ORACLE

ADVISORY: ORACLE CLOUD APPLICATIONS (SAAS) AND GERMAN CRITICAL INFRASTRUCTURES (KRITIS) GUIDELINES

KRITIS guidelines defined in the "Specification of the requirements for the measures to be implemented in accordance with Section 8a Paragraph 1 BSIG"

May 2023, Version 2.1

Public

Disclaimer

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle cloud services in the context of the requirements applicable to you under KRITIS Guidelines. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document as the information in this document is not intended and may not be used as legal advice about the content, interpretation or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

KRITIS Requirements are subject to periodic changes or revisions by the German Federal Office for Information Security - BSI. The current version of KRITIS Guidelines is available here.

This document is based upon information available at the time of drafting, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

Introduction

The Federal Office for Information Security in Germany (BSI) defines Critical infrastructures (KRITIS) as "*organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences*".

Germany has defined strict regulations and guidelines for the facilities and installations part of it's critical infrastructures like the sectors of energy, information technology and telecommunications, transport and traffic, health, water, food, finance and insurance as well as municipal waste disposal.

More on KRITIS regulations can be found on the BSI official website and BBK official website.

The BSI has released "Specification of the requirements for the measures to be implemented in accordance with Section 8a Paragraph 1 BSIG" to offer operators of critical infrastructures (KRITIS operators) and auditing bodies a specification of the requirements of Section 8a Paragraph 1 BSIG. In addition, the catalogue of requirements presents the testing bodies with suitable criteria for a proper examination of the security precautions used in order to be able to provide the required evidence in accordance with Section 8a Paragraph 3 BSIG.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Applications (SaaS) to assist you in determining the suitability of using SAAS Applications in relation to KRITIS Guidelines.

The Oracle products in scope of this document are:

- Oracle Fusion Cloud Services:
    - Human Capital Management (HCM)
    - Supply Chain Management and Manufacturing (SCM)
    - Enterprise Resource Planning (ERP)
    - Oracle Sales Cloud (CX Sales)
- Enterprise Performance Management (EPM)
- Eloqua (CX Marketing)
- European Union Restricted Access (EURA) for Fusion (HCM, SCM, ERP) and EPM.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle in regard to their specific legal and regulatory requirements.

About Oracle Cloud Applications

Oracle Cloud Applications (SaaS) is the world's most complete, connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to the success of your organization with continuous updates and innovations across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information about Oracle Cloud Applications, see https://oracle.com/applications.

Table of contents

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud environments. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), and customers are responsible for securely configuring and using their cloud resources. For more information, you should refer to your cloud service documentation.

The following figure illustrates this division of responsibility at high level.

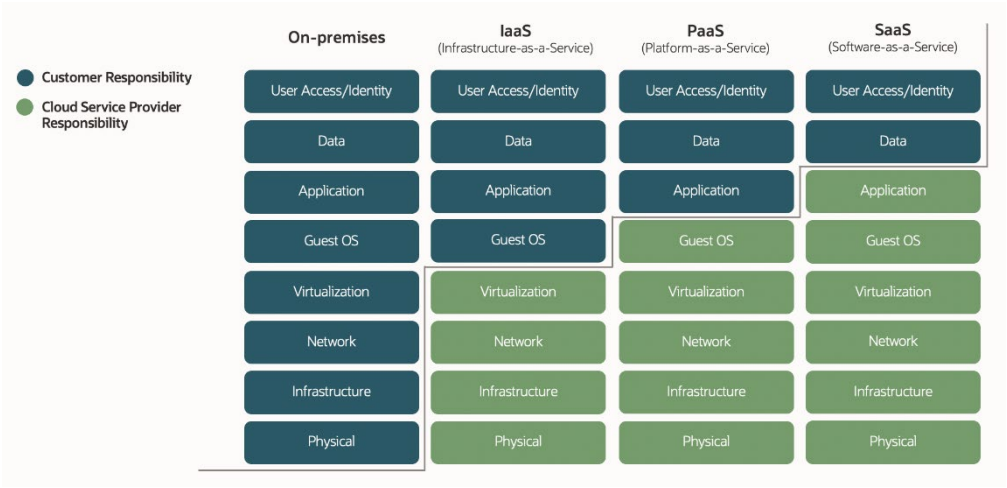

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Critical Infrastructure – KRITIS - Regulated by the German Federal Office for Information Security- BSI

It is the KRITIS Operator's responsibility to take the necessary measure to avoid any disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes in order to maintain the operability of the Critical infrastructures.

KRITIS Operators could use cloud services from cloud service providers, but the KRITIS Operator is the one that decides which processes or critical services and other supply services, may be implemented with cloud services. The KRITIS Operator can use the cloud services only for supporting, non-critical processes.

The KRITIS Operators responsibility for the availability of the critical services they provide cannot be passed to the cloud service provider. The KRITIS Operator is responsible to ensure the availability of the critical services they are providing.

Any operation or compliance risks, legal obligations are also the responsibility of the KRITIS Operator, and they should not transfer it to the cloud service provider when outsourcing cloud services.

The BSI Section 8a Paragraph 1 BSIG requirements are based on the "Catalogue of Requirements for Cloud Computing (C5)". The BSI has adapted the C5 controls to be specific to KRITIS Operators. The C5 original control ID & Names were kept for easy comparison.

Oracle has developed this document as a part of its continuing efforts to help KRITIS Operators meet their unique obligations under the German "Section 8a Paragraph 1 BSIG requirements".

We want to make it easier for you as a KRITIS Operators to identify the controls Oracle has implemented that pertain to the requirements in Section 8a Paragraph 1 BSIG requirements for KRITIS Operators.

In this document, you will find a list of relevant Information Security Requirements for KRITIS Operators, along with a short description of the relevant controls implemented by the Oracle Cloud Applications (SaaS). For further guidance, please read this document in conjunction with Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen (bund.de).

For more information on other German cloud regulations please visit https://www.oracle.com/cloud/compliance/

The mapping has been done to show the relevant Oracle practices in place for the systems Oracle manages, the customers still have significant responsibilities in these areas.

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
2.1 Information Security Management System (ISMS)	1. OIS-01 - Information security management system 2. OIS-02 - Strategic requirements for information security and responsibility of the company management 3. OIS-03 - Competences and responsibilities in the context of information security 4. OIS-04 - Segregation of duties	Oracle has established, implemented and is maintaining and continually improving an information security management system (ISMS) in accordance with the requirements of ISO/IEC 27000 series. Oracle's Corporate Security programs are designed to protect Oracle and customer information assets, such as: • The mission-critical systems that customers rely upon for cloud, technical support and other services • Oracle source code and other sensitive data against theft and malicious alteration • Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data in Oracle's systems More details: https://www.oracle.com/corporate/cloud-compliance/
2.2 Asset Management	5. AM-01 - Asset inventory 6. AM-02 - Assignment of asset owners	Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems,

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
	7. AM-03 - Asset Usage Instructions 8. AM-04 - Delivery and return of assets 9. AM-05 - Classification of information 10. AM-06 – Labelling of information and handling of assets 11. AM-07 - Management of data carriers 12. AM-08 - Transfer and Removal of Assets	hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services. Oracle's formal Information Protection Policy provides guidelines for all Oracle personnel and business partners regarding information classification schemes and minimum handling requirements associated with those classifications. Oracle categorizes information into four classes 'Public, Internal, Restricted, and Highly Restricted' with each classification requiring corresponding levels of security controls, such as encryption requirements for data classified as Restricted or Highly Restricted. More details: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
2.3 Risk Analysis Method	13. OIS-06 - Guideline for the organization of risk management 14. OIS-07 - Identification, analysis, assessment, and impact assessment of IT risks 15. BCM-02 - Impact Assessment Guidelines 16. B3S - Derivation of measures	Global Information Security (GIS) defines policies for the management of information security across Oracle.GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle by means of: • Leading development and review of information security policies Providing global oversight of information security risk management • Managing and overseeing security assessment programs, including security testing and penetration testing • Directing information security incident management and response. Oracle Global Physical Security uses a risk-based approach to physical and environmental security to effectively balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) to plan for and response to potential business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability across lines of business and geographies. It authorizes a centralized Program Management Office (PMO) to manage a global Risk Management Resiliency Program (RMRP) which oversees LOB plans and preparedness, in alignment with ISO 22301 international standard for business continuity management and defines the compliance oversight responsibilities for the program. Critical LOBs are required to conduct an annual review of their business continuity plans with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes and technology. More details: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
2.4 Continuity Management	17. BCM-01 - Responsibility of the legal representatives of the operator of the critical infrastructure 18. BCM-03 - Business continuity planning 19. BCM-04 - Business continuity verification, update and testing	Oracle's Risk Management Resiliency Policy defines requirements for all Oracle Lines of Business (LOBs) to plan for and respond to potential business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability across LOBs and geographies. It authorizes a centralized Program Management Office (PMO) to manage a global Risk Management Resiliency Program (RMRP) which oversees LOB plans and preparedness, in alignment with ISO 22301 international standard for business continuity management. More details: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
2.5 Technical Information Security	20. RB-01 & RB-02 - Necessary/sufficient human and IT resources (operation and IT security)	Human Resource - Oracle has a Resource Management process that involves the planning, scheduling and future allocation of resources to the right project at the right time and cost including optimal Utilization of Resources and also accurate forecasting. Resource Management aims to find a balance between maximizing the productivity of your available resources while avoiding over-utilization, Avoid Unforeseen Challenges & Conflicts. Improve Project Delivery, Transparency.

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
	21. RB-05 - Protection against malicious programs	Oracle policy requires the use of antivirus, intrusion protection and firewall software on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization. Antivirus software must be scheduled to perform daily threat definition updates and virus scans.
	22. RB-06 & RB-09 - Data backup and recovery 23. RB-07 - Data backup and recovery - monitoring 24. RB-08 - Data backup and recovery - regular testing	Disaster recovery is a key sub-program of Oracle Risk Management Resiliency Program (RMRP). To understand resilience, business continuity, and disaster recovery practices for cloud services, please see Oracle Cloud Hosting and Delivery Policies. Oracle Lines of Business (LOBs) are required to maintain and test their Disaster Recovery (DR) plans, including backup and recovery strategies, as part of their business continuity efforts. More details: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html
	25. RB-22 - Dealing with vulnerabilities, malfunctions, and errors - system hardening	Oracle products and services are required to be secure by default. Products and services should only install the essential components to perform their intended functions. Any features not intended for a production deployment, such as demonstration content, default accounts and debug tools, should not be installed by default. This is commonly referred to a minimizing the attack surface. By default, the product or service should only use secure protocols and algorithms. More details: https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html
	26. IDM-07 - Confidentiality of Authentication Information 27. IDM-08 - Secure login procedures 28. IDM-10 - System access control 29. IDM11 - Password Requirements and Validation Parameters 30. IDM 12 - Restriction and control of administrative software	The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. This policy does not apply to publicly accessible, internet-facing Oracle systems or end users. **User Access Management** Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. **Privilege Management** Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: - Need to know: Does the user require this access for his job function? - Segregation of duties: Will the access result in a conflict of interest? - Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? **User Password Management** Oracle enforces strong password policies for the Oracle network, operating system, and database accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. When Oracle compliance organizations determine that a password is not in compliance with strong password standards, they work with the applicable employee and line of business to bring the password into compliance with the standards. **Periodic Review of Access Rights** Oracle regularly reviews network and operating system accounts regarding the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
		Password Policy The use of passwords is addressed in the Oracle Password Policy. Oracle employees are obligated to follow rules for password length and complexity, and to keep their passwords confidential and secured at all times. Passwords may not be disclosed to unauthorized persons. Under certain circumstances, authorized Oracle employees may share passwords for the purpose of providing support services. **Network access controls** Oracle has implemented and maintained strong network controls to address the protection and control of customer data during its transmission from one end system to another. The Oracle Use of Network Services Policy states that computers, servers, and other data devices connected to the Oracle network must comply with well-established standards for security, configuration, and access method. More details: https://www.oracle.com/contracts/cloud-services/ https://www.oracle.com/corporate/security-practices/corporate/access-control.html
	31. IDM-13 - Access control to source code	Oracle maintains strong security controls over its source code. Oracle's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories. Oracle's objectives with protecting its source code are twofold: 1. Protect the company's intellectual property while fostering innovation 2. Protect Oracle and its customers against malicious attempts to alter Oracle's source code or exploit security vulnerabilities More details: https://www.oracle.com/corporate/security-practices/assurance/source-code-protection/
	32. KRY-01 - Policy on the use of encryption methods and key management 33. KRY-02 - Encryption of data during transmission (transport encryption) 34. KRY-03 - Encryption of sensitive data at rest 35. KRY-04 - Secure key management	Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. Oracle's corporate security technical controls, includes secure configurations and encryption for data at rest and in transit. Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle defines requirements for encryption, including, cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: - Locations and technologies for storing encryption keys - Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures - Changing default encryption keys - Replacement schedule for various types of encryption keys
	36. KOS-01 - Technical protective measures 37. KOS-02 - Monitor Connections	Oracle's network protections include solutions designed to provide continuity of service, defending against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Events are analysed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Oracle reviews logs for forensic purposes and incidents and identified anomalous activities feed into the security-incident management process. Access to security

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
		logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.
	38. KOS-03 - Cross-network access 39. KOS-04 - Networks for administration 40. KOS-06 - Documentation of the network topology 41. KOS-07 - Data Transfer Policies	Not applicable for SaaS
	42. KOS-08 - Confidentiality Agreement	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
	43. AT-01 - Guidelines for developing/procuring information systems	To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal Secure Coding Standards, Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc., and provide specific guidance on topics such as data validation, Common Gateway Interface, and user management, and more. All Oracle developers must be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal product assessment team. Oracle provides that developers are familiar with its coding standards The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed and validated throughout the supported life of all Oracle products. More details: https://www.oracle.com/corporate/security-practices/assurance/development/
	44. AT-02 - Outsourcing development	Oracle requires security reviews for any third-party components embedded in Oracle products and cloud services. The development teams must use current and actively maintained versions of third-party software. Teams must verify that third-party components are free of publicly reported vulnerabilities at the time of their inclusion in an Oracle product distribution or use by a cloud service. They must also verify that there is active maintenance for any third-party component selected and must confirm that component maintenance (either by the component source, by a fourth party, or by Oracle) extends throughout the support life of the embedding product. Development teams are required to compile binaries for third party open-source components from source code. This ensures that the binaries used in Oracle products derive from known source code, which improves Oracle's ability to support that code if needed and reduces the risk of malicious functionality being embedded in third party binaries. More details: https://www.oracle.com/corporate/security-practices/assurance/development/third-party-software.html
	45. AT-03 - Policies for changing information systems 46. AT-04 - Risk assessment of the changes	Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software that is provided by Oracle as part of the Oracle Cloud Services, to maintain operational stability, availability, security, performance, and currency of the Oracle Cloud Services. Oracle follows formal change management procedures to review, test, and approve changes prior to application in the production service.

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
	47. AT-05 - Categorization of changes 48. AT-06 - Prioritization of changes 49. AT-07 - Testing the changes 50. AT-08 - Roll back changes 51. AT-09 - Verify proper test execution and approval 52. AT-10 - Emergency changes 53. AT-11 - System environment 54. AT-12 - Segregation of duties	Changes to infrastructure configurations and services supporting the System are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with the change management requirements. The mandatory fields require a description of: - The nature of the proposed change - The impacted systems (direct and indirect) - The impact of the change - Required updates to system documentation after the change - The test plan(s) - The internal and external notification plan (if necessary) - The rollback plans - The post-implementation verification process - The workflow prevents the ticket from being moved into the scheduled or implementation phase without the required review and approval of child tickets being in the closed state. Changes to infrastructure configurations and services supporting the System must be peer reviewed prior to implementation. A member of the same team with knowledge of the impacted service, who can technically review the Change for accuracy and potential issues, typically acts as the reviewer. Changes to infrastructure configurations and services supporting the System must be tested prior to implementation. The type of test is dependent on the nature of the change but may include unit, regression, manual, and/or integration tests. The development and testing environment is separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. Emergency changes to infrastructure configurations and services supporting the System require approval of a Senior Manager or above. Code changes are implemented through Continuous Integration/Continuous Deployment (CICD) tools. Except where dependencies exist across multiple availability domains (e.g., updates to domain name services), changes are implemented separately in each region and availability domain. CSSAP is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with: • Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template • CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review • Security assessment review: based on risk level, systems and applications undergo security verification testing before production use CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with: • Oracle Corporate Security Architecture strategy and direction • Oracle Corporate security, privacy and legal policies, procedures and standards More details: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html Oracle Cloud Hosting and Delivery Policies Section 4 - Oracle Cloud Hosting and Delivery Policies
	55. MDM-01 - Policies and procedures for minimizing the risk of access via	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile device operating systems and platforms. OIT and corporate security

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
	mobile devices of the KRITIS operator	organizations regularly promote awareness of mobile device security and good practice. More details: https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
2.6 Personal and organizational security	56. HR-01 - Recruitment and Security Check 57. HR-02 - Recruitment and Employment Agreements	In the United States, Oracle uses an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Personnel screening in other countries varies according to local laws, employment regulations, and local Oracle policy. More details: https://www.oracle.com/careers/background-check/
	58. IDM-01 - Role allocation and dual control principle or separation of functions 59. IDM-02 - Identity and Permissions Management - User Registration 60. IDM-03 - Identity and Authorization Management - Access Authorization 61. IDM-04 - Allocation and modification (provisioning) of access authorizations 62. IDM-05 - Identity and Permissions Management - Reviews 63. IDM-06 - Identity and Permissions Management - Administrators 64. IDM-09 - Identity and Permissions Management - Emergency Users	See 2.5 Technical Information Security - 26. IDM-07 - Confidentiality of Authentication Information
	65. SA-01 - Determination of necessary competencies (operation and IT security) 66. SA-02 - Review and approval of policies and instructions 67. SA-03 - Deviations from existing guidelines and instructions	Oracle's Corporate Security Program is designed to Oracle and customer information assets, such as: - The mission-critical systems that customers rely upon for Cloud, technical support and other services - Oracle source code and other sensitive data against theft and malicious alteration - Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data residing in Oracle's internal IT systems.
	68. HR-03 - Training and awareness	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. More details: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
	69. HR-04 - Disciplinary proceedings 70. HR-05 - Termination of employment	Employees who fail to comply with Oracle policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
2.7 Structural/Physical Security	71. BCM-05 - Data center supply	See section 2.7 –Structure/Physical Security. PS-04. More details: https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
	72. PS-01 - Perimeter protection 73. PS-02 - Physical access protection 74. PS-03 - Protection against external threats 75. PS-04 - Protection against disruptions caused by power outages and other such risks	Oracle Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. Oracle has implemented the following protocols: Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle. Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination. Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations. Oracle use a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability. The access logs are kept for a minimum of six months. Furthermore, the retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level. Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation that considers environmental threats, power availability and stability, vendor reputation and history, neighbouring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. More details: https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
	76. PS-05 - Infrastructure maintenance	For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization, and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measure standards defined by Global Physical Security (GPS). Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use virtual private networks (VPN) that have been approved via the Corporate Security Solution Assurance Process (CSSAP). Access to the Oracle corporate network by suppliers and third parties is subject to limitations and prior approval per Oracle's Third-Party Network Access Policy. For Decommissioning Servers and Other Computing Resources. Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
		longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media include laptops, hard drives, storage devices, and removable media such as tape. More details: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html https://www.oracle.com/corporate/security-practices/corporate/data-protection/
2.8 Incident Detection and Handling	77.SIM-01 - Responsibilities and process model 78. SIM-03 - Processing of security incidents 79. SIM-04 - Documentation and reporting of security incidents 80. SIM-05 - Security Incident Event Management 81. SIM-06 - Obligation of users to report security incidents to a central office 82. SIM-07 - Evaluation and learning process	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets. In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not shared externally. More details: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
2.9 Operations	83. RB-17 - Event-related tests - concept 84. RB-21 - Dealing with vulnerabilities, disruptions and errors - checking open vulnerabilities	The Oracle Critical Patch Update (CPU) and Security Alert Implementation Policy require the deployment of the Oracle CPU and Security Alert patches as well as associated recommendations within a reasonable time of their release. Additional policies require remediation of vulnerabilities in non-Oracle technology. The Oracle Server Security Policy requires servers (both physical and virtual) owned and managed by Oracle and servers managed by third parties for Oracle to be physically and logically secured in order to prevent unauthorized access to the servers and associated information assets. More details: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
	85. SPN-01 - Informing the management 86. SPN-02 - Internal reviews of compliance of IT processes with internal information security policies and standards 87. SPN-03 - Tests in other, otherwise specified test cycles - internal IT tests	Not Applicable, customer responsibility
	88. COM-02 - Tests in other, otherwise specified test cycles - planning of external audits 89. COM-03 - Tests in other, otherwise specified test cycles - implementation of external audits	Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews identified risks or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors. More details: https://www.oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/
	90. RB-10 - Systematic log evaluation - concept	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log

CATEGORY NO & NAME	REQUIREMENT	RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES
	91. RB-12 - Systematic log evaluation - critical assets 92. RB-13 - Systematic log evaluation - storage 93. RB-15 - Systematic log evaluation - configuration 94. RB-16 - Systematic log evaluation - availability 95. RB-18 - Penetration test 96. RB-19 - Dealing with vulnerabilities, disruptions and errors - integration with change and incident management	file media becoming exhausted, failing to record events, and/or logs being overwritten. Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible. Oracle maintains teams of specialized security professionals for the purpose of assessing the security strength of the company's infrastructure, products, and services. Oracle IT organizations are responsible for security scanning of the Oracle corporate systems and Cloud services they manage, per Oracle's Server Security Policy and associated technology standards. Oracle requires that external facing systems and cloud services undergo penetration testing performed by independent security teams. Oracle has formal monitoring requirements for security events and incidents. Alerts are sent to the relevant IT security and cloud security operations teams for review. Oracle requires that these alerts be monitored within the Lines of Business 24x7x365. More details: https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html https://www.oracle.com/corporate/security-practices/assurance/development/ethical-hacking.htmlhttps://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
2.10 External information supply and support	97. OIS-05 - Contact to relevant authorities and interest groups	Not Applicable, customer responsibility
2.11 Suppliers, Service Providers and Third Parties	98. DLL-01 - Guidelines for handling and security Requirements for service providers of the KRITIS operator 99. DLL-02 - Control of the provision of services and the security requirements for service providers and suppliers of the KRITIS operator	Not Applicable, customer responsibility
2.12 Reporting	100. Establishment of a contact point	Not Applicable, customer responsibility

Conclusion

Organizations operating in the Critical Infrastructure sectors in Germany face stringent regulatory requirements to ensure that no disruptions occur. KRITIS Operators are responsible to make sure there is no failure or impairment that would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences.

KRITIS Operators can take advantage of cloud computing technology, especially SaaS services.

By using SaaS, a KRITIS operator can add new capabilities and applications quickly without a major up-front investment in, infrastructure and IT staff, to set up and deploy the applications and supporting hardware themselves.

SaaS provides numerous advantages to companies by greatly reducing the resources required to install, manage, and upgrade software. SaaS also lets application users access applications and data from anywhere.

KRITIS Operators could use cloud services from cloud service providers but it's the KRITIS Operator's responsibility to decide which processes or critical services and other supply services may be implemented with cloud services or whether only supporting, non-critical processes may use the cloud services.

The responsibility for the availability of the critical services provided remains with the KRITIS operator, these are not to be passed to the cloud service provider.

The Security controls that support The Oracle Cloud Applications (SaaS) in scope of this advisory have been attested against the C5 criteria by an independent third-party.

More details: https://www.oracle.com/corporate/cloud-compliance/

Oracle has developed this advisory to help KRITIS Operators meet their unique obligations under the German "Section 8a Paragraph 1 BSIG requirements".

The advisory list the controls that could apply to Oracle Cloud Applications (SaaS) and gives short descriptions on the controls Oracle has implemented that pertain to the requirements in Section 8a Paragraph 1 BSIG requirements for KRITIS Operators.

Customers are solely responsible for determining the suitability of a cloud service in the context of KRITIS. The information in the report compiled by Oracle is provided to aid KRITIS operators in their evaluation of Oracle Cloud Applications.

Please reach out to your Sales Representative and/or Account Manager to request access to the C5 attestation report. To learn more of our compliance activities, check out the Compliance page on our website and Compliance Considerations for Cloud Services blogpost.