linford & co llp
cpa firm

BIS | SAFETY SOFTWARE

TYPE II SOC 2

REPORT ON CONTROLS RELEVANT TO SECURITY

JANUARY 1, 2023 TO DECEMBER 31, 2023

BIS Safety Software Inc.

Report on BIS Safety Software Inc.'s Description of Its Compliance and Learning Management Software and Controls Relevant to Security

Table of Contents

BIS Safety Software Inc.

Report on BIS Safety Software Inc.'s
Description of Its Compliance and Learning Management Software
and Controls Relevant to Security

Table of Contents (continued)

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Leadership Team of BIS Safety Software Inc.:

Scope

We have examined BIS Safety Software Inc.'s (BIS or the Company) accompanying description of its compliance and learning management software titled, "BIS' Description of Its Compliance and Learning Management Software" throughout the period January 1, 2023 to December 31, 2023 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that BIS' service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

BIS uses the subservice organization, Amazon Web Service (AWS), to provide hosting services and uses the subservice organization, Microsoft Office 365 (O365), for digital file storage, authentication enforcement, and end-point management. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BIS, to achieve BIS' service commitments and system requirements based on the applicable trust services criteria. The description presents BIS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BIS' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BIS, to achieve BIS' service commitments and system requirements based on the applicable trust services criteria. The description presents BIS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of BIS' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

BIS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that BIS' service commitments and system requirements were achieved. BIS has provided the accompanying assertion titled "Assertion of BIS Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. BIS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating

the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- ✓ Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- ✓ Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- ✓ Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- ✓ Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section IV of this report titled, *Independent Service Auditor's Description of Tests of Controls and Results*.

Opinion

In our opinion, in all material respects:

a. The description presents BIS' compliance and learning management software that was designed and implemented throughout the period January 1, 2023 to December 31, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that BIS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of BIS' controls throughout that period.
c. The controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that BIS' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of BIS' controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of BIS, user entities of BIS' compliance and learning management software during some or all of the period January 1, 2023 to December 31, 2023, business partners of BIS subject to risks arising from interactions with the compliance and learning management software, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- ✓ The nature of the service provided by the service organization.
- ✓ How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.

- ✓ Internal control and its limitations.
- ✓ Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- ✓ User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- ✓ The applicable trust services criteria.
- ✓ The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

linford&co llp

January 27, 2024
Denver, Colorado

Section II – Assertion of BIS Management

January 27, 2024

We have prepared the accompanying description of BIS Safety Software Inc.'s (BIS or the Company) compliance and learning management software titled, "BIS' Description of Its Compliance and Learning Management Software" throughout the period January 1, 2023 to December 31, 2023 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the compliance and learning management software that may be useful when assessing the risks arising from interactions with BIS' system, particularly information about system controls that BIS has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

BIS uses the subservice organization, AWS, to provide hosting services and uses the subservice organization, Microsoft O365, for digital file storage, authentication enforcement, and end-point management.

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BIS, to achieve BIS' service commitments and system requirements based on the applicable trust services criteria. The description presents BIS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BIS' controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BIS, to achieve BIS' service commitments and system requirements based on the applicable trust services criteria. The description presents BIS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of BIS' controls.

We confirm, to the best of our knowledge and belief, that:

a) The description presents BIS' compliance and learning management software that was designed and implemented throughout the period January 1, 2023 to December 31, 2023 in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that BIS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of BIS' controls throughout that period.
c) The controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that BIS' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of BIS' controls operated effectively throughout that period.

Statement of Confidentiality

This document is the property of BIS and contains information that is confidential and proprietary. This information shall not be disclosed by the party to whom it is directed, and shall not be duplicated, used, or disclosed, in whole or in part, for any purpose other than to evaluate this document. The recipient of this document, by its retention and use, agrees not to disclose this document to any other party and to protect the same, and the information herein from loss, theft, and compromise.

Disclosure of this information to third parties may cause damage to BIS' commercial interests.

The ideas and concepts presented in this document are claimed by BIS as intellectual property, and, as such, are subject to the above stated restrictions of use.

Dan MacDonald
President

Section III – BIS' Description of Its Compliance and Learning Management Software

Overview of the Organization

Headquartered in Alberta, Canada and founded in 2006, BIS is a compliance and learning management software firm. BIS is a leader in learning and compliance software solutions that enable businesses to have an integrated learning management system, training record management system, equipment management system, digital document and form system, and performance and compliance reporting system in a centralized, accessible online platform. The BIS team is dedicated to delivering leading edge learning and compliance software and integrating the software seamlessly into its client systems and processes, enhancing the customer experience and driving growth.

BIS' proprietary enterprise-level learning and compliance technology provides an all-in-one solution for industries that require a high level of safety and compliance including manufacturing, construction, energy (electricity, hydrocarbon, oil sands, and infrastructure), mining, transportation, and government. The solutions that BIS provides help its clients develop, manage, and maintain safety programs to drive engagement and compliance with their employees, customers, product and service providers, and partners.

With the use of BIS' software, environment, health, and safety professionals and company managers can access classroom, online, and field-level training to build and foster an exemplary safety culture that is crucial for the sustainability of any high-stakes business. BIS brings together people, data accessibility, and solutions to provide greater value for its clients and customers in a rapidly evolving digital world.

Description of BIS' Services

BIS' compliance and learning management software has been developed through ongoing feedback, engagement, and collaboration with its clients to produce a solution that its clients need to manage workplace health and safety. The software helps companies to prevent incidents by providing rich, engaging training experiences to enhance learning and understanding of safety concepts and helping companies to provide the right safety training to their employees and contractors for their job responsibilities and tasks. These companies who are clients of BIS are referred to as "User Entities" or collectively as the "User Entity" throughout this report.

BIS' compliance and learning management software is a cloud-based SaaS platform called BIStrainer with an integrated Android/iOS compatible mobile app called SafeTapp. Through this software technology, clients can implement and sustain a robust, effective safety program within their facilities and field sites. BIS works with its clients to integrate the BIStrainer platform and SafeTapp mobile app into their core business intelligence systems, digital assets, and other software systems to provide a long-term, effective, and adaptive solution to the ongoing field-level, operational, social, and environmental challenges of a business. BIStrainer also provides automated notifications and reporting dashboards to assist companies

with tracking their compliance with their operational regulations. BIS' compliance and learning management software was developed to fit clients' needs in order to meet their day-to-day requirements and achieve their long-term safety vision.

BIStrainer is a cloud and app-based SaaS platform with various integrated modules:

- Learning management system (LMS)
    - The LMS is a comprehensive online training system with an integrated e-commerce store to access thousands of third-party training courses or private internal training programs, a course permission, and a management system, full shareable content object reference model (SCORM) compatibility, and a comprehensive exam engine.
    - There are application programming interface (API) and single sign-on (SSO) integrations, enterprise-level scalability, secure cloud hosting, mobile compatibility, and access to advanced reporting and analytics tools.
    - Through the LMS, companies can build and deliver orientation, onboarding, multi-level certification programs, and management training and leadership development programs.
    - The LMS features a seamless integration with a training matrix application, certificate generators, document uploaders, and customizable digital forms.
- Training record management system (TRMS)
    - The TRMS integrates with the LMS to build a centralized database of historical user training records, where certifications can be stored, tracked, and viewed from any training provider.
    - Training management and compliance performance reports and a training expiry notification system that allows companies to track whether their employees' and contractors' trainings are up to date.
    - Using the SafeTapp mobile app, companies can verify training records onsite immediately to ensure workers satisfy all the necessary training requirements.
- Classroom calendar management system
    - The classroom calendar management system integrates seamlessly with the LMS and digital forms features for blending online learning, field competency assessments, and practical training.
    - The management system includes classroom calendar functionality that allows training providers and companies to manage and provide internal and external instructor-led training for their employees and customers both virtually and in person.
    - Classroom training management allows for coordination and management of training resources, such as instructors, facilities, materials and classroom registration requirements or restrictions.
- Digital form system
    - Digital forms provide a cost-effective and reliable technology for companies to build, edit, and send important employee and contractor safety-related forms that can be completed online, offline, and remotely.

  - Digital forms can be customized and executed in stages to align with each company's unique internal workflow processes, or a series of forms can be assigned to be completed based on a triggering event.
  - Companies can create, complete, and store digital forms for incident investigations, site audits, field-level hazard assessments, pre-trip inspections, human resources documentation, equipment maintenance, and any other forms a company may need.
- Folders system
  - Companies can efficiently and reliably store, view, organize, and distribute documents, forms, and materials to employees, customers, and contractors through a digital folder system.
  - The digital folder system can also be configured to collect acknowledgments and signatures on documents that are assigned to users, including confidentiality, harassment prevention, cell phone best practice, and more, depending on a company's needs.
- Asset management system
  - Companies may manage assets through the equipment management module, which provides a centralized, online hub for storing equipment information, maintenance requirements and history, procurement and replacement requirements, and other essential equipment documents.
  - The equipment management system integrates seamlessly with digital forms to automate the scheduling, assignment, collection, and storage of documentation, such as inspections and assessments.
  - The equipment management software allows employees from all levels of a company's organizational structure to access and maintain asset information.
- Task administration system
  - Integrated with digital forms, companies can schedule and assign tasks to employees and track them efficiently to ensure critical activities are carried through to completion.
  - Task administration helps companies ensure that critical inspection, maintenance, and other activities are performed on assets.
- Site access management system
  - Companies can monitor access to physical sites and establish site-specific training requirements.

BIStrainer is customizable to meet each company's specific needs through the selective activation of these system modules and additional features as follows.

Effective features in BIStrainer can be applied to enhance the performance of system modules, such as:

- Training Matrix
- Exam Engine/Competency Assessments
- Reporting/Analytic Dashboards and Excel Reports
- Event Management
- Driver Management System
- Virtual Proctoring

- Lone Worker Check-in System
- Health & Safety Audit System
- Incident Management System
- Toolbox Talks
- Employee Reward System
- Datasets
- Project Management System

Components of the System Used to Provide the Services

The systems used by BIS to deliver BIStrainer are comprised of a combination of components that not only includes the products (services provided by BIS) and the data processed, but also extends to the underlying infrastructure, subservice organizations' services supporting the platform, the Company's employees and contractors, and the best practices and procedures followed to maintain the security of BIS' services and client data. The following is a summary of the components that comprise the system. Specific processes and controls relevant to the security criteria are described in the remainder of this section of the report.

Subservice Organizations: BIS uses subservice organizations to help achieve operating efficiency and obtain specific expertise. BIS uses AWS to host its application production environment. BIS configures its AWS environment to maintain portions of the logical security surrounding its system and data and perform data backup, retention, and recovery. BIS uses Microsoft O365 for digital file storage, authentication enforcement, and endpoint management.

AWS and Microsoft undergo annual PCI DSS and SOC 2 examinations. Attestations of compliance may be obtained directly from them. BIS obtains the PCI DSS and SOC 2 attestations of compliance provided by its subservice organizations related to the services provided to verify they have controls that are designed and operating effectively within their environments.

Infrastructure: BIS has a hybrid workforce in addition to its physical head office. The head office does not store physical IT hardware for the application production environment because BIS relies on the subservice organization, AWS, to provide IT infrastructure resources. The subservice organization, Microsoft, provides IT infrastructure resources for BIS' internal Company network and endpoint management. BIS computing infrastructure includes network devices, servers, domain controllers, routers, firewalls, and switches, which are hosted by AWS. The architecture of the AWS environment is designed specifically to protect the security of BIS' client data, and position resources in a secure and redundant environment to minimize risk and downtime.

Software: The BIStrainer compliance and learning management software is a SaaS platform that is developed and maintained by BIS' own team members and long-standing contractors. The software development team enhances and maintains BIStrainer to provide the system and future enhancements to its clients. Access to the BIStrainer is governed by the principle of least privilege and administered by BIS. Clients are responsible for managing, administering, and securing their environments. Additionally, clients

administer the access for the users from their organization and for the security of those devices used to access BIStrainer. Complementary user entity controls are noted within this description (Section III) to highlight control activities that BIS believes should be considered and/or present with each client.

People: The direction of BIS is guided by its Leadership team, and the BIS team is comprised of skilled, specialized members in Technology, Customer Experience, Client Success, Course Development, Sales, Marketing, People & Culture, Legal, and Accounting. BIS recruits and retains talented and passionate employees and contractors, herein referred to as "team members," based on resource requirements and the People & Culture team onboarding and hiring processes. The People & Culture onboarding and hiring processes facilitate the hiring of team members who exemplify BIS' core values and contribute to the success of BIS' mission and vision.

Team members work and collaborate within functional areas defined by BIS, so that client services are delivered efficiently and in a timely manner. BIS has implemented various information and communication channels to exchange data in order to help team members understand and fulfill their roles and responsibilities related to internal control within the organization.

Data: BIS provides clients with control over the information and data they add, upload, import, store, request, require, transmit, and maintain for any user in their portal. Client data is held securely and protected in accordance with safeguards, information integrity measures, system redundancies, access controls, hardware and software disposal practices, change management processes, and risk mitigation strategies. Client data is not processed outside of the AWS environment. The data housed in BIS systems includes any information, data, or files, regardless of form or format, uploaded or imported into or created within BIStrainer directly through the client's portal, including information related to the client itself and its users. Data in BIStrainer also includes any personal information derived from any source other than those uploaded or imported directly into client portals and any shared data.

In BIS client agreements, BIS also offers its clients with client-specific data requirements which are defined in BIS client agreements, if necessary. BIS establishes definitions with clients for confidential, private, and shared data within BIS client agreements. These agreements make explicit confidentiality and privacy practices required between the clients and BIS. BIStrainer provides security tools to clients to protect data of their choosing. Client data within BIStrainer is encrypted at rest. Additionally, data transfers between users and BIStrainer are secured using Transport Layer Security (TLS) and industry-standard encryption.

Processes and Procedures: BIS strives to define, implement, and continuously improve company-wide best practices and procedures, referred to as "best practices." The best practices make clear the conduct and actions of team members in carrying out their tasks and roles, holding paramount the security of BIS and client data. The best practices are made available to team members in company or department playbooks, training programs, and procedure documents, which are available on BIS' SharePoint site or in the team member's compliance and learning management software account for reference. BIS requires team members to review the best practices applicable to their role during the onboarding process and through continuous training and awareness sessions. BIS has established and maintains security policies and

procedures, also known as best practices, over its compliance and learning management software covering the following areas:

- Access control
- Security incident management
- Encryption
- System security
- Information security
- Business continuity
- Code of conduct
- Technology use
- Backup
- Password management
- Data classification
- Data deletion/destruction
- Risk assessment
- Change management
- Vendor management

BIS makes these internal best practices, including security best practices, available to its team members to provide direction regarding their responsibilities related to the functioning of internal control. The processes and the controls within them, pertinent to the applicable criteria, are documented throughout the remainder of this description.

Principal Service Commitments and System Requirements: BIS designs its processes and procedures to meet objectives for its compliance and learning management software. Those objectives are based on the service commitments that BIS makes to clients and the compliance requirements that BIS has established for their services.

Security commitments to clients are documented and communicated in their client agreements. Security practices are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of BIStrainer are (1) implemented to permit system users access to the information they need based on their role in the system while restricting them from accessing information not needed for their role, and (2) designed to allow clients to control and restrict access to system modules and features by its users through various system user roles, which are assigned based on the needs of their role.
- Controlled access to the production application and the supporting infrastructure.
- Segregation of client data.
- Data backups on secured private networks.
- Monitoring of system performance metrics and critical application services.

All users must agree to BIS' privacy policy and terms and conditions prior to accessing BIStrainer. The privacy policy and terms and conditions are published on all BIS websites and made accessible on BIStrainer login pages, within user accounts, and in various other webpages in BIStrainer.

BIS establishes operational requirements that allow it to achieve and uphold its security commitments and other system requirements. Such requirements are communicated in BIS' system best practices and procedures, system design documentation, and client agreements. Various best practices and processes,

such as technology use, define a company-wide approach to how systems and data are protected. These include best practices around how the service is designed and developed, how BIStrainer is operated, how the internal networks are managed, and how team members are hired and trained.

(The remainder of this page is left blank intentionally.)

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities for the Security Criteria

Note: Parenthetical references have been included in the following narratives as a cross reference to the applicable control activities included in Section IV of this report.

A company's entity-level controls reflect the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the Company's best practices, procedures, methods, and organizational structure. Entity-level controls are not specific to any individual transaction but apply to the Company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting BIStrainer.

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them protect the system against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report, and in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results.*

Control Environment

The control environment is the umbrella under which all of the control components of internal control fall. The control environment at BIS includes "tone at the top," which the Leadership team sets by example in adhering to ethical business practices and company best practices and by conducting business with integrity. The Leadership team's example and direction are the primary mechanisms used to guide team members in the execution of BIS' operations. The control environment is the collective responsibility of the BIS Leadership team, as well as managers and team leads of various departments.

Integrity and Ethical Values: The cornerstone of ethics and compliance at BIS is the code of conduct. The code of conduct provides guidance towards reaching decisions that are legal and ethical. The code of conduct is complemented by additional best practices, which are also communicated to and accepted by team members during the onboarding process. The best practices at BIS include, but are not limited to, the confidentiality and intellectual property; harassment, sexual harassment, and violence; and technology use agreements. Changes to company best practices are communicated during meetings or through email, and the most up-to-date versions of the best practices are made available on BIS' SharePoint site for ongoing reference.

The organizational core values and behavioural standards at BIS are built into the day-to-day activities. The Leadership team, managers, and team leads lead by example and encourage ethical behaviour in every aspect of the business. BIS has documented information security best practices within a company resource book, and a code of conduct that identifies expectations and core values, which are acknowledged by new team members upon hire **(1.1)**. Integrity and ethical values are emphasized during the hiring and onboarding

process. These values are also documented in the Company team member agreement, which is reviewed and acknowledged by individuals when they join BIS.

Leadership Team: The Leadership team stays abreast of needs and challenges facing the Company through their involvement in day-to-day operations. The Leadership team maintains oversight of BIS' strategic direction, operational performance, and internal control, meeting at least monthly **(1.2)**. The Leadership team plays an important role in the oversight and governance of the Company. They also help monitor that the Company is operating within established parameters and is complying with sound business practices.

Management Philosophy and Operating Style: The Leadership team, managers, and team leads understand the importance of oversight and governance and believe that this is best accomplished when they are highly involved in the day-to-day operations of BIS. In this environment, they are able to address business issues in a timely manner and, consequently, reduce risks to the Company and its valued clients.

Organizational Structure: A properly defined organizational structure is critical for operating a sound control environment. BIS' organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities **(1.3)**. In addition, lines of authority are clearly established throughout BIS. These lines of authority are communicated through the operational style of managers and team leads, the organizational structure, and team member position profiles (job descriptions). The organizational structure is documented and defines functional responsibilities and lines of authority throughout BIS. To increase the operational effectiveness of team members within this structure, BIS maintains position profiles for all team members so that individuals understand and perform their responsibilities effectively **(1.4)**.

Onboarding: The People & Culture team has defined formal onboarding practices and guidelines that assist in selecting qualified and talented applicants for specific job responsibilities that meet identified company needs. Hiring practices require minimum education and experience based on position and job requirements. Depending on the role, additional background screening, verification and reference checks, and specifically designed skills tests may be conducted to help determine that the candidate's experience and skills are accurately presented. BIS has a culture that encourages team members to enhance their skillset, solicit feedback, and provide a long-term horizon for development.

Competency Checks: BIS' hiring practices are designed to facilitate the hiring of competent team members in order to provide clients the highest quality of services. When a position is open at BIS, a job description and listing are created and posted on various job forums, and potential applicants are searched for through business-related networking sites. Resumes of applicants are received and reviewed by the People & Culture team, team leads, and managers. Applicants who pass the initial resume review are invited to participate in a number of interviews based on the position they are applying for. In order to assess the competence of potential applicants, BIS conducts a skills assessment during the employment evaluation process **(1.5)**.

Background Checks: After the necessary competency checks are complete, BIS maintains templates of applicable offer letters for candidates that includes at-will employment language depending on the role and

physical country location of the candidate **(1.6)**. The applicant will sign off on the offer letter in person or via a scanned email attachment stating they agree to the best practices provided by BIS. The BIS People & Culture team conduct reference checks for all applicants selected for full time employment, and they conduct background checks on US-based team members **(1.7)**. For US applicants, criminal, employment, and educational checks are performed. Team members and applicable contractors are required to follow to and acknowledge the technology use best practices and the confidentiality and intellectual property agreements during onboarding **(1.8)**.

Onboarding Training: BIS team members are required to attend security awareness training during the onboarding process within one month of their start date and annually thereafter **(1.9)**. The security training is prepared and updated regularly by the IT team, a third-party vendor who operates under the oversight and responsibility of BIS, and includes current and relevant BIS security risks and concerns.

Performance Reviews: Team member development meetings, referred to as touchpoint meetings, are conducted with all BIS team members by their team leads and/or manager, and on occasion, a member of the Leadership team as needed. Also, the Leadership team, managers, and team leads conduct performance evaluations of their team members and discuss the team members' strengths and areas of improvement **(1.10)**. The cadence of performance reviews is defined by the Company based on the team members' role. Reviews are completed within one year of hire and annually thereafter for team members and within two years of hire or their last review for team leads and Leadership roles. Team members are provided feedback on their performance and actionable steps for growth, and a plan is maintained for team member skills development. BIS evaluates team members' performance against defined standards of conduct and performance measures. Disciplinary actions may be taken up to and including termination of employment.

Information and Communication

The information and communication component of internal control consists of procedures designed to initiate, authorize, record, process, and report transactions affecting BIS' clients. To assist with this aspect of internal control, the Leadership team has implemented information systems that are used to provide services to clients. The Leadership team's ability to conduct operations with efficiency and precision is partially contingent on the timeliness and accuracy of the information that they receive from these systems. BIS' systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls **(2.1)**.

Information and communication controls also consist of procedures designed to provide company team members with an understanding of their roles and responsibilities pertaining to day-to-day operations. BIS has implemented various communication methods used to exchange data to help team members understand and fulfill their roles and responsibilities related to internal control within the organization. In addition to best practices and procedures, BIS uses internal communication tools and methods that are used for collaboration and communication including responsibilities related to security. Communication with team members is maintained using the Company's SharePoint network, emails, weekly company meetings, and announcements made on Microsoft Teams. The communications include, but are not limited to,

communication of BIS best practices, company events, system changes and upgrades, new initiatives, and awareness and training on security and availability of information. Important company events, team member news, and cultural updates are communicated using email and Microsoft Teams announcements, as well as in team lead meetings and company-wide meetings.

Security updates relevant to all team members are announced via communication tools or by the Leadership team during recurring Monday morning meetings. The Monday morning meetings are recorded in a spreadsheet accessible to all team members on SharePoint **(2.2)**. BIS maintains security best practices, which highlight important internal controls that strengthen BIS' overall control environment. BIS SharePoint and Teams are central repositories of best practices, methodologies and tools, documentation, training, and development materials. BIS maintains security best practices to communicate security responsibilities to team members and these best practices are maintained within the BIS Playbook that is accessible to all team members on SharePoint **(2.3)**.

BIS has an organizational reporting structure with clear reporting lines and authority hierarchy, which delineates roles and responsibilities **(2.4)**. New team members, are required to sign a Confidentiality and Intellectual Property agreement and a technology use agreement as part of the onboarding process. The Confidentiality and Intellectual Property agreement prohibits any disclosure of confidential information and any other data to which team members have been granted access. The technology use agreement defines legal, ethical, and professional use of work resources and related technology. These agreements are communicated to the BIS team through BIStrainer as part of the onboarding process and made available in the Resource Book on BIS' SharePoint. See the *Control Environment* section for additional details. Managers and team leads are involved in the day-to-day operations and provide additional guidance as needed.

BIS maintains communications with its clients using email, third party software, the BIStrainer Project Management (PM) tool, and system notifications from BIStrainer. Other important information is made accessible on the BIS public website or directly through BIStrainer. BIS has created a high-level overview of the BIS infrastructure and systems used to describe the services provided to the clients that it serves on its website **(2.5)**. This information is included on its website at https://trainanddevelop.ca/.

Complementary User Entity Controls: *User Entities are responsible for making sure that data, including personal information that they maintain within BIStrainer, is protected for privacy using the available security tools BIStrainer provides.*

BIS has a client service level agreement (SLA) and defined its terms of service that together contains information regarding the design and operation of the system and its boundaries, as well as acceptable use of the system **(2.6)**. The terms of service are implicitly accepted as part of accepting the service and cover service terms, acceptable use, and security. To assist with BIS' commitments to security, BIS management provides annual security awareness training for all team members that covers information security-related topics and tracks the completion of training **(2.7)**.

Complementary User Entity Controls: *User Entities are responsible for complying with their agreements with BIS.*

For external users, the Company website and the SLA describes the process for reporting operational failures, incidents, problems, and concerns. For BIS team members, issue reporting procedures are documented within the incident management best practices **(2.8)**. BIS team members may communicate with their team leads, managers, and members of the Leadership team during their daily activities or by email. Additionally, team members may escalate concerns directly to the Technology team manager. The Technology team is comprised of the software development group.

Each client has a Client Success representative they may contact to address any questions or concerns during the client onboarding process and an Account Manager that they may contact thereafter. Their contact information is provided to the client as part of the launch process. Additionally, clients may contact BIS via email or telephone using the contact information included on BIS' public website and on the Help & Support page within BIStrainer.

The Leadership team has a process to communicate security or privacy changes to external users, related parties, and vendors, as needed **(2.9)**. For additional information on communicating system changes, see the *Change Management* section.

Risk Assessment

An organization's risk assessment process is its identification, analysis, and management of risks relevant to its platform and services. The Leadership team and their designees are responsible for performing ongoing risk assessments. Risk management is a key component of BIS' governance and operations. BIS approaches risk management strategically and takes measures to reduce risk as low as reasonably practicable and undertakes contingency planning if critical risks are realized. BIS is committed to the health and safety of the BIS team and any other persons at the workplace.

The BIS team, including the Leadership team, managers, and key team members contribute to the establishment and implementation of the risk management processes for all functions and activities of BIS. BIS' risk management practices work to align with national, regional, and local requirements, as well as accepted industry best practices. Risk management results are used to form parts of the strategic, operational, and team lead and manager responsibilities. The results are integrated into strategic and service planning, as well as BIS' best practices, supporting team members with their efforts towards contributing to risk management.

The BIS risk management processes involve four steps:

- Identifying Hazards: Potential causes and sources of harm, damage, and any negative consequences.
- Assessing Risks: The severity of consequences and likelihood of their occurrence.

- Controlling Risks: Implementation of the most effective controls and measures that are reasonably practicable.
- Reviewing Control Measures: Ongoing monitoring of control and risk mitigation performance.

The BIS Leadership team performs and maintains a formal risk assessment and treatment plan that includes the framework for identifying and assessing the key risks related to the Company and outlines the approach to identifying, assessing, mitigating, and monitoring risks **(3.1)**.

The Leadership team performs a formal risk assessment annually, and the risks identified are formally documented and monitored **(3.2)**. The risk assessment includes, but is not limited to, the evaluation of infrastructure, people, procedures, software, safeguarding of data, and third parties. Relevant and necessary participants are present to comprehensively identify potential risks, and the risk assessment identifies the key roles and responsibilities in risk management **(3.3)**.

The risk assessment and treatment plan documents the Company's considerations related to fraud risks, natural risks, technical risks, physical risks, environmental risks, regulatory risks, and vendor risks **(3.4)**. Participants in the risk assessment consider threats that include, but are not limited to, malicious intent, natural disasters, technical issues, hardware and software concerns, and physical theft. Risk controls currently in place are also reviewed during the risk assessment process to determine their ongoing effectiveness.

Key business and operational risks are closely monitored, particularly those related to the security of BIS' production environment, as these are especially critical risks that have the potential to affect the services provided to its clients. BIS reduces and mitigates business risks by evaluating and applying necessary controls, leveraging industry best practices where applicable and practicable.

The risk assessment plan guides the risk assessment participants to consider the various types of impacts that each risk may pose to BIS. BIS management considers obstacles and threats that may prevent the achievement of meeting business objectives, commitments, and requirements when documenting and rating the risks. Each risk is assessed and given a risk rating in relation to the potential impact on the Company and its services **(3.5)**. Risks are mapped to mitigating factors that address some or all the risk. Vulnerabilities identified as part of the risk assessment process are prioritized and remediated based on the assessed risk, as part of the BIS risk assessment program. Remediation activities are reviewed and approved by the Leadership team and an owner is assigned for each remediation plan **(3.6)**. The risk assessment is documented and stored on BIS' SharePoint for recordkeeping.

BIS' best practices and procedures take into consideration the business and IT risks noted within the risk assessment **(3.7)**. The best practices and procedures address the following: vendor management, business continuity, network security, incident management, risk management, physical security, end-point security, and information security. Team members are required to review applicable best practices relevant to their responsibilities, some of which are part of their onboarding, so that they understand their responsibilities

and are willing to comply with them. Refer to the *Control Environment* section for more details related to best practice acknowledgements during onboarding.

BIS informs its team members on how to report potential risks, security incidents, and concerns. Refer to the *System Operations* section for more details related to incident reporting. Individuals may share these concerns in person or via email with their team leads or managers, as well as escalate them if needed to the Leadership team if their team lead or manager is unavailable. Significant risks or concerns raised by team members are added to the risk matrix and assessed. Accordingly, the risk assessment is updated periodically to take into consideration relevant changes in BIS' operations and relevant risks raised within the organization **(3.8)**.

Monitoring of Controls

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. The Leadership team has implemented tools, such as the Project Management module within BIStrainer, and mechanisms to ascertain that any potential problems within the organization are identified and resolved. The Leadership team delegates responsibilities for monitoring the quality of the products and services provided to clients and regularly engaging with client contacts to obtain feedback and establish that their needs are met in a timely manner.

Application and Infrastructure Monitoring: Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity **(4.1)**. Monitoring software is configured to send automated notifications **(4.2)**. When alerts from the tools are received, team members assess them and take appropriate action to resolve them. To maintain the stability and availability of the infrastructure environment, BIS monitors key performance parameters, such as CPU utilization, memory, and response times on the production system, and is notified when such parameters exceed configured thresholds **(4.3)**.

External Vulnerability Assessments: BIS has a third-party application penetration test performed on an annual basis. The vulnerabilities identified in the penetration testing for BIStrainer are reviewed by the Technology team manager and high/critical vulnerabilities are resolved **(4.4)**.

Internal Vulnerability Assessments: Internal vulnerability scans are initiated by BIS and performed on BIStrainer at least quarterly and performed on the corporate network at least annually. The vulnerabilities identified in the quarterly vulnerability scans for BIStrainer are reviewed by the Technology team manager and high/critical vulnerabilities are resolved **(4.5)**. The vulnerabilities identified in the annual vulnerability scans for the corporate network are reviewed by the IT team and tracked to resolution **(4.6)**. These evaluations identify missing security updates and common security misconfigurations that might lead to the exposure of sensitive information or result in otherwise unauthorized systems access.

Third-Party Monitoring: BIS engages a third-party auditor to perform a security audit annually. A Type II SOC 2 audit under the security trust services criteria is performed by an independent auditor, who prepares a report for distribution to BIS' clients. Additionally, relevant team members, including the Technology team member, review compliance reports from the subservice organizations to determine whether controls upon which BIS relies are operating effectively **(4.7)**. The review assesses whether adequate controls are in place at subservice providers to meet BIS' service commitments and system requirements.

Control Activities

BIS selects and develops control activities that help mitigate, to acceptable levels, risks to the achievement of objectives. Control activities include a variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls as well as preventive and detective controls.

BIS maintains best practices and procedures and documents operating technology standards and procedures to provide its team members with a centralized, up-to-date reference and training aid. The Leadership team, with the support of managers and team leads, have established and implemented best practices and procedures so that periodic assessments and evaluations are performed that consider elements of security as they apply to the AICPA trust services criteria. BIS communicates findings, remediation options, and recommendations to key stakeholders. BIS has developed best practices that establish expected behaviour **(5.1)**. The best practices include control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the Company's assets from external threats. BIS Leadership segregates responsibilities and duties **(5.2)**.

BIS has defined and approved best practices and procedures that address control processes and company risks **(5.3)**. BIS utilizes an internal project management software tool to communicate internal control deficiencies in a timely manner to Leadership and enable cross-functional teams to take appropriate corrective actions **(5.4)**.

Logical and Physical Access

User Access Administration: BIS has developed a user access best practice and an accompanying process to register and authorize team members and contractors prior to being issued system credentials and granted access the system. Under the direction of Leadership, the People & Culture team utilizes checklists for onboarding new team members and offboarding terminations to determine that all necessary control steps and IT system access considerations are tracked and completed **(6.1)**. This process is guided by the principle of least privilege.

Account Management: New team members are granted access using a "learner" system user role within BIStrainer. Once established within their department, additional access is granted based on job responsibilities by providing additional system user roles with higher levels of access. When a team member is hired, the People & Culture team communicates access requests to the IT team, who is a third-party vendor that manages SharePoint and Office 365 access. The Leadership team, team leads, or managers must

approve additional access for team members that report to them before the IT team provides the requested access. Access to AWS is approved and managed by the Leadership team and the Technology team manager at BIS. Access requests and associated approvals are tracked using BIStrainer. Documented approval is obtained for team members prior to being granted access to the environment **(6.2)**. BIS team members are granted access to BIStrainer according to their role and team **(6.3)**.

Complementary User Entity Controls: *User Entities are responsible for protecting established usernames, passwords, security keys, and other credentials within their organizations.*

BIS performs user access reviews periodically to assess the appropriateness of their team members' and contractors' access and privileges within BIS. The responsible team will conduct periodic reviews of user accounts and privileges in BIStrainer and follow-up, as needed **(6.4)**.

Complementary User Entity Controls: *User Entities are responsible for managing and reviewing user access to BIStrainer and periodically validating their users' access levels to make sure permissions are appropriate for their tasks and roles.*

In addition, BIS has a process to monitor that access is removed when a user is terminated. For terminations, the People & Culture team completes termination tasks which include tasks to remove logical and physical access. A terminated team member's system and physical access is removed in a timely manner **(6.5)**.

Administrator Access: Full administrative system access to the production system is only granted to appropriate individuals after successful completion of training and onboarding. Only the President and Technology team manager can grant full administrative system access. Administrator-level access privileges are restricted to only those individuals who require such access to perform their respective job functions **(6.6)**.

Complementary User Entity Controls: *User Entities are responsible for provisioning and removing access to their BIStrainer portal by only those individuals who are authorized.*

Client Segregation: BIStrainer is a multi-tenant SaaS application. Within the databases, client data is logically separated such that users from one client cannot access data from another client. In BIStrainer, data is associated with unique client identification (ID) codes and the software checks the ID codes when users perform actions. BIStrainer prevents users from accessing data if the client ID codes do not match the ID code of the portal the user is located in. Technical implementations are in place to maintain segregation of client data within the database **(6.7)**.

Access to Client Data: Access to client data within the production database is restricted to authorized users **(6.8)**. Role-based access control (RBAC) governs the actions that users can execute within the BIStrainer production database.

Password Management: BIS has a system control that defines password standards for access to BIStrainer and its infrastructure **(6.9)**. BIS has a system control that enforces multifactor authentication (MFA) for access to BIStrainer and its infrastructure **(6.10)**.

Physical Access: BIS' head office is located in Sherwood Park, Alberta, Canada. Team members with access can opt to use a physical proxy card or a mobile application to access the building. Team members with access to the office are restricted to active employees and contractors **(6.11)**.

End-point Protection: BIS' best practices require workstations to have appropriate end-point protection. Malware detection software is deployed on workstations **(6.12)**. BIS applies security patches to user workstations, so at any given time, workstations are on supported operating system versions **(6.13)**. To minimize the risk of data being compromised in the event hardware or data is lost or stolen, workstations are encrypted **(6.14)**. Workstations are configured to automatically log out after a modest period of inactivity **(6.15)**.

Inventory of Information Assets: BIS maintains an inventory listing of information assets in order to identify and implement controls to protect them from security events **(6.16)**.

AWS Security Groups: To protect the production environment, security groups are configured for servers within AWS, which limit access to specified ports and IP addresses **(6.17)**.

Firewalls: A firewall is applied to servers on both the corporate network and application environment. In the application environment, firewalls are configured to restrict inbound traffic **(6.18)**. Access to modify firewall rules and security groups are restricted to appropriate team members **(6.19)**.

Encryption in Transit and at Rest: BIS understands the sensitivity of its clients' data and has, therefore, implemented security controls to protect the confidentiality of the data. Data transfers between clients and BIStrainer are secured using TLS and industry-standard encryption **(6.20)**. Client data within the production database is encrypted at rest **(6.21)**.

Complementary User Entity Controls: *User Entities are responsible for the security and integrity of their transmission facilities, operating facilities, and equipment that are used to access BIStrainer.*

Data Destruction and Disposal: Procedures are in place to establish that all hardware (i.e. hard drives, laptops) is securely wiped prior to being removed from company ownership **(6.22)**.

System Boundaries: BIS establishes the boundaries of the environment by maintaining an architecture diagram **(6.23)**.

System Operations

Incident Response Program: BIS' security incident management protocol establishes the procedures to be undertaken in response to information security incidents **(7.1)**.

The best practice addresses the phases of incident response:

- Detection and assessment of security risk severity
- Establishing and enforcing a plan of action
- Containment and elimination of vulnerabilities
- Mitigation of future risks
- Communication to relevant parties
- Investigative analysis to determine additional potential risks
- Establishing long-term strategies from investigation and lessons learned

It also identifies the incident response team, their associated roles and responsibilities, and communication protocols. The security incident management protocol is updated at least annually **(7.2)**. If an incident occurs that needs to be communicated to clients, updates about the incident are communicated with established contacts.

In years that security incidents do not occur, BIS conducts a test of the security incident management protocol and the ability of the Incident Response team to execute the plan on an annual basis and documents the test procedures and test results **(7.3)**. Gaps, areas of improvement, and lessons learned are utilized to modify the plan, as needed.

Incident Monitoring and Recordkeeping: BIS maintains a record of security incidents which defines root cause(s) of the incident and provides relevant information to prevent reoccurrence of the security incident. A log of all security incidents is maintained in a Risk and Compliance SharePoint document library **(7.4)**. Security incidents are tracked within a folder that only the Leadership team, Legal team, and Risk and Compliance team members may access. The incident records include the following: a) a description of the incident and relevant facts (e.g., information that was disclosed), b) mitigations, c) root cause, d) immediate and long-term resolution, and e) lessons learned.

Complementary User Entity Controls: *User Entities are responsible for notifying BIS promptly of any security incident or vulnerability that is discovered which may directly or indirectly affect BIStrainer.*

Complementary User Entity Controls: *User Entities are responsible for maintaining a data security and data privacy complaint and response process for capturing, tracking, and responding to their disclosing party's security and privacy concerns and issues.*

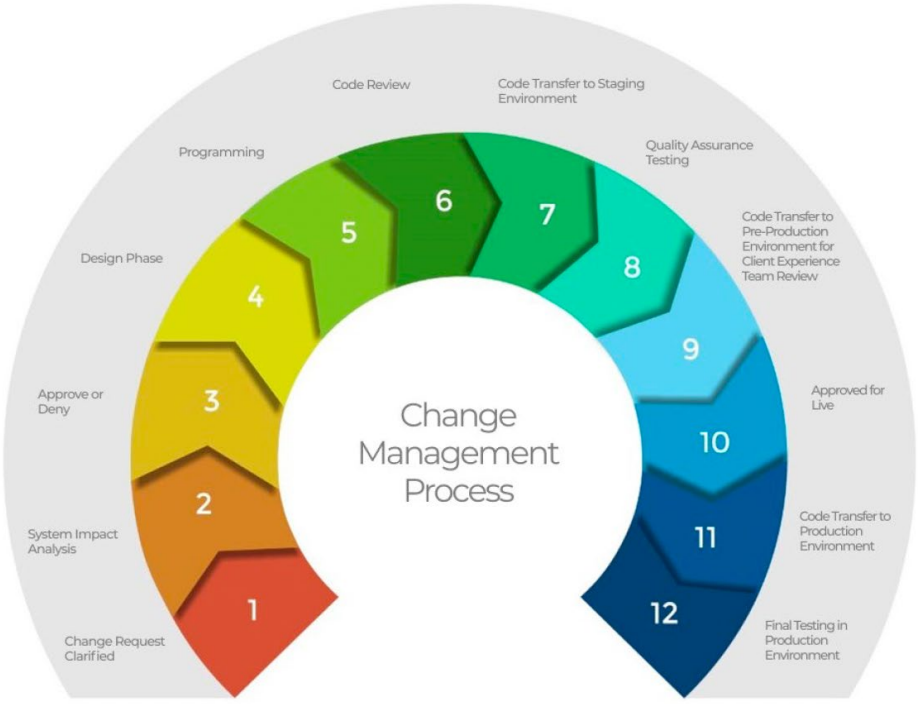
System Redundancy and Restores: Data is a critical part of BIS' compliance and learning management software, and BIS maintains suitable measures to protect data from accidental destruction or loss. BIS has

forms of system redundancy in place to prevent destruction and loss of data **(7.5)**. Backups of data are performed on a periodic basis to prevent the loss of client data **(7.6)**. To exercise backup and restore procedures, backups are restored regularly as part of operational activities. A backup of the Company data is also restored periodically **(7.7)**.

Infrastructure Patching: Infrastructure production servers are patched on a periodic basis to reduce the risk of compromise **(7.8)**.

Change Management

An effective system development and maintenance process is critical to the security of BIStrainer. BIS follows a defined change management best practice for making changes to the systems used to support the services provided to its clients. BIS' change management best practice describes how changes to BIStrainer and its infrastructure are proposed, reviewed, deployed, and managed **(8.1)**.



The BIStrainer change management process is a 12-step process detailed in the BIStrainer LMS Security Practice as summarized:

1. Change request initiated and clarified.
2. System impact analysis is completed for each requested change.
3. The change is approved or denied and communicated to stakeholders.
4. The design phase is completed.

5. Programming is performed by the software engineering team.
6. A code review is completed by a senior software engineer.
7. The code is moved to the staging environment for quality assurance (QA) and quality control (QC) testing and review.
8. Quality assurance testing is completed by the quality assurance and quality control team.
9. Code is moved to pre-production for the team members to review.
10. Upon successful review, BIS approves the update for the production environment (live).
11. Code is moved to the production environment.
12. Final testing is completed in the production environment, including quality control, quality assurance, client experience, and client testing (as necessary).

A request for a change can come any team member, including team leads and manager, or externally from a client. BIS Leadership uses a project management tool to manage and record activities related to the change management process **(8.2)**. The tool enforces version control and is used to document control points within the change management process. The tool facilitates the change management process; proposed or requested changes are assessed, prioritized, and approved at multiple stages of development, including prior to development and implementation. The project management tool allows for clear communication and monitoring of progress by stakeholders. Testing occurs during multiple stages in the change management process to mitigate risks. The Technology team uses a code development platform to manage and record activities related to the change management process **(8.3)**. To initiate a change, the developer first creates a feature branch with the updated code. When a code change is completed, the developer performs testing and submits the code for peer review. Separate development, QA, and production environments exist to support development, testing, and production **(8.4)**. Infrastructure and software changes are required to be tested prior to implementation. Depending on the complexity of the change, the testing includes evidence of peer review and QA activities **(8.5)**. The changes are implemented in the production environment after results of the final testing are approved.

Complementary User Entity Controls: *User Entities are responsible for testing and approving user requested changes in a timely manner to determine that the requested changes are designed and operating in the manner expected.*

Infrastructure and software changes are required to be approved for implementation by the Leadership team, key team members and the client requesting the change, as applicable **(8.6)**. The approval documentation required is structured based upon the complexity of the change. Once approved, the change is released to production. The changes are implemented and communicated to the BIS team and clients that will be affected. As a part of the change process, clients and BIS team members are notified of relevant changes deployed that may impact their services security or delivery to provide continued client awareness and understanding of the products **(8.7)**. The notification provides recipients an ability to review the details related to the deployed change. After implementation and communications, the change request is closed in the project management tool.

The change management best practice is designed to mitigate the risks of:

- corrupted or destroyed information
- degraded or disrupted computer performance
- project execution inefficiencies
- productivity loss
- introduction of new vulnerabilities, configuration errors, and software bugs in infrastructure and code
- exposure to reputation risk

In order to restrict and control changes being pushed to production, BIS applies strict requirements on team members with the ability to make changes. BIS restricts the ability to implement changes into the production environment to only those individuals who require this ability as part of their job function **(8.8)**. If users implement changes that are not in accordance with the BIS change management best practices, corrective actions up to and including dismissal are taken. Key members of the Leadership team periodically perform evaluations of the changes deployed to production to determine that appropriate changes are being made. BIS maintains immutable logs of all changes pushed to production for a minimum of a year **(8.9)**.

If an emergency change is identified as necessary, BIS addresses the risk of emergency changes, and BIS determines that the appropriate change management steps and procedures to follow. BIS has processes in place for emergency changes, referred to as the "Express Lane" change process. Express Lane changes are required to receive change approval, undergo QA, and testing, and have documentation of at least two software development team members involved with every change **(8.10)**.

Risk Mitigation

BIS follows a formal risk assessment process to identify, assess, and mitigate threats that may prevent the achievement of the Company's service commitments and system requirements. See the *Risk Assessment* section for BIS' process to identify and assess risks to the organization. The Leadership team and key team members determine whether an action plan is needed to reduce risks to acceptable levels by considering the mitigating factors already in place within the Company. The risk assessment team prepares an action plan for each item in the risk assessment matrix that has a risk level deemed unacceptable. Risk and Compliance team members review and track the status of open action plans to closure to prevent the risk from being realized. See the *Risk Assessment* section for BIS' process to identify and assess risks to the organization.

Subservice Providers Monitoring: BIS understands that risks exist when engaging in business relationships, and as a result, continuously considers those risks that could potentially affect the Company's ability to meet its internal and external business objectives.

The third-party management best practice provides a framework for managing the lifecycle of third-party relationships **(9.1)**. BIS maintains long-standing relationships with vendors to assist with elements of securing and delivering the services they provide to their clients. BIS manages their vendors effectively in a variety of ways. Risk and Compliance team members monitor and document their review of third-party

assurance reports from key third-party outsourced service providers on an annual basis **(9.2)**, which includes applicable vendor security reports. If a vendor is unable to provide a third-party security report or certification, BIS management provides the vendor with a security questionnaire to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix. BIS follows its standard risk assessment processes to assess and mitigate vendor risks. BIS maintains insurance coverage to protect against threats that may impact business operations **(9.3)**.

(The remainder of this page is left blank intentionally.)

Complementary Subservice Organization Controls (CSOC)

BIS' controls related to BIStrainer cover only a portion of the overall internal control for each User Entity of BIS. It is not feasible for the applicable trust services criteria related to BIStrainer to be achieved solely by BIS. Therefore, each User Entity's internal control must be evaluated in conjunction with BIS' controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations described as follows:

	AWS Complementary Subservice Organization Controls	**Related Control Criteria**
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.	CC6.4-CC6.5
2.	The subservice organization is responsible for managing and resolving security and availability incidents related to the data centre facility in a timely manner.	CC7.2-CC7.5
3.	The subservice organization is responsible for maintaining the availability of the hosted environments at any time, all year round.	CC7.1-CC7.2
4.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	CC7.1-CC7.2

	Microsoft Complementary Subservice Organization Controls	**Related Control Criteria**
1.	The subservice organization is responsible for providing the physical security controls protecting the Microsoft-managed AD services from unauthorized access.	CC6.4-CC6.5
2.	The subservice organization is responsible for providing the environmental controls protecting the Microsoft managed AD services.	CC7.2-CC7.5
3.	The subservice organization is responsible for maintaining the availability of the hosted environments at any time, all year round.	CC7.2-CC7.5
4.	The subservice organization is responsible for managing and resolving incidents and problems reported by BIS in a timely manner.	CC7.2-CC7.5

BIS' Complementary User Entity Controls (CUEC)

The compliance and learning management software, BIStrainer, provided by BIS for User Entities and the controls at BIS cover only a portion of the User Entity's overall system of internal control. It is not feasible for the applicable trust services criteria related to BIStrainer to be achieved solely by BIS. Therefore, each User Entity's internal control must be evaluated in conjunction with BIS' controls and the related tests and results described in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results* of this report, taking into account the related complementary user entity controls identified under each area, where applicable.

This section highlights additional control activities that BIS believes should be considered and/or present at each User Entity. Each User Entity must evaluate its own system of internal control to determine if the following controls are in place. This list is not intended to be, and is not a complete listing of, the controls that provide a basis for the achievement of the security control criteria.

	Complementary User Entity Controls	**Related Control Criteria**
1.	User Entities are responsible for making sure that data, including personal information that they maintain within BIStrainer, is protected for privacy using the available security tools BIStrainer provides.	CC2.2
2.	User Entities are responsible for complying with their agreements with BIS.	CC2.3
3.	User Entities are responsible for protecting established usernames, passwords, security keys, and other credentials within their organizations.	CC6.2-CC6.3
4.	User Entities are responsible for managing and reviewing user access to BIStrainer and periodically validating their users' access levels to make sure permissions are appropriate for their tasks and roles.	CC6.2-CC6.4
5.	User Entities are responsible for provisioning and removing access to their BIStrainer portal by only those individuals who are authorized.	CC6.2
6.	User Entities are responsible for the security and integrity of their transmission facilities, operating facilities, and equipment that are used to access BIStrainer.	CC6.7
7.	User Entities are responsible for notifying BIS promptly of any security incident or vulnerability that is discovered which may directly or indirectly affect BIStrainer.	CC7.4

	Complementary User Entity Controls (continued)	Related Control Criteria
8.	User Entities are responsible for maintaining a data security and data privacy complaint and response process for capturing, tracking, and responding to their disclosing party's security and privacy concerns and issues.	CC7.4
9.	User Entities are responsible for testing and approving user requested changes in a timely manner to determine that the requested changes are designed and operating in the manner expected.	CC8.1

(The remainder of this page is left blank intentionally.)

Section IV – Independent Service Auditor's Description of Tests of Controls and Results

Purpose and Objective of the Independent Auditor's Examination

This report on controls placed in operation is intended to provide users of the report with information sufficient to obtain an understanding of those aspects of BIS' controls that may be relevant to client's internal controls. This report, when coupled with an understanding of the internal controls in place at each client, is intended to assist in the assessment of the total internal control surrounding the compliance and learning management software, BIStrainer, provided by BIS.

Our examination was limited to those controls performed at BIS' Alberta, Canada, location. It is each stakeholder's responsibility to evaluate this information in relation to the internal controls in place at each client to obtain an overall understanding of the internal controls and assess control risk. The portion of controls provided by each client and BIS must be evaluated together. If effective control activities are not in place at the client, BIS' controls may not compensate for such weaknesses.

Our examination included inquiries of appropriate management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls for the suitability of design and operating effectiveness surrounding BIStrainer. Our tests of controls were performed January 1, 2023 to December 31, 2023 and were applied to those controls relating to the applicable trust services criteria.

The description of controls is the responsibility of BIS' management. Our responsibility is to express an opinion on the suitability of the design and operating effectiveness of the controls to provide reasonable, but not absolute, assurance that the control criteria, specified by the AICPA, were achieved during the period covered by our report.

Any exceptions noted by Linford & Company LLP regarding the suitability of the design and operating effectiveness of the controls identified to achieve service commitments and system requirements based on the trust services criteria relevant to security are presented in this section under the caption, "Results of Testing." Concerns identified herein are not necessarily weaknesses in the total system of internal control at BIS, as this determination can only be made after consideration of controls in place at each client. Complementary user entity controls that should be exercised by clients in order to complement the controls of BIS to attain the stated criteria are presented in Section III when considered applicable.

Overview of the Internal Control Environment

Entity-Level Controls

Our examination considered the control environment and included inquiry of appropriate management and staff, inspection of documents and records, and observation of activities and operations. Our examination covered the period January 1, 2023 to December 31, 2023 and was applied to those controls relating to control criteria specified by the AICPA.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to our review of the controls placed into operation, our procedures included tests of the relevant elements of BIS' control environment, including BIS' organizational structure and management control methods.

Our evaluation of the control environment included the following procedures, to the extent necessary:

- ✓ *Inspected* BIS' organizational structure, including the segregation of functional responsibilities, team member best practices, and other best practices and procedures.
- ✓ *Inquired* through discussion with managers and team leads responsible for developing, monitoring, and enforcing controls.
- ✓ *Observed* team members in the performance of their assigned duties.

No exceptions were noted in entity-level testing.

* * * * *

The results of these procedures were considered in planning the nature, timing, and extent of evaluation procedures around the design and operating effectiveness of controls.

Controls Specified by BIS, Testing Procedures, and Results of Tests

The following tables include a description of the control activities, testing procedures performed, and results of tests. BIS management specified the control activities, and the AICPA specified the related control criteria in *Section V – SOC 2 Requirements and Controls.*

Control Activities Relevant to the Security Criteria

Control Environment

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
1.1	BIS has documented information security best practices within a company resource book, and a code of conduct that identifies expectations and core values, which are acknowledged by new team members upon hire.	*Inspected* the BIS company resource book and code of conduct and noted that the documents identified the Company's expectations for team members and its core values. For a sample of team members onboarded during the period, *inspected* the Company resource book and code of conduct for each individual selected and noted that each had acknowledged the best practices upon hire.	No exceptions noted. No exceptions noted.
1.2	The Leadership team maintains oversight of BIS' strategic direction, operational performance, and internal control, meeting at least monthly.	For a sample of months during the period, *inspected* meeting minutes and noted that the Leadership team met for each month selected and discussed strategic direction, operational performance, and internal controls.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
1.3	BIS' organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities.	*Inspected* BIS' detailed organizational chart and ascertained that the chart defined the roles of each individual with BIS and the lines of authority within the organization.	No exceptions noted.
1.4	To increase the operational effectiveness of team members within this structure, BIS maintains position profiles for all team members so that individuals understand and perform their responsibilities effectively.	For a sample of position profiles, *inspected* the documented profile descriptions and noted that the descriptions existed and included the profile's responsibilities so that individuals were made aware of their requirements and responsibilities for their positions.	No exceptions noted.
1.5	In order to assess the competence of potential applicants, BIS conducts a skills assessment during the employment evaluation process.	For a sample of team members onboarded during the period, *inspected* the documented skills assessments and noted that the candidates' technical competence was assessed during the evaluation process.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
1.6	After the necessary competency checks are complete, BIS maintains templates of applicable offer letters for candidates that includes at-will employment language depending on the role and physical country location of the candidate.	*Inspected* each of the offer letter templates utilized by BIS and noted that the offer letters were customized based on role and geographic location of the candidate. *Inspected* the US candidate offer letter and noted that it was contingent on a successful background check and included at-will employment language. For a sample of team members onboarded during the period, *inspected* the signed team member agreement forms and noted that the candidates acknowledged at-will employment, when applicable.	No exceptions noted. No exceptions noted. No exceptions noted.
1.7	The BIS People & Culture team conduct reference checks for all applicants selected for full time employment, and they conduct background checks on US-based team members.	For a sample of team members onboarded during the period, *inspected* the reference checks and background checks (if a US-based applicant) that were performed and noted that the appropriate checks were performed for each individual and the results were documented.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
1.8	Team members and applicable contractors are required to follow to and acknowledge the technology use best practices and the confidentiality and intellectual property agreements during onboarding.	For a sample of team members onboarded during the period, *inspected* their Company best practices guide acknowledgements, which included security best practices and acceptable use, as well as their confidentiality and intellectual property agreements, and noted that each had acknowledged the best practices upon hire.	No exceptions noted.
1.9	BIS team members are required to attend security awareness training during the onboarding process within one month of their start date and annually thereafter.	For a sample of team members onboarded during the period, *inspected* the security awareness onboarding training logs and noted that each individual selected had completed the onboarding training within one month of being hired. For a sample of team members, *inspected* the annual security awareness training logs and noted that each individual selected completed the annual training during the period.	No exceptions noted. No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
1.10	The Leadership team, managers, and team leads conduct performance evaluations of their team members and discuss the team members' strengths and areas of improvement.	For a sample of current employees, *inspected* their most recent performance reviews and noted that each individual selected had a discussion with the Leadership team, their team lead, or their manager regarding their performance, the discussions were documented, completed within the Company time requirements based on team members' role, and the reviews highlighted the individuals' strengths and areas of improvement.	No exceptions noted.

Information and Communication

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
2.1	BIS' systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	*Inspected* the output from automated monitoring solutions and noted that management monitored BIStrainer and the organization's internal controls through the use of relevant and quality information.	No exceptions noted.
2.2	Security updates relevant to all team members are announced via communication tools or by the Leadership team during recurring Monday morning meetings. The Monday morning meetings are recorded in a spreadsheet accessible to all team members on SharePoint.	For a sample of weeks during the period, *inspected* the weekly Monday morning meeting spreadsheet and noted that security and other company-related topics were communicated to team members. *Inspected* the SharePoint site and the team members with access to the site and noted that the Monday morning spreadsheets were maintained on SharePoint and all company team members had access to the SharePoint site.	No exceptions noted. No exceptions noted.
2.3	BIS maintains security best practices to communicate security responsibilities to team members and these best practices are maintained within the BIS Playbook that is accessible to all team members on SharePoint.	*Inspected* the Company's SharePoint site and noted that the security best practices were maintained there and the best practices communicated responsibilities to team members within the BIS Playbook.	No exceptions noted.
2.4	BIS has an organizational reporting structure with clear reporting lines and authority hierarchy, which delineates roles and responsibilities.	*Inspected* BIS' organization chart and noted that reporting lines and authority were delineated in the chart.	No exceptions noted.

Information and Communication (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
2.5	BIS has created a high-level overview of the BIS infrastructure and systems used to describe the services provided to the clients that it serves on its website.	*Inspected* the Company's website and noted that the description of services was made available to internal and external users.	No exceptions noted.
2.6	BIS has a client SLA and defined its terms of service that together contains information regarding the design and operation of the system and its boundaries, as well as acceptable use of the system.	*Inspected* the terms of service on the Company's website and an example MSA and ascertained that BIS and client obligations regarding the acceptable use of BIS services were included within the terms of service. For a sample of clients onboarded during the period, *inspected* their executed MSAs and noted that each selected client executed an MSA with the Company showing their willingness to act in the acceptable manner per the contract.	No exceptions noted. No exceptions noted.
2.7	To assist with BIS' commitments to security, BIS management provides annual security awareness training for all team members that covers information security-related topics and tracks the completion of training.	*Inspected* the curriculum and noted that BIS facilitated annual security awareness training and required its team members to complete a security awareness training assessment annually. For a sample of team members, *inspected* their training reports for the annual training and noted that each selected individual completed the training during the period.	No exceptions noted. No exceptions noted.

Information and Communication (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
2.8	For external users, the Company website and the SLA describes the process for reporting operational failures, incidents, problems, and concerns. For BIS team members, issue reporting procedures are documented within the incident management best practices.	*Inspected* the BIS system and a sample ticket and noted that the Company had provided external users with methods to report failures, incidents, concerns, and other complaints, and items received were researched and resolved. *Inspected* the Company's incident reporting process and ascertained that BIS had provided team members with a way to report failures, incidents, concerns, and other complaints, and items received were researched and resolved.	No exceptions noted. No exceptions noted.
2.9	The Leadership team has a process to communicate security or privacy changes to external users, related parties, and vendors, as needed.	Through *inspection* of the release notes posted on the Company's website, noted that BIS communicated client-impacting changes.	No exceptions noted.

Risk Assessment

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
3.1	The BIS Leadership team performs and maintains a formal risk assessment and treatment plan that includes the framework for identifying and assessing the key risks related to the Company and outlines the approach to identifying, assessing, mitigating, and monitoring risks.	*Inspected* the risk assessment and treatment plan and noted that BIS Leadership performed the assessment during the period and the document included the framework for identifying and assessing the key risks related to the Company, including the approach to assessing, mitigating, and monitoring the risks.	No exceptions noted.
3.2	The Leadership team performs a formal risk assessment annually, and the risks identified are formally documented and monitored.	*Inspected* the BIS risk assessment and noted that the Company performed the assessment annually and the risks identified were formally documented and monitored.	No exceptions noted.
3.3	Relevant and necessary participants are present to comprehensively identify potential risks, and the risk assessment identifies the key roles and responsibilities in risk management.	*Inspected* the BIS risk assessment and noted that the relevant participants were documented as present and worked as a team to comprehensively identify potential risks, and the risk assessment identified the team members with key risk management roles and responsibilities.	No exceptions noted.
3.4	The risk assessment and treatment plan documents the Company's considerations related to fraud risks, natural risks, technical risks, physical risks, environmental risks, regulatory risks, and vendor risks.	*Inspected* the BIS risk assessment and noted that the document included the Company considerations related to the following risks: fraud, natural, technical, physical, environmental, regulatory, and vendor.	No exceptions noted.

Risk Assessment (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
3.5	Each risk is assessed and given a risk rating in relation to the potential impact on the Company and its services.	*Inspected* the BIS risk assessment and noted that each risk was assessed and given a risk rating in relation to the potential impact and likelihood of occurrence.	No exceptions noted.
3.6	Vulnerabilities identified as part of the risk assessment process are prioritized and remediated based on the assessed risk, as part of the BIS risk assessment program. Remediation activities are reviewed and approved by the Leadership team and an owner is assigned for each remediation plan.	*Inspected* the BIS risk assessment and noted that each vulnerability identified had a remediation plan that was approved by management and the status of the remediation activity was tracked and had an owner assigned.	No exceptions noted.
3.7	BIS' best practices and procedures take into consideration the business and IT risks noted within the risk assessment.	*Inspected* the BIS security best practice and noted that the best practice took into consideration the business and IT risks noted within the risk assessment.	No exceptions noted.
3.8	The risk assessment is updated periodically to take into consideration relevant changes in BIS' operations and relevant risks raised within the organization.	*Inspected* the BIS risk assessment and noted that it reflected current risks facing the Company and had been updated periodically during the period.	No exceptions noted.

Monitoring of Controls

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
4.1	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	*Inspected* the application and infrastructure monitoring tools and noted that they were used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
4.2	Monitoring software is configured to send automated notifications.	*Inspected* the application and infrastructure monitoring tools and resulting notifications received from the tools and noted that the tools were configured to send automated notifications and the functionality was operating as intended.	No exceptions noted.
4.3	To maintain the stability and availability of the infrastructure environment, BIS monitors key performance parameters, such as CPU utilization, memory, and response times on the production system, and is notified when such parameters exceed configured thresholds.	*Inspected* the monitoring tools utilized by BIS and noted that CPU utilization, memory, and response times were monitored on the BIS infrastructure.	No exceptions noted.

Monitoring of Controls (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
4.4	BIS has a third-party application penetration test performed on an annual basis. The vulnerabilities identified in the penetration testing for BIStrainer are reviewed by the Technology team manager and high/critical vulnerabilities are resolved.	For the most recent BIStrainer penetration test, *inspected* the scan outputs from the external penetration test and noted that the scan was completed during the period and the results were documented and retained. For a sample vulnerability detected during the period, *inspected* the penetration retest and internal communication and noted that the vulnerability was resolved.	No exceptions noted. No exceptions noted.
4.5	The vulnerabilities identified in the quarterly vulnerability scans for BIStrainer are reviewed by the Technology team manager and high/critical vulnerabilities are resolved.	For a sample of quarters during the period, *inspected* the BIStrainer vulnerability scans and noted that the scans were completed and vulnerabilities were resolved, as needed. *Inspected* the Technology team playbook and noted that the Technology team was responsible for implementation and maintenance of security controls.	No exceptions noted. No exceptions noted.
4.6	The vulnerabilities identified in the annual vulnerability scans for the corporate network are reviewed by the IT team and tracked to resolution.	*Inspected* the annual corporate network vulnerability scan and noted that the scan was completed during the period and vulnerabilities were resolved, as needed.	No exceptions noted.

Monitoring of Controls (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
4.7	Relevant team members, including the Technology team member, review compliance reports from the subservice organizations to determine whether controls upon which BIS relies are operating effectively.	*Inspected* the subservice organization review documentation and determined that BIS management reviewed the compliance report from their subservice providers and assessed the adequacy of controls to meet the Company's service commitments and system requirements.	No exceptions noted.

Control Activities

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
5.1	BIS has developed best practices that establish expected behaviour.	*Inspected* BIS' best practices and procedures and determined that the best practices existed and the procedures had been implemented as designed. *Inspected* the resource book for team access and noted that it established a code of conduct and expected behaviour.	No exceptions noted. No exceptions noted.
5.2	BIS Leadership segregates responsibilities and duties.	*Inspected* the security best practice and noted that responsibilities and duties were segregated and it restricted technology access rights to authorized users commensurate with their job responsibilities to protect the entity's assets from external threats.	No exceptions noted.
5.3	BIS has defined and approved best practices and procedures that address control processes and company risks.	*Inspected* best practice review documentation and noted that management had reviewed the Company control activities during the period.	No exceptions noted.

Control Activities (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
5.4	BIS utilizes an internal project management software tool to communicate internal control deficiencies in a timely manner to Leadership and enable cross-functional teams to take appropriate corrective actions.	*Inspected* management's priority case tracker and noted that management monitored and took corrective action on compliance-related items when issues were identified. *Inspected* the detection and resolution of a vulnerability that occurred during the period and noted that management took corrective action on vulnerabilities, when identified.	No exceptions noted. No exceptions noted.

Logical and Physical Access

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.1	Under the direction of Leadership, the People & Culture team utilizes checklists for onboarding new team members and offboarding terminations to determine that all necessary control steps and IT system access considerations are tracked and completed.	*Inspected* BIS's playbook and the checklists and noted that the documents included procedures for onboarding new team members and offboarding terminations.	No exceptions noted.
6.2	Access requests and associated approvals are tracked using BIStrainer. Documented approval is obtained for team members prior to being granted access to the environment.	For a sample of team members onboarded during the period, *inspected* BIStrainer and noted that each of their access requests and approvals were tracked.	No exceptions noted.
6.3	BIS team members are granted access to BIStrainer according to their role and team.	For a sample of team members onboarded during the period, *inspected* BIStrainer and noted that access was granted based on the individuals' departments and roles.	No exceptions noted.
6.4	The responsible team will conduct periodic reviews of user accounts and privileges in BIStrainer and follow-up, as needed.	For a sample of months during the period, *inspected* the Risk and Compliance team's review of the user access and privileges for BIStrainer and noted that they occurred during the months selected and follow-up occurred as needed.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.5	A terminated team member's system and physical access is removed in a timely manner.	For a sample of terminations during the period, *inspected* the system access listings, offboarding notes, and date of password resets and noted that the terminations were not listed as active users within the information systems and production infrastructure and their accounts were deactivated within one business day. For a sample of terminations during the period, *inspected* the physical access listings and noted that the terminated team members did not have active physical access to the office.	No exceptions noted. No exceptions noted.
6.6	Administrator-level access privileges are restricted to only those individuals who require such access to perform their respective job functions.	For users with administrator access to the application, infrastructure, network, and VPN, *inspected* the associated job titles and noted that the access appeared aligned with the team member's responsibilities. *Inquired* of management and ascertained that the individuals with administrative access required this access for their job duties and were appropriate and approved.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.7	Technical implementations are in place to maintain segregation of client data within the database.	*Observed* as two different user accounts that were logged into and noted that each user account that was logged into was unable to access the other user account's data.	No exceptions noted.
6.8	Access to client data within the production database is restricted to authorized users.	For a sample of users with access to client data within the production database, *inspected* the associated job titles and noted that the access aligned with the users' responsibilities. *Inquired* of management and ascertained that the sampled individuals with access to client data required this access for their job duties and were appropriate and approved.	No exceptions noted. No exceptions noted.
6.9	BIS has a system control that defines password standards for access to BIStrainer and its infrastructure.	*Inspected* the application, infrastructure, and network password configurations and determined that access to the systems required a complex password.	No exceptions noted.
6.10	BIS has a system control that enforces MFA for access to BIStrainer and its infrastructure.	*Inspected* the application, infrastructure, and VPN authentication configurations and determined that MFA was enabled.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.11	Team members with access to the office are restricted to active employees and contractors.	For a sample of people with access to the BIS office suite, *inspected* the list of users with physical access and noted that the individuals were active employees or contractors. *Inquired* of management and ascertained that the sampled individuals with access to the BIS office suite required this access for their job duties and were appropriate and approved.	No exceptions noted. No exceptions noted.
6.12	Malware detection software is deployed on workstations.	For a sample of workstations, *inspected* the workstation configurations and determined that anti-malware software was installed and up to date.	No exceptions noted.
6.13	BIS applies security patches to user workstations, so at any given time, workstations are on supported operating system versions.	*Inspected* the IT patching console and noted that operating system patching was enforced for company workstations. For a sample of workstations, *inspected* the workstation operating system versions and determined the workstations were on a supported version.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.14	To minimize the risk of data being compromised in the event hardware or data is lost or stolen, workstations are encrypted.	*Inspected* the Azure global policy encryption configuration and noted that encryption was enforced for company workstations on the domain. For a sample workstation, *inspected* the workstation encryption status in Azure and the encryption configurations on the device and determined that the workstation encryption status in Azure tied without exception to the device settings and the configurations in Azure appeared accurate. For a sample of workstations, *inspected* the domain workstation inventory in Azure and noted that the workstations selected were each included in the domain inventory and the domain inventory appeared complete.	No exceptions noted. No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.15	Workstations are configured to automatically log out after a modest period of inactivity.	*Inspected* the Azure global policy for inactivity lockout and noted that the setting for lockout was enforced after 10 minutes of inactivity for workstations on the domain. For a sample workstation, *inspected* the workstation inactivity timeout setting in Azure and the inactivity timeout configurations on the device and determined that the workstation inactivity timeout settings in Azure tied without exception to the actual device settings, the device settings were unable to be modified, and the configurations in Azure appeared accurate. For a sample of workstations, *inspected* the domain workstation inventory in Azure and noted that the workstations selected were each included in the domain inventory and the domain inventory appeared complete.	No exceptions noted. No exceptions noted. No exceptions noted.
6.16	BIS maintains an inventory listing of information assets in order to identify and implement controls to protect them from security events.	*Inspected* the information asset inventory listing and noted that BIS maintained an up-to-date record of assets to identify and implement controls and protect the Company from security events.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.17	To protect the production environment, security groups are configured for servers within AWS, which limit access to specified ports and IP addresses.	*Inspected* the AWS admin console and determined that security groups were configured for servers in AWS, which limited access to specified ports and IP addresses.	No exceptions noted.
6.18	In the application environment, firewalls are configured to restrict inbound traffic.	*Inspected* the firewall configurations and noted that firewall rules were configured to restrict inbound traffic.	No exceptions noted.
6.19	Access to modify firewall rules and security groups are restricted to appropriate team members.	For users with the ability to modify the firewall rules and security groups, *inspected* their associated job titles and noted that the access appeared to be aligned with the users' responsibilities. *Inquired* of management and ascertained that the individuals with access to modify the firewall rules and security groups required this access for their job duties and were appropriate and approved.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
6.20	Data transfers between clients and BIStrainer are secured using TLS and industry-standard encryption.	*Inspected* SSL server test reports and noted that data transfers between users and BIStrainer used TLS and industry-standard encryption.	No exceptions noted.
6.21	Client data within the production database is encrypted at rest.	*Inspected* database configurations within AWS and determined that client data within the production database was encrypted at rest.	No exceptions noted.
6.22	Procedures are in place to establish that all hardware (i.e. hard drives, laptops) is securely wiped prior to being removed from company ownership.	*Inspected* the location where data deletion requests were tracked and noted that BIS maintained deletion requests. For a sample device that was requested to be deleted during the period, *inspected* the ticket and noted that the device had its data deleted.	No exceptions noted. No exceptions noted.
6.23	BIS establishes the boundaries of the environment by maintaining an architecture diagram.	*Inspected* the BIS architecture diagram and noted that it established the boundaries of the environment.	No exceptions noted.

System Operations

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
7.1	BIS' security incident management protocol establishes the procedures to be undertaken in response to information security incidents.	*Inspected* the incident management protocol and the BIStrainer security practice document and noted that there was an established process to follow in the event of a security incident.	No exceptions noted.
7.2	The security incident management protocol is updated at least annually.	*Inspected* the communications including management's review of the recent security incident management protocol and noted that a review occurred during the period.	No exceptions noted.
7.3	In years that security incidents do not occur, BIS conducts a test of the security incident management protocol and the ability of the Incident Response team to execute the plan on an annual basis and documents the test procedures and test results.	*Inspected* a sample of incidents that occurred during the period and noted that a test of the security incident management protocol was not required as at least one incident occurred during the period that enacted the security incident management protocol. Per *inquiries* of management, noted that the incidents that occurred during the period did not result in a breach or data loss to the systems.	No exceptions noted. No exceptions noted.

System Operations (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
7.4	A log of all security incidents is maintained in a Risk and Compliance SharePoint document library.	Through *inspection* of the incident tracking tool, noted that BIS maintained a record of security incidents. For a sample of incidents during the period, *inspected* the incident assessments and determined that the root cause, incident assessment, and lessons learned were documented.	No exceptions noted. No exceptions noted.
7.5	BIS has forms of system redundancy in place to prevent destruction and loss of data.	*Inspected* the BIStrainer security practice document and noted that it established the forms of system redundancy to prevent destruction and loss of data. *Inspected* the status of replication between the database servers and noted that the primary database server was being replicated for redundancy to prevent destruction and/or loss of data.	No exceptions noted. No exceptions noted.

System Operations (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
7.6	Backups of data are performed on a periodic basis to prevent the loss of client data.	*Inspected* backup configurations and noted that the critical server and storage buckets were backed up daily to protect the Company from data and configuration loss in the event of a system failure. *Inspected* retention configurations and the oldest backup and noted that backups were retained for at least six days.	No exceptions noted. No exceptions noted.
7.7	A backup of the Company data is also restored periodically.	*Inspected* the systematic documentation for a restore completed during the period and noted that it was initiated as requested and the backup was restored successfully.	No exceptions noted.
7.8	Infrastructure production servers are patched on a periodic basis to reduce the risk of compromise.	For a sample of servers, *inspected* the most recent patch update for each server selected and noted that the updates each occurred during the past quarter.	No exceptions noted.

Change Management

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
8.1	BIS' change management best practice describes how changes to BIStrainer and its infrastructure are proposed, reviewed, deployed, and managed.	*Inspected* the documented change management best practice and noted that BIS followed a defined development process for making changes to the systems that support the services provided, including how changes are proposed, reviewed, deployed, and managed.	No exceptions noted.
8.2	BIS Leadership uses a project management tool to manage and record activities related to the change management process.	*Inspected* the project management tool and noted that BIS used the tool to manage and record the activities related to the change management process. For a sample of changes implemented into the production environment during the period, *inspected* the change request details and noted that the selected changes were managed via the project management tool.	No exceptions noted. No exceptions noted.
8.3	The Technology team uses a code development platform to manage and record activities related to the change management process.	For a sample of changes implemented into the production environment during the period, *inspected* the change request details and noted that the selected changes were developed, managed, and recorded in the code development platform.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
8.4	Separate development, QA, and production environments exist to support development, testing, and production.	*Inspected* system platforms and noted that BIS had separate development, testing, staging, and production environments that facilitated the change management process.	No exceptions noted.
8.5	Infrastructure and software changes are required to be tested prior to implementation. Depending on the complexity of the change, the testing includes evidence of peer review and QA activities.	For a sample of changes implemented into the production environment during the period, *inspected* the change tickets and pull requests and noted that the changes were peer reviewed by a different user than the author and were tested prior to being moved to production.	No exceptions noted.
8.6	Infrastructure and software changes are required to be approved for implementation by the Leadership team, key team members and the client requesting the change, as applicable.	For a sample of changes implemented into the production environment during the period, *inspected* the change tickets and noted that they included implementation approval and client approval prior to release to production and live environment.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
8.7	As a part of the change process, clients and BIS team members are notified of relevant changes deployed that may impact their services security or delivery to provide continued client awareness and understanding of the products.	For a sample of changes implemented in the production environment during the period, *inspected* the project management tool configuration and the change tickets and noted that by default, there was a watchlist assigned to each ticket and knowledgeable team members or BIS Leadership received notifications for status changes related to the system changes. For a sample of changes implemented into the production environment during the period, *inspected* the change notification emails that were sent to the client contacts that the change impacted and noted that the emails provided the clients with continued awareness and understanding of the impacts of the deployed changes.	No exceptions noted. No exceptions noted.

Change Management (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
8.8	BIS restricts the ability to implement changes into the production environment to only those individuals who require this ability as part of their job function.	*Inspected* the system configuration of the branch rules within the code development tool and noted that change pull requests could only be merged to the production branch by a restricted group of users.	No exceptions noted.
		For a sample of users with access to the code development tool, *inspected* the team member roster and noted that it appeared that the users with access to implement and deploy changes to production systems were current team members with job responsibilities that required this ability.	No exceptions noted.
		Performed *inquiries* of BIS Leadership and managers and ascertained that the sample of individuals with access to implement changes to the production environment were current team members with job responsibilities that required this ability, and they were appropriate and approved.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
8.9	BIS maintains immutable logs of all changes pushed to production for a minimum of a year.	*Inspected* the change log that was maintained by BIS in the Company's change repository tool and noted that logging was taking place and the logs were retained for more than five years and immutable. *Inspected* communications between BIS Leadership via the internal communication tool and noted that the communications were related to inspection and follow up from periodic informal reviews of the logs.	No exceptions noted. No exceptions noted.
8.10	Express Lane changes are required to receive change approval, undergo QA, and testing, and have documentation of at least two software development team members involved with every change.	*Inspected* a recent "express lane" change ticket and noted that the change was referred to as an Express Lane change, was approved, tested, and had two team members involved with the change.	No exceptions noted.

Risk Mitigation

Ref	Controls Specified by BIS	Testing Performed by Linford & Company	Results of Testing
9.1	The third-party management best practice provides a framework for managing the lifecycle of third-party relationships.	*Inspected* the BIS compliance playbook, which includes the third-party management program, and noted that the risk management process was formally documented and included the framework for managing the life cycle of third-party relationships.	No exceptions noted.
9.2	Risk and Compliance team members monitor and document their review of third-party assurance reports from key third-party outsourced service providers on an annual basis.	*Inspected* BIS' review of the compliance report for each of the subservice organizations and determined that BIS had assessed the subservice organizations for the adequacy of controls to support its service commitments. For a sample of vendors utilized during the period, *inspected* the vendors security reviews performed by BIS and noted that a review was performed over each vendor selected for appropriateness of continued use of their services, and it was performed during the period.	No exceptions noted. No exceptions noted.
9.3	BIS maintains insurance coverage to protect against threats that may impact business operations.	*Inspected* BIS' insurance certificate and noted that BIS maintained coverage to protect against threats that may impact business operations, including cyber threats.	No exceptions noted.

Section V – SOC 2 Requirements and Controls

The BIS management team is responsible for establishing and maintaining effective controls over its compliance and learning management software. The controls are designed to provide reasonable assurance to BIS' management that the following SOC 2 security control criteria are achieved.

In the table that follows, the columns have the following meaning:

SOC 2 Criteria – This column contains, for each criterion evaluated, the reference citation. Each criterion sources from a requirement of the trust services criteria.

Requirement(s) – This column contains the text of the criterion (requirement) directly from the trust services criteria.

Reference – This column contains the reference to the control activities in *Section III – BIS' Description of Its Compliance and Learning Management Software*, which are relevant to the achievement of the criterion.

The purpose of this table is to demonstrate that all SOC 2 control criteria in scope were assessed and that the control activities described in *Section III – BIS' Description of Its Compliance and Learning Management Software,* address the SOC 2 control criteria.

Many of the criteria used to evaluate a system are shared amongst security, availability, processing integrity, confidentiality, and privacy. For example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy criteria. As a result, the criteria for the security, availability, processing integrity, confidentiality, and privacy criteria are organized into the criteria that are applicable to all five criteria (Common Criteria) and criteria applicable to only a single criterion. The Common Criteria (CC1.0 through CC9.0 in the table that follows) constitute the complete set of criteria for the security criteria.

Common Criteria/Security Criteria

Security. The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CC1.0 Common Criteria Related to Control Environment

SOC 2 Criteria	Requirement(s)	Reference
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1.1
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	N/A[1]
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.2-1.4

[1] BIS has an executive management (Leadership team), not a board of directors.

CC1.0 Common Criteria Related to Control Environment (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.5-1.10, 2.7
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.8-1.10

CC2.0 Common Criteria Related to Information and Communication

SOC 2 Criteria	Requirement(s)	Reference
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1-2.3, 2.7
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	1.1-1.3, 1.6-1.8, 2.2-2.5, 3.7
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.6, 2.8, 2.9

CC3.0 Common Criteria Related to Risk Assessment

SOC 2 Criteria	Requirement(s)	Reference
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.1

CC3.0 Common Criteria Related to Risk Assessment (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	3.2-3.8
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.4
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	3.3-3.4, 3.6, 3.8

CC4.0 Common Criteria Related to Monitoring Activities

SOC 2 Criteria	Requirement(s)	Reference
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	4.1-4.3
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	2.2-2.3, 2.9, 3.6-3.7, 4.1-4.7, 5.4

CC5.0 Common Criteria Related to Control Activities

SOC 2 Criteria	Requirement(s)	Reference
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	1.1-9.3

CC5.0 Common Criteria Related to Control Activities (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	5.1-5.4, 6.1-8.7
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	1.1, 2.3, 3.1, 3.7, 5.1, 6.1, 7.1, 7.5, 8.1

CC6.0 Common Criteria Related to Logical and Physical Access

SOC 2 Criteria	Requirement(s)	Reference
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	6.4, 6.7-6.10, 6.14, 6.16, 6.17, 6.20-6.23
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	6.1-6.6, 6.10

CC6.0 Common Criteria Related to Logical and Physical Access (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	6.1-6.10, 6.18, 6.19
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	6.5, 6.11, AWS CSOC, Microsoft CSOC
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	6.4-6.5, 6.11, 6.22, AWS CSOC, Microsoft CSOC
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	6.9-6.10, 6.12-6.15, 6.17, 6.19, 7.8
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	6.14, 6.20, 6.21
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	6.12

CC7.0 Common Criteria Related to System Operations

SOC 2 Criteria	Requirement(s)	Reference
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	4.1-4.5 AWS CSOC
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	4.1-4.5 AWS CSOC, Microsoft CSOC
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	7.3-7.4, AWS CSOC, Microsoft CSOC
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	7.1-7.5, AWS CSOC, Microsoft CSOC
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.6-7.7, AWS CSOC, Microsoft CSOC

CC8.0 Common Criteria Related to Change Management

SOC 2 Criteria	Requirement(s)	Reference
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	8.1-8.10

CC9.0 Common Criteria Related to Risk Mitigation

SOC 2 Criteria	Requirement(s)	Reference
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	9.1-9.3
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	4.7, 9.3

(The remainder of this page left blank intentionally.)