CoBro Consulting's Compass system

– Report on CoBro Consulting's Description of its Compass system and on the Suitability of the Design of its Controls

– System and Organization Controls (SOC) – SOC 2 Type 1 Report

– For the Period as of October 31, 2024

Contents

1. INDEPENDENT SERVICE AUDITOR'S REPORT 1
2. ASSERTION OF COBRO CONSULTING, LLC'S MANAGEMENT 4
3. COBRO CONSULTING, LLC'S DESCRIPTION OF ITS COMPASS SYSTEM 5

Overview of Company 5

Scope of the Description 5

Principal Service Commitments and System Requirements 6

Components of the Compass system Used to Provide the Services 7

- Infrastructure 7
- Software 7
- People 7
- Data 8
- Procedures 8

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, and Monitoring 9

- Control Environment 9
- Risk Assessment 14
- Information and Communication 15
- Monitoring 15

Complementary Subservice Organization Controls 16

User Entity Responsibilities 17

4. TRUST SERVICE CATEGORY, CRITERIA, AND RELATED CONTROLS 18

1. Independent Service Auditor's Report

To the management of CoBro Consulting, LLC:

Scope

We have examined CoBro Consulting, LLC's (CoBro Consulting) accompanying description of its Compass system titled "CoBro Consulting, LLC's Description of its Compass system" as of October 31, 2024 (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 (With Revised Implementation Guidance – 2022)*, in AICPA, *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of October 31, 2024, to provide reasonable assurance that CoBro Consulting's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA, *Trust Services Criteria*.

CoBro Consulting uses a subservice organization for application and database server hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CoBro Consulting, to achieve CoBro Consulting's service commitments and system requirements based on the applicable trust services criteria. The description presents CoBro Consulting's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CoBro Consulting's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

CoBro Consulting 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 CoBro Consulting's service commitments and system requirements were achieved. CoBro Consulting has provided the accompanying assertion titled "Assertion of CoBro Consulting, LLC's Management" (assertion) about the description and the suitability of design of controls stated therein. CoBro Consulting 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 of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to with the description criteria and the controls stated therein were suitably designed to provide reasonable

assurance that the service organization's service commitments and system requirements would be 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.

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

- Obtaining an understanding of the system and the 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
- 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
- Evaluating the overall presentation of the description

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

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. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description presents CoBro Consulting's Compass system that was designed and implemented as of October 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of October 31, 2024, to provide reasonable assurance that CoBro Consulting's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization applied the complementary controls assumed in the design of CoBro Consulting's controls as of October 31, 2024.

Restricted Use

This report is intended solely for the information and use of CoBro Consulting, user entities of CoBro Consulting's Compass system as of October 31, 2024, business partners of CoBro Consulting subject to risks arising from interactions with CoBro Consulting Compass system, 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 subservice organization controls and how these controls interact with the controls at the service organization to achieve the service organization's service commitments and 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.

Baker Tilly US, LLP

Los Angeles, California
December 26, 2024

2. Assertion of CoBro Consulting, LLC's Management

We have prepared the accompanying description of CoBro Consulting, LLC's (CoBro Consulting) Compass system titled "CoBro Consulting, LLC's Description of its Compass system" as of October 31, 2024 (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 (With Revised Implementation Guidance – 2022)*, in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Compass system that may be useful when assessing the risks arising from interactions with CoBro Consulting's Compass system, particularly information about system controls that CoBro Consulting 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, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA*, Trust Services Criteria.*

CoBro Consulting uses a subservice organization for application and database server hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CoBro Consulting, to achieve CoBro Consulting's service commitments and system requirements based on the applicable trust services criteria. The description presents CoBro Consulting's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CoBro Consulting's controls. The description does not disclose the actual controls at the subservice organization.

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

a. The description presents CoBro Consulting's Compass system that was designed and implemented as of October 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of October 31, 2024, to provide reasonable assurance that CoBro Consulting's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of October 31, 2024and if the subservice organization applied the complementary controls assumed in the design of CoBro Consulting's controls as of October 31, 2024.

3. CoBro Consulting, LLC's Description of its Compass system

Overview of Company

CoBro Consulting, LLC (DBA CoBro Consulting) is a research and consulting firm that provides data management and program evaluation services in support of education reform programs, nationwide. Since 2005, CoBro Consulting has provided over 100 federal education programs with database design and development, data management, and technical support services.

CoBro Consulting is a provider of cloud-based enterprise software solutions, including the Compass system for use within federal education grant programs. CoBro Consulting provides process automation and seamless integration for Compass system users.

The Compass system (also known as "Compass") is a secure, web-based tool designed to collect, organize, store, and report data about students, their parents, educators, and program staff. CoBro Consulting's technicians customize the Compass system to meet each client's needs and to maximize the efficiency and evaluation capacity of each client's federal grant program.

The system links existing student-level demographic, academic, and outcome data available electronically from school district or state education entities with GEAR UP student service participation data via unique student IDs. Compass also links such student data to GEAR UP service participation data for parents and program staff.

For other types of data such as program service participation, Compass contains user-friendly data entry screens to facilitate staff manual entry of individual student/parent/staff data. This process is also greatly expedited by Compass features such as our batch entry function for rapid recording of student or parent group activities, as an alternative to entering participant data individually.

Compass allows users to generate a large variety of data reports, each of which is customizable using predesignated filters, resulting in user-defined reports on-demand. With the ability to generate such customized real-time reports, clients have access to immediate feedback on program service efficacy, allowing program staff to conduct ongoing, formative evaluations to drive continuous program improvement.

CoBro Consulting is headquartered in San Diego, California.

CoBro Consulting's Compass' key functions of the platform are:

- System options are customized to conform to unique client needs.
- Web-based formatting ensuring access from multiple settings, devices, and web browsers.
- Data entry screening to facilitate input of program service and activity data.
- Student demographics and academic data files are uploaded directly into Compass.
- A variety of user-defined, pre-formatted reports available to users.
- All Compass data resides within secure, SSL certificated servers.

Scope of the Description

The report describes the control structure of CoBro Consulting as it relates to its Compass system as of October 31, 2024 for the Security, Confidentiality, and Availability Trust Services Criteria.

CoBro Consulting uses a subservice organization to provide application and database server hosting services. The description includes only the related controls of CoBro Consulting and excludes the controls of the subservice organization.

Principal Service Commitments and System Requirements

CoBro Consulting provides client access and use of its software subscription services as specified in the Master Services Agreement (MSA) and Software-as-a-Service (SaaS) Agreement. The overarching service commitment is to provide and secure CoBro Consulting's cloud-based enterprise software, which is designed for use by federal education grant programs.

In order to meet client obligations, as well as abide by applicable laws and regulations for its services, CoBro Consulting is responsible for ensuring that Compass is available to meet those requirements. With a commitment to availability in mind, CoBro Consulting maintains documented processes and employs redundancies as necessary to ensure that it meets its service level objective of system uptime.

CoBro Consulting's service commitments to their clients (and their respective Compass system users) are documented in its contracts with clients. Among other items, these service commitments include:

- Security principles within the fundamental designs of the CoBro Consulting applications are designed to permit users access to the information they need based on their role as defined in the system while restricting them from accessing information not needed for their role. Roles are defined by each client and are assigned a list of permissions accordingly.
- CoBro Consulting's service automatically locks up if left unattended for a specific period of time. Correct user credentials must be provided to re-access the application.
- Passwords are created by the client and are required to be at least eight characters long and maintain a certain level of complexity. The password expiration term and reuse limit are configurable by the client.
- The CoBro Consulting service communicates with secure CoBro Consulting hosted and controlled servers and networks with the use of encryption technologies that protect user entities' information both in transit and at rest. CoBro Consulting disallows the use of low cipher strength in its Production service.
- CoBro Consulting ensures physical and technical security protections of client data, as it uses highly secured hosting providers that are subject to System and Organization Controls (SOC) 2 Type 2 examinations.
- CoBro Consulting employs redundant, next-generation firewalls, intrusion detection, and prevention services that are monitored twenty-four hours a day, seven days a week. CoBro Consulting uses internal and external threat prevention, delivering timely and accurate reports of its Production services.
- In addition to these controls, CoBro Consulting deploys up-to-date advanced threat protection services that help identify, block, and track hacking attempts, scams, data breaches, adware, malware, spyware, trojans, phishing attempts, and other equally malicious requests.

Within CoBro Consulting, the Compass system requirements are documented and communicated to CoBro employees through internal policies, standards, and procedures. These system requirements include:

- System access is implemented according to need-to-know, least privilege, and separation of duties.
- System changes are managed according to change control procedures.
- Confidential data are encrypted in transit and at rest.
- System components are monitored for security performance.
- Risks are managed and acknowledged by leadership.

CoBro Consulting's operational requirements that support the achievement of service commitments are communicated in its policies, procedures, and agreements with user entities. CoBro Consulting's policies and procedures define an organization-wide approach to how the system and data are protected. These include policies around how the service is designed and developed, how the Compass system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Compass system.

Components of the Compass system Used to Provide the Services

Infrastructure

Compass utilizes Microsoft Azure (MS Azure) to host the application servers, database servers, and supporting services. CoBro Consulting uses San Diego as its principal region for tasks, and utilizes alternate regions for secondary backups, disaster recovery planning, and replicated backups.

The web application uses MS Azure, which serves the application through a redundant MS Azure Elastic Load Balancer connected to several MS Azure Elastic Compute Cloud instances that host the web server. Once connected to the MS Azure Load Balancer through Hypertext Transport Protocol Secure (HTTPS)/SSL, CoBro Consulting reaches one of the MS Azure instances in the Virtual Private Cloud (VPC), which securely connects to the Transactional database to retrieve or add data.

All the data transferred between the user's browser and CoBro Consulting's web servers and databases is encrypted in transit on the database and at rest. CoBro Consulting uses SSL v1.2 and AES-256 encryption for transit.

CoBro Consulting employs separate environments in the Software Development Lifecycle (SDLC)--Development, Testing, and Production. CoBro Consulting keeps the code and its revisions in a source code repository (GitHub), and every contribution is added as a pull request (PR) that requires at least two approvals to be included in the next build. CoBro Consulting is able to perform a rollback within ten minutes in case of a failure in the new version of code.

Given that the Compass system is hosted in Microsoft Azure, physical security and the controls related to CC6.4, *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives*, are the responsibility of Microsoft Azure and are described in the complimentary subservice organization controls presented later in the description.

Software

CoBro Consulting leverages third-party and cloud-based software to support the delivery of its services. These include the following:

Application	Business Use
Microsoft Azure	Application and database server hosting services

People

The three company Principals oversee all management activities. As one of the Principals, the Chief Executive Officer (CEO) is responsible for the overall operation of CoBro Consulting. Another company Principal, the Chief Information Officer (CIO), oversees CoBro Consulting's information security activities.

Reporting to the CEO, each member of the senior management team has a distinct, separate responsibility within the organization. Roles and responsibilities have been segregated to the extent possible, and a formal organizational chart has been developed. The CEO is responsible for the overall operation of CoBro Consulting. CoBro Consulting's CIO and Director of Evaluation, report directly to the CEO.

CoBro Consulting's organizational structure is reflective of its CoBro Consulting culture, nature, and scope of its operations. It also provides a framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. An organizational chart is available for all employees on the CoBro Consulting Teams website. The organizational chart presents the senior management team (i.e., the CoBro Consulting Principals), reporting relationships, and CoBro Consulting's overall organizational hierarchy. The senior management and other stakeholders of management review the reporting relationships and organizational structures on a periodic basis as part of organizational planning, as well as to respond timely to changing entity commitments and requirements.

Data

For any sensitive personally identifiable information (PII), such as Social Security Numbers (SSNs) or financial information, CoBro Consulting employs robust encryption mechanisms to secure this data before it is stored in CoBro Consulting's database. This encryption ensures that sensitive information is protected against unauthorized access, both at rest and during transmission. By adhering to industry best practices for data encryption and security, CoBro Consulting helps ensure that sensitive PII is handled with the utmost care, aligning with CoBro Consulting's commitment to safeguarding user data and complying with relevant data protection regulations.

CoBro Consulting has a Data Deletion and Retention Policy that has been communicated to its employees. IT Operations reviews the Data Deletion and Retention Policy annually. The Data Deletion and Retention Policy contains details on how data is classified and protected.

CoBro Consulting has a Privacy Policy that is available on the public website and is reviewed at least annually. CoBro Consulting has a Non-Disclosure Agreement (NDA) in place with any third-party hosting providers that could potentially have access to confidential data. The appropriate personnel update the NDA and Privacy Policy whenever changes to commitments and requirements are needed.

Procedures

CoBro Consulting's procedures are reviewed at least annually and updated as necessary to remain consistent with the Compass system's commitments and requirements.

CoBro Consulting's Code of Conduct, security, and disciplinary policies are communicated to employees upon hire. The policies are also available on an internal system for employees to reference, and any changes are communicated to employees via email. Additionally, with the acceptance of the employment offer, the employee acknowledges abiding by the policies communicated by HR.

CoBro Consulting's managed services and related support processes/procedures include but are not limited to:

- Onboarding procedures for new personnel and contractors to evaluate competency.
- Implementation support for new clients to help ensure they have been provided with information on how to report failures, incidents, concerns, and other complaints to appropriate CoBro Consulting personnel.
- Access management procedures to help ensure access to data, software, functions, and other IT resources are authorized, modified, or removed based on roles, responsibilities, or Compass system design.
- Compass development and maintenance procedures, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
- Change management procedures to help ensure changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet CoBro Consulting's commitments and system requirements.

- Incident response procedures that address incidents to help ensure logical and physical security breaches, failures, and vulnerabilities are identified and reported to appropriate CoBro Consulting personnel and acted upon in a timely manner.
- Disaster recovery procedures that help ensure environmental protection, software, data backup process, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet CoBro Consulting's commitments and system requirements.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, and Monitoring

The Security, Confidentiality, and Availability categories and applicable trust services criteria were used to evaluate the suitability of design of controls stated in the description. Security, Confidentiality, and Availability criteria and controls designed, implemented, and operated to meet them, help ensure that the Compass system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in section 4 of this report. Although the applicable trust services criteria and related controls are included in section 4, they are an integral part of CoBro Consulting's description of the Compass system.

Control Environment

Personnel Management

CoBro Consulting has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. CoBro Consulting has an organizational chart that defines the organizational structure and reporting lines.

CoBro Consulting maintains a diverse, talented, high-performing organization and ensures that new hires have the appropriate knowledge, tools, and system access to perform successfully in their roles as soon as possible after joining the team. CoBro Consulting maintains and follows vetting, onboarding, and performance review procedures.

Prior to publishing a new job requisition, the hiring manager, in coordination with HR and any other relevant stakeholders, meets to discuss the business need for the new role, as well as other relevant attributes. The official role and responsibilities are then defined in the agreed-upon job description and published. Job descriptions are included with offers of employment to ensure the new hire has a clear understanding of the job duties and responsibilities, as well as CoBro Consulting expectations of the new hire.

Each candidate must meet minimum educational and/or experience requirements. The candidate's submitted credentials are verified during the interview process. The process is role-specific and department-specific to ensure the candidate's skills and knowledge set are accurately assessed.

Each candidate to whom a conditional offer of employment has been extended undergoes and must pass an employment background check prior to being hired and starting work. This check may include a credit check and federal and state criminal records check. While the background screening results for each applicant are individually assessed, CoBro Consulting operates in a highly regulated industry. As such, individuals convicted of crimes related to insurance fraud, theft, embezzlement, and moral turpitude may be automatically disqualified from employment.

After an offer of employment has been accepted, an HR team member informs IT of the new hire's start date. The IT department contacts the new hire regarding work equipment and systems access. IT works with the HR and Department that the new hire belongs to, determines what systems and access are needed for the new hire, and establishes them to coincide with the new hire start date. Within 30 days of their start date, each new hire must successfully complete information security training.

Each employee undergoes at least one performance review on an annual basis consisting of a manager's review. These reviews, in addition to regularly scheduled one-on-one meetings, serve to recognize successful work, identify and respond to areas of improvement, and ensure the employee is sustaining the degree of professionalism, work productivity, and client care that CoBro Consulting standards require.

Although all CoBro Consulting employees work remotely, each of them has the same responsibilities as personnel situated within an office, such as the use of complex passwords, information security training, virus protection, lock screen, data backup, and encryption for any communication, including email and file sharing.

Policies and Procedures

HR has defined formal hiring policies and guidelines that assist in selecting qualified applicants for specific job responsibilities. Hiring policies require that certain levels of education and experience are met based on position and job requirements. Recruitment and termination duties and actions are defined in CoBro Consulting's HR policies and procedures. Appropriate levels of management and the Chief Executive Officer concurrently approve all hires.

CoBro Consulting maintains specific job descriptions which are available to personnel and intended to assist with employee development while also communicating job responsibilities. These job descriptions are drafted by HR and the hiring managers and include relevant requirements that CoBro Consulting looks for in potential candidates when filling the positions.

Training

CoBro Consulting provides Company-wide information security awareness training, which informs employees on how to detect and report security incidents.

Separation Procedures

Employee and contractor access to all data systems, files, and email account access is revoked within one business day upon termination of employment.

Vendor and Third-Party Management

When vendors or third-party providers have access to sensitive data or could impact the security of data within the environment, CoBro Consulting ensures that the appropriate agreements are in place and reviews their compliance status at least annually.

Physical Security and Environmental Controls

All servers are located in Microsoft Azure data centers. As such, the entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives, are the responsibility of the subservice organization.

Security Management Policies and Procedures

The CoBro Consulting security process is described in the CoBro Consulting Information Security Policy, which consists of the following:

- Physical access security
- Electronic access security
- Definition of data, privacy, and how to transfer information when required
- Instructions to manage IT and digital assets such as virtual machines, servers, workstations, workspaces, application servers, web servers, database servers, and mail servers
- Instructions on how to proceed under emergency or disaster events
- Instructions related to IP and the way employees keep it safe

CoBro Consulting keeps client information confidential and data up-to-date and error-free. CoBro Consulting also keeps the internal systems well-managed, replete with operating system updates and security patches, and limits access to authorized clients, authorized employees, and consultants.

As part of the security efforts, CoBro Consulting uses several strategies to detect issues such as:

- Static and dynamic code analysis
- Logging user access to any activity on MS Azure accounts
- Logging of work performed on servers
- Tracking unusual network activity
- Tracking vulnerabilities and updates related to the server's operating system and applications
- Managing desktops and applying needed updates to anti-virus, security patches, etc.
- Machine image update notification alerts when the next version is ready for use
- Security Content Automation Protocol (SCAP) scanning and monitoring that helps to identify any operating system/network vulnerability
- Uptime tracking related to the Service Level Agreement (SLA) or other services to the clients

Security Policies

CoBro Consulting has designed several policies to protect the security of the systems, the privacy of client data, and internal confidential information related to the ability to calculate applicable plans and rates for quotes and proposals. These security policies include:

- **Security Council**: This team is responsible for performing the Continuous Risk Analysis. The Security Council meets monthly to discuss security issues and review concerns that have come up during prior months. The Security Council identifies areas that should be addressed during annual training and reviews and updates security policies as necessary.
- **Employee Responsibilities**: CoBro Consulting trains team members to implement proper security practices, including writing secure code, keeping a "clean desk," challenging unrecognized personnel, using anti-virus and anti-malware on CoBro Consulting computers, defining protected data, and restricting access to client data. Hard drive encryption and manual password entry after screen lock-out is the default for all CoBro Consulting devices.
- **Report Security Incidents**: All personnel are instructed to report any security issues such as a lost laptop, phone, or any issue that is perceived as suspect.
- **Transfer of Sensitive Data**: CoBro Consulting employs procedures about who, how, and what data can be shared with clients, contractors, developers, and/or all relevant stakeholders.

- **Definition of PII/PHI**: All personnel have a clear understanding of what constitutes PII, PHI, and the process the Customer Success team is required to follow to de-identify or anonymize it.
- **Agreements**: Non-Disclosure Agreement, Confidential Agreement (data management), Intellectual Property, and other legal processes are in place to protect clients from security and data breaches.
- **Timeout/Disable Accounts**: CoBro Consulting has several policies in place such as forced timeout from systems, disabling accounts after several failed password connection attempts, disabling accounts after receiving a report of a lost or stolen device, and providing automatic warnings if connections from unknown external IP addresses should occur. Accounts can also be disabled in the case of an emergency.
- **Network Security and Firewalls**: CoBro Consulting only allows approved devices to connect to the office network and a limited number of users from the DevOps team to connect to servers via special keys. Workstations, servers, database servers, load balancers, and workspaces all have a firewall that blocks almost all activity except for those expressly approved.
- **Encryption**: CoBro Consulting uses encryption in several processes, such as data on transit (SSL v1.2 – HTTPS/SFTP), data on rest (AES-256 encryption, at field level in databases and in all hard drives for any server), and in workstations/workspaces.

Software Development Lifecycle (SDLC) Workflow

CoBro Consulting's development framework emphasizes trustworthy computing with continuous development, deployment, and testing phases. Each environment has unit testing, automated QA testing, and manual QA testing. In addition, CoBro Consulting performs static code analysis, dynamic code analysis, and manual penetration testing over the deployed code.

Development, Quality Control, and Production Environments

Engineers start the single tenant environment development cycle in the Development environment. Branches are created off of the primary development branch for each ClickUp ticket. When Engineers are ready to introduce the code into the Quality Control branch, they verify the work in their local environments and perform unit tests against the application. When all unit tests pass, a pull request (PR) is initiated in Github for the work to be pulled into the Quality Control environment. A different Engineer reviews the PR for code quality and accuracy. The Engineer who performed the work is not allowed to approve their own work. The QA team tests the Quality Control environment against the acceptance criteria of the ClickUp ticket to ensure the work that was pulled is correct in appearance and function through automated and manual testing. Once the environment has passed these tests, the code is deployed into the Production environment.

New Features

Executive, Customer Success, and Engineering teams routinely collaborate with ideas and suggestions in order to make a better product. The Customer Success team continually interviews prospective clients to discover their needs. Feature requests are handled by the Product team, who work with the clients to understand the business requirements, which are translated into ClickUp for Engineering so they can calculate the time and resources needed to accomplish such enhancements into the platform. The Product team updates the list of features with time and resource capacity, then members of the Executive, Engineering, and Customer Success teams decide which ones should be implemented and by when. The new desired features are proposed and accommodated in an upcoming sprint according to engineering capacity.

Change Management, Approval, and Tracking

All code changes require Engineering review from at least one Developer other than the author of the code. These changes are tracked in ClickUp. All code going from Development to Quality Control and ultimately to Production receives a static analysis of its code to prevent security issues. CoBro Consulting has strict control of changes such as:

- To add a change to the code, a PR must be created, which requires at least one Developer to approve the change.
- Once the change is approved, the team lead will merge it into the code branch.
- When the code is in the Quality Control environment, the QA team will perform automated and manual testing in a test environment. If approved by QA, the process continues to Production.
- In the instance of a bug, CoBro Consulting employs an expedited process that puts a hotfix into Production. The teams create a fix, tests the fix in Quality Control and deploys it to Production.

Service Monitoring

CoBro Consulting validates and monitors the functionality of its services and dependencies on a continuous basis aligned to SLA guarantees. CoBro Consulting keeps an uptime monitor for Compass systemand its components. For each of these components, MS Azure monitors and alerts for quality of service and failure in the components.

Incident Management and Response

It is the responsibility of each CoBro Consulting employee and contractor to immediately report potential security incidents to the appropriate supervisor or security personnel.

A user is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the Information Security Policy immediately to the Information Security Officer or Chief Privacy Officer.

Each incident is analyzed to determine if changes to the existing security structure are necessary. All reported incidents are logged and the remedial action is indicated. It is the responsibility of the Information Security Officer or Chief Privacy Officer to provide training on any procedural change that may be required as a result of the investigation of an incident.

Security breaches are promptly investigated. If criminal action is suspected, the Security Officer or Chief Privacy Officer will contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the Federal Bureau of Investigations.

Customer incidents are documented and tracked by the Customer Success team via ClickUp.

Security Incidents

No system incidents were identified that either (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of the service commitments and system requirements as of October 31, 2024.

Data Backup and recovery

CoBro Consulting maintains a schedule for backups to keep synced with the Disaster Recovery Plan (DRP):

- A daily full backup is created and kept for up to 35 days (Point-in-time-Restore).
- Differential backup is 24 hours
- Long Term Retention Period is 1 month

Disaster Recovery Plan drills are held annually.

In addition to the Information Security Policy, other organizational policies and procedures include, but are not limited to:

- Asset Management
- Data Deletion and Retention
- Data Security Protocols
- Incident Response
- Change Management
- Logical Access

Risk Assessment

A risk assessment is completed annually to review mission-critical aspects of the business, including technology, environment, market, compliance, regulation, fraud, and risk mitigation. The risk assessment is used to define and maintain a current set of controls based on the Trust Services Criteria. A vulnerability self-assessment, including external dynamic security testing, is performed quarterly in order to identify any technical service vulnerabilities.

Quarterly security meetings are conducted in which details surrounding policy updates, responses to risks, and reviews of any possible security breaches are documented. After reviewing past risks, new risks discovered from the previous quarter are listed along with the corresponding impact on different parts of the Company: business continuity, data security, operation security, etc. As stated in the CoBro Consulting Information Security Policy, the Security Council is comprised of representatives from different groups such as the senior management team, Engineering, Data, DevOps, and Human Resources (HR).

Management performs a vendor assessment for new vendors, business partners, and subservice organizations and reviews the SOC 2 Type 2 examination reports for Microsoft Azure to assess potential risks, including security, environmental, and technological changes that impact CoBro Consulting’s risk management strategy.

Information and Communication

CoBro Consulting has implemented methods of communication to help ensure that all employees understand their individual roles and responsibilities to process its controls and ensure that significant events are communicated in a timely manner. These methods include:

- Orientation for newly hired employees
- Ongoing training programs
- Annual re-confirmation of understanding of and compliance with the Information Security Policy
- Publishing diagrams, standards, and procedures regarding the design and operations of the system

CoBro Consulting provides clients with a description of the Compass system in the MSA. The MSA has documented procedures for the identification and escalation of availability issues, security breaches, and other incidents.

Release notes for application changes are made available to employees and contractors (internal users) in ClickUp and are published and made available for external parties for each release.

Monitoring

The controls implemented by CoBro Consulting are measured and monitored through a number of tools and processes, including:

- Compass system performance is monitored using Azure Monitor for overall system performance such as CPU, memory, and disk storage.

Monitoring of the Subservice Organization and Third Parties

CoBro Consulting uses the following subservice organization to assist in the delivery of the Compass system:

- Microsoft Azure provides service to CoBro Consulting such as host the application servers, database servers, and supporting services.

Through its daily operational activities, management of Compass monitors the services performed by the subservice organizations to help ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively. Additionally, CoBro performs annual vendor reviews and reviews SOC reports for any inconsistencies and resolves issues as necessary.

Complementary Subservice Organization Controls

CoBro Consulting controls related to the Compass system cover only a portion of overall internal control for each user entity of Compass. Certain service commitments and system requirements can only be achieved if the subservice organization's controls contemplated in the design of Compass controls are suitably designed and operating effectively along with the related controls at CoBro Consulting. Therefore, each user entity's internal controls must be evaluated in conjunction with CoBro Consulting controls, taking into account the complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Complementary Subservice Organization Controls	Related Criteria
Microsoft Azure	Logical and physical controls are in place and operating effectively involving: - Information Security policy - Enterprise password policy - Multifactor authentication - Role-based access control - Logical access monitoring - Intrusion detecting and monitoring - Security event logging - Encrypted VPN - Firewall management and redundancy - Periodic physical access reviews - Restricted privilege access - EDR anti-virus and malware protection - Periodic penetration testing and vulnerability assessment - SIEM monitoring to protect from cyberattacks - Web application firewall - DDOS protection - Security and facilities administration - Badge and key card administration, surveillance cameras - Environmental controls and monitoring are in place	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.2, A1.2
Microsoft Azure	Information security controls are in place and operating effectively involving: - Segregation of duties - Provisioning and de-provisioning process for employees, contractors, vendors, and customers - Approved customer list administration - Access reviews	CC6.2, CC6.3, CC6.5
Microsoft Azure	Operational controls are in place and operating effectively involving: - Business Continuity - system monitoring	CC7.5, A1.1, A1,3

User Entity Responsibilities

Each user entity must evaluate its own system of internal control for effective risk management and compliance. The internal controls described in this report occur at and are managed by CoBro Consulting and only cover a portion of a comprehensive internal control structure. Each user entity must address the various aspects of internal control that may be unique to its particular organization. This section highlights those portions of the internal control structure that clients have the responsibility to develop and maintain.

- Controls are in place for user organizations to ensure compliance with contractual requirements.

- Controls are in place to provide reasonable assurance the information provided by CoBro Consulting is complete and accurate. Any discrepancies identified by the client are communicated to CoBro Consulting in writing in a timely manner.

- Controls are in place to provide reasonable assurance that proper segregation of duties is appropriately designed and implemented.

- Controls are in place to provide reasonable assurance that procedures and documentation are established for authorizing user access to their own systems and to application functions that interfere with the Company's systems and applications.

- Controls are in place to provide reasonable assurance that individuals authorized to transmit data to the Company are approved by appropriate levels of management and receive adequate and appropriate training.

4. Trust Service Category, Criteria, and Related Controls

Information Provided by Baker Tilly

This section identifies the applicable trust services criteria along with the related controls specified by CoBro Consulting for the following categories:

- ***Security:*** Information and systems are protected against unauthorized access, unauthorized disclosures of information, and damage to the systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- ***Availability:*** Information and systems are available for operation and use to meet the entity's objectives.
- ***Confidentiality:*** Information designated as confidential is protected to meet the entity's objectives.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Control Environment	
CC1.1	The entity demonstrates a commitment to integrity and ethical values. (COSO Principle 1)
1.04	An Employee Handbook is available to all employees and includes a Code of Conduct. New employees are required to sign off acknowledging they have read and received the Employee Handbook and Information Security Policy.
1.05	Performance reviews are conducted at least annually to evaluate employee performance and are based on whether the employee is meeting expectations.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. (COSO Principle 2)
1.01	CoBro Consulting maintains a current organizational chart that outlines the organizational structure and reporting lines.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. (COSO Principle 3)
1.01	CoBro Consulting maintains a current organizational chart that outlines the organizational structure and reporting lines.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.03	Responsibilities and authorities for roles within CoBro Consulting are documented in written job descriptions.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (COSO Principle 4)
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.03	Responsibilities and authorities for roles within CoBro Consulting are documented in written job descriptions.
1.04	An Employee Handbook is available to all employees and includes a Code of Conduct. New employees are required to sign off acknowledging they have read and received the Employee Handbook and Information Security Policy.
1.05	Performance reviews are conducted at least annually to evaluate employee performance and are based on whether the employee is meeting expectations.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (COSO Principle 5)
1.03	Responsibilities and authorities for roles within CoBro Consulting are documented in written job descriptions.
1.04	An Employee Handbook is available to all employees and includes a Code of Conduct. New employees are required to sign off acknowledging they have read and received the Employee Handbook and Information Security Policy.
1.05	Performance reviews are conducted at least annually to evaluate employee performance and are based on whether the employee is meeting expectations.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Communication and Information	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (COSO Principle 13)
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. (COSO Principle 14)
1.01	CoBro Consulting maintains a current organizational chart that outlines the organizational structure and reporting lines.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.03	Responsibilities and authorities for roles within CoBro Consulting are documented in written job descriptions.
2.01	The CoBro Consulting website, Privacy Policy, and Terms of Use are available for internal and external users and outline security commitments and description of the system.
2.02	Internal and external users are provided information on how to report security incidents, failures, concerns, and other complaints, and any high-risk and critical-risk security incidents are evaluated and tracked to resolution.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control. (COSO Principle 15)
2.01	The CoBro Consulting website, Privacy Policy, and Terms of Use are available for internal and external users and outline security commitments and description of the system.
2.02	Internal and external users are provided information on how to report security incidents, failures, concerns, and other complaints, and any high-risk and critical-risk security incidents are evaluated and tracked to resolution.
Risk Assessment	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (COSO Principle 6)
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
CC3.2	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. (COSO Principle 7)
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Risk Assessment	
CC3.2	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. (COSO Principle 7)
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk vulnerabilities are tracked through a ticket to resolution.
10.01	Third-party vendors are subject to non-disclosure agreements, other contractual confidentiality provisions, and CoBro Consulting's vendor screening and management process.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives. (COSO Principle 8)
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
3.02	Management reviews the SOC reports for all relevant subservice organizations to assess potential risks, including security, environmental, and technological changes that impact CoBro Consulting's risk management strategy.
10.01	Third-party vendors are subject to non-disclosure agreements, other contractual confidentiality provisions, and CoBro Consulting's vendor screening and management process.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control. (COSO Principle 9)
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
4.01	A monitoring tool is used to monitor the production environment. Alerts have been configured to notify responsible personnel at certain levels of performance, processing capacity, and availability, and any critical-risk items are tracked through resolution.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk-risk vulnerabilities are tracked through a ticket to resolution.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Monitoring Activities	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (COSO Principle 16)
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
4.01	A monitoring tool is used to monitor the production environment. Alerts have been configured to notify responsible personnel at certain levels of performance, processing capacity, and availability, and any critical-risk items are tracked through resolution.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk-risk vulnerabilities are tracked through a ticket to resolution.
6.04	User access reviews are performed at least annually to assess the access assigned to users based on job descriptions, roles, and responsibilities.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan weekly.
10.01	Third-party vendors are subject to non-disclosure agreements, other contractual confidentiality provisions, and CoBro Consulting's vendor screening and management process.
CC4.2	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. (COSO Principle 17)
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
2.02	Internal and external users are provided information on how to report security incidents, failures, concerns, and other complaints, and any high-risk and critical-risk security incidents are evaluated and tracked to resolution.
Control Activities	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. (COSO Principle 10)
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk-risk vulnerabilities are tracked through a ticket to resolution.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Control Activities	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. (COSO Principle 10)
6.04	User access reviews are performed at least annually to assess the access assigned to users based on job descriptions, roles, and responsibilities.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives. (COSO Principle 11)
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
6.01	Internal and external users require unique user IDs and passwords, including password history, minimum length, and complexity enabled.
7.02	Multifactor authentication is used to authenticate users into systems.
8.01	Firewalls are configured and utilized for protection against threats.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. (COSO Principle 12)
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
2.01	The CoBro Consulting website, Privacy Policy, and Terms of Use are available for internal and external users and outline security commitments and description of the system.
8.03	CoBro Consulting disposes hardware after the retention period has expired, according to the Data Disposal Policy.
10.04	The Disaster Recovery Plan is tested annually and has been established to continue operating in the face of a disaster or other incidents that could disrupt normal business operations.
Logical and Physical Access Controls	
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.
6.01	Internal and external users require unique user IDs and passwords, including password history, minimum length, and complexity enabled.
6.04	User access reviews are performed at least annually to assess the access assigned to users based on job descriptions, roles, and responsibilities.
7.01	Databases are encrypted.
7.02	Multifactor authentication is used to authenticate users into systems.
8.01	Firewalls are configured and utilized for protection against threats.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan weekly.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Logical and Physical Access Controls	
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.
6.02	New and modified access requests are submitted and approved by HR or the department manager for employees and contractors who require access.
6.03	Employee and contractor access is revoked within one business day upon termination of employment.
6.04	User access reviews are performed at least annually to assess the access assigned to users based on job descriptions, roles, and responsibilities.
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.
6.01	Internal and external users require unique user IDs and passwords, including password history, minimum length, and complexity enabled.
6.02	New and modified access requests are submitted and approved by HR or the department manager for employees and contractors who require access.
6.03	Employee and contractor access is revoked within two business days upon the termination of employment.
6.04	User access reviews are performed at least annually to assess the appropriateness of access assigned to users based on job descriptions, roles, and responsibilities.
7.02	Multifactor authentication is used to authenticate users into systems.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
Given that the Compass system is hosted in Microsoft Azure, physical security and the controls related to CC6.4 are the responsibility of Microsoft Azure and are described in the complimentary subservice organization controls presented in Section 3.	
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.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
8.03	CoBro Consulting disposes hardware after the retention period has expired, according to the Data Disposal Policy.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk-risk vulnerabilities are tracked through a ticket to resolution.
7.01	Databases are encrypted.
7.02	Multifactor authentication is used to authenticate users into systems.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Logical and Physical Access Controls	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
7.02	Multifactor authentication is used to authenticate users into systems.
7.03	Management utilizes Transport Layer Security (TLS) and HTTPS for data transmission encryption when transferring data.
8.01	Firewalls are configured and utilized for protection against threats.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan monthly.
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.
7.02	Multifactor authentication is used to authenticate users into systems.
7.03	Management utilizes TLS and HTTPS for data transmission encryption when transferring data.
8.01	Firewalls are configured and utilized for protection against threats.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan weekly.
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.
4.01	A monitoring tool is used to monitor the production environment. Alerts have been configured to notify responsible personnel at certain levels of performance, processing capacity, and availability, and any critical-risk items are tracked through resolution.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk-risk vulnerabilities are tracked through a ticket to resolution.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan monthly.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Systems Operations	
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.
4.01	A monitoring tool is used to monitor the production environment. Alerts have been configured to notify responsible personnel at certain levels of performance, processing capacity, and availability, and any critical-risk items are tracked through resolution.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk vulnerabilities are tracked through a ticket to resolution.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan weekly.
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.
4.01	A monitoring tool is used to monitor the production environment. Alerts have been configured to notify responsible personnel at certain levels of performance, processing capacity, and availability, and any critical-risk items are tracked through resolution.
4.02	Vulnerability scanning of the production environment is completed at least annually, and any critical-risk-risk vulnerabilities are tracked through a ticket to resolution.
8.02	Anti-virus software is installed on laptops, workstations, and production servers, and virus definitions are kept up-to-date and configured to scan weekly.
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.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
2.02	Internal and external users are provided information on how to report security incidents, failures, concerns, and other complaints, and any high-risk and critical-risk security incidents are evaluated and tracked to resolution.
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.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Systems Operations	
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.
2.02	Internal and external users are provided information on how to report security incidents, failures, concerns, and other complaints, and any high-risk and critical-risk security incidents are evaluated and tracked to resolution.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
2.02	Internal and external users are provided information on how to report security incidents, failures, concerns, and other complaints, and any high-risk and critical-risk security incidents are evaluated and tracked to resolution.
10.02	Backups are conducted nightly with a 30-day backup retention period, and any backup failures are reviewed and resolved.
10.03	Restoration testing of backup files is performed at least annually.
10.04	The Disaster Recovery Plan is tested annually and has been established to continue operating in the face of a disaster or other incident that could disrupt normal business operations.
Change Management	
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.
1.02	Policies and procedures have been established to direct CoBro Consulting's work requirements and practices. This includes the Information Security, Logical Access, Change Management, Incident Management, and Incident Response policies.
9.01	A source code repository and versioning tool is used to manage code throughout the development and deployment process.
9.02	Separate environments exist for development, staging, and production.
9.03	Changes are documented, tracked, tested, and approved by authorized IT personnel.
9.04	Changes are peer-reviewed and approved by someone other than the developer.
Risk Mitigation	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
1.06	The Senior Leadership Team, including individuals independent of operations, meets at least quarterly to discuss CoBro Consulting's activities, including the performance of internal controls, results of operations, system availability and capacity, deficiencies, risk assessment, incidents, and fraud.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
10.02	Backups are conducted nightly with a 30-day backup retention period, and any backup failures are reviewed and resolved.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Risk Mitigation	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
10.03	Restoration testing of backup files is performed at least annually.
10.04	The Disaster Recovery Plan is tested annually and has been established to continue operating in the face of a disaster or other incident that could disrupt normal business operations.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.
3.01	An annual risk assessment is performed to identify threats and vulnerabilities for CoBro Consulting. The risk assessment considers factors including information security, application security, physical security, operations, compliance with regulations, and fraud.
3.02	Management reviews the SOC reports for all relevant subservice organizations to assess potential risks, including security, environmental, and technological changes that impact CoBro Consulting's risk management strategy.
10.01	Third-party vendors are subject to non-disclosure agreements, other contractual confidentiality provisions, and CoBro Consulting's vendor screening and management process.
Additional Criteria for Availability	
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
4.01	A monitoring tool is used to monitor the production environment. Alerts have been configured to notify responsible personnel at certain levels of performance, processing capacity, and availability, and any critical-risk items are tracked through resolution.
8.01	Firewalls are configured and utilized for protection against threats.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
10.02	Backups are conducted nightly with a 30-day backup retention period, and any backup failures are reviewed and resolved.
10.03	Restoration testing of backup files is performed at least annually.
10.04	The Disaster Recovery Plan is tested annually and has been established to continue operating in the face of a disaster or other incident that could disrupt normal business operations.
3.02	Management reviews the SOC reports for all relevant subservice organizations to assess potential risks, including security, environmental, and technological changes that impact CoBro Consulting's risk management strategy.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
10.03	Restoration testing of backup files is performed at least annually.
10.04	The Disaster Recovery Plan is tested annually and has been established to continue operating in the face of a disaster or other incident that could disrupt normal business operations.

Trust Services Criteria / Controls Specified by CoBro Consulting, LLC	
Additional Criteria for Confidentiality	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
8.03	CoBro Consulting disposes hardware after the retention period has expired, according to the Data Disposal Policy.
8.04	The Data Retention Policy is in place to help ensure that confidential data is secure and records are retained according to the policy or as otherwise required by applicable state or federal law.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
8.03	CoBro Consulting disposes hardware after the retention period has expired, according to the Data Disposal Policy.
8.04	The Data Retention Policy is in place to help ensure that confidential data is secure and records are retained according to the policy or as otherwise required by applicable state or federal law.