ANNEX II

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

This Annex II forms part of the DPA and EU/UK SCCs and must be completed by the parties.
The below includes description of the technical and organizational security measures implemented by the Data Importer:

Overview

This document serves as an overall listing of the controls in place at Impartner to maintain the security of our office and data. Impartner follows the COSO framework for organizational controls. These controls are always in force and audited for compliance at least annually by a certified public accounting firm. They form the backbone of our SOC 2 processes.

Management

Impartner management is ultimately responsible for overseeing these controls. On a semi-annual basis each control owner is required to review the controls under their jurisdiction. Management observes the controls in action over the course of the year to ensure functionality and to recommend changes where needed.

Definitions

- **Company** – Company is defined as Impartner, Inc.
- **Client** – Client is defined as any user of Impartner systems.

Integrity and ethical values

Control Description
The Company's views on personal and corporate integrity and ethical values, along with guidelines for employee conduct are contained within the Code of Conduct. The Code of Conduct provides a framework for how employees conduct business and perform their duties.
The Company maintains a Contractor Agreement, which outlines the Company's associated standards of conduct. Third-party contractors working on behalf of the Company are required to read, accept, and abide by the Agreement before commencing work.
Background checks are performed on all new employees using a third-party service. The results are reviewed by HR for appropriateness and appropriate action is taken, as deemed necessary.
According to the Code of Conduct, Company personnel witnessing any improper behavior should report such incidents promptly to management and/or HR.
On an annual basis, all relevant employees are subject to a formal performance review to assess the employee's performance in their current roles and to identify opportunities for growth and job performance improvement.
The Code of Conduct reiterates that employees who violate company policies are subject to appropriate disciplinary action up to and including termination.

Board oversite and development of controls

Control Description
The Company is managed by a Board comprised of key investors who are independent of day-to-day management of the Company and the founders/executives. The Board is governed by a charter, meets in executive session on a quarterly basis, and retains full and free access to officers, employees, and the books and records of the Company. The Board and its committees have authority to hire independent legal, financial, or other advisors as deemed necessary or appropriate in the discharge of their duties, including oversight of the development and performance of internal control.
Quarterly, the Board meets with members of executive management to discuss operational and financial results and significant matters, risks, and issues facing the Company.

Management reporting lines & responsibility over objectives

Control Description

HR maintains formal organizational charts to clearly identify positions of authority and the lines of communication and escalation.
Employee duties and responsibilities are defined and communicated through job descriptions and policies and procedures. Job descriptions exist for common positions and are periodically reviewed by HR and management for accuracy and updated as needed.
The Company maintains an internal control policy which outlines management's responsibility regarding internal controls, frameworks, audit observations (from internal and external sources), and remediation of findings. The policy is reviewed and approved by the Audit and Risk Committee on an annual basis.
The responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving relevant system controls is assigned to appropriate personnel with authority to perform their related duties.
The Company maintains a third-party (vendor) risk management policy, which outlines the policies, procedures, and responsibilities associated with onboarding new vendors and monitoring existing vendors who will have access to Company's customers' personal information, including their implementation and execution of applicable internal controls. The policy is reviewed and approved by a member of InfoSec on an annual basis.
On a periodic basis, control owners sign an acknowledgement form, certifying that they have read applicable SOC control descriptions and, as needed, narratives, and understand their related process and control responsibilities. Desired updates, if any, are communicated to applicable internal and external (auditors) personnel to update appropriate documentation.

Employee recruitment, retention, and training

Control Description
Internal policy and procedure documents relating to security and availability are maintained and made available on the Company's box.com site. The policies are reviewed and approved by a member of IT management on an annual basis.
The Company maintains policies related to computer usage and security awareness, which reflect its commitment to provide training to its employees on guarding against, detecting, and reporting malicious software that poses a risk to the Company's information systems. In accordance with the policies and the annual security awareness training, Company personnel are trained on appropriate computer usage and security awareness. Company personnel are instructed to notify IT immediately of any abnormal system behavior or suspicion of a threat.
Job requirements are documented in formal job descriptions. Prior to fulfilling positions within the Company, management evaluates a candidate's abilities and background (experience, education, training, etc.) to meet the requirements of the position.
IT provides company-wide security awareness training to all new employees upon hire, and to all company personnel at least once per calendar year, to help employees understand their obligations and responsibilities to comply with the Company's security and confidentiality policies and procedures, including the identification and reporting of incidents.
The Company provides on-the-job training and/or external training of new hires and/or existing employees, as deemed necessary, to empower them with the skills needed to carry out job responsibilities, as they relate to security and availability.
As part of its ongoing efforts in business planning, budgeting, and risk assessments, senior management evaluates the need for additional tools and resources in order to achieve its business objectives.
Before the Company engages or otherwise works with relevant vendors/third parties (e.g., colocation facilities), the Company requests and reviews relevant supporting documentation and information (e.g. business licenses, entity standing, industry standard assurance/attestation reports, inquiries, completed questionnaires) before engaging in a business relationship. Entities found to be lacking in or non-compliant with relevant commitments and requirements (e.g., security, availability) and other relevant policies and procedures are refused.

Formal agreements are in place with relevant vendors and third parties. The agreements establish, as applicable, the commitments and requirements of the vendor or partner, such as the scope of services and product specifications, roles and responsibilities, compliance and control requirements (e.g., security, availability), and service level expectations. These agreements require the vendors to notify Company personnel should a security incident occur involving PRM data and/or services.
The Company evaluates relevant service providers (e.g., colocation facility, cloud providers) annually in accordance with its vendor management process. Relevant supporting documentation and information (e.g. industry standard assurance/attestation reports (e.g., SOC 2), inquiries, completed questionnaires) are obtained and assessed to (a) re-evaluate the services provided and identify any new risks arising from the relationship, b) evaluate the appropriateness and effectiveness of relevant vendor controls and the impact of control exceptions, if known, and c) validate the Company is adhering to relevant complementary user-entity control considerations, if any. Results of the evaluations are included in threat/risk analysis discussions for planning and possible mitigation, where deemed necessary.

Generation & use of quality information

Control Description
The Company has a dedicated technology support team, consisting of development, IT, and Quality Assurance personnel, which is focused on maintaining the quality of internal information systems.
In support of Company initiatives (e.g., SOC), the Company has designed, documented, and implemented IT General Controls (change management; logical and physical access and security; and computer operations) over its relevant information systems to support automated control activities and the quality of information captured, generated, processed, and/or stored therein.
The Company maintains a master list of all relevant spreadsheets and system-generated reports/information from internal and external sources used in support of the performance of internal control (IT-dependent manual controls) related to the PRM Application System. The master list is updated as needed, but formally reviewed by applicable department management on an annual basis to ensure completeness and accuracy. On the list, management also specifies how it obtains reasonable assurance that the information being used is sufficiently reliable (e.g., completeness, accuracy, level of detail, change-control) for its intended purpose.

Internal communication of objectives & responsibilities

Control Description
The Company maintains an information security incident management policy. The policy defines the protocols for identifying, reporting, investigating, responding to, mitigating, communicating, and documenting suspected or known security incidents and is made available to relevant internal users in the Company's Box.com site.
The Company maintains documentation of system and service descriptions outlining relevant aspects of the design and operation of the system, its boundaries, and components. Documentation is available to relevant internal and/or external users through PRM support pages, the Company's box.com site, master IT system asset listings, and system/network diagrams.
Changes that may affect the Company's security and/or availability commitments and requirements and/or the related responsibilities of internal or external users are communicated directly to the relevant users (via means such as PRM messages, support pages, and user guides; broadcast emails; direct outreach by Project Managers; department meetings; and/or educational events).
For user story requests, authorization is given by the Product Owner or management to ensure they meet user needs and the PRM design vision. For reported bugs, authorization occurs once the bugs are verified by internal personnel or automation processes.

External communication of internal controls

Control Description

The Company communicates its security and availability commitments regarding the system to external users via the Subscription Agreement (Terms of Use) and Privacy Policy, which are posted on the Company's website.
External user roles and responsibilities are communicated via several mediums, including the Subscription Agreement (Terms of Use) and Privacy Policy, which are posted on the Company’s website.
Support contact information is readily available to customers through the Company's website and other Company-provided documentation (e.g., training documentation, Subscription Agreement (Terms of Use)). Customers and/or associated users are encouraged to contact appropriate Company personnel if they become aware of items such as operational or security failures, incidents, system problems, concerns, or other complaints.

Identification and assessment of risks

Control Description
The Executive Team maintains a strategic plan, which includes department objectives and goals for the coming year. Consideration is given to operational, reporting (external financial, external non-financial, and internal), and compliance objectives. At least quarterly, the Executive Team meets to monitor progress against the Company objectives/goals and to discuss specific business developments, department results, and various risks and opportunities facing the Company.
Management communicates business objectives and goals to all team members through various means, including quarterly Company-wide meetings, Company-wide emails, and other messaging systems, as appropriate.
The Company has established a Security Council, consisting of members of the IT Operations, Development, Dev/Ops, and Security teams. The Security Council meets regularly to evaluate whether the Company's security initiatives are aligned with operational risks, objectives, and goals.

Risk analysis and management

Control Description
The Company maintains master lists of IT system components (e.g., servers, software, network devices) supporting PRM. The lists are reviewed and updated as needed, but at least annually, for completeness and accuracy.
At least annually, the Company performs a formal risk assessment, which includes the identification of relevant internal and external threats (including those arising from customers and the use of vendors/third parties) to system components, an analysis of the risks associated with the identified threats, the determination of appropriate risk mitigation strategies (including procedures over assessing and monitoring vendors/third parties), and the development or modification and deployment of controls consistent with the risk mitigation strategy.

Fraud assessment

Control Description
As part of the Company's formal risk assessment, management identifies fraud risks and assesses the likelihood of occurrence and potential impact on the Company's operational, reporting, and compliance objectives.

Identification of changes that impact the system

Control Description
Several mediums, such as the formal risk assessment process, quarterly Board of Directors meetings, weekly Executive management team meetings, industry (including security) news feeds/resources, and customer security questionnaires (in RFPs), assist Company personnel in identifying relevant changes (e.g., environmental, regulatory, technology) that could impact business objectives; commitments and

requirements to security and availability; and internal and external operations. In response to relevant changes, the risk assessment and related mitigation strategies are updated where deemed necessary.

Evaluation of the effectiveness of controls

Control Description
As part of the risk assessment and mitigation processes, the Company identifies, designs, develops, and implements key controls where deemed necessary. The Company uses several mediums, including customer feedback, application / system security and performance monitoring, and internal performance reviews, to monitor the overall effectiveness of its underlying control environment. Identified discrepancies are appropriately investigated and, where needed, resolved. The resolution of such discrepancies may include updating the risk assessment and related mitigation strategies.
The Company employs host and network-based intrusion detection/intrusion prevention (IDS/IPS) systems and logging and monitoring software to a) collect data from PRM application and supporting infrastructure components (e.g., servers, databases, network devices) and endpoint systems, b) monitor the related systems for security and operational matters (e.g., latency, throughput, uptime, utilization), and c) detect unusual system activity. Based on configured events, the software systems automatically generate email, console, and/or MS Teams alerts to IT support personnel for further investigation and, if needed, resolution.
On an annual basis, IT personnel review production servers and network devices to ensure relevant configuration settings are maintained in accordance with the current hardening policy and procedure document and out-of-compliance configurations are appropriately corrected.
Quarterly vulnerability scans and annual third-party penetration tests are performed on Impartner's core applications to identify vulnerabilities and variances from Company standards. Results are evaluated by appropriate personnel and remediation actions are performed, where deemed appropriate.

Internal communication of control deficiencies

Control Description
The Company uses a Third-party service to actively forward relevant system alerts to on-call personnel. At any given time, there are three individuals on call: a primary contact, a backup contact, and an escalation contact. The on-call rotation includes at least one member of the Operations team at all times.

Protection of information assets

Control Description
The Company maintains a Hardening Policy, which establishes internal standards for asset hardening and configuration (e.g., access and service restrictions, logging and monitoring mechanisms (including host-based agents), patching). The Policy is reviewed and approved by a member of IT management on an annual basis.
Firewalls are implemented at external points of connectivity and network segment boundaries (DMZ, internal) and are configured (e.g., access control lists, rules) to protect against unauthorized external access. Firewall rules are restrictive by default, and are configured to restrict connectivity and data flow to pre-approved network destinations and ports.
Traffic flowing to PRM also passes through a web application firewall designed to inspect traffic for malicious content and mitigate or prevent denial-of-service attacks.
Customers do not have direct access to the PRM database. Customers authenticate to PRM which connects to the production database via a restricted private connection.
A unique user ID and password are required to access PRM. PRM provides Customers the ability to set their own password policies within PRM, including Expiration, History, Minimum Length, Complexity, Login attempts and Lockout duration.

In order to remotely access relevant production network devices and PRM systems (web, database, and support services servers; and the database), users must pass through several layers of authentication. First, users must connect to the corporate network through a local physical connection, corporate WiFi via LDAP authentication, or VPN via a username and two factors of authentication. Next, users authenticate at the system or device layer using a separate username and password. Password parameters are configured according to the Company's password policy and include, where system functionality permits, settings such as minimum length, complexity, expiration, history, and lockout.
Internal user account passwords for PRM web, database, and support services servers are stored in an encrypted hash.
Customers' PRM account passwords are hashed and salted in accordance with industry standards.
External access to PRM is restricted through the use of user authentication and a minimum of TLS encryption. TLS is used during customer logins and throughout customer sessions, providing encryption of data transmissions between customer browsers and PRM application servers. In addition, VPN, TLS, SSH, and/or other encryption-based technologies are required for communications between other remotely accessible endpoints and the systems and users connecting to them.
The Company uses a combination of private circuit technologies (IPsec and a private leased layer 2 connection) in order to protect data transmitted between its facilities (corporate office, colocation facilities).
The PRM database is encrypted at rest using full-disk encryption.
Database and file backups are encrypted at rest and access to the backups is restricted to appropriate IT personnel.
PRM supports the use of role-based security, allowing customer account administrators the capability to assign pre-defined access levels (roles) and associated permissions to applicable users, based on job functions.
Administrative access to the production network domain, network devices, PRM super user functionality, and PRM supporting systems (web, database, and support services servers; database; SparkPost; and cloud storage) is restricted via logical access rights to appropriate IT administrators / support personnel and required system accounts. Access is granted on a minimum necessary basis in order for Company personnel to effectively carry out job functions and responsibilities.
Company access to view or manage customer instances of PRM is restricted via logical access rights to appropriate support personnel.

Control of access to the system and supporting services

Control Description
Requests for new or modified access to the production network domain, network devices, PRM super user functionality, and PRM supporting systems (web, database, and support services servers; the database; SparkPost; and cloud storage) are approved by an appropriate supervisor before access is granted. System administrators provision access rights that are in accordance with the request and/or are commensurate with the user's job responsibilities.
As part of the onboarding process for PRM, an administrator account is created for the customer's primary contact, enabling him/her to manage all customer user accounts going forward. In order to log in, the user must change the initial password, thus preventing Company personnel from using that password to access the customer's application instance.
The Privacy Policy, which is posted on the Company's website, instructs external users to maintain the secrecy of their PRM passwords and account information. Additionally, account sharing of end-user-based accounts on internal systems is prohibited (unless exempted by management) by internal policies. The policies also state that violators may be subject to appropriate disciplinary action

In accordance with the Company’s Hardening Policy, only system/service accounts that serve a valid business purpose are enabled on production servers, databases, and network devices, and default (built-in) passwords have been changed where applicable.
HR personnel notify IT system administrators of employee terminations. Upon notification, system administrators proceed to disable/delete the employee’s access to applicable systems, including the production network domain, network devices, PRM super user functionality, and PRM supporting systems (web, database, and support services servers; the database; SparkPost; and cloud storage). A checklist listing relevant Company systems is utilized in the process to ensure that access rights are checked and, where applicable, disabled/deleted.
Passwords to sensitive built-in administrator and other master-level accounts are changed in a timely manner when an employee with knowledge of them departs or changes roles and no longer needs such access. A checklist listing all relevant systems, utilities, and colocation facilities is utilized in the process to ensure all accounts are appropriately updated.
All production network domain accounts that are inactive for 90 days are automatically disabled. If the accounts are still inactive after 180 days, notification is sent to IT management for review.
On an annual basis, a user account audit of the production network domain, network devices, PRM super users, and PRM supporting systems (web, database, and support services servers; the database; SparkPost; and cloud storage) is performed by a member of IT management to validate the ongoing appropriateness of all internal accounts and related access levels.

Physical access

Control Description
All new requests for access to the colocation facilities must be approved by a member of IT senior management.
Upon notification of an applicable employee termination, the Sr. Director of IT or other authorized Company account administrator updates the master access list at the colocation facilities to disable the employees associated physical access rights.
On a semi-annual basis, the list of personnel with physical access rights to the colocation facilities are reviewed by a member of IT senior management to validate the ongoing appropriateness of access.

Asset management

Control Description
The Information Security team maintains an End of Life Policy, which outlines the policies governing the disposition of obsolete or unwanted IT assets and any accompanying software and data stored therein.
IT maintains a master list of relevant IT hardware assets. As IT assets containing sensitive software and/or data are deemed end-of-life and ready for sale or disposal, the storage media is removed and securely wiped. The master list is updated to reflect the actions taken on disposed assets.

Logical access

Control Description
The Sr. Director of IT reviews configured firewall rules on a semi-annual basis for appropriateness and adherence to Company standards. Requests for changes, if any, are documented and submitted to appropriate network personnel for implementation.

Data movement

Control Description
The Company maintains policies relating to data transmission and storage, which prohibit the transmission of sensitive information over the Internet or other public communication paths (for example, e-mail), unless it is encrypted. In addition, these policies prohibit the storage of customer information on removable media, mobile devices, or other unencrypted end-user storage media.

Unauthorized or malicious software

Control Description
Endpoint security software has been implemented to assist Company personnel in preventing, detecting, and analyzing security-related events, including the introduction of potentially malicious software, on end-user systems and production servers. Endpoints are configured to receive updated threat and virus signatures from the vendor continuously. The software sends a consolidated report to IT at least daily outlining threats detected on relevant endpoints, action taken, etc. Relevant issues are appropriately investigated and, if needed, resolved.

Patch management

Control Description
The Company maintains a patch management policy, which establishes internal standards for identifying, evaluating, and implementing patches to remediate relevant vulnerabilities. The policy is reviewed and approved by the Sr. Director of IT on an annual basis.
IT monitors the availability of patches to network devices and PRM supporting systems (web, database, and support services servers) on a daily basis. Relevant patches are applied in a timely manner, in a phased approach starting with non-production network devices and servers to assess the potential for service disruptions before application to the production servers.

Incident management

Control Description
For security events deemed to be an "incident," as defined in the Incident Response Policy, the Security Incident Response Team is activated and executes the incident response program, which includes analysis, containment, eradication, recovery, communication to affected parties (internal and external), and post-incident activity, as appropriate. Details of key information gathered and actions performed relating to the incident and associated response are documented in an Incident ticket.
The Company’s IT team performs periodic tabletop incident response simulations to test the Company’s Security Incident Response Plan, taking into account the threat, likelihood, magnitude, business impact analysis, availability, etc. The Security Incident Response Plan and related policies / processes / systems are revised, as needed, based on the test results.
At least annually, the Company tests its ability to failover PRM to the disaster recover colocation facility.

Change management

Control Description
The Company maintains a formal application change management policy, which outlines considerations for planning, design, testing, implementation, and maintenance of changes.
For each change, automated application regression tests are performed to identify common issues.
Application-related changes are appropriately tested by Quality Assurance (QA) personnel prior to implementation in production.

Changes are approved by appropriate personnel, as defined in the application change management policy, prior to implementation in production.
For PRM and its related database, separate development, test, and production environments exist in support of the Company's application change management process.
PRM changes are deployed to production servers by appropriate personnel, who are separate from the development function.
PRM code can be rolled back as needed during and after deployment.
The Company maintains a formal infrastructure change management policy, which defines the relevant types of changes that can be made to the Company's infrastructure and sets forth the procedures for the associated testing, approval, and documentation. The policy is reviewed and approved on an annual basis by a member of IT for ongoing appropriateness.
During the ongoing risk assessment processes and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created where appropriate.
When relevant system deficiencies are identified, change requests are generated, analyzed, prioritized, assigned, authorized, tested, approved, and implemented in accordance with the Company’s change management procedures.

Risk mitigation

Control Description
The Company maintains a Disaster Recovery policy, which outlines tasks and procedures to be executed for disaster recovery, to minimize the amount of downtime caused by a disaster.
The Company maintains a formal Backup Policy, which is reviewed and approved by the Sr. Director of IT on an annual basis.
PRM production runs in a redundant environment with clusters of servers, enabling load balancing and continued operation in the event of a logical or hardware failure of any given server.
The Company currently contracts with Flexential, utilizing two geographically distinct colocation facilities. The Company mirrors production technology and functionality (e.g., software, systems, data) between the facilities to permit the resumption of PRM operations in the event of a disaster at the production facility.
On a daily basis, incremental and/or full backups of production network device configurations and PRM data and locally-stored customer files are generated, stored locally to disk, and subsequently copied to tape. IT monitors the backup and copy processes for completion using log files and/or automated email alerts. Issues are appropriately investigated and, if needed, resolved.
PRM production databases and website content reside at the production Flexential colocation facility (in Las Vegas) or the Azure IaaS and are replicated, in real-time, to redundant hardware sets both locally and at either the disaster recovery Flexential colocation facility (in SLC), or multi-zone Azure IaaS facilities. Email alerts are automatically sent out by monitoring utilities in the event of a replication issue or noteworthy lag. Issues are appropriately investigated and, if needed, resolved by IT and/or database personnel.
The Company tests its ability to restore PRM database data quarterly, and customer files semi-annually, from backup data.
The Company has established an Insurance Committee headed by the CFO which meets at least annually with a broker to review the insurance coverage of the business, taking into account risks that may threaten achievement of applicable Company objectives. The Insurance Committee makes appropriate changes to the insurance coverage, as deemed necessary.

Capacity management

Control Description

Monitoring software is used to track processing, storage, memory, and other system performance metrics and demands in PRM and compare them to historical trends on an ongoing basis. Based on pre-defined capacity thresholds, the software automatically generates email and logged alerts to IT support personnel for further investigation. Significant events (e.g., increasing trend in usage) are further discussed in the weekly Engineering meeting. Change requests are initiated as needed to maintain or improve the system.
The Company maintains a master list of PRM system components at its production and disaster recovery locations. The list includes information about hardware assignment and redundancy.

[Remainder of Page Intentionally Blank]