Requirements for Cloud Platforms in the Federal Administration

Version v1.0.0

Contents

Requirements for Cloud Platforms in the Federal Administration

Introduction

This document constitutes the main security requirements of the German Federal Government for cloud platforms in the German Federal Administration.

Purpose

The purpose of this document is to convey security requirements to potential cloud platform providers and to allow for *efficient identification of major obstacles* to the adaptation of the concerning cloud platforms by the Federal Administration.

Approach

The assessment of these requirements for a cloud platform follows a *risk based approach*. I.e. it is most desirable that the provided requirements are fulfilled in the described manner. However: **Appropriate alternatives may be proposed**.
These can be considered acceptable if they address the stated requirements comprehensively and lead to an overall equivalent level of security. This also applies to MUST requirements.

Definitions

The cloud: The cloud infrastructure to be evaluated for the Federal Administration including technology, documentation and description of operational processes.
The vendor: The commercial entity providing the cloud.
The federal operator: The entity operating the cloud, i.e. performing the necessary processes.

The use of MUST and SHOULD in the requirements follows RFC 2119.

Requirements

Geographical autonomy

R.german_soil The cloud MUST be located completely on German soil.
R.german_jurisdiction The cloud MUST be under German jurisdiction.

Infrastructural autonomy

R.private_cloud The cloud MUST be a private on-premises cloud.
R.federal_infrastructure The cloud MUST be in a federal infrastructure.
R.no_thirdparty_access Third parties MUST NOT have any general access to the cloud and its infrastructure.
R.physical_separation Cloud operation MUST be physically separated from third parties and the vendor.
R.no_external_connections Cloud operation MUST be possible without external data connections to third parties or the vendor.
R.only_gov_network The cloud MUST operate if solely connected to the German government network.
R.no_internet_dependency Cloud operations MUST NOT depend on connections to the internet or third-party owned systems outside of federal infrastructure (e.g. license servers or some commercial public cloud).

Operational autonomy

R.federal_operator The cloud MUST be operated by the Federal Government or its employees.

R.single_contractual_partner The federal operator MUST be the single contractual partner for customers.

R.federal_sla_responsibility The federal operator MUST be accountable and responsible in terms of service level agreements and security.

R.independent_reinit The federal operator MUST be able to autonomously re-initiate failed services.

R.no_export_regulations If export regulations influence cloud operations, on the request of the German government the vendor MUST ensure continuous operations and alignment with worldwide functionalities.

R.crisis_takeover In case of crisis and war scenarios, the vendor MUST permit and enable the German government to take over capabilities required for operating the cloud including material assets and German personnel.

Support cases

R.operational_tools The vendor MUST continuously provide the necessary tools, knowledge base and training of personnel to enable operations by the federal operator.

R.knowledge_provision Requests by the federal operator regarding the knowledge base MUST be answered by the vendor in a qualified manner with defined SLAs. Exceptions (e.g. where full disclosure is not possible) MUST be explicitly stated and explained.

R.support_permission Third parties including the vendor MAY provide knowledge and support if requested by the federal operator.

R.support_control Support MUST be controlled by the federal operator in accordance with security requirements, e. g. security clearances.

R.backup_connection_support The cloud MUST support secured backup connections controlled by the German government for emergency support and release updates.

R.secure_communication_system The cloud MUST support these connections to be established via a secure communication system chosen by the German government.

R.emergency_support For emergency support, the cloud MUST allow controlled temporary access using those connections.

Capacity and functionality

R.no_resource_limit Usage of cloud resources MUST NOT be limited by the vendor with regard to the extent, the intensity and the duration of use.

R.no_functional_limit The vendor MUST NOT be able to limit the cloud functionality by any technical means.
R.no_vendor_interference The vendor MUST NOT be able to interfere in any way with customer cloud service usage and deployment.
R.no_artificial_hardware_limit The usage of hardware resources MUST NOT be artificially limited by licensing or similar mechanisms.
R.independent_capacity_mgmt Capacity management and monitoring of resource usage MUST be solely performed by the federal operator.

Intercommunication autonomy

R.no_data_ingress_egress Third parties MUST NOT be able to extract data from or inject data into the cloud.
R.no_data_exchange The cloud SHOULD NOT exchange any data and meta data with any third parties including the vendor.
R.no_customer_data_egress Customer data MUST NOT be transferred outside the cloud without customer approval.
R.no_classified_data_egress Classified user created data MUST NEVER be exchanged (even in provider support cases).
R.client_telemetry_termination The cloud MUST be the terminating point for any telemetry data of client devices or client-side software, if those are products of the vendor.

Indispensable connections

R.data_exchange_exception_whitelisting The specification of exceptions MUST follow a whitelisting approach.
R.data_exchange_exception_minimal_amount The number of exceptions MUST be minimal.
R.data_exchange_exception_justification For each exception it MUST be evaluated, whether the data exchange is indispensably necessary for operating the cloud.
R.data_exchange_selected_metadata_egress BSI and the federal operator MAY specify metadata which MAY be transferred to the vendor.
R.data_exchange_exception_risk_analysis A risk analysis MUST be performed for each exception.
R.data_exchange_exception_security_impact Exceptions MUST NOT negatively affect security.

Data exchange exception handling

R.data_exchange_monitoring Any data exchange specified as exception MUST always be monitored, controlled and logged.

R.data_exchange_gateways Any data exchange specified as exception MUST occur via known and defined gateways.
R.data_exchange_formats Any data exchange specified as exception MUST be clearly defined in terms of a data exchange format.
R.data_exchange_hum_readable These data exchange formats MUST be human readable.
R.data_exchange_mach_readable These data exchange formats MUST be machine readable to allow automated control and review.
R.data_exchange_scrub_egress Egress data SHOULD be scrubbed and aggregated.

Billing connections

R.billing_is_exception All requirements for data exchange exceptions MUST be applied to the transfer of billing data.
R.aggregate_billing_data Billing data MUST be sanitized and aggregated with respect to restricted content before submission.

Lifecycle management

R.bugfixing Bug fixing MUST be performed by the vendor.
R.release_development Release development MUST be performed by the vendor.
R.release_testing Release testing MUST be performed by the vendor in a stage approach (test environment / public cloud). The corresponding test results MUST be provided to the federal operator as part of the release,
R.longterm_availability The vendor MUST contractually assure long term availability and maintenance of functionality at the time of purchase.
R.longterm_roadmaps The vendor MUST continuously provide long term roadmaps for expected changes of APIs and interfaces.
R.support_periods The vendor MUST assure resilient support periods in order to ensure safe and robust operations.
R.sundowns The vendor, BSI and the federal operator MUST agree on a process for announcements of sun downs (end of support) of services and acting upon possible continuation needs.
R.availability_guarantee The federal operator MUST provide a contractual statement for cloud customers which guarantees availability of crucial core functionality and interfaces for important services for a sufficiently long period of time.
R.migrationplan Before important administrative procedures (“Fachverfahren”) are deployed in the cloud, a migration plan MUST exist which can be fully realized between the announcement and the execution of the sun down of a needed service.
R.migration_timeframes The vendor MUST ensure sufficiently long time frames for these migration plans.

Update management

R.update_availability Updates MUST be made available by the vendor to the federal operator.

R.update_dmz The vendor MUST supply updates and additional data for operating the cloud to a secured network area (e.g. DMZ) managed by the federal operator.

R.update_verification Updates MUST be verifiable by the federal operator.

R.release_security_testing Releases SHOULD be subject to security investigations and tests performed by the federal operator before deployment.

R.deployment_responsibility Release deployment MUST be performed by the federal operator.

R.updates_after_reconnection After reconnection from autark operation to standard operation, the federal operator MUST be able to update the cloud to the latest release.

Update content

R.updates_include_docs Updates MUST include documentation by the vendor satisfying the needs of the federal operator.

R.release_notes_provision Release notes MUST be provided by the vendor to the federal operator prior to deployment.

R.update_threat_analysis Technical measures to analyze software prior to deployment MUST be provided by the vendor. This encompasses threats like malicious code, viruses, spyware, ransomware and addresses the cloud in terms of its services, management systems, workflows and configuration data.

R.sourcecode_insight Source code of updates MUST be available for BSI to review.

Operational security

R.federal_opsec Operational security management MUST be performed by German government personnel.

R.federal_opsec_alt Alternatively, operational security management MAY also be performed by a national IT service provider chosen by the German government.

R.vuln_reporting Detected vulnerabilites MUST be reported to the vendor.

R.vuln_mgmt Reported vulnerabilites MUST be managed and mitigated by the vendor.

Security operations center

R.soc A SOC (Security Operations Center) MUST be established for the cloud.
R.soc_federal_infrastructure The SOC MUST be in a federal infrastructure.
R.soc_german_soil The SOC MUST be located completely on German soil.

Change management

R.change_mgmt A change management process MUST be developed by the federal operator, BSI and the vendor.
R.change_mgmt_steps The change management process SHOULD include test and approval steps.
R.change_mgmt_future_changes The change management process MUST include the obligation of the vendor to inform BSI and the federal operator about future changes in a timely manner.
R.change_mgmt_sec_assessment The change management process MUST include an assessment of security relevant aspects of the changes in question.
R.change_mgmt_denial The change management process MUST include an option to deny the implementation of a change.
R.change_mgmt_denial_report If changes have not been implemented due to security concerns, the federal operator MUST report these changes including the concerns to the vendor.
R.change_mgmt_denial_reaction Upon those reports, the vendor MUST provide updated changes addressing the security concerns.
R.change_mgmt_contract The change management process MUST be contractually agreed on by the federal operator and the vendor.

Involvement of the BSI

R.support_bsig BSI MUST be able to fulfil all rights and duties of BSIG with respect to the cloud; in particular BSIG §5 and BSIG §7a.
R.no_bsig_conflicts The rights of the BSI MUST NOT be affected by contractual means.

Information provision

R.technical_doc_provision The vendor MUST provide detailed technical documentation of the cloud infrastructure, the components and the used protocols.

R.changelog_provision The vendor and the federal operator MUST ensure that BSI is comprehensively and continuously informed about changes in the cloud.

BSOC interface

R.bsi_av The cloud itself SHOULD support BSI's anti-virus signatures (ClamAV, Yara).

R.bsi_av_ext If the cloud does not support BSI's anti-virus signatures, it MUST be extensible by components providing this support.

R.prb_network_sensors Sensors MUST to be placed on every network boundary based on PR-B (external and internal).

R.prb_interfaces Required interfaces (as specified in PR-B) MUST to be available.

R.prb_mirrors It MUST be possible to redirect or mirror traffic flows.

R.prb_tls_offload The cloud MUST enable BSI to detect malware or malicious communication, also if protected with cryptographic measures (e. g. SSL-/TLS-Proxy).

R.prb_independent_logging_inf All relevant events MUST be provided to an independent logging infrastructure of BSI.

R.network_intercept_support The cloud MUST support the federal operator and BSI to capture and interpret network traffic in full detail, even if vendor-specific hardware or overlay networks are used.

R.network_segregation The communications of different government agencies (tenants) have to be segregated. All communications between tenants have to be routed either completely out of the cloudsystem or (in north/south direction) through AP combinations (A~Application Level Gateway(ALG); P~Packet filter(PF)) with Common Criteria EAL4+ Certification. East/west connections are prohibited.

R.network_segregation_rules ALG/PF communication rules are controlled by BSI (SoC). New communication channels, to or from third party networks and in between tenants have to be approved by BSI (SoC).

Normative security requirements

R.current_security_reqs The cloud MUST meet the current and applicable requirements for security of the BSI.

R.case_by_case_reqs On a case-by-case basis, the BSI MUST evaluate whether additional security requirements have to be fulfilled by the cloud, the vendor, the federal operator or any other stakeholder.

R.case_by_case_reqs_fulfil The identified additional security requirements MUST be fulfilled accordingly.

IT-Grundschutz

R.itgs The German information security standard “IT-Grundschutz” MUST be implemented in the latest version.
R.itgs_audits Regular audits of the cloud MUST be performed in accordance to BSI IT-Grundschutz.
R.itgs_module_doc BSI IT-Grundschutz module documentation for the cloud MUST be produced by the federal operator with support of the vendor.
R.itgs_module_choice The selection of modules MUST be agreed in-between BSI, the vendor and the federal operator.
R.itgs_strict All measures of the BSI IT-Grundschutz that “should” be applied MUST be applied.

VSA

R.vsa The cloud MUST meet the “General Administrative Instructions for the Physical and Organizational Protection of Classified Material” in the respective current version if processing of classified information in the cloud is expected. This includes the approval of products with information technology security functions by the BSI as stated in the VSA.
R.need_to_know_principle The “need-to-know”-principle MUST be observed.
R.id_rbac An identity based role and permission concept and access controls for handling data MUST be implemented, which are suitable to support the “need-to-know”-principle.

Minimum Standards

R.msts The applicable minimum standards published by BSI MUST be implemented.
R.mst_prb The minimum standard “Protokollierung und Detektion von Cyber-Angriffen” (PR-B) MUST be fulfilled.
R.mst_hv The minimum standard “HV Benchmark kompakt” MUST be implemented.
R.mst_tls The minimum standard “SSL/TLS Protokoll” MUST be implemented.

C5

R.c_five All offered cloud services MUST be audited at least yearly according to BSI C5.
R.c_five_reporting The corresponding C5 reports MUST be provided to BSI in a timely manner.

Datenschutz

R.gdpr The vendor's offered services MUST meet European General Data Protection Regulations.

Netze des Bundes

R.ndb If connection to the NdB is expected, the "NdB Dienstleisterpflichten" MUST be fulfilled.

Interoperability

R.migration_interoperation Migration between different providers and services MUST be supported by the cloud.
R.modular_composition System architecture SHOULD follow the paradigm of modular composition and loose coupling.
R.open_apis Open protocols and interfaces (e.g. for SaaS offerings) SHOULD be used.
R.integrate_others The cloud MUST be able to integrate cloud services offered by federal service providers.
R.integrate_self The cloud MUST support its integration into cloud services offered by federal service providers.
R.open_interfaces Vendor-independent interfaces SHOULD be used (e.g. enabling usage of proxies).
R.api_doc The vendor MUST provide detailed information about internally and externally used protocols and data formats to the federal operator and BSI.

Identifiers

german_soil, german_jurisdiction, private_cloud, federal_infrastructure, no_thirdparty_access, physical_separation, no_external_connections, only_gov_network, no_internet_dependency, federal_operator, single_contractual_partner, federal_sla_responsibility, independent_reinit, no_export_regulations, crisis_takeover, operational_tools, knowledge_provision, support_permission, support_control, backup_connection_support, secure_communication_system, emergency_support, no_resource_limit, no_functional_limit, no_vendor_interference, no_artificial_hardware_limit, independent_capacity_mgmt, no_data_ingress_egress, no_data_exchange, no_customer_data_egress, no_classified_data_egress, client_telemetry_termination, data_exchange_exception_whitelisting, data_exchange_exception_minimal_amount, data_exchange_exception_justification, data_exchange_selected_metadata_egress, data_exchange_exception_risk_analysis, data_exchange_exception_security_impact, data_exchange_monitoring, data_exchange_gateways, data_exchange_formats, data_exchange_hum_readable, data_exchange_mach_readable, data_exchange_scrub_egress, billing_is_exception, aggregate_billing_data, bugfixing, release_development, release_testing, longterm_availability, longterm_roadmaps, support_periods, sundowns, availability_guarantee, migrationplan, migration_timeframes, update_availability, update_dmz, update_verification, release_security_testing, deployment_responsibility, updates_after_reconnection, updates_include_docs, release_notes_provision, update_threat_analysis, sourcecode_insight, federal_opsec, federal_opsec_alt, vuln_reporting, vuln_mgmt, soc, soc_federal_infrastructure, soc_german_soil, change_mgmt, change_mgmt_steps, change_mgmt_future_changes, change_mgmt_sec_assessment, change_mgmt_denial, change_mgmt_denial_report, change_mgmt_denial_reaction, change_mgmt_contract, support_bsig, no_bsig_conflicts, technical_doc_provision, changelog_provision, bsi_av, bsi_av_ext, prb_network_sensors, prb_interfaces, prb_mirrors, prb_tls_offload, prb_independent_logging_inf, network_intercept_support, network_segregation, network_segregation_rules, current_security_reqs, case_by_case_reqs, case_by_case_reqs_fulfil, itgs, itgs_audits, itgs_module_doc, itgs_module_choice, itgs_strict, vsa, need_to_know_principle, id_rbac, msts, mst_prb, mst_hv, mst_tls, c_five, c_five_reporting, gdpr, ndb, migration_interoperation, modular_composition, open_apis, integrate_others, integrate_self, open_interfaces, api_doc