General Terms and Conditions

Revision Date: March 24, 2020

These General Terms and Conditions ("Legal Terms") when incorporated by a Statement of Work, or Proposal ("SOW") shall govern the services to be provided ("Services") and constitute the full agreement (collectively the "Agreement") between the Customer and the Datasite entity ("Datasite") (each a "Party") named in the SOW. In the event of a conflict between the Legal Terms and any SOWs, the SOW shall govern.

1. Fees, Taxes, Billing Disputes.

(a) Fees. Customer shall pay to Datasite the fees (the "Fees") set forth in any SOW. If the Customer is represented by an advisor in furtherance of the Services, Customer shall pay all costs incurred by such advisor for the performance of the Services. All Fees are payable in the currency used in the applicable SOW.

(b) Payment. Customer shall pay all Fees owing under this Agreement within 30 days of receipt of an invoice from Datasite. Datasite may suspend Services upon non-payment. Interest may be added to all past due invoices in accordance with local laws.

(c) Taxes. Amounts payable by Customer under this Agreement are exclusive of all applicable taxes (including VAT and withholding taxes).

2. Ownership and Requirements.

(a) Customer Ownership. Customer has sole responsibility for the accuracy, quality, integrity, and appropriateness of all original data, content and information provided to Datasite in conjunction with the Services. Customer owns any document that is uploaded to the Services by or on behalf of the Customer (the "Content,") and the Customer's trademarks or logos, which, together are referred to as the "Customer Material."

(b) Datasite Ownership. All materials, documents, methodologies, source code, websites and software that Datasite uses in providing the Services, and any and all future enhancements or modifications thereto however made and any intellectual property rights therein, are owned by Datasite.

(c) Content. Customer will (i) use reasonable efforts to provide Datasite with clear and legible copies of the Content in the best possible condition; (ii) cooperate with Datasite in correcting any problems associated with Content; (iii) report promptly to Datasite any problems or errors that Customer observes or discovers with the Content; and (v) notify Datasite, in writing, of all court orders restricting the use, distribution or disposition of the Content delivered to Datasite.

3. Representations and Warranties.

(a) General Representations. Each Party represents and warrants that (i) it has full power and authority to enter into and perform its obligations under this Agreement; (ii) it will comply with all applicable laws; and (iii) it will use up-to-date, generally accepted virus detection devices and procedures to ensure that any electronic data transmitted to Datasite will not contain a virus or other harmful component.

(b) Datasite Representations. Datasite represents and warrants that (i) all of the Services will be rendered using sound, professional practices and in a competent and professional manner; and (ii) it has all necessary permissions, software licenses and ownership rights to provide the Services.

(c) Customer Representations. Customer represents and warrants that (i) it has a legitimate business interest or obtained all permissions and consent required by law to transfer the Content so that Datasite may lawfully use and process in accordance with this Agreement; (ii) it has delegated authority to its advisors in providing instructions in connection with the Services, and Datasite has no duty to verify such instructions with Customer; and (iii) it will not use the Services for any fraudulent or unlawful purposes, not allow others to do so.

(d) Disclaimer of Warranties. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, THE SERVICES ARE PROVIDED AS-IS, WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR MERCHANTABILITY.

4. Confidentiality.

(a) "Confidential Information" means proprietary information of a Party, including but not limited to Customer Material (including personal data controlled by the Customer), inventions, copyright, trade secrets, marketing plans, programs, source code, data and other documentation, customer and shareholder information, other information related to the business of that party, and the terms and pricing of this Agreement. The term Confidential Information does not include: (i) information that was in the receiving party's possession or was known to it prior to its receipt from the disclosing party; (ii) information that is or becomes publicly available without the fault of the receiving party; (iii) information that is or becomes rightfully available on an unrestricted basis to the receiving party from a source other than the disclosing party; or (iv) information that was independently developed by the receiving party.

(b) Each Party acknowledges that the other Party owns or possesses valuable Confidential Information. Each Party shall hold such Confidential Information of the other Party in strict confidence and will not make any disclosures without the written consent of the disclosing Party, except as needed in furtherance of the Services, and will take all reasonable steps

to maintain the confidentiality of all Confidential Information. This Agreement expressly supersedes and replaces in its entirely any non-disclosure agreement executed by Datasite in connection with preliminary discussions regarding the proposal of Services to Customer.

(c) If a Party is compelled by court order, subpoena, or other requirement of law to disclose Confidential Information, the Party will provide the other Party with prompt notice (unless such notice is prohibited by law) so that the Party may, at its option and expense, seek a protective order or other remedy.

(d) Upon termination of the Agreement, all Content uploaded to the Services shall be destroyed or returned to the Customer. The parties agree, that upon Customer's request, Datasite shall provide a certification of deletion or destruction of the Content. Notwithstanding the provisions of this Section 6(b), Datasite is not obligated to immediately erase Content contained in an archived computer system backup made in accordance with such party's security or disaster recovery procedures, provided that such archived copy will remain fully subjected to these obligations of confidentiality until such destruction or erasure.

(e) All Content is stored in the European Union unless otherwise requested by Customer and stored at secure third-party hosting facilities within the European Union. Datasite may transfer Content to its wholly owned Affiliates for specialized Services or localization of customer support. Any personal data within the Content is protected in accordance with the General Data Protection Regulations. Datasite shall process and use personal data only for and on behalf of Customer, for the purpose of performing Services, as per the instructions of Customer, and in accordance with the law. In addition to the obligations set forth above, the parties agree to the Data Processing Addendum 1 attached to this Agreement.

5. Limitation of Liability. NEITHER DATASITE NOR CUSTOMER SHALL BE LIABLE TO THE OTHER PARTY OR ANY OTHER THIRD PARTY UNDER ANY THEORY OF RECOVERY, WHETHER BASED IN CONTRACT, IN TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), UNDER WARRANTY, OR OTHERWISE, FOR ANY PUNITIVE, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL LOSS INCLUDING: LOSS OF PROFITS, BUSINESS, GOODWILL, REPUTATION, OR LOSS RESULTING FROM BUSINESS INTERRUPTION. CUSTOMER EXPRESSLY AGREES THAT UNLESS OTHERWISE STATED HEREIN, THE REMEDIES PROVIDED IN THIS AGREEMENT ARE EXCLUSIVE AND THAT UNDER NO CIRCUMSTANCES SHALL THE TOTAL AGGREGATE LIABILITY OF EITHER PARTY UNDER ANY THEORY OF RECOVERY, WHETHER BASED IN CONTRACT, IN TORT, UNDER WARRANTY, OR OTHERWISE, EXCEED THE TOTAL PRICE PAID OR PAYABLE TO DATASITE UNDER THE APPLICABLE SOW FOR THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE LIABILITY. THE PROVISIONS OF THIS PARAGRAPH SHALL NOT APPLY TO A PARTY'S BREACH OF THE OWNERSHIP PROVISIONS CONTAINED IN THIS AGREEMENT NOR TO A PARTY'S GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT.

6. Hosting Terms. The following provisions apply to the extent that the Services include hosting Customer's Content on an Internet-based platform (the "Website"):

(a) Website Users.

(i) Definitions. The Website users ("Users") are those individuals authorized by Customer, and enabled by Datasite or Customer, to access the Content on the Website. "Managers" are those Users who are authorized by Customer to initiate and conclude Services, upload and manage Content, invite other Managers and Users and access reports. Customer will pay any Fees incurred by Manager.

(ii) Obligations. Users must consent to the Terms of Use and Privacy Notice included in the Website and which may be amended from time to time. Datasite retains the right to deregister any User from the Service upon request of the employer of such User.

(iii) Go Live Date, Sandbox. Prior to the Go Live Date or if Customer elects to utilize the sandbox (as described in the SOW), Customer agrees to only use such Services for the purpose of managing and distributing Content within the sell-side team, including Customer's employees, clients, and advisors in connection with an actual or proposed merger, acquisition, joint venture or other transaction involving the sale or exchange of assets or voting securities of Customer or Customer's clients. Datasite retains, in its sole discretion, the right to terminate a Sandbox.

(iv) Storage. All content uploaded to the Website is converted to PDF format, unless otherwise designated by the Manager as download only files ("Special Media"). Price is totaled based on the outcome of the conversion, either on a per "210 x 297 mm" page basis ("Page") or per storage basis ("MB" or "GB"), as described in the SOW, and which shall increase in the increments set forth therein. Datasite storage and Page counts excludes Fees for Optional Products & Services and shall be conclusive except in cases of material error. Incremental storage fees and charges of Optional Products & Services will be invoices as they occur.

(b) Service Level Agreements.

(i) Scheduled Maintenance. Datasite performs periodic maintenance on the Website for system upgrades, and maintenance ("Scheduled Maintenance"). Advanced notice is provided on the Website. Scheduled Maintenance will not exceed four (4) hours per calendar month. Datasite reserves the right to update, modify, improve, support operate and modify the Website and Services based on Customer's use, as applicable. Any updates or modifications will not materially diminish the functionality or security of the Website.

(ii) Availability Guarantee. Aside from Scheduled Maintenance, Datasite guarantees that the Website will be available at least 99.5% of the time measured on a calendar month basis (the "Availability Guarantee").

(iii) Exceptions. No period of inoperability will be included in calculating the Availability Guarantee to the extent that such downtime is due to *(x)* failure of Customer or its Users' internet connectivity; or *(y)* internet or other traffic problems other than problems arising from networks controlled by Datasite.

(iv) Service Credits. If Datasite fails to meet the Availability Guarantee during the Term, Customer may *(x)* terminate the SOW and request Datasite to deliver, as soon as commercially practicable, the Content on the Website to Customer, if Customer does so within five (5) days of Datasite's failure to meet the Availability Guarantee; or *(y)* request that Datasite provide Customer the credits described in the table below, provided Customer makes such request within twenty (20) days after Datasite's failure to meet the Availability Guarantee.

Actual Percentage the Website is Available	Credit
99.5% or more	None
97% to less than 99.5%	10% of Monthly Fees
96% to less than 97%	25% of Monthly Fees
95% to less than 96%	50% of Monthly Fees
Less than 95%	100% of Monthly Fees

(c) Termination. The following will occur upon termination or expiration of a SOW or this Agreement:

(i) Upon Manager contacting Datasite Service carrying out Datasite's closing instructions, Datasite will terminate Customer's and all Users' access to the Website(s).

(ii) Datasite will permanently delete all Content maintained by Datasite on the Website. Upon termination or expiration of the SOW, Datasite's obligation to host Content will cease.

(iii) If, within ten (10) days of notice of default, invoices are not paid in full, Datasite will have no obligation to preserve or return the Content.

7. General.

(a) Analytics. Upon anonymizing Content by removing all references to numeric values, dates, times, proper names, addresses, location, titles, and personal data ("Anonymized Content") and incorporating such Anonymized Content with or into similar information derived or obtained from other customers of Datasite (collectively "Aggregated Content"), Customer hereby grants to Datasite a nonexclusive, fully paid, world-wide and irrevocable license to use Aggregated Content exclusively for enhancing features and functionality of the Services.

(b) Restricted Parties. Datasite reserves the right to prohibit Services to any company or individual from a sanctioned or embargoed country, or restrict access or use of Services to any restricted party based on any published government list.

(e) Assignment. This Agreement is binding upon and for the benefit of the parties and their respective successors and assigns. It is agreed and understood that neither Party may assign, in whole or in part, without the other Party's prior written consent. Notwithstanding the forging, upon providing prior written notice, either Party may assign its rights, interests and obligations in this Agreement or any SOW pertaining thereto to any parent, subsidiary or affiliate, or to a successor of all its assets or stock of the Party.

(f) Notices. Wherever provision is made in this Agreement for the giving, service or delivery of any notice, such notice shall be in writing and shall be given using a method providing for proof of delivery.

(g) Force Majeure. If a delay or failure of a Party to comply with any obligation set forth in this Agreement is caused by force majeure, that obligation (other than the obligation to pay money when due and owing) will be suspended during the continuance of the force majeure condition and will not be considered a breach of this Agreement. A Party whose performance is suspended hereunder shall give prompt written notice of any event of force majeure and such Party's best reasonable estimate of when such event will abate.

(h) Marketing Support. Upon the public announcement of an applicable transaction, Datasite may identify Customer as a Datasite customer and use Customer's name or logo on any Datasite's websites or other marketing materials.

(i) Entire Agreement. This Agreement, together with any applicable SOWs, constitutes the entire agreement between the Parties and supersedes all previous agreements, proposals, and negotiations, whether written or oral regarding the subject matter herein. Datasite rejects the inclusion of any different or additional terms, unless expressly agreed to in writing.

Data Processing Addendum 1

This Addendum on Data Processing (hereinafter: "Addendum") is made on the Effective Date, by and between:

Customer as defined by the SOW

– hereinafter referred to as "**Controller**" –

and

Datasite entity as defined by the SOW

– hereinafter referred to as "**Processor**" –

Hereinafter each individually referred to also as the "**Party**" and collectively as the "**Parties**"

Preamble:

(A) The Parties have entered into an Agreement which outlines the Services to be provided (definitions provided in Section 1 below). As part of the provision of Services by the Processor, Personal Data may be transferred by the Controller to the Processor.

(B) In the event of any conflict between the provisions in this Addendum and the provisions set forth in the Agreement, the provision or provisions of this Addendum will prevail. Capitalized terms not defined in this Addendum are defined in the Agreement.

(C) To ensure compliance by the Parties with Processing obligations pursuant to the Data Protection Rules, as amended from time to time, the Parties hereby agree as follows:

1. Definitions

1.1. "**Appendix**" means the appendix annexed to and forming an integral part of this Addendum;

1.2. "**Data Protection Country**" or "Data Protection Countries" means a country or countries where privacy, data protection or information security laws are in place that regulate personal or private information or Personal Data, including but not limited to the European Economic Area, Brazil, Hong Kong, Australia, Singapore, Canada, United Kingdom and Switzerland.

1.3. "**Data Protection Rules**" means the relevant national laws that apply to the Processing of Personal Data in Data Protection Countries, including but not limited to any applicable privacy and information security laws and regulations that apply from time to time;

1.4. "**Data Subject**" means an identified or identifiable natural person whose Personal Data is subject to Processing; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity;

1.5. "**Information Security Incident**" means any transfer, access and disclosure to third parties, or Processing in breach of this Addendum or the Data Protection Rules or any event directly or indirectly affecting the confidentiality, integrity, authenticity of Personal Data;

1.6. "**Privacy Shield**" means the EU-U.S. Privacy Shield Framework, which became effective August 1, 2016, and Swiss-US Privacy Shield Framework, which became effective April 12, 2017.

1.7. "Agreement" means the Statement of Work and the General Terms and Conditions between the Controller and the Processor;

1.8. "**Personal Data**" means any information relating to a Data Subject contain within the Content.

1.9. "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

1.10 "**Services**" means the provision of services as described in the Agreement and this Addendum;

1.11 "**Special Categories of Data**" means the Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data that uniquely identify a natural person, as well as Personal Data concerning health, sex life or sexual orientation

2. Processing Activities

The Controller shall have sole responsibility for the accuracy, quality, and legality of Processing of Personal Data, and shall comply with and is responsible for its invited Users compliance with applicable Data Protection Rules. The Processor agrees to Process the Personal Data to provide Services in accordance with this Addendum and the Agreement, pursuant to Controller's written instructions as set forth in Appendix 1 of this Addendum, and as may be communicated by the Controller from time to time. If the Processor believes that an instruction infringes applicable Data Protection Rules, it will immediately notify the Controller. The Processor undertakes to Process the Personal Data in accordance with applicable Data Protection Rules.

3. Duration and Termination of this Addendum

3.1. This Addendum is effective as of the Effective Date and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of any SOW.

3.2. Notwithstanding the termination of this Addendum, the Processor and any subcontractors shall continue to be bound by their obligations of confidentiality.

4. International Transfers

The Processor is certified under Privacy Shield frameworks and is committed to its principles. Controller acknowledges that Processor may Process Personal Data outside the EEA, United Kingdom and United States; however, Personal Data will continued to be stored in a Data Protection Country or in the United States. The Processor will only onward transfer Personal Data in compliance with Data Protection Rules and notify Controller if it can no longer provide adequate level of protection as required by Data Protection Rules.

5. Confidentiality and Information Security Standards

5.1. The Processor shall keep Personal Data strictly confidential. The Processor shall ensure that its employees are aware of the applicable privacy and information security requirements and are held by legally binding confidentiality obligations.

5.2. The Processor will implement appropriate operational, technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access described in Appendix 2.

5.3. The Processor will update the technical and organizational security measures in line with reasonable technological developments as determined by Processor and provide updated documentation to the Controller on request in the form of its current ISO 27001 certification.

6. Cooperation and Notification Obligations

6.1. The Parties will co-operate with each other to promptly and effectively handle enquiries, complaints, and claims relating to the Processing of Personal Data from any government authority or Data Subjects. If a Data Subject should apply directly to the Processor to exercise his/her Personal Data rights, the Processor must forward this request to the Controller without undue delay. The Processor will notify the Controller immediately if the Personal Data is subject to a control or investigation by public authorities and will not disclose any Personal Data without the prior consent of the Controller. The Processor will provide the public authorities, upon request, with information regarding Processing under this Addendum as well as allow inspections within the scope stated in this Section 7.

6.2. The Processor will notify the Controller of an Information Security Incident that is determined to affect Controller's Personal Data without undue delay. The Processor shall provide Controller with the information to help and reasonably assist Controller as required by Data Protection Rules.

7. Controller's Audit and Inspection Rights

Upon Controller's request, Processor shall make available to Controller information necessary to demonstrate Controller's compliance with the obligations in the Addendum and Data Protection Rules and allow for and contribute to audits, including inspections conducted by Controller or an independent third party auditor mandated by Controller for the purpose of verifying the Processor's compliance with this Addendum, subject to the persons performing such audit sign a non-disclosure agreement with the Processor. All inspections shall be conducted during normal working hours and without interfering with the course of the Processor's business.

8. Use of Subcontractors

8.1 Controller hereby acknowledges and agrees that Processor may use Subcontractors to Process Personal Data. Processor will make available to Controller its current list of Subcontractors upon request. Any Subcontractor will be permitted to Process Personal Data only to deliver the Services Processor has retained them to provide and will be

contractually bound by contractual obligations no less protective than this Addendum. Processor shall be liable for the acts and omissions of any Subcontractor as if the acts or omissions were performed by Processor. The Processor will keep the Controller updated of any changes to the subcontracted Processing and provide the Controller with a copy of this subcontracting agreement upon request.

8.2 If the Processor intends to appoint or replace a Subcontractor covered by this Addendum, the Processor shall inform Controller of this advance and give Controller the opportunity to reasonably object to such changes. The Supplier shall provide Controller with all information that Controller may reasonably request to assess whether the appointment of the proposed Subcontractor complies with the Controller's obligations under this Addendum and applicable Data Protection Rules.

9. Return and Deletion of Personal Data

Upon the request of the Controller or upon termination of this Addendum, the Processor will, return or destroy all Personal Data and copies thereof. Upon the request of the Controller, the Processor will certify that this has been done.

10. Liability & Indemnification

10.1 The Liability of the Parties and the limitation thereof shall be in accordance with the Agreement.

10.2 The Controller shall indemnify Processor against all claims by any third party with regard to the processing of personal data provided to the Processor if the processing of such data was not permitted by Data Protection Rules.

Appendix 1: Processed Personal Data and Purposes

Personal Data are transferred and Processed for the **following purposes**:

- Secure online repository and data sharing for corporate due diligence, related transactions or internal business purposes.

Scope of Processing:

- As described in the Statement of Work, Processor provides virtual data room, a secure online repository for storing, managing, collaborating on and distributing data and documents.

Categories of Personal Data:

- Names, address, company email address, company phone number, national identification numbers, compensation and benefits, holiday and pension information, job titles and functions and potentially all other types of personal data embedded in the business information uploaded by Controller's Administrator onto the virtual data room.

Special Categories of Data (if applicable):

The Personal Data concerns the following Special Categories of Data (please specify):

- None, unless otherwise identified by Controller

Data Subjects:

The Personal Data concerns the following categories of Data Subjects:

- Business information that may include owner, employee, customer, contractor and vendor data.

Appendix 2: Information Security Measures

Appendix 2 includes:

Section I: Processor's General Data Security Plan
Section II: Processor's Information Security Procedure/Process

I. General Data Security Plan

The Processor undertakes to institute and maintain the following data protection measures:

	Security Requirement	How the Processor implements the specific information security measure
	Please describe the access control (physical) measures in your company to prevent unauthorized persons from gaining access to Processing systems within which Personal Data are Processed or used (If your company has several subsidiaries or branches please distinguish the differences between the locations).	All data centers hold ISO 27001:2013 and SOC 2 Type 2 certifications. In addition, the data centers are certified under the Privacy Shield Frameworks. A perimeter of multiple security controls are in place for all data centers which include multiple require authentication methods in order to gain access.
2.	Please describe the admission control measures taken in your company to prevent Processing systems from being used without authorization.	Authorized users are based on business requirements and require management role identification and approval. Time out features, strong authentication requirements and access rights are implemented and trackable.
3.	Please describe the access control (virtual) measures taken in your company to ensure that persons entitled to use a Processing system have access only to Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of Processing or use and after storage.	Authorized user access is managed through a formal registration and de-registration procedure for granting and revoking access to all systems and services based on job role. Audit reporting allows for the accurate monitoring of user activity and access controls are in place to protect data integrity and confidentiality.
4.	Describe the transmission control measures taken in your company to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities are envisaged.	Processor has removable media policy with the appropriate technical controls in place to protect data integrity and confidentiality and prohibit unauthorized Personal Data transfer. Remote access is controlled using multifactor authentication. Data is encrypted at rest and in-transit using government approved encryption technologies.

5.	Describe the measures of input control to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into Processing systems, modified or removed.	Processor is agnostic to the data the client chooses to upload. All user actions with respect to data integrity and confidentiality are tracked and reportable. Controller has sole determination on what data is provided to Processor.
6.	Describe the assignment control measures in your company to ensure that, in the case of commissioned Processing, the Personal Data are Processed strictly in accordance with the instructions.	Audits are conducted annually as part of ISO 27001 Certification and SOC 2 Type 2 Report to ensure compliance requirements are being met. Authorized users complete Training and acknowledge compliance with company code of conduct and policies annually. All employees and contractors are required to sign NDA.
7.	Describe the availability control measures your company takes to ensure that Personal Data are protected from accidental destruction or loss.	Processor has redundancy with each platform and maintains logs of system availability. In addition, redundancy allows for continuous system backups. Processor has Disaster Recovery and Business Continuity Plans that are reviewed, updated and tested annually.
8.	Describe the separation control measures your company has taken to ensure that Personal Data collected for different purposes can be Processed separately.	Logical separation is maintained within the same multi-tenant database. Authorized users are restricted to the project to which they are authenticated. Processor maintains a 3-tiered application with separation of data; development, test and production.

II. Processor's Information Security Procedure/Process

The Processor implements and follows the following standards, processes, and procedures:

Datasite operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope: The management of information security applies to processes for the protection of client information regarding the global services of financial transactions and reporting, marketing and communications for regulatory industries, and customer content and collaborations.