SIEMENS
Ingenuity for life

MindSphere Cloud Security Alliance questionnaire

Abstract
This document is intended to provide public cloud customers of MindSphere®, the industrial IoT as a service solution from Siemens with detailed information about industry-standard general cloud computing compliance questions, specifically the Cloud Security Alliance (CSA) questionnaire. Please refer to the MindSphere Region Table to understand where the CSA questionnaire is applicable. For all other questions related to MindSphere and its technical functions, please refer to the public MindSphere.io webpage.

As an organization that leads in automation and connected devices, Siemens understands the importance of having in-depth, proactive cybersecurity policies. For MindSphere, knowledge is embedded in the foundation of the security model. By working with cloud infrastructure providers and customers, Siemens can enforce consistent shared policies and practices for MindSphere. A multilayered security concept enables the guarding of sensitive data, applications, operating systems and infrastructures. As such, the MindSphere approach integrates cybersecurity throughout the lifecycle of the industrial Internet of Things (IIoT) solution.

The CSA is a nonprofit organization that researches and recommends best practices for secure cloud computing. CSA leverages the knowledge of experts across industries and domains to offer research, education, certification, events and products.

CSA certifications are available to any interested parties at varying levels of stringency specific to businesses at different stages of cloud adoption. These certifications help cloud service providers address security in their software delivery models. Currently, MindSphere is working on its CSA security, trust and assurance registry (STAR) Certification.

CSA STAR Certification is a rigorous, third-party, independent assessment of the security of a cloud service provider. The STAR Certification is based on achieving International Organization of Standards (ISO)/International Electrotechnical Commission (IEC) 27001, as well as the specified set of criteria detailed in the Cloud Controls Matrix. This detailed cloud security information about MindSphere can be found in subsequent pages of this document.

Powering IoT solutions
MindSphere is a leading industrial IoT as a service solution. MindSphere powers IoT solutions from the edge to the cloud with advanced analytics and artificial intelligence (AI) to connect and analyze data from connected products, plants and systems to optimize operations, create better products, and enable new business models. Built on the Mendix™ application platform, MindSphere enables the Siemens organization, its global partner ecosystem and its customers to quickly build and integrate personalized IoT applications.

Legal disclaimer
All statements made in this questionnaire have been diligently drafted based on the product features and information. The statements are for informational purposes only and do not create any kind of obligations or warranties on behalf of Siemens, which are subject conclusively to a written agreement between Siemens and its customers.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Application and interface security Application security	AIS-01.1	Do you use industry standards (for example, OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Yes	MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, for additional details. The MindSphere SDLC incorporates industry best practices that include threat modeling, risk assessments, vulnerability scans, penetration testing and other procedures.
	AIS-01.2	Do you use an automated source-code analysis tool to detect security defects in code prior to production?	Yes	Source code and related builds are scanned for vulnerabilities, security-related code smells, virus and malware as part of the SDLC.
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	Yes	Manual security reviews are performed continuously by designated security experts outside of the MindSphere development team.
	AIS-01.4	Do you verify that all your software suppliers adhere to industry standards for SDLC security?	Yes	MindSphere core products and applications (beyond Open Source) are developed in-house. For outsourced development the same security requirements apply. Compliance with industry standards is verified as part of the supplier management process, for example with attestation for industry standards such as SOC 1 reports, SOC 2 reports, ISO 27001 certificates and audit reports.
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes	The vulnerability scans in MindSphere are performed daily, in non-production and production environments and in each stage of the release process. Findings are classified, tracked and fixed according to MindSphere SDLC and Siemens Policy Framework.
Application and 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?	Yes	MindSphere customers retain responsibility to ensure their usage of MindSphere complies with applicable laws and regulations. MindSphere communicates its security and control environment to customers through appropriate Terms and Conditions (T&Cs) (refer to www.mindsphere.io/terms. https://new.Siemens.com/global/en/general/privacy-notice.html), industry certifications, third-party attestations and white papers.
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	Yes	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Application and interface security Data integrity	AIS-03.1	Do your data management policies and procedures require audits to verify data input and output integrity routines?	N/A	MindSphere relies on public cloud provider data integrity controls as described in system and organization controls (SOC) reports illustrates the data integrity controls maintained through all phases including transmission, storage and processing. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Data Security is an important keystone. Refer to ISO 27001 standard, Annex A, domain 14 for additional details.
	AIS-03.2	Are data input and output integrity routines (for example, MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Yes	
Application and interface security Data security/ integrity	AIS-04.1	Is your Data Security Architecture designed using an industry standard (for example, CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	Yes	MindSphere architecture was designed to incorporate industry-leading practices.
Audit assurance and compliance Audit planning	AAC-01.1	Do you develop and maintain an agreed upon audit plan (for example, scope, objective, frequency, resources, etc.) for reviewing the efficiency and effectiveness of implemented security controls?	Yes	MindSphere maintains an extensive compliance audit program that has been aligned to industry-best practices, regulatory, federal/ state, international laws, regional laws and industry-specific requirements. MindSphere adheres to Siemens Policy Framework Regular internal audits that verify the implementation of the Siemens Policy Framework. External audits are regularly performed as independent third-party attestation for industry standard. MindSphere is certified according to: • The SDLC is certified according to IEC 62443-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS) • ISO/IEC 27001:2013 certified for information security management system (ISMS)
	AAC-01.2	Does your audit program consider effectiveness of implementation of security operations?	Yes	
Audit assurance and compliance Independent audits	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	No	MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. The required evidences are available for external certifying bodies and independent auditors only for certification purposes.
			Yes	SOC reports of public cloud providers are available on request.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Audit assurance and compliance Independent audits *(continued)*	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure annually?	Yes	Use MindSphere to conduct penetration tests on infrastructure and application level on a regular base. Findings and recommendations are categorized and fixed according to Siemens Policy Framework. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Refer to Control A18.2.1 for additional details with respect to penetration tests.
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry-best practices and guidance?	Yes	
	AAC-02.4	Do you conduct annual internal audits at least annually?	Yes	With MindSphere you can maintain an extensive compliance audit program that has been aligned to industry-best practices, regulatory, federal/state, international laws, regional laws, and industry-specific requirements. MindSphere adheres to Siemens Policy Framework. Regular internal audits verify the implementation of the Siemens Policy Framework. External audits are regularly performed as independent third-party attestation for industry standard. MindSphere is certified according to: • The SDLC is certified according to IEC 62442-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS) • ISO/IEC 27001:2013 certified for information security management system (ISMS)
	AAC-02.5	Do you conduct independent audits at least annually?	Yes	
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	No	The results of penetration tests may contain sensitive information and are not made available. Example reports can be presented to customers under a non-disclosure agreement (NDA) upon request.
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	No	The results of internal audits may contain sensitive information and are not made available. Upon request and with a signed NDA the setup, organization and procedures (for example, TRA, penetration test, HSC) are available.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Audit assurance and compliance Information system regulatory mapping	AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes	Siemens has processes and procedures to monitor changes to the regulatory requirements. The security program and Siemens Policy Framework is changed accordingly on a regular basis. MindSphere adheres to Siemens Policy Framework. There are processes in place to supports services and project managers to efficiently ensure the compliance of products and services with relevant laws and regulations.
Business continuity management and operational resilience Business continuity planning	BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	Yes	MindSphere is not an Infrastructure as a Service (IaaS) offering but it uses well known public cloud providers. These providers are responsible for business continuity management on IT infrastructure level. For MindSphere services MindSphere provides business continuity management plans according to ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	BCR-01.2	Do you have more than one provider for each service you depend on?	Yes	MindSphere services are available worldwide on many major platforms, including AWS®, Azure® and Alibaba® in China.
	BCR-01.3	Do you provide a disaster recovery capability?	Yes	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These providers are responsible for providing disaster recovery capabilities on IT infrastructure level. For MindSphere services, MindSphere provides disaster recovery capability according to ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	Yes	MindSphere service continuity is monitored continuously as well as continuity of all services on infrastructure level provided by public cloud providers.
	BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?	Yes	Operation redundancy is in place and is monitored and reported continuously. Reports are shared with customers upon request as needed.
	BCR-01.6	Do you provide a tenant-triggered failover option?	Yes	MindSphere is a Software as a Service (SaaS) offering. Their means failover is triggered by MindSphere. Tenants do not need to take any actions to trigger a failover.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Business continuity management and operational resilience Business continuity planning *(continued)*	BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?	Yes	Business continuity and redundancy plans are in place and are monitored and reported continuously. Plans and reports are shared with customers upon request.
Business continuity management and operational resilience Business continuity testing	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes	MindSphere Business Continuity and Incident Response Plans have been developed and tested in alignment with ISO 27001 standards. Business Continuity Plans define roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Incident Response Plans cover internal roles and responsibilities as well as suppliers and customers. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Business Continuity and Incident Response Plans are reviewed annually.
Business continuity management and operational resilience Power/ Telecommunications	BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	N/A	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers adhere to industry standards like ISO 27001, IEC 62443 and ISO 9001.
	BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	N/A	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers have implemented procedures and controls to secure utility services and mitigate environmental conditions.
Business continuity management and operational resilience Documentation	BCR-04.1	Are information system documents (for example, administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes	Information System Documentation is made available to MindSphere personnel using the Siemens Intranet site. Access must be authorized on a need-to-know principle. MindSphere maintains detailed documentation (for example, architecture diagrams, system configuration and documentation, operating procedures), stores the documentation securely and makes it available to authorized personnel.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Business continuity management and operational resilience Environmental risks	BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	Yes	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers have implemented appropriate countermeasures against physical damage. Based on that, MindSphere services are capable of handling physical damage.
Business continuity management and 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.)?	N/A	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers have implemented appropriate countermeasures against environmental risks.
Business continuity management and operational resilience Equipment maintenance	BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	N/A	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers have implemented appropriate controls and procedures for equipment maintenance.
	BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	N/A	
Business continuity management and operational resilience Equipment power failures	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (for example, power failures, network disruptions, etc.)?	N/A	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers have implemented appropriate security mechanisms and redundancies to protect equipment from utility service outages.
Business continuity management and operational resilience Impact analysis	BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (for example, criticality of services and recovery priorities, disruption tolerance, RPO and RTO, etc.)?	Yes	As part of Business Continuity planning, MindSphere has implemented processes, controls and procedures for analyzing the business impact of any disruption of services. Business Continuity plans define roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Business Continuity and Incident Response plans are reviewed annually.
	BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	Yes	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Business continuity management and operational resilience Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes	MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, for additional details. MindSphere adheres to Siemens Policy Framework. Regular internal audits verify the implementation of the Siemens Policy Framework. Siemens Policy Framework is available to all personnel. Roles and responsibilities are defined and regularly trained for information security.
Business continuity management and operational resilience Retention policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	Yes	Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual or business requirements. MindSphere customers retain control and ownership of their data. It is the customer's responsibility to enforce data retention according to their own requirements.
	BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	Yes	In its agreements, Siemens contractually commits to specific procedures when a customer terminates MindSphere services. This includes deleting customer data from systems under MindSphere control. Also data privacy related topics are addressed there. Refer to https://siemens.mindsphere.io/en/terms for more details.
	BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes	MindSphere backup and recovery policies, procedures and controls are verified, documented and audited both internally and by third-party assessors according to ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Yes	MindSphere is not an IaaS offering but it uses well known public cloud providers instead. These cloud providers have implemented appropriate controls and procedures for independent hardware restore and recovery capabilities.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Business continuity management and operational resilience Retention policy *(continued)*	BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	N/A	MindSphere services are responsible for managing the virtual infrastructure provided by specific public cloud providers.
	BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	No	MindSphere is not an IaaS offering but it uses different public cloud providers instead. These cloud providers have implemented capabilities and services for data restoration and recovery which are certified according to industry standards.
	BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	Yes	MindSphere backup and redundancy mechanisms are tested at least once a year.
Change control and 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?	Yes	MindSphere has established software development and release management processes and procedures to control the implementation of major changes including management authorization for development or acquisition. Customers are responsible for their own applications hosted on MindSphere.
Change control and configuration management Outsourced Development	CCC-02.1	Are policies and procedures for change management, release and testing adequately communicated to external business partners?	Yes	MindSphere core products and applications (beyond Open Source) are developed in-house based on MindSphere SDLC process and policies. Refer to ISO 27001 standard, Annex A, domain 14 for additional details.
	CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	Yes	For outsourced development, the same security requirements apply. Compliance with industry standards is verified as part of the supplier management process, for example with attestation for industry standards such as SOC 1 reports, SOC 2 reports, ISO 27001 certificates and audit reports. MindSphere is certified according to: • The SDLC is certified according to IEC 62443-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS) • ISO/IEC 27001:2013 certified for information security management System (ISMS)

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Change control and configuration management Quality testing	CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality and integrity?	Yes	Industry best practices for quality change control and testing processes are part of MindSphere SDLC. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. MindSphere is certified according to: • The SDLC is certified according to IEC 62443-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS) • ISO/IEC 27001:2013 certified for information security management system (ISMS)
	CCC-03.2	Is documentation describing known issues with certain products/services available?	Yes	The MindSphere Maintenance and Status Information Bulletin notifies customers of security and privacy events. Refer to page https://status.mindsphere.io/ for additional details.
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes	Reported bugs and vulnerabilities are classified, tracked and fixed according to MindSphere SDLC and Siemens Policy Framework. Software updates to implement fixes are controlled by industry-best practices, release management processes and procedures.
	CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	Yes	Any software developer for MindSphere is obligated to follow and is trained on MindSphere SDLC. Quality controls are in place to ensure compliance. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. MindSphere is certified according to: • The SDLC is certified according to IEC 62443-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS) • ISO/IEC 27001:2013 certified for information security management system (ISMS)

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Change control and configuration management Quality testing *(continued)*	CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?	Yes	MindSphere develops software based on MindSphere SDLC process and policies generally inhouse. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. MindSphere is certified according to: • The SDLC is certified according to IEC 62443-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS). • ISO/IEC 27001:2013 certified for information security management system (ISMS). Wherever MindSphere uses Open Source components, these components are checked daily on source code security defects.
	CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?		Project teams perform security testing in the implementation, verification and release phases as part of MindSphere SDLC to identify flaws and weaknesses in software. The identified flaws and vulnerabilities are classified, tracked and fixed according to MindSphere SDLC. Software on production is continuously inspected to ensure it is consistent with the approved build release.
Change control and 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?	Yes	MindSphere processes and procedures for managing malicious software are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. MindSphere has been certified by an independent auditor to confirm alignment with ISO 27001 standard.
Change control and 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?	Yes	Customers have access to various reports and guidelines describing controls relevant to change management. Refer to https://status.mindsphere.io/ and https://developer.mindsphere.io/concepts/concept-roles-scopes.html
	CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	Yes	All changes in production go through the Change Management process described in CCC-01. Prior to release to production, software code is inspected, reviewed and tested in non-production environments strictly separated from production environments.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Change control and configuration management Production changes *(continued)*	CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing service level agreements (SLAs)?	Yes	To fulfill existing SLAs, MindSphere software updates are controlled for unauthorized changes through MindSphere SDLC and release management processes. Automated scans are active to detect system anomalies or unauthorized changes.
Data security and information lifecycle management Classification	DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (for example, tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Yes	Resources owned by MindSphere are tagged in a proper and MindSphere-specific way. Untagged resources are removed. MindSphere is not an IaaS offering: hardware is managed by public cloud providers only.
	DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (for example, TXT/TPM, VN-Tag, etc.)?	N/A	
Data security and 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?	Yes	Internally, MindSphere tracks data flows and network connectivity. MindSphere will not transfer customer data outside the data center selected by a customer upon onboarding. For customers, MindSphere provides a high-level overview about data flows in context of MindSphere security architecture. Refer to the whitepaper "MindSphere Security Model" for additional details.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	Yes	
Data security and information lifecycle management E-commerce transactions	DSI-03.1	Do you provide standardized (for example, ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants for them to protect their data if it is required to move through public networks (for example, the internet)?	Yes	MindSphere encrypts data at rest and in transit using standard encryption algorithms. For customer-managed applications, MindSphere allows customers to use their own encryption mechanism. Customers may also use third-party encryption technologies.
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (for example, internet-based replication of data from one environment to another)?	Yes	Communication between infrastructure components via public networks is always encrypted with industry-standard transport protocols such as transport layer security (TLS).

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Data security and information lifecycle management Handling/Labeling/ Security policy	DSI-04.1	Are policies and procedures established for data labeling and handling to ensure the security of data and objects that contain data?	Yes	A formal policy regarding data labeling and handling has been implemented using MindSphere. The policies and procedures define and check what labels are used. It is also required to have an assigned person responsible for data and objects that contain data (storage, compute, network). The responsibility includes maintaining related up-to-date information. Infrastructure resources are labeled by assigning tags which give information about the infrastructure component. Untagged resources are removed from the system. All employees, contractors and third parties acting as responsible persons must ensure that data and objects containing data are handled securely according to ISO 27001 standard.
	DSI-04.2	Do you follow a structured data-labeling standard (for example, ISO 15489, Oasis XML Catalog Specification, CSA data type guidance, etc.)?	N/A	
	DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes	For aggregated data objects the maximum principle applies (highest relevant classification should be applied).
Data security and information lifecycle management Nonproduction data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes	The MindSphere production environment is separated from any other environment used for other purposes, for example development and quality assurance. No customer data is replicated to a non-production environment.
Data security and information lifecycle management Ownership/ stewardship	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	Yes	MindSphere customers retain control and ownership of their own data. Refer to https://siemens.mindsphere.io/en/terms for additional details.
Data security and information lifecycle management Secure disposal	DSI-07.1	Do you support the secure deletion (for example, degaussing/ cryptographic wiping) of archived and backed-up data?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. So secure deletion and sanitizing is handled by the cloud provider.
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	N/A	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Datacenter security Asset management	DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations and operational continuity requirements?	Yes	MindSphere is not an IaaS offering but it uses public cloud providers instead. Nevertheless, all virtual assets are classified according to Siemens Policy Framework and industry-best practices like ISO 27001 standard.
	DCS-01.2	Do you maintain a complete inventory of all your critical assets located at all sites/or geographical locations and their assigned ownership?	Yes	MindSphere allows you to maintain a central inventory of all used assets. The inventory is updated and reviewed daily to ensure consistency and completeness.
Datacenter security Controlled access points	DCS-02.1	Are physical security perimeters (for example, fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols, etc.) implemented for all areas housing sensitive data and information systems?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. Any cloud provider used by MindSphere manages physical security according to industry standard and best practices. Cloud providers have been validated and certified by independent third parties.
Datacenter security Equipment identification	DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	Yes	Geo-location is used to restrict authentication, based on IP addresses, in specific geographies.
	DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. For data center purposes, it is handled by the cloud provider.
Datacenter security Offsite authorization	DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software or data to an offsite premise?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. For data center purposes, it is handled by the cloud provider. MindSphere will not transfer customer data outside the data center selected by the customer upon onboarding.
Datacenter security Offsite equipment	DCS-05.1	Can you provide tenants with your asset management policies and procedures?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. For data center purposes, it is handled by the cloud provider. For MindSphere customers asset management policies and procedures are described in https://Siemens.mindsphere.io/en/terms

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
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?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. For data center purposes, it is handled by the cloud provider. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. The required evidences are available for external certifying bodies and independent auditors only for certification purposes.
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. For data center purposes, it is handled by the cloud provider. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A for additional details. MindSphere adheres to Siemens Policy Framework. Regular internal audits verify the implementation of the Siemens Policy Framework. Siemens Policy Framework is available to all personnel. Roles and responsibilities are defined and regularly trained for information security.
Datacenter security Secure area authorization	DCS-07.1	Are physical access control mechanisms (for example, CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. For data center purposes, it is handled by the cloud provider. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A for additional details. MindSphere adheres to Siemens Policy Framework. Regular internal audits verify the implementation of the Siemens Policy Framework. Siemens Policy Framework is available to all personnel. Roles and responsibilities are defined and regularly trained for information security.
Datacenter security Unauthorized persons entry	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?	N/A	
Datacenter security User access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	N/A	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Encryption and key management Entitlement	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	Yes	MindSphere has established policies, procedures and controls for key management according to ISO 27001 standard.
Encryption and key management Key generation	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Yes	MindSphere allows customers to use their own encryption mechanisms that are the customer's responsibility. Internally, MindSphere establishes and manages its own cryptographic keys based on cloud provider infrastructure.
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	N/A	MindSphere is not an IaaS offering but it provides higher level services for IoT use cases. This includes encryption and decryption of data in rest and data in motion.
	EKM-02.3	Do you maintain key management procedures?	Yes	MindSphere has established policies, procedures and controls for key management according to ISO 27001 standard.
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes	
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Yes	MindSphere uses https://www.vaultproject.io/ as an open source key management system as well as cloud provider-specific technologies like AWS KMS or Azure Key Vault.
Encryption and key management Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes	MindSphere as SaaS offering is committed to encryption at rest for all customer data.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine (VM) images during transport across and between networks and hypervisor instances?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead. Encryption of data and VM images between networks and hypervisors is managed by the public cloud provider.
	EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	Yes	MindSphere has established policies, procedures and controls for key management according to ISO 27001 standard. Siemens Policy Framework is available to all personnel. Roles and responsibilities are defined and regularly trained for information security. For customers, MindSphere provides an overview about its encryption strategies. Refer to the "MindSphere Security Model" for additional details. Please contact a MindSphere representative for access.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Encryption and key management Storage and access	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Yes	MindSphere relies on strong cryptography using standard, validated formats including AES-256, IPsec, TLS and SSH.
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Yes	MindSphere uses https://www.vaultproject.io/ as an open source key management system as well as cloud provider-specific technologies like AWS KMS or Azure Key Vault.
	EKM-04.3	Do you store encryption keys in the cloud?	Yes	
	EKM-04.4	Do you have separate key management and key usage duties?	Yes	According to the "segregation of duties" principle as mentioned in ISO 27001 standard, MindSphere has established and implemented procedures to enforce segregation of key management and key usage duties.
Governance and risk management Baseline requirements	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (for example, hypervisors, operating systems, routers, DNS servers, etc.)?	Yes	In compliance with ISO 27001 standard, MindSphere maintains all corresponding baseline security requirements.
	GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes	Infrastructure security compliance checks are conducted continuously. Findings are immediately reported to responsible DevOps teams to deal with identified vulnerabilities.
Governance and risk management Risk assessments	GRM-02.1	Does your organization's risk assessments consider awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	Yes	MindSphere performs an annual internal risk assessment in addition to the regular ISO 27001 surveillance audits. Legal and statutory requirements are addressed in that context. All residual risks are managed following the standard risk management process.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes	European Data Privacy Laws and ISO 27018 requirements are addressed by MindSphere baseline security requirements. Compliance is monitored regularly by the Siemens data privacy organization and as part of the annual ISO 27001 surveillance audit. For more information refer to https://siemens.mindsphere.io/en and https://new.siemens.com/global/en/general/privacy-notice.html for additional details.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Governance and risk management Management oversight	GRM-03.1	Are your technical, business and executive managers responsible for maintaining awareness of and compliance with security policies, procedures and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Yes	Every MindSphere employee is provided with and must complete security-related periodic trainings, provided by ISMS coordinators and Siemens Global Learning Platforms. Each manager is responsible for respective Annex A security controls in their functional roles and responsibilities.
Governance and risk management Management program	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Yes	Customers are provided with our ISO 27001 certification, reflecting the capability of our internal processes to follow ISO 27001 standard. In addition, MindSphere provides technical and training material from the stock and on-demand.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	Yes	ISMS is reviewed at least annually and audited by an independent third party as part of the ISO 27001 certification.
Governance and risk management Management support/involvement	GRM-05.1	Do executive and line management take formal action to support information security through clearly documented direction and commitment and ensure the action has been assigned?	Yes	The MindSphere ISMS has an information security "Leadership and Commitment" policy, as well as a clearly documented ISMS roles and responsibility model ensuring that each executive and functional line management has been assigned and is supporting respective activities.
Governance and risk management Policy	GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (for example, ISO 27001, SOC 2)?	Yes	The MindSphere ISMS implements all ISO 27001 and Annex A controls and is published for internal use by any employee. Business partners are informed respectively via supplier and business partner contracts about MindSphere information security requirements.
	GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	Yes	Information Security Policies start at the highest level of the company and are detailed for any subordinate management level. Any Information Security Policy is approved by appropriate management level.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Governance and risk management Policy *(continued)*	GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes	Information security requirements are contractually agreed on with business partners via MindSphere supplier and business partner management.
	GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Yes	Compliance Control Documents are available for third party accredited independent auditors.
	GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	Yes	MindSphere complies with ISO 27001 and European data privacy laws. Information is available on www.mindsphere.io Certificates can be provided upon request. MindSphere is certified according to: • The SDLC is certified according to IEC 62443-4-1 • ISO/IEC 9001:2015 certified for an effective Quality Management System (QMS) • ISO/IEC 27001:2013 certified for information security management system (ISMS)
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?	Yes	The Business Conduct Guidelines are our corporate code of conduct and as such are at the heart of our global Siemens Compliance System. Its contents are built from our values and are mandatory for all Siemens employees. The Business Conduct Guidelines clearly state that any employee must protect the company. For that reason, Siemens provides security policies and security training to employees to educate them as to their role and responsibilities concerning information security. The Business Conduct Guideline are part of employment contracts.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes	
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?	Yes	As part of its ISMS and based on ISO 27001 framework, MindSphere performs annual risk assessments. All relevant policies, procedures and standards are updated continuously.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
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?	N/A	Our security-related documentation is available at www.mindsphere.io and is updated on a regular basis to reflect updates of MindSphere Information Security Policies.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes	As part of its ISMS and based on ISO 27001 framework, an annual review of data privacy and security policies is performed using MindSphere.
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?	Yes	MindSphere performs annual risk assessment as part of the overall ISMS framework based on ISO 27001 standard. Any risk is evaluated with respect to likelihood and impact using qualitative and quantitative methods based on Siemens Enterprise Risk Management Framework.
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	Yes	Any risk is assigned to a specific risk level by determining the likelihood of occurrence and impact. Security measures are evaluated, planned and implemented to mitigate risk to the highest extent possible.
Governance and risk management Program	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	Yes	Based on the Siemens Enterprise Risk Management Framework and ISO 27001 standard, MindSphere maintains its certified ISMS as a framework to manage security-related risks.
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	Yes	Documents are available for third party accredited independent auditors.
Human resources Asset returns	HRS-01.1	Upon termination of a contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally owned assets?	Yes	Siemens HR drives the employee termination process in coordination with management. An automated workflow ensures proper information of all involved people and departments.
	HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	Yes	Siemens HR drives the employee termination process in coordination with management. An automated workflow ensures all Siemens-owned assets are returned upon employee termination.
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?	Yes	Siemens HR conducts background checks, as permitted by local laws and regulations, as part of pre-employment screening practices as needed (according to the employee's position and responsibilities).

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Human resources Employment agreements	HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Yes	Upon hire, employees are required to sign Siemens Information Security Guidelines and Business Conduct Guidelines as part of any employment contract.
	HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources and assets?	Yes	
Human resources Employment termination	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	Yes	Siemens HR policies, procedures, workflows and guidance cover all aspects of termination and changes of employment.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes	Siemens HR termination policies and procedures cover all aspects of separation including return of badges, computer equipment, data and other assets.
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 (for example, laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (for example, desktop computers at the provider organization's facilities)?	Yes	Siemens does not allow any access to its sensitive data and customer data especially with mobile or portable devices unless the requesting users have been approved for that by responsible management.
Human resources Non-disclosure 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?	Yes	Siemens HR maintain policies and procedures defining the implementation and execution of nondisclosure and confidentiality agreements. Siemens requires employees to sign non-disclosure and confidentiality agreements upon hire.
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?	Yes	Tenant roles and responsibilities are clearly defined in MindSphere policies, which are acknowledged by tenants when subscribing to services. The Master Agreement is available at https://Siemens.mindsphere.io/en/terms

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Human resources Acceptable use	HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and IT infrastructure network and systems components?	Yes	Siemens HR provides policies defining acceptable use guidelines for various assets (corporate network, email, computers, removable media, printed documents etc.). All Siemens employees are required to follow their policy. Also MindSphere has policies in place defining the general code of conduct for usage of MindSphere services (Refer to https://Siemens.mindsphere.io/en/terms)
	HRS-08.2	Do you define allowance and conditions for bring your own devices (BYOD) and its applications to access corporate resources?	N/A	Siemens does not support BYODs to access corporate resources.
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 (for example, multitenancy, nationality, cloud delivery model, segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	Yes	Each Siemens employee receives mandatory annual web-based information security trainings. In addition, MindSphere employees receive annual role-based ISMS awareness trainings. Functional specific security trainings are in addition determined between the employee and their manager on demand.
	HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Yes	Each Siemens employee receives mandatory annual web-based information security trainings. In addition, MindSphere employees receive annual role-based ISMS awareness trainings. Functional specific security trainings are in addition determined between the employee and their manager on demand.
	HRS-09.3	Do you document employee acknowledgment of training they have completed?	Yes	All trainings are tracked and documented.
	HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes	Successful completion of mandatory security training is required for all employees with access to sensitive systems.
	HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	Yes	Each Siemens employee receives mandatory annual web-based information security trainings. In addition, MindSphere employees receive annual role-based ISMS awareness trainings. Functional specific security trainings are in addition determined between the employee and their manager on demand.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Human resources Training/awareness *(continued)*	HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities regarding security and data integrity?	Yes	Each Siemens employee receives mandatory annual web-based information security trainings. In addition, MindSphere employees receive annual role-based ISMS awareness trainings. Functional specific security trainings are in addition determined between the employee and their manager on demand.
Human resources User responsibility	HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	Yes	All Siemens employees are made aware of their roles and responsibilities using multiple methods including regular newsletters, poster sessions and role-based ISMS awareness trainings.
	HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	Yes	
	HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	Yes	
Human resources Workspace	HRS-11.1	Are all computers and laptops configured as such that there is a lockout screen after a predefined amount of time?	Yes	Siemens corporate IT departments deploy and update specific session lock functionality on all computers and laptops and enforce session lockouts after a defined period of inactivity.
	HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (for example, on a desktop) sensitive documents?	Yes	Siemens Policy Framework defines specific controls for secure operation of any kind of equipment and offices.
Identity and access management Audit tools access	IAM-01.1	Do you restrict, log and monitor access to your information security management systems (for example hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes	According to ISO 27001 standard, access to MindSphere information security management systems is granted: • based upon business requirements • based upon need-to-know and least-privilege principles • based upon fine-grained and role-based access controls MindSphere services and components are configured to log and collect security events.
	IAM-01.2	Do you monitor and log privileged access (for example, administrator level) to information security management systems?	Yes	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Identity and 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?	Yes	According to ISO 27001 standard, access to MindSphere systems is removed in case it is no longer required for business purposes.
	IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	Yes	Siemens has established and implemented policies and procedures to ensure adherence to legal, statutory and regulatory compliance requirements in all jurisdictions in which it operates.
	IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de/provisioning based on the rule of least privilege?	Yes	MindSphere has established and implemented procedures and technical measures for on/offboarding of user accounts based on the least privilege principle.
	IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multitenant system architectures?	Yes	MindSphere has established and implemented procedures and technical measures to ensure clear tenant separation in all aspects, also with respect to data access.
	IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	N/A	MindSphere relies on the AAA capabilities of public cloud providers on the network and infrastructure level.
	IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	Yes	MindSphere supports multifactor authentication for customers.
	IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	Yes	MindSphere has established and implemented metrics to track offboarding of user accounts.
Identity and access management Diagnostic/ Configuration ports access	IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	N/A	MindSphere is not an IaaS offering, so it does not provide any diagnostic and configuration ports on the hardware and infrastructure level. Diagnostic Data of MindSphere Connectivity Elements is available for customers owning the element only. Refer to https://documentation.mindsphere.io/resources/html/agent-diagnostic/en-US/index.html for additional details.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Identity and 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?	Yes	According to ISO 27001 access to MindSphere information security management systems is granted: • based upon business requirements • based upon need-to-know and least-privilege principles • based upon fine-grained and role-based access controls For that, MindSphere manages the identity of all internal users assigned to some role ("normal" and "high privileged"). Because MindSphere is a SaaS offering, there is no need for MindSphere customers to care about resources on infrastructure and network level.
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	Yes	
Identity and 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?	N/A	MindSphere is a SaaS offering, so there is no need for customers to care about segregation of duties in MindSphere. Internally, MindSphere aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6 for additional details. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
Identity and 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?	Yes	According to ISO 27001 industry standard, MindSphere has established and implemented formal policies, procedures and controls to protect MindSphere source code.
	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?	Yes	Customers object source code for applications deployed to MindSphere Cloud Foundry environment, is protected by MindSphere. The customer can access their source code using SSH. Refer to https://developer.mindsphere.io/paas/paas-cloud-foundry-ssh.html for additional details.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Identity and access management Third party access	IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?	Yes	Identification of access-control related risks related to third-party suppliers is conducted as part of our Supplier and Risk Management program in alignment with ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Service Level Agreements and other metrics (access to specific services) are monitored continuously to initiate proper preventive, detective and corrective actions.
	IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	Yes	
Identity and access management User access restriction/ authorization	IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/ customer credentials following the rules of least privilege?	Yes	For MindSphere customers developing their own applications, concepts and controls are in place to support customers implementing their specific access control procedures. Internally, MindSphere access control policies, procedures and controls are established and implemented based on “need to know” and “least privilege” principles according to ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	Yes	
	IAM-08.3	Do you limit identities’ replication only to users explicitly defined as business necessary?	Yes	
Identity and access management User access authorization	IAM-09.1	Does your management provision the authorization and restrictions for user access (for example, 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?	Yes	For MindSphere customers, a customer’s administrator is responsible for providing initial authorization and restrictions in a proper way. Internally, MindSphere access control policies, procedures and controls are established and implemented based on “need to know” and “least privilege” principles according to ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IAM-09.2	Do you provide upon the request of users with legitimate interest access (for example, 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?	Yes	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Identity and access management User access reviews	IAM-10.1	Do you require a periodical authorization and validation (for example, at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants) based on the rule of least privilege, by business leadership or other accountable business role or function?	Yes	For customers, any account must be revalidated on a yearly base. Any revalidation is logged. Internally, and according to ISO 27001 standard, all users are requested to renew their access grants at least once a year. In case of missing re-approvals, access rights are automatically revoked. Any revalidation is logged. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	Yes	
	IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	Yes	
	IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes	Customers will be notified in case their data was inappropriately accessed. Entitlement and remediation reports may be shared on a case-by-case basis.
Identity and 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?	Yes	For MindSphere customers, user access can be deactivated and reactivated under certain conditions that are further defined in the customer agreement. Internally, access is automatically revoked when an employment contract is terminated. Changes in an employee's role may lead to revocation as needed. Continued access must be explicitly requested by the employee.
	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?	Yes	
Identity and access management User ID credentials	IAM-12.1	Do you support the use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Yes	For customers, MindSphere IAM provides identity federation with customer-specific identity providers. Internally, MindSphere IAM supports integration with Siemens entitlement services.
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	Yes	For customers, MindSphere IAM provides identity federation with customer-specific identity providers.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Identity and access management User ID credentials *(continued)*	IAM-12.3	Do you support identity federation standards (for example, SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Yes	For customers, MindSphere IAM provides identity federation with customer-specific identity providers.
	IAM-12.4	Do you have a Policy Enforcement Point capability (for example, XACML) to enforce regional legal and policy constraints on user access?	Yes	To comply with specific legal constraints, MindSphere controls and prevents logins and access from certain countries based on IP address policies.
	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?	Yes	MindSphere has implemented identity management and access control based on roles and scopes. Refer to https://developer.mindsphere.io/concepts/concept-roles-scopes.html for additional details.
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (for example, digital certs, tokens, biometrics, etc.) for user access?	Yes	For customers, MindSphere provides Multi-Factor Authentication with a specific set of strong (multifactor) authentication options.
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	Yes	OAuth 2 standard is supported by MindSphere.
	IAM-12.8	Do you support password (for example, minimum length, age, history, complexity) and account lockout (for example, lockout threshold, lockout duration) policy enforcement?	Yes	In alignment with ISO 27001 standard, MindSphere has established and implemented policies and procedures for password expiration, length and complexity. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	No	
	IAM-12.10	Do you support the ability to force password changes upon first logon?	N/A	
	IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (for example, self-service via email, defined challenge questions, manual unlock)?	Yes	
Identity and access management Utility programs access	IAM-13.1	Is access to utility programs used to manage virtualized partitions (for example, shutdown, clone, etc.) appropriately restricted and monitored?	N/A	MindSphere is not an IaaS offering but it uses public cloud providers instead to manage virtualized partitions.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Infrastructure and 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?	Yes	MindSphere relies on public cloud provider data integrity controls as described in SOC reports which illustrate the data integrity controls maintained through all phases including transmission, storage and processing. MindSphere relies on public cloud provider IDS tools to detect, investigate and respond to attacks on infrastructure level. MindSphere has implemented specific IDS tools to detect, investigate and respond to attacks on application level.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Yes	Access to audit logs is restricted to authorized personnel only based on job responsibilities.
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	N/A	MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. The required evidences are available for external certifying bodies and independent auditors only for certification purposes.
	IVS-01.4	Are audit logs centrally stored and retained?	Yes	In alignment with ISO 27001 standards, MindSphere logs security-related events in a central place and ensures its integrity. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (for example, with automated tools)?	Yes	MindSphere uses automated monitoring systems and various tools to provide a high level of service performance and availability. A dedicated MindSphere operations team is always available to respond to operational issues. This includes a pager system to raise alarms quickly and reliably.
Infrastructure and virtualization security Change detection	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (for example, dormant, off or running)?	N/A	MindSphere is not an IaaS offering, so customers do not access virtual machines, infrastructure systems and network components directly. Virtual machines utilized and managed by MindSphere are built, configured and monitored according ISO 27001 standard requirements. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	N/A	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Infrastructure and virtualization security Change detection *(continued)*	IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (for example, portals or alerts)?	N/A	
Infrastructure and virtualization security Clock synchronization	IVS-03.1	Do you use a synchronized time-service protocol (for example, NTP) to ensure all systems have a common time reference?	Yes	MindSphere relies on public cloud provider internal system clocks. MindSphere has been certified by an independent auditor to confirm alignment with ISO 27001 standard.
Infrastructure and virtualization security Capacity/resource planning	IVS-04.1	Do you provide documentation regarding what levels of system (for example, network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Yes	MindSphere Service Limits are described on the MindSphere website at https://documentation.mindsphere.io/resources/html/upgrade/en-US/index.html
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	N/A	MindSphere is not an IaaS offering, so customers do not access hypervisors directly. MindSphere provides higher level services for IoT use cases, using the public cloud provider for the management of lower level resources like memory and hypervisor.
	IVS-04.3	Do your system's capacity requirements consider current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	Yes	MindSphere system resources are scaled up and down to address agreed SLAs and system limits according to MindSphere offerings, based on current, projected and anticipated capacity needs.
	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?	Yes	System performance is monitored continuously. When thresholds are reached or an irregular event occurs, operations staff is triggered to mitigate.
Infrastructure and virtualization security Management - vulnerability management	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (for example, virtualization aware)?	Yes	MindSphere executes continuous vulnerability scans considering virtualization technologies based on CIS-Benchmarks (https://www.cisecurity.org/cis-benchmarks/) MindSphere is not an IaaS offering, so no virtualization technologies (like hypervisor) are provided to our customers. MindSphere provides higher level services for IoT use cases, using a public cloud provider for the management of virtualization technologies.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Infrastructure and 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?	N/A	MindSphere is not an IaaS offering, so no virtualization technologies (like hypervisor) are provided to our customers. MindSphere provides higher level services for IoT use cases, using the public cloud provider for the management of virtualization technologies.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes	Network architecture diagrams are updated regularly or in case of relevant changes.
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (for example, firewall rules) between security domains/zones within the network?	Yes	Firewall rules are documented and reviewed on a regular basis. All changes are required to follow MindSphere SDLC. Access Control Lists are scanned on appropriateness daily. Any violation is classified, tracked and fixed according to MindSphere SDLC.
	IVS-06.4	Are all firewall access control lists documented with business justification?	Yes	Firewall rules are defined and documented to address legal, business and security needs.
Infrastructure and 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 (for example, antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	Yes	Virtual machines utilized and managed by MindSphere are built, configured and monitored according ISO 27001 standard requirements and Siemens Policy Framework. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
Infrastructure and virtualization security Production/ non-production environments	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Yes	MindSphere customers are provided with separated environments for production and test processes according to MindSphere developer and operator offerings.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	N/A	MindSphere is not an IaaS offering, customers do not create their own environments, for example, production and test environments. Instead, MindSphere provides ready-to-use environments for fast and easy app development to our customers.
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	Yes	MindSphere production and non-production environments are clearly separated by using different accounts and subscriptions.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Infrastructure and 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?	Yes	MindSphere has implemented an in-depth defense strategy according to ISO 27001 standard, including firewalls, network segmentation and ACL restrictions. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	Yes	MindSphere firewall rules clearly address legal, regulatory and contractual requirements.
	IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory and regulatory compliance obligations?	Yes	MindSphere is not an IaaS offering, so customers do not access infrastructure system and network components directly. MindSphere Services implement tenant separation according to ISO 27001 standard, addressing established policies, legal, statutory and regulatory compliance obligations. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IVS-09.4	Do you can logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes	MindSphere Services implement tenant separation according to ISO 27001 standard, ensuring that a specific tenant's data cannot be accessed by another tenant without proper agreement. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Yes	MindSphere protects sensitive data against unauthorized access by utilizing in-depth defense strategies including firewalls, ACLs and other access control policies.
Infrastructure and 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?	N/A	MindSphere uses only virtualized managed services from the public cloud provider.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	N/A	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Infrastructure and 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 (for example, two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications) to the administrative consoles?	Yes	MindSphere has implemented the concept of least privilege allowing only the necessary access for users according to their roles and responsibilities.
Infrastructure and virtualization security Wireless security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	N/A	MindSphere is not a wireless network provider. It is the responsibility of the MindSphere customer to manage mobile security devices and services used to access data in MindSphere. Each Siemens employee receives mandatory annual information security trainings, addressing any mobile security-related topic as needed.
	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 (for example, encryption keys, passwords, SNMP community strings)?	N/A	
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	N/A	
Infrastructure and 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?	No	MindSphere has not been designed for high-risk environments. The customer agreement states this explicitly and the customer remains responsible for the individual usage scope.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Infrastructure and virtualization security Network architecture *(continued)*	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (for example, deep packet analysis, traffic throttling and blackholing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (for example, MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Yes	MindSphere is not an IaaS offering, so MindSphere relies on the public cloud provider and its related capabilities. MindSphere has implemented security measures like Web Application Firewalls to protect against network-based attacks.
Interoperability and portability APIs	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Yes	MindSphere publishes and updates as needed a list of all APIs available for customers. Refer to https://developer.mindsphere.io/apis/index.html for additional details.
Interoperability and portability Data request	IPY-02.1	Is unstructured customer data available on request in an industry-standard format (for example, .doc, .xls, or .pdf)?	Yes	Specific unstructured data related solely to the customer is available upon request in appropriate standard formats.
Interoperability and portability Policy and legal	IPY-03.1	Do you provide policies and procedures (service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Yes	MindSphere enables customers to integrate their cloud-based software as an application in MindSphere with other cloud-based applications. Refer to https://documentation.mindsphere.io/resources/html/mindconnect-integration/en-US/index.html for additional details.
	IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	N/A	MindSphere is not an IaaS offering, so customers do not access infrastructure components directly, like virtual machines and their images.
	IPY-03.3	Do you provide policies and procedures (service level agreements) governing the migration of application data to and from your service?	Yes	MindSphere enables customers to integrate their cloud-based software as an application in MindSphere with other cloud-based applications. Refer to https://documentation.mindsphere.io/resources/html/mindconnect-integration/en-US/index.html for additional details.
Interoperability and portability Standardized network protocols	IPY-04.1	Is data import, data export, and service management conducted over secure (for example, non-clear text and authenticated), industry accepted standardized network protocols?	Yes	MindSphere enables customers to ingest data in the MindSphere Platform and to analyze data based on industry- accepted standardized authentication and communication protocols.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Interoperability and portability Standardized network protocols *(continued)*	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes	On the cloud-level, industry accepted standardized network protocols are used. Refer to https://Siemens.mindsphere.io/en/developer for additional details. On the field-level, MindSphere supports a specific set of standardized and proprietary communication protocols. Refer to MindConnect® hardware to connect to MindSphere API description (https://documentation.mindsphere.io/resources/pdf/getting-connected-en.pdf) for additional details.
Interoperability and portability Virtualization	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (for example, OVF) to help ensure interoperability?	N/A	MindSphere is not an IaaS offering, so customers do not access infrastructure components directly, like virtual machines and hypervisor.
	IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	N/A	
	IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	N/A	
Mobile security Anti-malware	MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	N/A	MindSphere customers are responsible to manage mobile security devices and services used to access their data in MindSphere. Each Siemens employee receives mandatory annual information security trainings, addressing any mobile security-related topic as needed.
Mobile security Application stores	MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	N/A	
Mobile security Approved applications	MOS-03.1	Do you have a policy enforcement capability (for example, XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	N/A	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Mobile security Approved software for BYOD	MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	N/A	
Mobile security Awareness and training	MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and require-ments for mobile devices?	Yes	
Mobile security Cloud-based services	MOS-06.1	Do you have a documented list of pre-approved cloud-based services that can be used for use and storage of company business data via a mobile device?	N/A	
Mobile security Compatibility	MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application com-patibility issues?	Yes	
Mobile security Device eligibility	MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligi-bility requirements allowed for BYOD usage?	N/A	
Mobile security Device inventory	MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (for example, operating system and patch levels, lost or decom-missioned, device assignee)?	Yes	
Mobile security Device management	MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit or process com-pany data?	Yes	
Mobile security Encryption	MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technol-ogy controls for all mobile devices?	Yes	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Mobile security Jailbreaking and rooting	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (for example, jailbreaking or rooting)?	Yes	
	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?	Yes	
Mobile security Legal	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	N/A	
	MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	N/A	
Mobile security Lockout screen	MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company-owned devices?	N/A	
Mobile security Operating systems	MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	Yes	
Mobile security Passwords	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	N/A	
	MOS-16.2	Are your password policies enforced through technical controls (for example, MDM)?	N/A	
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (for example, password/PIN length) via a mobile device?	N/A	
Mobile security Policy	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	N/A	

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Mobile security Policy *(continued)*	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	N/A	
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	N/A	
Mobile security Remote wipe	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	N/A	
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Yes	
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?	Yes	
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	Yes	
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?	N/A	
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	N/A	
Security incident management, e-discovery and 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?	Yes	Siemens maintains contacts with local authorities and regulatory bodies across all jurisdictions in which it operates. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
Security incident management, e-discovery and cloud forensics Incident management	SEF-02.1	Do you have a documented security incident response plan?	Yes	The MindSphere incident response plan has been developed in alignment with ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Security incident management, e-discovery and cloud forensics Incident management *(continued)*	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	No	In case a customer is impacted by a security event, MindSphere has defined generic incident response plans and notification channels.
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you versus your tenants are responsible for during security incidents?	No	MindSphere publishes information on Security Incident Notification.
	SEF-02.4	Have you tested your security incident response plans in the last year?	Yes	Security incident response plans are continually updated and tested on a monthly basis.
Security incident management, e-discovery and cloud forensics Incident reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Yes	Siemens provides security trainings to all employees according to their roles and responsibilities. Trainings and exercises occur annually. In addition to that, MindSphere conducts regular fire drills to exercise response operation teams.
	SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory or regulatory compliance obligations?	Yes	Robust and easy-to-use procedures are implemented in MindSphere to facilitate incident reporting and management.
Security incident management, e-discovery and 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?	Yes	For the MindSphere incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes	For the MindSphere incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. Actions for troubleshooting and analyzing the root cause of an incident include the collection of evidences like log files. Siemens CERT will provide support with forensic analysis and the preservation of legally admissible forensic data if required. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Security incident management, e-discovery and cloud forensics Incident response Legal preparation *(continued)*	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?	No	MindSphere never stops collecting and analyzing data. To support potential legal action, evidence can be presented based on log data.
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes	In case a security incident involves legal action such as subpoena form, the guidelines described in the MindSphere terms and conditions (T&Cs) are followed.
Security incident management, e-discovery and cloud forensics Incident response Metrics	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Yes	Any security incident is categorized, monitored and reported according to ISO 27001 standard, Siemens Policy Framework and MindSphere incident response plan.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	No	MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Statistical data about security incidents are shared with independent auditors for certification proposes only.
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?	Yes	The MindSphere operations staff monitors data quality continuously. Any deviation is categorized, tracked and fixed according to MindSphere SDLC.
	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?	Yes	MindSphere has implemented proper trainings, controls and procedures to protect against threats throughout the supply chain lifecycle. Separation of duties, role-based access and least-privileged access are part of that. For MindSphere customers there is a set of appropriate rules to be followed. Refer to https://developer.mindsphere.io/concepts/concept-roles-scopes.html for additional details.
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 (for example, portals)?	Yes	MindSphere notifies customers of events with potential impact on security of services through an online portal. Refer to https://status.mindsphere.io/ for additional details.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
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?	Yes	MindSphere manages capacity and utilization data in alignment with ISO 27001 standard. MindSphere has been certified by an independent auditor to confirm alignment with ISO 27001 standard.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	Yes	MindSphere supports customers by providing appropriate APIs. Refer to https://developer.mindsphere.io/apis/core-usagetransparency/api-usagetransparency-overview.html for additional details.
Supply chain management, transparency and accountability Provider internal assessments	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures and supporting measures and metrics?	Yes	MindSphere adheres to Siemens Policy Framework. Regular internal audits verify the implementation of the Siemens Policy Framework. MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A for additional details. Regular surveillance audits are conducted by an independent third party.
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?	Yes	Siemens has established controls and procedures to assess and safeguard enterprise compliance in IT outsourcing and offshoring. According to that, MindSphere providers are selected and monitored regarding compliance with laws and regulations in the involved countries. Our data centers are communicated to our customers. Refer to https://developer.mindsphere.io/concepts/concept-regions.html for additional details.
	STA-05.2	Do you select and monitor outsourced providers to ensure that they follow applicable legislation?	Yes	Siemens has established controls and procedures to assess and safeguard enterprise compliance in IT outsourcing and offshoring. According to that, compliance with applicable legislation is ensured, including data protection laws.
	STA-05.3	Does legal counsel review all third-party agreements?	Yes	Siemens has established controls and procedures to assess and safeguard enterprise compliance in IT outsourcing and offshoring.
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Yes	Siemens third-party agreements always include standard contract clauses, providing security-related sections.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Supply chain management, transparency and accountability Third party agreements *(continued)*	STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes	MindSphere provides backup and recovery capabilities to help customers against unexpected data loss.
	STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes	MindSphere services are deployed in specific regions only. Refer to https://developer.mindsphere.io/concepts/concept-regions.html for additional details.
	STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?	N/A	MindSphere is not an IaaS offering but it uses the public cloud provider instead. MindSphere services and tenants are deployed in specific regions only. Refer to https://developer.mindsphere.io/concepts/concept-regions.html for additional details.
	STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	N/A	
	STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	No	
	STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes	MindSphere customer agreements describe procedures on how customers will be notified of potential breaches.
	STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	No	MindSphere customer agreements describe how MindSphere services are provisioned and monitored.
	STA-05.12	Do you provide the client with a list and copies of all sub processing agreements and keep them updated?	Yes	MindSphere provides a detailed list of sub processors on its public website. Refer to https://Siemens.mindsphere.io/en/terms for additional details.
Supply chain management, transparency and accountability Supply chain governance reviews	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	Yes	MindSphere maintains formal agreements with third-party suppliers and has implemented appropriate supplier management procedures according to ISO 27001 standard. MindSphere has been certified by an independent auditor to confirm alignment with ISO 27001 standard.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Supply chain management, transparency and accountability Supply chain metrics	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (for example, SLAs) between providers and customers (tenants)?	Yes	Siemens has established controls and procedures to assess and safeguard enterprise compliance in IT outsourcing and offshoring. MindSphere agreements with providers and customers are based on that.
	STA-07.2	Can you measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/ downstream)?	Yes	MindSphere manages supply chain quality in alignment with ISO 27001 standard. MindSphere has been certified by an independent auditor to confirm alignment with ISO 27001 standard.
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes	Services provided by third-party vendors are monitored against agreed SLAs continuously. Procedures for handling issues with vendors are established.
	STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes	Customers are informed continuously on the MindSphere web portal. Refer to https://siemens.mindsphere.io/en for additional details.
	STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Yes	The MindSphere CSA questionnaire is available for customers.
	STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes	Customers are informed continuously on the MindSphere web portal. Refer to https://status.mindsphere.io/ for additional details.
	STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes	Siemens Business Conduct Guidelines that need to be accepted by any employee upon hire provide appropriate guidance.
	STA-07.8	Do you review all service level agreements at least annually?	Yes	SLAs for MindSphere services are reviewed on a regular basis, at least annually.
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?	Yes	A once a year a review of supplier security activities is triggered and conducted.
	STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	N/A	Siemens executes annual reviews of partners/third-party providers as needed, according to Siemens controls and procedures.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Supply chain management, transparency and accountability Third party audits	STA-09.1	Do you mandate annual information security reviews and audits of your third-party providers to ensure that all agreed upon security requirements are met?	N/A	Siemens mandates annual information security reviews and audits of third-party providers as needed, according to Siemens controls and procedures.
	STA-09.2	Do you have external third-party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	No	MindSphere uses independent Siemens in-house assessors to perform penetration testing of MindSphere on a regular basis.
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 your IT infrastructure network and systems components?	Yes	MindSphere IT infrastructure is based on public cloud provider offerings, so anti-virus/malware programs for IT infrastructure are managed by cloud providers. MindSphere anti-virus/malware program is in alignment with ISO 27001 standard and protects all MindSphere services. Customers are responsible to protect their data against virus and malware.
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	Yes	
Threat and vulnerability management Vulnerability/patch management	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	MindSphere has established procedures to scan for vulnerabilities on network layer on a regular basis according to industry best practices.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	MindSphere has established procedures to scan for application layer vulnerabilities on a regular basis according to industry best practices.
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Virtual machines utilized and managed by MindSphere are built, configured and scanned for vulnerabilities according to ISO 27001 standard requirements.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	No	MindSphere has been validated and certified by an independent auditor to confirm alignment with ISO 27001 standard. Results of vulnerability scans are shared with independent auditors for certification purposes only.

MindSphere Cloud Security Alliance questionnaire

Control domain	Q ID	Consensus assessment questions	Yes / No / N/A	MindSphere response
Threat and vulnerability management Vulnerability/patch management *(continued)*	TVM-02.5	Do you have a capability to patch vulnerabilities across all your computing devices, applications and systems?	Yes	MindSphere is not an IaaS offering, so computing devices and IT infrastructures are managed by public cloud providers. MindSphere services and applications are monitored continuously and patched as needed according to ISO 27001 standard requirements. MindSphere has been certified by an independent auditor to confirm alignment with ISO 27001 standard.
	TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part of the service and/or the customer (tenant) has some shared responsibility over implementation of control?	Yes	MindSphere customers are notified of potential changes and events that may impact security or availability of the services through an online Service Dashboard (refer to https://status.mindsphere.io/) and through direct bidirectional communication as needed.
Threat and vulnerability management Mobile code	TVM-03.1	Is a 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?	N/A	MindSphere customers are responsible to manage mobile security devices, services and code used to access data in MindSphere.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	N/A	

Siemens Digital Industries Software
siemens.com/software

Americas +1 314 264 8499
Europe +44 (0) 1276 413200
Asia-Pacific +852 2230 3333

83155-C5 1/21 H