<table>
<thead>
<tr>
<th>Control Domains</th>
<th>Control ID</th>
<th>Question ID</th>
<th>Control Specification</th>
<th>Consensus Assessment Questions</th>
<th>Consensus Assessment Answers</th>
<th>Note(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network &amp; Web Application Security Controls</td>
<td>G1 - 04.1</td>
<td>G1 - 04.1</td>
<td>Source code analysis is done annually</td>
<td>Does your organization have a plan or framework for business continuity management or disaster recovery management?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Information System Planning &amp; Control</td>
<td>G1 - 02.6</td>
<td>G1 - 02.6</td>
<td>Defined lines of communication, roles, and responsibilities</td>
<td>Are the results of internal and external audits available to tenants at their request?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Information System Planning &amp; Control</td>
<td>G1 - 02.3</td>
<td>G1 - 02.3</td>
<td>Business continuity planning and management is established, documented, and adopted to ensure all business processes are reflected.</td>
<td>Does your audit program take into account effectiveness of implementation of security operations?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Data Input &amp; Output Integrity Checks</td>
<td>G1 - 01.1</td>
<td>G1 - 01.1</td>
<td>Data input and output integrity checks (i.e., reconciliation and edits)</td>
<td>Do you have a program in place that includes ability to monitor changes to the regulatory requirements in real-time?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Information System Planning &amp; Control</td>
<td>G1 - 00.2</td>
<td>G1 - 00.2</td>
<td>Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses noncompliance issues.</td>
<td>Does your organization have a plan or framework for business continuity management or disaster recovery management?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Information System Planning &amp; Control</td>
<td>G1 - 00.1</td>
<td>G1 - 00.1</td>
<td>Track data shall be developed and maintained to assess system source code analysis. Auditing data shall focus on assessing the effectiveness and implementation of the organization's security operations.</td>
<td>Does your organization have a plan or framework for business continuity management or disaster recovery management?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Information System Planning &amp; Control</td>
<td>G1 - 00.1</td>
<td>G1 - 00.1</td>
<td>Independent reviews and assessments of the organization's security operations and corporate governance should be performed at least annually.</td>
<td>Does your organization have a plan or framework for business continuity management or disaster recovery management?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Information System Planning &amp; Control</td>
<td>G1 - 00.1</td>
<td>G1 - 00.1</td>
<td>Independent reviews and assessments of the organization's security operations and corporate governance should be performed at least annually.</td>
<td>Does your organization have a plan or framework for business continuity management or disaster recovery management?</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Determine and implement a business continuity plan in line with ISO27001 directives. Wolters Kluwer Italia is obliged to respect this Policy.

Do you have a formal Disaster Recovery Plan? 2

A disaster recovery plan is implemented and monitored. Wolters Kluwer Italia is in compliance with ISO27001 standards.

Do you consider equipment and infrastructure redundancy and monitoring processes? 2

A disaster recovery plan is implemented and monitored. Wolters Kluwer Italia is in compliance with ISO27001 standards.

Do you provide a disaster recovery capability? 2

An agreement with SLAs (Service Level Agreements) to customers.

Do you share your business continuity and redundancy plans with your tenants? 2

The locations where the data centers are placed are far from 90% earthquakes.

Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks? (fires, tornados, earthquakes, hurricanes, etc.)? 2

No. The baseline where the data centers are placed have a low environmental risk.

Does your organization maintain a list of critical products and services that require operational resilience or who have operational resilience requirements, that are required by local or national regulations, and/or whose failure would cause significant losses or significant impact on the business? 2

No, not applicable to IT services.

Are you aware of your organization’s risk profile and have you carried out a risk assessment? 2

Are you aware of your organization’s risk profile and have you carried out a risk assessment? 2

Are you aware of your organization’s risk profile and have you carried out a risk assessment? 2

Is physical damage anticipated and are countermeasures included in the design of physical protection? 2

Do you have a defined and documented method for determining the impact of any disaster to your organization’s critical assets? 2

The locations where the data centers are placed are far from 90% earthquakes.

Do you have a defined and documented method for determining the impact of any disaster to your organization’s critical assets? 2

The locations where the data centers are placed are far from 90% earthquakes.

Is physical damage anticipated and are countermeasures included in the design of physical protection? 2

Do you have a defined and documented method for determining the impact of any disaster to your organization’s critical assets? 2

The locations where the data centers are placed are far from 90% earthquakes.

Do you have a defined and documented method for determining the impact of any disaster to your organization’s critical assets? 2

The locations where the data centers are placed are far from 90% earthquakes.
Yes, we have policies that define SW in Blacklist and we use CCC-01.1

Confidential company documents are shared only on demand.

The connection to SAAS service are available in transit via HTTPS.

The data stored in the data centres where the service is provided.

Lifecycle

Information

Data Security & Information

Management

Data Inventory / Management

Production Changes

Configuration

New Development / Management

Change Control & Retention Policy

Management & Business Continuity

BCR-11

CCC-04

CCC-03

CCC-05.3

CCC-05.2

CCC-03.5

CCC-03.1

CCC-02.2

CCC-02.1

DSI-04.2

DSI-03.2

DSI-02.2

DSI-02.1

aggregate containers for data.

the security of data and objects which contain data. Mechanisms for policies and procedures shall be established for labeling, handling, and aggregate containers for data.

Policies and procedures shall be established for managing the risks associated with applying changes to:

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to review the impact or remediation the issue before the change is released.

Technical measures shall be implemented to provide assurance that changes will not introduce vulnerabilities or functionality issues.

Processes and technical measures implemented, to inventory, analyze, and monitor the logs events

WK - Data Classification and Handling GBS-STD-1202.pdf

ISO Standards and in compliance with GDPR.

information into 4 clusters, and defines the marking, based on

cannot be migrated to other states than Italy.

customer indicate that data are stored in the Italian data centre.

WK - Asset Management GBS-STD-1201

WK - Asset Management GBS-STD-1203a.pdf

WK - Information Security Standards for WK Suppliers-STD-1203a.pdf”

Partner and Suppliers meet contractual requirements in order to

monitoring the logs events.

Do you have a defined quality change control and change processes and their roles/rights/responsibilities within it?

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have controls in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in accordance for effectiveness.

Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and

Do you have controls in place to detect or rule out any defects for new and existing software development activities?
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?</td>
<td>Yes</td>
</tr>
<tr>
<td>Do you restrict physical access to information assets and functions by users and support personnel?</td>
<td>Yes</td>
</tr>
<tr>
<td>Do you maintain key management procedures?</td>
<td>Yes</td>
</tr>
<tr>
<td>Do you have a capability to allow creation of unique encryption keys per tenant?</td>
<td>Yes</td>
</tr>
<tr>
<td>Can you provide tenants with your asset management policies and procedures?</td>
<td>Yes</td>
</tr>
<tr>
<td>Can you provide evidence that policies, standards, and procedures have been established to maintain risk and asset management for all areas housing sensitive data and information systems?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are you able to validate connection authentication integrity based on known connection authentication?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, prevented, controlled and isolated from data storage and process?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are you able to maintain and update asset control mechanisms to ensure that only authorized personnel are allowed access?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are access controls, security controls, or application control mechanisms in place to ensure compliance with security policies, standards, and procedures?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are you able to maintain adequate asset classification and handling mechanisms for all assets containing information that is critical, sensitive, or private?</td>
<td>Yes</td>
</tr>
<tr>
<td>Does your organization have a documented plan for the management of data classification and handling?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Yes, Virtual Machine Images are encrypted at-rest. Measures and controls are in place to keep the infrastructure in a secure state. All documentation relating to security policies and procedures is protected and kept secure. The RA framework considers the processing of data through encryption and secure data transmission. Encryption protocols for protection of sensitive data in storage (e.g., data at-rest) are adopted. Policies and procedures shall be established, and supporting business and technical standards are adopted in the configuration of applications and infrastructure system and network components that are relevant to their area of responsibility.

Do your information security management programs include the following: encryption, key management, key usage and key distribution, and standards that are relevant to their area of responsibility?

Are your information security policies and procedures made available to all impacted personnel and business partners, and/or contractors, and are they readily accessible? Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you have separate key management and key usage duties?

Do you have separate encryption keys to thecrawl? Do you have separate encryption keys to the cloud server or a trusted key management provider?

Do you have separate encryption keys to the cloud server or a trusted key management provider?

Do you have clear definitions of responsibilities associated with data governance requirements?

Does the organization’s IT governance framework outline the following: a statement, strategy, policies, and standards that are relevant to their area of responsibility?

Do your information security management programs include the following: encryption, key management, key usage and key distribution, and standards that are relevant to their area of responsibility?

Do you have clear definitions of responsibilities associated with data governance requirements?

Are you leveraged encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?

Are you leveraging encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?

Do you encrypt data, databases, and end-user workstations) and data in storage (e.g., data at-rest) with encryption protocols for protection of sensitive data in storage (e.g., data at-rest) are adopted. Policies and procedures shall be established, and supporting business and technical standards are adopted in the configuration of applications and infrastructure system and network components that are relevant to their area of responsibility.

Do you have separate key management and key usage duties?

Do you have separate encryption keys to the cloud server or a trusted key management provider?

Do you have separate encryption keys to the cloud server or a trusted key management provider?

Do you have clear definitions of responsibilities associated with data governance requirements?

Do your information security management programs include the following: encryption, key management, key usage and key distribution, and standards that are relevant to their area of responsibility?

Do you have clear definitions of responsibilities associated with data governance requirements?

Do you have separate key management and key usage duties?

Do you have separate encryption keys to the cloud server or a trusted key management provider?

Do you have separate encryption keys to the cloud server or a trusted key management provider?

Do you have clear definitions of responsibilities associated with data governance requirements?

Do your information security management programs include the following: encryption, key management, key usage and key distribution, and standards that are relevant to their area of responsibility?

Do you have clear definitions of responsibilities associated with data governance requirements?

Do you have separate key management and key usage duties?
The Risk Assessments is performed on a standard framework.

A dedicated Department manages this scope.

Annual risk assessments aligned with the reactive risk framework and protection of data security, and planned actions, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods.

The list of assessments is performed at least annually.

Non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities).

Workforce personnel user access to corporate facilities, resources, and assets shall be managed. When an employee changes jobs or leaves the company, appropriate review or termination actions are taken.

Requirements for non-disclosure or confidentiality agreements regarding data protection and operational details for data in process (e.g., payment or healthcare), as identified, documented, and reviewed at least annually.

In case the transfer must take place according to specific rules, policies, procedures, questionnaires and evaluations carried out during background checks are performed by normal recruitment procedures, questionnaires and evaluations carried out during background checks, appropriate review or termination actions are taken.

The list of assessments of business associates shall be performed at least annually.

The Risk Assessments are performed at least annually or at planned intervals, (and in all likelihood and impact of all identified risks, using qualitative and quantitative methods.

Monthly risk assessments are performed at least annually.

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?

Do you have asset return procedures outlining how assets should be returned within an established period?

Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant obligations for returning organizationally-owned assets?

Do the above procedures and guidelines account for timely revocation of access and return of assets?

Do you have an acceptable use policy for personal devices and are they reviewed at least once a year?

Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?

Do all employees receive updates to security policies, procedures, standards, and controls that ensure they remain relevant and effective?

Do you document employee acknowledgment of training they have completed?

Do you provide a formal, role-based, security awareness training program for cloud-related access and data management

Do you train and manage your security awareness training program by a security awareness program manager?

Do you perform, at minimum, annual reviews to security policies?

Do you document security policies, procedures, standards, and controls that ensure they remain relevant and effective?

Do you document security policies, procedures, standards, and controls that ensure they remain relevant and effective?

Do you document that the department responsible for security is aware of and has access to all the policies and procedures?

Do you document that the department responsible for security is aware of and has access to all the policies and procedures?

Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?

Do you document that the department responsible for security is aware of and has access to all the policies and procedures?

Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?

Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?

Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?

Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?
Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?

De-identification, encryption, and other security tools shall be made available to ensure that de-identification efforts do not change identity, or result in unauthorized access.

Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?

The agreement is executed annually and is subject to termination upon a sixty (60) day written notice. Termination of this Agreement may not be unilaterally terminated by either party without cause. Upon termination of this Agreement, the customer shall cease all use of the Services and return allEquipment and any other property delivered under this Agreement.

Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?

Do you have policies, procedures and technical measures in place to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) personal identifiers?

Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?

Do you have policies and procedures to ensure that equipment is secured and not left unattended when not in use?

Are you aware of all personnel (e.g., employees, contractors, visitors) who have access to the IT environment?

Are you aware of all personnel (e.g., employees, contractors, visitors) who have access to the IT environment?
Periodic checks are carried out on the authorisations granted to users.

All changes to user permissions are recorded, and if necessary, the authorisations are reviewed.

Enforcement Point Policy features are not integrated in our environment.

User ID Credentials Management

User Access Management

Authorization Management

Identity & Access Management

Authentication, authorization, and accounting (AAA) rules (e.g., account credential and/or identity store minimization or re-use and revocation) are in place. Information processing interoperability (e.g., SSO and Federation) is used to enhance security. Entitlement, and access management and in accordance with established policies and procedures and based on rules of least privilege and replication limitation for users and service delivery boundary.

User access shall be authorized and revalidated for entitlement and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation.

Policies and procedures are established for permissible storage and distribution of data (tenants), business partners and/or suppliers (e.g. employees, contractors, customers, business partners, and/or suppliers) to data and any owned or managed physical and virtual applications, infrastructure systems, and network components. The organization shall implement controls to limit identity replication. Prevent and detect data breaches. Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to data?

Do you support the ability to force password changes upon first logon?

Do you allow tenants/customers to define password and account lockout policies for their accounts?

Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user authenticating/authorizing users?

Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based access control and entitlement management by the business?

Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?

Do you use open standards to delegate authentication capabilities to your tenants?

Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?

Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?

Do you provide third-party identity and access services?

Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based access control and entitlement management by the business?

Are preventive, detective, and corrective compensating controls in place to mitigate the impacts of unauthorized or inappropriate access?

Does your organization conduct third-party unauthorized access risk assessments?

Do you limit identities' replication only to users explicitly defined as business necessary?

Do you support the ability to force password changes upon first logon?
On customer’s request, SOC1 and SOC2 Reports Type II are available.

In accordance to our security policy:

- The monitoring will be completed during 2020 with IAM-13.1, IVS-07.1.

- As required by our ISO 27001 processes, the basic network Environments are hardened to provide only the necessary ports, protocols, and services to meet business needs using strong/multi-factor, expireable, non-shared authentication secrets.

- Running systems are immediately available to customers through electronic methods (e.g., portals or alerts).

- The results of a change or move of an image and the subsequent validation of the image’s integrity, are immediately available to customers through electronic methods (e.g., portals or alerts).

- Account credential lifecycle management from instantiation through reuse.

- Are audit logs centrally stored and retained?

- Do changes made to virtual machines, or moving of an image and subsequent validation of the image’s integrity, be made immutable, available to customers through electronic methods (e.g., portals or alerts)?

- Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., containers)?

- Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or sleeping)?

- Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones?

- Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using strong/multi-factor, expireable, non-shared authentication secrets.

- Do you regularly update network architecture diagrams that include data flows between security domains/zones?

- Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or sleeping)?

- Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones?

- 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?

- Are you a member of a security policy.

- Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or sleeping)?

- Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones?

- Are audit logs centrally stored and retained?

- Are you a member of a security policy.

- Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones?

- Are audit logs centrally stored and retained?

- Are you a member of a security policy.

- Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones?
The company shall have a documented application validation process to identify and fix potential vulnerabilities in deployed applications before they are released to users. This process must ensure that applications are tested using automated and manual methods, and that any issues identified are resolved before the application is deployed to end-users.

All cloud-based services used by the company’s mobile devices or applications must be validated before they are implemented. This includes ensuring that the services meet the company’s security requirements and are able to support the intended use of the mobile device.

Mobile device_policy shall require the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting). The mobile device policy shall prohibit the usage of unapproved application stores, rooting, or bypassing application validation. All mobile devices shall have the latest version of anti-malware software installed by the vendor. Unauthorized anti-malware software will be included for each device in the managed mobile device solution.

Remote wipe feature that is able to remotely wipe the entire device or its data. The feature shall be tested to ensure it is effective and reliable.

All mobile device policies shall be documented in the company’s mobile device policy statement, which includes a documented definition for mobile devices and the criteria for determining whether a device is a mobile device.

Severance and notification, customers and/or other external business partners are provided a means to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.

Mobile devices shall have the latest security patches or updates by company IT personnel. The mobile device policy must require the use of encryption for either the entire device or for data identified as sensitive.

The mobile device policy shall require the use of encryption for data stored on mobile devices by employees. The policy shall also require that anti-malware software is installed and maintained on all mobile devices.

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., in active/active, decommissioned status, and to whom the device is assigned or leased)?

Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the applications that may be used for BYOD usage?

WK - IT Awareness and Training GBS-STD-1205

Do you have a policy that requires all sensitive data to be encrypted when transmitted over external networks?

Do you have a policy that requires all sensitive data to be encrypted when stored on mobile devices?

Do you maintain logs and prints of reports with regard to company business data via a mobile device?

Do you have training and awareness programs for employees regarding mobile device security issues?

WK - Blocked Applications List GBS-GDL-1300

Do you have approval processes for applications to be deployed on mobile devices?

Do you have a policy that requires all sensitive data to be encrypted when transmitted over external networks?

Do you have a policy that requires all sensitive data to be encrypted when stored on mobile devices?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you have a policy that requires BYOD users to use anti-malware software (where supported)?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you have a policy that requires BYOD users to use anti-malware software (where supported)?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you have a policy that requires BYOD users to use anti-malware software (where supported)?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you have a policy that requires BYOD users to use anti-malware software (where supported)?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you have a policy that requires BYOD users to use anti-malware software (where supported)?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?

Do you have a policy that requires BYOD users to use anti-malware software (where supported)?

Do you have a policy that requires BYOD users to perform backups of specified corporate data?
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you verify periodically and at least annually the respect of the SOC1 and SOC2 Reports?</td>
<td>Yes, SOC1 and SOC2 Reports Type II are available.</td>
</tr>
<tr>
<td>Do you provide customers with ongoing visibility and reporting of your full performance?</td>
<td>Yes, as documented and provided in accordance with our service level agreements.</td>
</tr>
<tr>
<td>Do you manage contractual secrets or information resulting from disparate supplier relationships?</td>
<td>Yes, we manage contractual secrets in accordance with the guidance of our security policy.</td>
</tr>
<tr>
<td>Can you manage contractual secrets or information resulting from disparate supplier relationships?</td>
<td>Yes, we manage contractual secrets in accordance with the guidance of our security policy.</td>
</tr>
<tr>
<td>Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?</td>
<td>Yes, we have a capability to patch vulnerabilities across all of your computing devices, applications, and systems.</td>
</tr>
<tr>
<td>Do you make external third-party vendors vulnerable information and periodic penetration tests on your applications and infrastructure systems?</td>
<td>Yes, we make external third-party vendors vulnerable information and periodic penetration tests on your applications and infrastructure systems.</td>
</tr>
<tr>
<td>Do you have a security maturity program, evidence of which is provided through annual reviews, the nature of which will include assessment of management, technical, and operational controls?</td>
<td>Yes, our security maturity program includes reviews performed by independent third parties.</td>
</tr>
<tr>
<td>Are policies and procedures established, and supporting business processes and technical measures implemented, for preventing unauthorized access to, modification of, or disclosure of information, or to interrupt or disable a computer network and systems components?</td>
<td>Yes, policies and procedures are established, and supporting business processes and technical measures are implemented, for preventing unauthorized access to, modification of, or disclosure of information, or to interrupt or disable a computer network and systems components.</td>
</tr>
<tr>
<td>Do you conduct enterprise-wide vulnerability scans regularly as prescribed by industry best practices?</td>
<td>Yes, we conduct enterprise-wide vulnerability scans regularly as prescribed by industry best practices.</td>
</tr>
<tr>
<td>Do you conduct application layer vulnerability scans regularly as prescribed by industry best practices?</td>
<td>Yes, we conduct application layer vulnerability scans regularly as prescribed by industry best practices.</td>
</tr>
<tr>
<td>Do you conduct application layer vulnerability scans regularly as prescribed by industry best practices?</td>
<td>Yes, we conduct application layer vulnerability scans regularly as prescribed by industry best practices.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans?</td>
<td>Yes, we have a capability to perform vulnerability scans.</td>
</tr>
<tr>
<td>Do you make available results of vulnerability scans performed by a 3rd party at least once a year?</td>
<td>Yes, we make available results of vulnerability scans performed by a 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
<tr>
<td>Do you have a capability to perform vulnerability scans performed by 3rd party at least once a year?</td>
<td>Yes, we have a capability to perform vulnerability scans performed by 3rd party at least once a year.</td>
</tr>
</tbody>
</table>