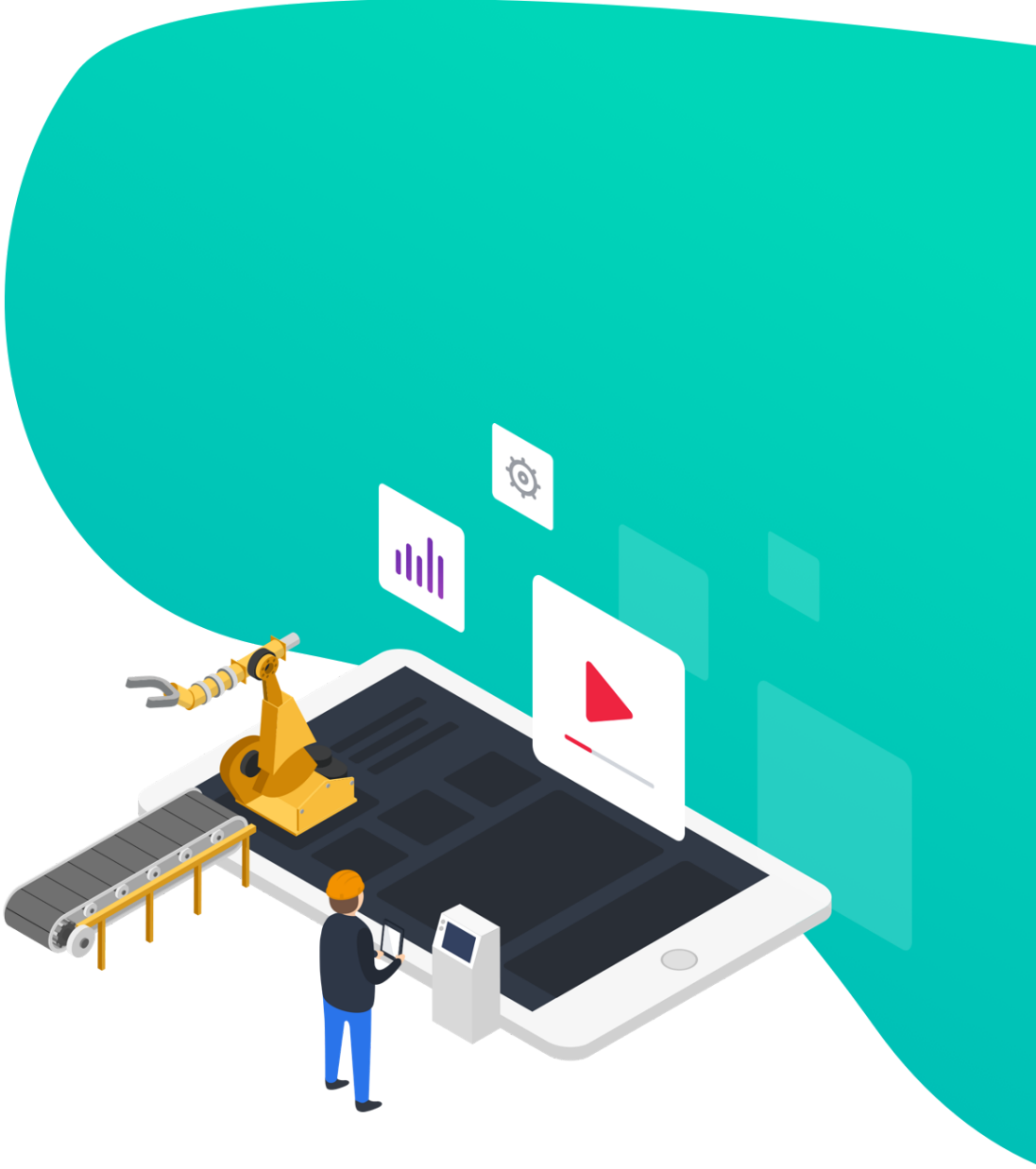

Poka Responses to Cloud Security Alliance Consensus Assessments Initiative Questionnaire

November 2019

Poka infosec team can be reached via e-mail at: infosec@poka.io

Introduction **2**

Poka Responses to CSA CAIQ V3.0.1 **3**

Application and Interface Security: Controls AIS-01 through AIS-04 3
Audit Assurance and Compliance: Controls AAC-01 through AAC-03 6
Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11 11
Change Control and Configuration Management: Controls CCC-01 through CCC-05 16
Data Security: Controls DSI-01 through DSI-07 17
Encryption and Key Management: Controls EKM-01 through EKM-05 25
Governance and Risk Management: Controls GRM-01 through GRM-11 27
Human Resources: Controls HRS-01 through HRS-11 31
Identity and Access Management: Controls IAM-01 through IAM-13 36
Infrastructure and Virtualization: Controls IVS-01 through IVS-13 43
Interoperability and Portability: Controls IPY-01 through IPY-05 50
Mobile Security: Controls MOS-01 through MOS-20 52
Security Incident Management: Controls SEF-01 through SEF-05 57
Supply Chain Management: Controls STA-01 through STA-09 60
Threat and Vulnerability Management: Controls TVM-01 through TVM-03 64

Introduction

The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when selecting a cloud vendor.

The CSA Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 provides a comprehensive set of questions that customers can use to evaluate the depth / breadth of cloud vendors" security, privacy, and compliance processes. Poka infosec team has compiled responses to all 294 questions of the questionnaire. This document will be a valuable resource for understanding how Poka meets and exceeds the requirements set forth by CSA.

If you require any further information, feel free to contact us.

Poka Responses to CSA CAIQ V3.0.1

Application and Interface Security: Controls AIS-01 through AIS-04

Control Group	CID	Consensus Assessment Questions	Poka Response
Application & Interface Security Application Security	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)?	Poka Software Development Lifecycle (SDLC) was designed to ensure that security and privacy are an integral part of our infrastructure and software development and delivery process. Here's an overview of some of the security and quality assurance practices: requirements identification (including security, privacy, compliance requirements), requirements review, design reviews , development controls (i.e. static analysis, code reviews), automated and manual testing, automated vulnerability scans, and change and deployment controls.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Automated and manual strategies to perform source code analysis and reviews are used to identify security vulnerabilities, improve the code quality and ensure Open Source Compliance prior to release the code in production. Penetration testing against our Production environment is performed on an annual basis by a qualified third party.
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	Both automated and manual strategies are employed supported by a peer review process combined with secure development training to ensure code entering the review cycle is of a high

			quality.
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	A Vendor Relationship policy is in place for managing the relationship between Poka and its vendors. It outlines how vendors are assessed and selected by Poka to ensure the security and privacy of information and compliance with applicable legislation.
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	At Poka, we conduct automated vulnerability scans of the infrastructure, operating systems, applications, application dependencies on an ongoing basis and manual scans to investigate vulnerabilities reported by the automated scans. We have a process to review reported vulnerabilities and promptly take action against them.
Application & Interface Security Customer Access Requirements	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?	Prior to granting customers access to their production instance of Poka, a Master Services Agreement must be in place. Customer data submitted to Poka SaaS by Poka's customers ("Customer Data") is managed by the customer in their use of the Poka SaaS. As such, Poka customers are responsible that their use of our services is in compliance with applicable laws and regulations.
	AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	Poka is available in a SaaS model. As such, there is a clear delineation between the administrative responsibilities of Poka and our Customers (in using the service including administering their organisational users accounts, permissions and data). The administrative responsibilities of both parties are explained in detail during the training and deployment provided by our implementation specialists and documented in our Help Center.

Application & Interface Security Data Integrity	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?	Data integrity controls are in place to prevent manual or systematic processing errors, corruption of data or misuse. Backups are available if and when required for restoring data in the event of data corruption.
Application & Interface Security Data Security / Integrity	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	The Poka Data Security Architecture was designed based on industry best practices including but not limited to: Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing and Amazon AWS security best practices. Poka's architecture is designed to balance the need for flexibility and agility with the need for robust controls ensuring the confidentiality, integrity, and availability of our customers' data.

Audit Assurance and Compliance: Controls AAC-01 through AAC-03

Audit Assurance & Compliance Audit Planning	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Poka does not currently support any of the listed assertion formats.
Audit Assurance & Compliance Independent Audits	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Poka's AICPA Service Organization Controls , SOC 2 Type 1 attestation report is available under NDA for all interested customers and potential customers.We are committed to completing our SOC 2 Type II report in by Q1 2020, which will further validate the effectiveness of our control environment over time. Our Information Security Management System is based on the ISO 27001 standard. However, we are not currently pursuing an ISO 27001 certification. Our IaaS provider (Amazon Web Services) provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports under NDA.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	At Poka, we use a combination of automated and manual vulnerability scanning/exploitation tools to evaluate our SaaS infrastructure and application on an ongoing basis. We have a process to review reported vulnerabilities and promptly take action against them. Penetration testing against our Production environment is performed on an annual basis by a qualified third party and an attestation of completion is available under NDA for all interested customers and potential customers. Poka's Security Team uses a combination
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by	

		industry best practices and guidance?	of automated and manual vulnerability scanning/exploitation tools to evaluate our SaaS infrastructure and application on an ongoing basis. Poka also mandates a third party security experts to perform authenticated and non-authenticated penetration testing against Poka SaaS infrastructure and application. The third party penetration testing is performed annually and an attestation of completion is available under NDA for all interested customers and potential customers.
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	As part of our continued dedication to information security and the protection of our customers' data, we are committed to get audited annually as part of our compliance program. Poka's AICPA Service Organization Controls, SOC 2 Type 1 attestation report is available under NDA for all interested customers and potential customers. As part of our continued dedication to information security and the protection of our customers' data, we are committed to get an external audit annually as part of our compliance program. Poka's AICPA Service Organization Controls, SOC 2 Type 1 attestation report is available under NDA for all interested customers and potential customers.
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	The third party penetration testing is performed annually and an attestation of completion is available under NDA for all interested customers and potential customers.
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	As part of our continued dedication to information security and the protection of our customers' data, we are committed to get an external audit performed annually as part of our compliance program. Poka's AICPA Service Organization Controls , SOC 2 Type 1 attestation report is available under NDA for all interested
	AAC-02.8	Do you have an internal audit program that allows for cross-functional	

		audit of assessments?	customers and potential customers.We are committed to completing our SOC 2 Type II report by Q1 2020, which will further validate the effectiveness of our control environment over time. As part of our continued dedication to information security and the protection of our customers' data, we are committed to get an external audit annually as part of our compliance program. Poka's AICPA Service Organization Controls, SOC 2 Type 1 attestation report is available under NDA for all interested customers and potential customers.
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03.1	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?	Cloud applications are multi-tenant by nature and are often based on a multi-tenant application and multi-tenant database architecture model. When designing Poka, customer data protection and privacy was and still is our top priority. The result is an architecture that enables us to segregate and isolate tenants from each other at all levels. Segregation allows us to allocate assets to different tenants, and isolation ensures that they can't access each other's assets. **Dedicated subdomain assigned per tenant:** Each tenant gets their own subdomain such as acme.poka.io. Using subdomains enables us to easily identify, filter and route requests using global and customer specific security controls. Using a DNS entry per customer provides us with more flexibility while performing maintenance on a tenant instance without impacting the other tenants. **Application Level Isolation:** Each tenant gets a dedicated instance of the Poka application running in a dedicated container cluster. These containers are assigned a tenant-specific security role based on the principle of least privilege that grants access only to the respective tenant database and

			object store. **Data Level Isolation:** - **Database level Isolation:** We leverage Amazon Aurora, database cluster instances are used to host multiple tenants. Tenant isolation is achieved by using a separate logical database (tables/schemas) and an associated role/permissions for each tenant within a database cluster instance. We leverage AWS Identity and Access Management (IAM) for database authentication which is based on short lived authentication token instead of relying on traditional database user credentials. The data is encrypted at rest using a KMS managed key per cluster instance. - **Object Storage Isolation:** Each tenant gets a dedicated AWS S3 Bucket used to store objects (photos, videos, misc documents) encrypted with a customer-specific key managed using AWS KMS. Access to the tenant bucket is controlled by using a combination of bucket ACLs, and IAM and bucket policies. Access is granted only to the tenant instance of Poka with the associated security role.
	AAC-03.2	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Customer data is backed up every hour and also replicated in near-real time at the designated secondary Amazon AWS Region. Backups are performed without stopping access to the customer instance of the Poka application, they are monitored, and restore testing performed at least every ninety (90) days. Customer data is always transmitted over a secure

			communication channel and encrypted at rest. Poka's DevOps team can restore or recover customer data on a per-customer basis.
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	We understand that you may have restrictions on where your data may be processed and stored. All customer instances of Poka and their associated data storage are assigned to one of our production environments when provisioned based on your data location requirement. We will move your Instance of Poka or your data to another geographic location (e.g country) without your prior approval. If your organization is based in the EU/EEA, we are able to process the personal data of your employees in compliance with GDPR for the transfer of personal data to processors established in third countries. Poka offers customers a Data Processing Addendum and the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data to our Poka SaaS.
	AAC-03.4	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?	We continuously monitor our legal and regulatory obligations to make sure that we remain in compliance.

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11

Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	Poka SaaS infrastructure leverages for resiliency, multiple availability zones within the AWS US-East (Virginia) , US-West 2 (Oregon), CA-Central (Canada) regions. AMAZON AWS Availability Zones are several independent data centers distributed in a geographical region.
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	N/A
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Poka's business continuity plan is focused on the continuation of our core corporate and Poka SaaS functions. From a Poka SaaS perspective: A Disaster Recovery Plan is in place and tested at least annually . Since every aspect of the Poka SaaS is managed as code (app. code, inf. code, configuration), this enables us to easily instantiate a new Poka SaaS infrastructure when required.
Business Continuity Management & Operational Resilience Power / Telecommunications	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	Customer data is always transported between customer's corporate network and Poka over secure communication channels using Transport Layer Security (TLS).
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	Customers can specify where their data will be processed and stored when subscribing to the service (refer to the SaaS Service Agreement) We continuously monitor our legal, regulatory and contractual obligations to make sure that we remain in compliance.
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel	Poka maintains information system and configuration documentation and make it available to its authorized personnel.

		to ensure configuration, installation and operation of the information system?	
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Our IaaS provider (Amazon Web Services) implements a wide variety of countermeasures and controls to mitigate these risks. More information can be found at: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
Business Continuity Management & Operational Resilience Equipment Location	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.)?	
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Not applicable. (Poka is a Software as a Service)
	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?	
	BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
	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?	
	BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	
	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Our IaaS provider (Amazon Web Services) implements a wide variety of countermeasures and controls to mitigate these risks. More information can be found at: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Logging and monitoring software are used to collect and monitor our SaaS infrastructure/application and are used to monitor the performance, availability, potential security threats and vulnerabilities, capacity and resource utilization, and to detect unusual system activity of our SaaS infrastructure and application. Poka makes available to our customer current and historical availability statistics on our Poka Status site available here: https://www.pokastatus.io
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Poka does not currently report security metrics to customers.
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	Logging and monitoring software are used to collect and monitor our SaaS infrastructure/application and are used to monitor the performance, availability, potential security threats and vulnerabilities, capacity and resource utilization, and to detect unusual system activity of our SaaS infrastructure and

			application. Poka makes available to our customer current and historical availability statistics on our Poka Status site available here: https://www.pokastatus.io
Business Continuity Management & Operational Resilience Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Policies, procedures and work instructions are maintained and communicated to ensure that consistent processes are followed in the management and support of the Poka SaaS. Those documents are available to all authorized personnel required to perform Operations functions and they are required to acknowledge that they have read and understand Poka's security policies and the code of conduct as part of the onboarding process and annually thereafter.
Business Continuity Management & Operational Resilience Retention Policy	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	Customers maintain ownership and control of their data either uploaded or created within Poka and may elect to implement their data retention policies.
	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	Poka will not disclose customer data to law enforcement unless required by law. Should law enforcement contact Poka with a demand to access customer data, Poka will attempt to redirect the law enforcement agency you are our customer. If compelled to disclose customer data to law enforcement, then Poka will promptly notify you our customer and provide a copy of the request, unless legally prohibited from doing so.
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Poka SaaS infrastructure and application implements multiple mechanisms for resiliency and redundancy of its service. Including:: • A stateless application architecture • Every aspect of the Poka SaaS is managed as code (app. code, inf. code, configuration) • CDN, Load Balancing, Clustering,
	BCR-11.5	Do you test your	

		backup or redundancy mechanisms at least annually?	automatic scaling • SaaS infrastructure distributed across multiple availability zones within the AWS US-East (Virginia) , US-West 2 (Oregon), CA-Central (Canada) regions. AMAZON AWS Availability Zones are several independent data centers distributed in a geographical region. • Customer data is backed up every hour and also replicated in near-real time at the designated secondary Amazon AWS Region. Those mechanisms are monitored and tested on a regular basis.

Change Control and Configuration Management: Controls CCC-01 through CCC-05

Change Control & Configuration Management New Development / Acquisition	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?	POKA has procedures in place that require prior authorisation for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities.
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	Information on getting started, using and managing Poka is available on our Help center.
Change Control & Configuration Management Outsourced Development	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	Poka has multiple controls in place to ensure that the code meets our quality standards prior to being released that include" automated and manual source code analysis (quality, vulnerabilities, Open Source compliance) peer code reviews, quality assurance tests and penetration testing.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	Poka does not outsource software development of its SaaS Application but, we use scanners to identify potential vulnerabilities, ensure Open Source license and copyright compliance.
Change Control & Configuration Management Quality Testing	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	
	CCC-03.2	Is documentation describing known issues with certain products/services	Known issues are documented in our Issue Tracking system.

		available?	
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Poka has a vulnerability management policy and processes are in place to ensure that defects (bugs) and potential vulnerabilities are managed in a timely manner.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Prior to release in production, all software codes are peer reviewed and approved.
Change Control & Configuration Management Unauthorized Software Installations	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	The Poka SaaS Infrastructure is completely documented, managedas code,deployed using AWS Cloudformation and is immutable once in production. All access, changes are logged and monitored continuously for unauthorized changes. We also monitor our systems usage, resource utilization, administrator activities, suspicious events, vulnerabilities, etc.
Change Control & Configuration Management Production Changes	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Poka is a Software as a Service, as such we are responsible for maintaining our SaaS Infrastructure and application. We notify our customers of the availability of new functionalities or changes to existing ones.

Data Security: Controls DSI-01 through DSI-07

Data Security & Information Lifecycle Management Classification	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	All customer instances of Poka and their associated data storage are assigned a one of our production environments when provisioned based on the data location requirement of our customers.

		from booting/instantiating/transporting data in the wrong country)?	
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Poka maintains an inventory of all production assets. Our Amazon AWS systems are not tracked at a hardware level due to the nature of the service.
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	Access Control restrictions based on IP addresses (reflecting geographic locations) are supported. GeoIP access control rules can be configured by our customers to be broad and apply to their instance of Poka or be very specific and apply only to a single user.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes, we understand that you may have restrictions on where your data may be processed and stored. All customer instances of Poka and their associated data storage are assigned to one of our production environments when provisioned based on your data location requirement. We will move your Instance of Poka or your data to another geographic location (e.g country) without your prior approval.
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Poka has a data classification policy in place. Data is classified into four general categories: Public, Internal, Confidential, and Restricted Customer data.
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	Yes, Poka understands that your organization may have restrictions on where your data can be processed and stored. Poka operates production environments in several geographic locations to address your data residency requirements.

Data Security & Information Lifecycle Management Data Inventory / Flows	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?	Internally, Poka tracks data flows and network connectivity among its SaaS infrastructure.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	Yes, we understand that you may have restrictions on where your data may be processed and stored. All customer instances of Poka and their associated data storage are assigned to one of our production environments when provisioned based on your data location requirement. We will move your Instance of Poka or your data to another geographic location (e.g country) without your prior approval.
Data Security & Information Lifecycle Management	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)?	All data in and out of our services is encrypted in transit using TLS 1.2 to protect it from unauthorised disclosure or modification. We enforce the use of strong ciphers as per AWS security best practices. The list of authorized ciphers are updated on a regular basis.
	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)?	
Data Security & Information	DSI-04.1	Are policies and procedures established for	Poka has a data classification policy in place. Data is classified into four general categories: Public, Internal, Confidential,

Lifecycle Management		labeling, handling and the security of data and objects that contain data?	and Restricted Customer Data. All customer data falls in the Restricted Customer Data category. Poka has a Customer Data handling work instruction that governs how the customer data can be accessed and handled in the context of providing support.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Data is classified in line with the Information Classification Policy, and controls implemented based on that. Label inheritance is implied through the controls being effectively applied.
Data Security & Information Lifecycle Management	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Poka environments are isolated at the AWS account level. There is no network connectivity between the different environments and IAM roles prevent cross account access. We also have policies, procedures and standards in place to ensure that customer data is protected and not replicated or used in non-production environments..
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	Poka SaaS assets have a designated owner who is responsible for asset classification and protection in accordance with classification.
Data Security & Information Lifecycle Management Secure Disposal	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	Poka has a procedure for the secure deletion of customer data at the term of the SaaS agreement. Poka can upon request provide you with a data destruction report that confirms that the data was deleted in accordance with the procedure. Our IaaS provider (Amazon Web Services) has a process for secure deletion and secure disposal of end of life equipment for our Poka SaaS. AWS Security is detailed at https://aws.amazon.com/security/
	DSI-07.2	Can you provide a published procedure for exiting the service	When approved for deletion, the procedure outlined in DSI-07.1 is followed to delete customer data.

		arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	

Datacenter Security: Controls DCS-01 through DCS-09

Datacenter Security Asset Management	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	Poka has implemented a formal policy that requires assets used to provide Poka services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets.
	DCS-01.1	Do you maintain a complete inventory of all of your critical supplier relationships?	Poka has a Vendor Relationship policy in place for managing the relationship between Poka and its vendors. It outlines how vendors are assessed and selected by Poka to ensure the security and privacy of information and compliance with applicable legislation. For vendor services where personal information is processed, Poka ensures that a Data Processing Addendum (DPA) is signed. Any issue, if present, is tracked to resolution.
Datacenter Security Controlled Access Points	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?	Our IaaS provider (Amazon Web Services) implements a wide variety of physical and environmental controls. More information can be found at: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
Datacenter Security Equipment Identification	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	Not applicable. (Poka provides a SaaS model based on an infrastructure provided by Amazon AWS.)
Datacenter Security Offsite Authorization	DCS-04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to	Yes, we are totally transparent regarding data location and transfer. All customer instances of Poka and their associated data storage are assigned to one of our production environments when provisioned based on the data

		another? (e.g., offsite backups, business continuity failovers, replication)	location requirement of our customers. We can also provide a detailed Data flow diagram to answer questions related to where the data is processed and stored.
Datacenter Security Offsite equipment	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	Poka has a procedure for the secure deletion of customer data at the term of the SaaS agreement. Poka can upon request provide you with a data destruction report that confirms that the data was deleted in accordance with the procedure. Our IaaS provider (Amazon Web Services) has a process for secure deletion and secure disposal of end of life equipment for our Poka SaaS. AWS Security is detailed at https://aws.amazon.com/security/
Datacenter Security Policy	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?	Our IaaS provider (Amazon Web Services) has controls, policies, standards and procedures for secure offices, rooms, facilities and secure areas. AWS Physical Security is detailed at https://aws.amazon.com/security/ Additionally, Poka annually reviews AWS' SOC2 report for expected physical controls.
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	All personnel must undergo security awareness training as part of the onboarding process and at least annually thereafter. All personnel must also acknowledge that they have read and understand Poka's security policies and the code of conduct as part of the onboarding process and annually thereafter.
Datacenter Security Secure Area Authorization	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)?	Yes, Poka understands that your organization may have restrictions on where your data can be processed, stored or transferred. Poka operates production environments in several geographic locations to address your data residency requirements.

Datacenter Security Unauthorized Persons Entr	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?	Non Applicable. Poka doesn't operate datacenters. Our IaaS provider (Amazon Web Services) implements a wide variety of controls to mitigate these risks. More information can be found at: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
Datacenter Security User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	Non Applicable. Poka doesn't operate datacenters. Our IaaS provider (Amazon Web Services) implements a wide variety of controls to mitigate these risks. More information can be found at: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Encryption and Key Management: Controls EKM-01 through EKM-05

Encryption & Key Management Entitlement	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	Poka has a key management policy for effective key management to support encryption of data in storage and in transmission for the key components of the Poka SaaS. Currently, Poka manages all encryption keys for our customers. Poka uses the Key Management Service from Our IaaS provider (Amazon Web Services)
Encryption & Key Management Key Generation	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Poka has a key management policy for effective key management to support encryption of data. We use unique customer encryption keys where technically feasible. Currently, Poka manages all encryption keys for our customers. Poka uses the Key Management Service from our IaaS provider (Amazon Web Services)
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	
	EKM-02.3	Do you maintain key management procedures?	
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes, Poka uses the Key Management Service from Our IaaS provider (Amazon Web Services) which enables us to have a complete audit trail for the lifecycle of the keys.
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Poka uses the Key Management Service from Our IaaS provider (Amazon Web Services)
Encryption & Key Management Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Poka encrypts your data at rest using 256-bit AES, one of the strongest block ciphers available.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport	Poka encrypts virtual machine storage using 256-bit AES.

		across and between networks and hypervisor instances?	
	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)?	Not currently support.
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	Poka has a policy which defines Poka's encryption standards.
Encryption & Key Management Storage and Access	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	All encryption used in Poka SaaS is based on open, validated and industry standard algorithms.
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Poka is responsible for managing encryption keys, we are leveraging AWS Key Management Service (KMS) and AWS Certificate Manager. AWS Certificate Manager stores the associated private key in a hardware security module (HSM).
	EKM-04.3	Do you store encryption keys in the cloud?	Poka is responsible for managing encryption keys, we are leveraging AWS Key Management Service (KMS) and AWS Certificate Manager. AWS Certificate Manager stores the associated private key in a hardware security module (HSM).
	EKM-04.4	Do you have separate key management and key usage duties?	Yes, we leverage AWS IAM roles to separate key management and key usage.

Governance and Risk Management: Controls GRM-01 through GRM-11

Governance and Risk Management Baseline Requirements	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.)?	Poka production servers and containers are validated, tested, scanned for vulnerabilities prior to deployment in the production environment.
	GRM-01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	The Poka SaaS Infrastructure is completely documented,managed as code,deployed using AWS Cloudformation and is immutable once in production. All access, changes are logged and monitored continuously for unauthorized changes.
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	Not applicable. (Poka is a Software as a Service based on an infrastructure provided by Amazon AWS.)
Governance and Risk Management Risk Assessments	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)?	
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	Poka performs a risk assessment on an annual basis.
Governance and Risk Management	GRM-03.1	Are your technical, business, and executive managers responsible for	Policies, procedures and work instructions have been developed and communicated to appropriate personnel to ensure the security of Poka SaaS. All

Management Oversight		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?	personnel must acknowledge that they have read and understood all policies as part of the onboarding process and annually thereafter.
Governance and Risk Management Management Program	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Poka can provide documentation describing the ISMP, which is aligned with ISO 27001, upon written request.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	We review our Information Security Management Program (ISMP) on an annual basis.
Governance and Risk Management Management Support / Involvement	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	Poka has a vendor relationship policy and procedure for managing the relationship between Poka and its vendors. Those documents outline how vendors are assessed and selected by Poka to ensure the security and privacy of information and compliance with applicable legislation.
Governance and Risk Management Policy	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	At Poka, our information security and privacy programs are aligned to a number of industry 'best practice' information security and privacy standards: ISO-27001, 27017, 27018 standards, Cloud Security Alliance Controls.
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Poka has a Vendor Relationship policy in place for managing the relationship between Poka and its vendors. It outlines how vendors are assessed and selected by Poka to ensure the security and privacy of information and compliance with applicable legislation. For vendor services where customer data

			and personal information is processed, Poka requires that a Data Processing Addendum (DPA) to be signed with those vendors which contains specific security and privacy contractual obligations for both parties.
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Poka can provide upon request an overview of our controls, standards, certifications and regulations we comply with.
	GRM-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Poka has a disciplinary process which include security policies and procedures violation, and which include the action taken in case of violation.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	
Governance and Risk Management Business / Policy Change Impacts	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	The risk assessments process considers updates to policies, procedures and controls to ensure when relevant. Additionaly, all risks are reviewed on a yearly basis.
Governance and Risk Management Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Customers are notified when necessary.

	GRM-09.1	Do you perform, at minimum, annual reviews to your privacy and security policies?	This is conducted as part of the annual ISMS review.
Governance and Risk Management Assessments	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?	Risk assessment is performed at least annually. All risks are evaluated based on their likelihood and impact using a mix of qualitative and quantitative methods.
	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)?	The likelihood and impact for inherent and residual risks are determined independently.
Governance and Risk Management Program	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	Poka has created an Information Security Risk Management policy to identify risks that may threaten the achievement of its business objectives. This policy details the process used for risk management including risk identification and analysis, risk tolerance, how risks should be managed and how risks should be reviewed afterwards.
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	No, these documents are deemed confidential.

Human Resources: Controls HRS-01 through HRS-11

Human Resources Asset Returns	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?	Monitoring systems and processes are in place to monitor for data breaches. Poka's incident management procedure includes notifying affected customers of confirmed data breaches. If any data breach is identified, we will notify our customer without undue delay. We will also notify the authorities when required (where breach notification requirements exist in a jurisdiction)
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	Poka's Privacy Policy is aligned with industry standards.
Human Resources Background Screening	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?	All employees are required to pass a pre employment background check that includes, as appropriate: - Confirmation of claimed academic qualifications when required - Confirmation of claimed professional qualifications when required - Verification of criminal records (background checks) - Additional screening may be necessary depending on the job requirements
Human Resources Background Screening Human Resources Employment Agreements	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Poka provides information security and privacy training for new hires, and on an ongoing basis to all employees.
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	Yes, we maintain formal records of completion of internal employee training.
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of	Poka has a Confidentiality Agreement & Employment Obligations policy. All employees are required to sign an employment contract that includes an NDA.

		employment to protect customer/tenant information?	
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Poka employees must complete the initial security awareness training during their onboarding in order to obtain their access to sensitive systems.
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	All employees must undergo security awareness training as part of the onboarding process and at least annually thereafter.
Human Resources Employment Termination	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	Poka Human resource security & Access Management policy defines internal management responsibilities to be followed for termination and role change of employees.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	In the case of termination of employment of personnel, the corresponding manager contacts the Finance, Legal and Human Resources team which initiates the termination process. All access to the production environment and to the source code is removed in a timely manner, and all assets lent to the personnel are retrieved in the exit interview. All legal requirements such as non-competition, non- solicitation, respect of intellectual property and confidentiality are reminded in the exit interview.
Human Resources Portable / Mobile Devices	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	Poka has a Customer Data handling policy that governs how the customer data can be accessed and handled by authorized Poka employees. Poka employees are provided corporate-owned mobile devices during onboarding. Access to the production environment is only permitted with corporate-owned devices. Poka has implemented a variety of controls in place to ensure the security of our customer's data. Furthermore, we have

		higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	technical controls and audit policies in place to ensure that any access to Customer data is logged in an audit trail.
Human Resources Nondisclosure Agreements	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?	Poka manages and periodically revises the Poka NDA to reflect Poka business needs.
Human Resources Roles / Responsibilities	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Poka is available as a SaaS model. As such, there is a clear delineation between the administrative responsibilities of Poka and our customers (in using the service including administering their organisational users and data). The administrative responsibilities of both parties are explained in detail during the training and deployment provided by our implementation specialists.
Human Resources Acceptable Use	HRS-08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	The operation of the Poka services requires that some authorized employees have access to the systems which process or store Customer data. However, employees are prohibited from accessing your data unless it is necessary to do so. For example, in order to reproduce or diagnose a problem a Customer is having with the Poka services, we may need to view Customer data. We have a Customer Data Handling policy and associated work instructions that limit and control the access to your data. Furthermore, we have technical controls and audit policies in place to ensure that any access to your data is logged. All of our employees and contract personnel were screened prior their
	HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	
	HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	

			employment and bound to our policies regarding Customer Data.
Human Resources Training / Awareness	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?	Poka provides information security and privacy training for new hires, and on an ongoing basis to all employees.
	HRS-09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	All employees are made aware of their responsibilities for maintaining the security, confidentiality, integrity and availability of customer data.
Human Resources User Responsibility	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?	Poka has implemented various methods of internal communication to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. Additionally, all employees must acknowledge that they have read and understand Poka's security policies and the code of conduct as part of the onboarding process and annually thereafter.
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources Workspace	HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of	Poka's policies and procedures have been created in support of customer service level requirements.

		interests?	
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Poka's policies include provisioning access according to least privilege, and monitoring systems are deployed for monitoring unauthorized access to systems and/or data.
	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?	Poka images and containers are built via version controlled software repositories and are 'read only' preventing tampering. Once deployed in an environment no changes are allowed. We use a Threat Detection solution to detect unauthorized changes or unusual behaviors.

Identity and Access Management: Controls IAM-01 through IAM-13

Identity & Access Management Audit Tools Access	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.)	Poka restricts, logs and monitors access to our information security management systems.
	IAM-01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	Poka restricts, logs and monitors privileged access to our security information systems.
Identity & Access Management User Access Policy	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Poka has a process to ensure the timely removal of access in a timely manner following the termination or change of employment of personnel.
	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?	For more info about this control please refer to our SOC 2 attestation report which is available under NDA for all interested customers and potential customers.
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Management access to our Poka SaaS infrastructure is restricted to authorised individuals and connections through the use of dedicated site to site to IPSec VPN from our corporate network to our infrastructure on Amazon AWS.
Identity & Access Management Policies and Procedures	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?	At Poka, we maintain separate identity stores for our corporate system and our SaaS infrastructure. Poka uses AWS IAM to manage user identities and access policies for our SaaS infrastructure.
	IAM-04.2	Do you manage and store the user identity of all personnel who	

		have network access, including their level of access?	
Identity & Access Management Segregation of Duties	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Poka enforces segregation of duties through user defined groups and access policies to minimize the risk of unintentional or unauthorized access or changes to production systems. System access is restricted based on the user's job responsibilities.
Identity & Access Management Source Code Access Restriction	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?	Access to our application, program or object source code is restricted to our devops and security teams. At Poka, we have a robust peer review system to ensure changes to source code are always reviewed.
	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?	Not applicable. (Poka is a Software as a Service)
Identity & Access Management Third Party Access	IAM-07.1	Do you provide multi-failure disaster recovery capability?	Our SaaS infrastructure was designed and optimized specifically to host our Poka application and has multiple levels of redundancy and disaster recovery capability built in.
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	We monitor our IaaS provider (Amazon Web Services) to ensure service continuity.
	IAM-07.3	Do you have more than one provider for each service you depend on?	Our critical dependency is limited to our IaaS provider (Amazon Web Services). We follow AWS best practices to ensure the availability our SaaS infrastructure. We also have the capability to recover in another AWS regions in the event of a major outage. We also assessed the Amazon AWS own resilience and fault tolerance practices to

			ensure they meet our overall service delivery and continuity requirements.
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	Details of our operational continuity performance is available to customers with specific SLA objectives.
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	Poka Disaster Recovery Plan requires authorized members of the Poka Disaster Recovery Team to declare a disaster. Customers do not have the ability to declare a disaster, customers may communicate service downtime to customer service.
	IAM-07.6	Do you provided a tenant-triggered failover option?	Not applicable. (Poka is a Software as a Service)
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	Poka's DR/BCP documents are considered internal. For more info about this control please refer to our SOC 2 attestation report which is available under NDA for all interested customers and potential customers.
Identity & Access Management User Access Restriction / Authorization	IAM-08.1	Do you document how you grant and approve access to tenant data?	Poka has a Customer Data handling work instruction that governs how the customer data can be accessed and handled in the context of supporting the Poka SaaS.
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Poka has established and defined a data classification methodologies and Poka classifies data into four categories: Public, Internal, Highly Confidential, and Restricted Customer data. Poka classifies all customer data into its most sensitive category "Restricted Customer Data".
Identity & Access Management	IAM-09.1	Does your management provision the authorization and restrictions for user	Access to Poka's assets are granted based on business justification, with the asset owner's authorization and limited based on "need-to- know" and "least-privilege" principles.

User Access Authorization		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?	
	IAM-09.2	Do your 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?	Poka uses a "need-to- know" and "least-privilege" approach to access provisioning.
Identity & Access Management User Access Reviews	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)?	Poka performs periodic reviews of access permissions, the reviews include administrative accounts to development systems, tools and all our SaaS infrastructures including the production.
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Remediation activities will be captured through the audit logs.
	IAM-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been	Inappropriate access to Customer Data is treated as a security incident and managed through our incident management process, which includes customer notification provisions.

		allowed to tenant data?	
Identity & Access Management User Access Revocation	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?	We have processes in place to ensure that all equipment is returned and accounts terminated without undue delay.
	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?	
Identity & Access Management User ID Credentials	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Poka supports SAML-based Single Sign-On (Federated authentication) using the Security Assertion Markup Language (SAML v2.0). You can integrate Poka with your Identity Management solution using SAML v2 to retain full control of the authentication process. You can also automatically provision and deprovision your users in Poka with System for Cross-domain Identity Management (SCIM) - an open standard used by identity providers and Single Sign-On (SSO) services to manage user accounts across of SaaS providers, including Poka.
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	
	IAM-12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g.,	

		XACML) to enforce regional legal and policy constraints on user access?	
	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?	Our customers are responsible for managing user-level access control to their data.
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	We recommend our customers to enable Federated authentication using the Security Assertion Markup Language (SAML v2.0) on their instance of Poka to have full control of the authentication process and authentication options used.
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	We recommend our customers to enable Federated authentication using the Security Assertion Markup Language (SAML v2.0) on their instance of Poka to have full control of the authentication process and authentication options used.
	IAM-12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	**SAML-based Single Sign-On (SSO):** We recommend our customers to enable Federated authentication using the Security Assertion Markup Language (SAML v2.0) on their instance of Poka to have full control of the authentication process and authentication options used. **Poka Cloud Accounts:** supports the enforcement of password complexity requirements. This is configurable by our customers in the administration section of their Poka instance. With Poka Cloud accounts, Multi-factor authentication is not currently available. We monitor suspicious login attempts and we will notify our customer of suspicious activities.
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	
	IAM-12.10	Do you support the ability to force password changes	**Poka Cloud Accounts:** Yes

		upon first logon?	
	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)?	Yes, it requires a user with administrative privileges to reactivate the Poka user account.
Identity & Access Management Utility Programs Access	IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	Access control to the Poka SaaS infrastructure is strictly controlled and monitored.
	IAM-13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	Not applicable. (Poka is a Software as a Service) Our IaaS provider (Amazon Web Services) implements controls to mitigate these risks. For more information: http://aws.amazon.com/security.
	IAM-13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	Not applicable. (Poka is a Software as a Service) Our IaaS provider (Amazon Web Services) implements controls to mitigate these risks. For more information: http://aws.amazon.com/security.

Infrastructure and Virtualization: Controls IVS-01 through IVS-13

Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	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?	For the Poka SaaS infrastructure, we use an IDS to detect unauthorized changes to key files and folders of servers and containers. We also forward all the logs to our security information and event management (SIEM).
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Poka restricts the ability to access audit logs to a limited number of authorized personnel.
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/ processes has been done?	Poka evaluates pertinent regulations, standards and best practices for our operations on a regular basis. Our architecture, processes and controls follow a continuous improvement model.
	IVS-01.4	Are audit logs centrally stored and retained?	We forward all the logs to our security information and event management (SIEM).
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Our security information and event management (SIEM) monitors audit log events for suspicious activities and alert the devops and security team for analysis and response. The raw audit logs are also used for post-incident investigation.
Infrastructure & Virtualization Security Change Detection	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)?	Poka's SaaS infrastructure is completely managed as code and is immutable once deployed in production. Servers and containers are treated as disposable. We never make any configuration changes to servers or containers in production. Instead, we go through a full DevSecOps pipeline to create new updated server or container images and then deploy them into production to replace the outdated ones. Poka's Security Team uses a combination
	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)?	of automated and manual vulnerability scanning/exploitation tools in order to detect or confirm the presence of vulnerabilities in our SaaS infrastructure and application. We also monitor for compliance, unauthorized changes or abnormal behaviors once in production.
Infrastructure & Virtualization Security Clock Synchronization	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Poka uses standard internet time services.
Infrastructure & Virtualization Security Capacity / Resource Planning	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Not applicable. (Poka is a Software as a Service)
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Not applicable. (Poka is a Software as a Service)
	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?	We monitor our Poka SaaS infrastructure on an ongoing basis and alerts are set up when metrics exceed predefined thresholds. Extra capacity can be provisioned in a matter of minutes to address increase service use.
	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?	
Infrastructure & Virtualization Security Management - Vulnerability Management	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	Not applicable. (Poka is a Software as a Service) The virtualization technologies are transparent to the Vulnerability tools that we utilize.
Infrastructure & Virtualization Security Network Security	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?	Not applicable. (Poka is a Software as a Service)
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	The Poka SaaS infrastructure is fully documented and managed as code. The zones (subnets), firewall rules, load balancers, Web Application Firewalls, etc. are all managed and deployed using Amazon AWS Cloud formation.
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Our Poka SaaS infrastructure has very little surface area that is exposed through the firewalls. We review firewall rules on a periodic basis. The performance of our load balancers, firewalls and other associated controls are also assessed regularly through our penetration testing program.
	IVS-06.4	Are all firewall access control lists documented with business justification?	Every firewall rules are documented and reviewed as per our SDLC.
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity	Poka server images and containers are built with only the necessary ports, protocols and services and include logging, IDS. The build template are managed via version controlled software repositories.

		monitoring and logging) as part of their baseline build standard or template?	
Infrastructure & Virtualization Security Production / Nonproduction Environments	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Typically, only the production environment is provided to our customers. However, a sandbox environment can be made available to customer when required.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	Not applicable. (Poka is a Software as a Service)
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	Poka's non-production environments (corporate, development, demo, Pen Test, Test, Staging) are logically and/or physically separate from Poka's production environment.
Infrastructure & Virtualization Security Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	The Poka SaaS infrastructure implements a variety of controls to ensure the protection and isolation of the environments, servers, containers, subnets such as: logical firewall, Web Application Firewall, Application Load Balancers, network ACL, etc. This ensures that only authorized traffic from the internet, our corporate network and between servers are allowed.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and	

		non-production environments?	
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	Not applicable. (Poka is a Software as a Service) No physical-to-virtual migrations are undertaken.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	
Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	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)?	Poka employs the concept of least privilege, allowing only the necessary access for authorized users to accomplish their job function. All accounts require two-factor authentication, management access is done over TLS, SSH or using AWS Session Manager and all access are logged in an audit trail.
Infrastructure &	IVS-12.1	Are policies and procedures	Corporate and Guest wireless network are isolated from each other and Poka

Virtualization Security Wireless Security		established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	implements a zero trust security model for its corporate 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)	Poka wireless network is secured and access is granted by our MDM solution and poka implements a zero trust security model for its corporate 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?	
Infrastructure & Virtualization Security Network Architecture	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	Poka SaaS Network architecture is documented and clearly defines boundaries and data flows between services.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth	Poka uses firewall rules, ip whitelisting, ip geolocation, network ACLs, Web Application Firewalls, load balancers to prevent spoofed traffic and restrict

		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?	incoming and outgoing traffic to our Poka SaaS infrastructure. Additionally, Poka has implemented automated Threat detection control to monitor and detect a wide variety of attacks. We leverage AWS Shield and AWS WAF for the DDOS mitigation along with the following services (as per AWS Best Practices for DDOS Resiliency): ● Layer 3 (e.g. UDP reflection) attack mitigation: Route 53, Elastic Load Balancing, VPC ● Layer 4 (e.g. SYN flood) attack mitigation: Route 53, Elastic Load Balancing, VPC ● Layer 6 (e.g. SSL) attack mitigation: Elastic Load Balancing, WAF, VPCReduce attack surface: Route 53, Elastic Load Balancing, WAF, VPCScale to absorb application layer traffic: Route 53, Elastic Load Balancing, EC2 autoscaling ● Layer 7 (application layer) attack mitigation: Route 53, WAF, (CloudFront and WAF the edge location is planned for this year)Geographic isolation and dispersion of excess traffic and larger DDoS attacks: Route 53, (CloudFront and WAF the edge location is planned for this year)

Interoperability and Portability: Controls IPY-01 through IPY-05

Interoperability & Portability APIs	IPY-01	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Poka will make available upon request the documentation and access to its Restful API.
Interoperability & Portability Data Request	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Any data our customers submitted to our Poka SaaS platform can be exported in JSON format and in their original format whenever applicable using Supplier's API (Application Programing Interface).
Interoperability & Portability Policy & Legal	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?	Refer to the documentation of our Restful API and the Acceptable use policy.
	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?	Customers are able to retrieve their data at any time using the Poka Restful API at anytime.
Interoperability & Portability Standardized Network Protocols	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?	All communications are encrypted in transit using Transport Layer Security (TLS).
	IPY-04.2	Do you have documented custom	Not applicable. (Poka is a Software as a Service)

		changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	

Mobile Security: Controls MOS-01 through MOS-20

Mobile Security Anti-Malware	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	Anti-malware training related to mobile devices is specifically included in our security awareness training program. Poka's information security awareness trainings address multiple subjects including mobile device malware. Additionally, Poka's acceptable usage of corporate owned device and BYOD policies address the subject of malware.
Mobile Security Application Stores	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	Poka has established a Bring Your Own Device Policy which addresses security and acceptable use of mobile devices (phones, tablets, etc.). Poka employees must adhere to the terms and conditions set forth our BYOD Policy in order to connect their devices to the company network. Employee BYOD devices can be used to access corporate resources such as: email, calendars, contacts, and documents. Employees can install applications as needed for business and personal uses. BYOD devices are prohibited from accessing Poka's production environment. We operate a heavily cloud based IT environment and as such provide a suite of cloud-based applications to our employees. All corporate owned devices are managed by a Mobile Device Management Solution. BYOD devices are required to have encrypted block-level storage encryption and a lock screen password. All devices accessing Poka's SaaS infrastructure are managed through corporate directory.
Mobile Security Approved Applications	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	
Mobile Security Approved Software for BYOD	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	
Mobile Security Awareness and Training	MOS-05	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?	
Mobile Security	MOS-06	Do you have a documented list of	

Cloud Based Services		pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	Poka has established a Bring Your Own Device Policy which addresses security and acceptable use of mobile devices (phones, tablets, etc.). Poka employees must adhere to the terms and conditions set forth our BYOD Policy in order to connect their devices to the company network. Employee BYOD devices can be used to access corporate resources such as: email, calendars, contacts, and documents. Employees can install applications as needed for business and personal uses. BYOD devices are prohibited from accessing Poka's production environment. We operate a heavily cloud based IT environment and as such provide a suite of cloud-based applications to our employees. All corporate owned devices are managed by a Mobile Device Management Solution. BYOD devices are required to have encrypted block-level storage encryption and a lock screen password. All devices accessing Poka's SaaS infrastructure are managed through corporate directory.
Mobile Security Compatibility	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	
Mobile Security Device Eligibility	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security Device Inventory	MOS-09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	
Mobile Security Device Management	MOS-10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	
Mobile Security Encryption	MOS-11	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?	Yes, we enforce encryption on all corporate owned devices.

Mobile Security Jailbreaking and Rooting	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Our Policies forbids jailbroken or rooted devices.
	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?	All Poka employees must comply with company policies. A disciplinary action policy is in place in case of sanction. At a technical level, all corporate owned devices are managed by a Mobile Device Management Solution.
Mobile Security Legal	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	Not applicable. e-Discovery and legal holds can be performed directly on our cloud services.
	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?	Poka has a sanctions policy which addresses obligations to comply with company policy (including security policies). At a technical level, all corporate owned devices are managed by a Mobile Device Management Solution.
Mobile Security Lockout Screen	MOS-14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Poka has detailed the requirement in a policy. Lockout screen is enforced for all corporate owned devices and BYOD devices.
Mobile Security Operating Systems	MOS-15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	All corporate owned devices are managed by a Mobile Device Management Solution and updates are applied either by the employees or by our MDM.

Mobile Security Passwords	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	Password policies are detailed in our Password policy documentation and enforced by our MDM.
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	
Mobile Security Policy	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	As per the BYOD policy, no corporate data should be stored on BYOD devices. Corporate data, within corporate applications, is backed up, where applicable, by Poka's IT team.
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	Our BYOD policy recommends the use of known / approved application stores anti-malware software when applicable.
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	
Mobile Security Remote Wipe	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	All corporate owned devices and BYOD devices are managed by a Mobile Device Management Solution and support remote wipe.
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	

Mobile Security Security Patches	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Company-owned devices are updated via MDM. Ou policy requires that BYOD devices must be kept up to date on security-related patches.
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	All corporate owned devices are managed by a Mobile Device Management Solution and support remote installation of security patches.
Mobile Security Users	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	Poka's BYOD Policy addresses the corporate services that can be accessed with a BYOD device.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	User roles are defined at the corporate services level and access to corporate data is enforced there.

Security Incident Management: Controls SEF-01 through SEF-05

Security Incident Management, E-Discovery & Cloud Forensics Contact / Authority Maintenance	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Poka liaises with security and privacy organizations, and industry associations where appropriate to help ensure security and privacy compliance. Poka cooperates with local authorities in all jurisdictions in which it operates as required by law or contract.
Security Incident Management, E-Discovery & Cloud Forensics Incident Management	SEF-02.1	Do you have a documented security incident response plan?	Poka has an information security incident process is formally documented and communicated to appropriate personnel. Responsibilities for detecting and managing security incidents are defined.
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	Poka will promptly notify its customers in the event of any security breach of the service resulting in an actual or reasonably suspected unauthorized disclosure of their Customer Data.
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	
	SEF-02.4	Have you tested your security incident response plans in the last year?	We have exercised our incident management process via live incident activity. We maintain a continuous improvement approach to optimising our response capabilities. After a high severity incident, the incident responder is encouraged to complete a post-incident review, communicate his findings to the rest of the team, and propose potential improvements to the system and/or handling of the event.
Security Incid ent Management, E-Discovery &	SEF-03.1	Does your security information and event management (SIEM) system merge data	Logs are all aggregated in our security information and event management (SIEM) where we are able to perform alerting and analysis.

Cloud Forensics Incident Reporting		sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes, our security information and event management enable us to perform the analysis of an event specific to a customer.
Security Incident Management, E-Discovery & Cloud Forensics Incident Response Legal Preparation	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	In the event of a security incident, proper forensic procedures including chain of custody will be performed for collection, retention, and presentation of evidence.
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	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?	Poka can provide a point in time copy the data from a single customer to support any litigation or law enforcement requests.
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Poka follows an incident management process, which includes security monitoring applications that are configured to send alerts to appropriate employees through Poka's incident management system. Alerts are categorized and analyzed.

Incident Response Metrics	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	Poka does not currently share statistical information with our customers.

Supply Chain Management: Controls STA-01 through STA-09

Supply Chain Management, Transparency and Accountability Data Quality and Integrity	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?	Not applicable. Poka does not outsource development of Poka SaaS services to subcontractors.
	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?	
Supply Chain Management, Transparency and Accountability Incident Reporting	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	Poka will promptly notify the customer in the event of a security incident resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data.
Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	Logging and monitoring software are used to collect data from system infrastructure components and are used to monitor system performance, potential security threats and vulnerabilities, capacity and resource utilization, and to detect unusual system activity or service requests. Alerts are sent to appropriate personnel based on an on-call schedule.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	Poka is available as a SaaS model. As such, we scale our service to handle increased usage and maintain its level of performance.
Supply Chain Management, Transparency and Accountability	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures,	Poka perform on an annual basis an assessment of conformance to and effectiveness of policies, procedures, and supporting measures and metrics. For more info please refer to our SOC 2

Provider Internal Assessments		and supporting measures and metrics?	attestation report which is available under NDA for all interested customers and potential customers.
Supply Chain Management, Transparency and Accountability Third Party Agreements	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?	Poka has a Vendor Relationship policy is in place for managing the relationship between Poka and its vendors. It outlines how vendors are assessed and selected by Poka to ensure the security and privacy of information and compliance with applicable legislation.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	We select and monitor outsourced providers to ensure compliance with laws including data protection laws and our contractual obligation with our customers.
	STA-05.3	Does legal counsel review all third-party agreements?	Third-party agreements are reviewed by our legal counsel (based on a risk analysis of the third party) as required but are always reviewed security team.
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Yes, our Poka Third-Party Agreements include security and privacy provisions.
	STA-05.5	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Poka makes available the list of its subprocessors and can provide copies of Data Processing Agreements under NDA for all interested customers and potential customers.
Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	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?	Poka has an information security risk management process is in place for identifying, assessing and treating risks that includes our vendors. Our critical third-party provider is Amazon AWS. Amazon AWS holds a SOC 2 certification which is validated by a third party. This assessment include consideration of supply chain management and governance for those organisations. AWS risk management and governance
Supply Chain Management, Transparency	STA-07.1	Are policies and procedures established, and	

and Accountability Supply Chain Metrics		supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	processes are detailed: http://aws.amazon.com/compliance Poka annually obtains and reviews AWS' SOC2 report.
	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)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Poka mitigates this risk by limiting our dependencies on critical providers and by using a variety of other controls. Amazon AWS is our most important supplier, it provides the necessary infrastructure (IaaS) to host our Poka SaaS. In order to mitigate the risks to our service level, we leverage Amazon AWS Availability Zones and Regions to implement a highly available architecture to support the availability of Poka SaaS in accordance with Poka's availability targets.
	STA-07.4	Do you review all agreements, policies and processes at least annually?	Poka reviews agreements, policies and processes considered critical annually or when material change occurs.
Supply Chain Management, Transparency and Accountability Third Party Assessment	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	
	STA-08.2	Does your annual review include all partners/third-party providers upon which your information	

		supply chain depends?	
Supply Chain Management, Transparency and Accountability Third Party Audits	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Poka contracts a specialized security firm to conduct vulnerability scans and penetration testing of Poka SaaS (applications and infrastructure) at least on an annual basis. We will provide to our customers upon request an attestation of the penetration test conducted. Poka allows penetration testing initiated by the customer at customer's expense. Customer testing may only be run against a test instance of the Poka SaaS that is a copy of production. Poka must be provided advanced notice before such testing. Customers can initiate this process by contacting Poka support.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	

Threat and Vulnerability Management: Controls TVM-01 through TVM-03

Threat and Vulnerability Management Antivirus / Malicious Software	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	Poka's SaaS infrastructure is completely managed as code and is immutable once deployed in production. Servers and containers are treated as disposable. We never make any configuration changes to servers or containers in production. Instead, we go through a full DevSecOps pipeline to create new updated server or container images and then deploy them into production to replace the outdated ones. We perform a series of vulnerability scans including malware at build time and we monitor for compliance, unauthorized changes or abnormal behaviors once in production. Furthermore, files uploaded by our customers to their instance of Poka are also inspected for the presence of malware.
	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?	Yes, IDS/IPS type of functionalities are distributed across our SaaS infrastructure, on the IaaS infrastructure of AWS and implemented using services that are continuously updated.
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Poka's SaaS infrastructure is completely managed as code and is immutable once deployed in production. Servers and containers are treated as disposable. We never make any configuration changes to servers or containers in production. Instead, we go through a full DevSecOps pipeline to create new updated server or container images and then deploy them into production to replace the outdated ones. Poka's Security Team uses a combination of automated and manual vulnerability
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.3	Do you conduct local operating	

		system-layer vulnerability scans regularly as prescribed by industry best practices?	scanning/exploitation tools in order to detect or confirm the presence of vulnerabilities in our SaaS infrastructure and application. We also monitor for compliance, unauthorized changes or abnormal behaviors once in production. Furthermore, files uploaded by our customers to their instance of Poka are also inspected for the presence of malware. Poka also mandates a third-party security firm to perform authenticated and non-authenticated penetration testing against Poka SaaS infrastructure and application. The third party penetration testing is performed annually.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	We will provide to our customers upon request an attestation of the penetration test conducted by a third party security firm.
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	A vulnerability management policy and process are in place, and discovered vulnerabilities are managed in a timely manner. For more info about this control please refer to our SOC 2 attestation report which is available under NDA for all interested customers and potential customers.
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	
Threat and Vulnerability Management Mobile Code	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?	Not applicable.
	TVM-03.2	Is all unauthorized mobile code prevented from	Not applicable.

		executing?	