JOHANSON GROUP

System and Organization Controls (SOC) 3 Report

Relevant to the Trust Services Criteria for Security Category

For the Period

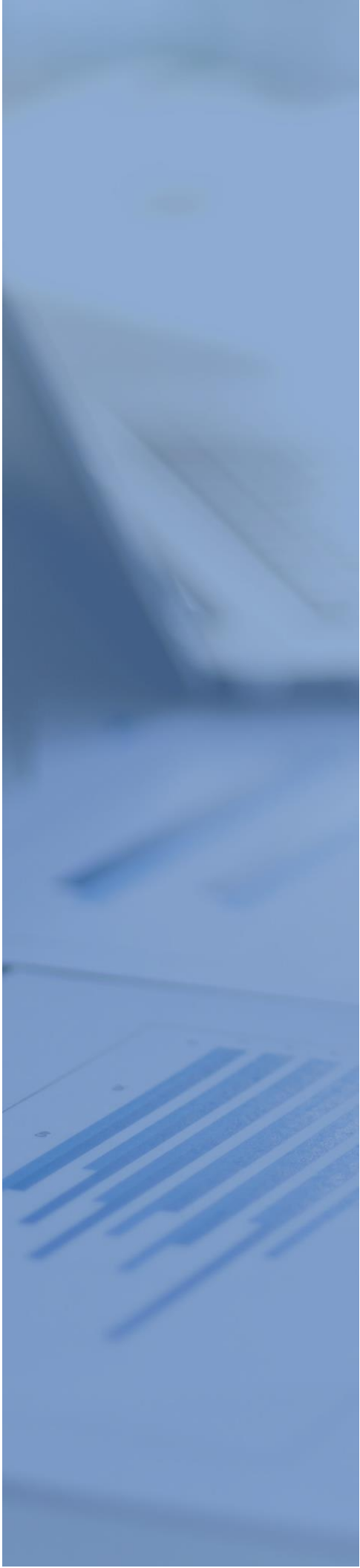
January 28, 2023 to April 28, 2023

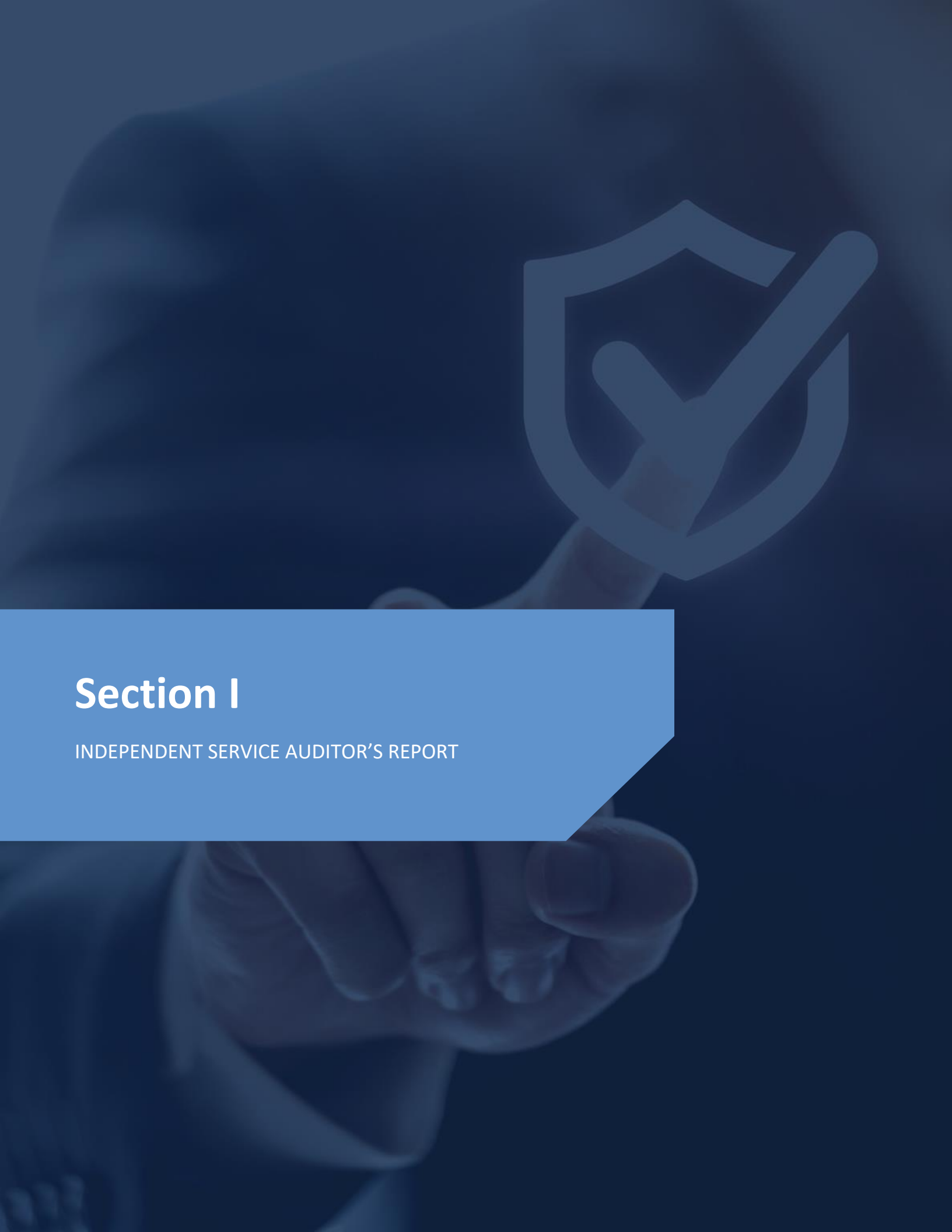
Together with Independent Service Auditor's Report

Report on Management's Assertion related to its

Follow Up Boss

TABLE OF CONTENTS





Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Enchant, LLC

Scope

We have examined Enchant, LLC's accompanying assertion titled "Assertion of Enchant, LLC Management" (assertion) that the controls within Enchant, LLC's Follow Up Boss System (system) were effective throughout the period January 28, 2023 to April 28, 2023, to provide reasonable assurance that Enchant, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (trust services criteria).*

Service Organization's Responsibilities

Enchant, LLC 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 Enchant, LLC's service commitments and system requirements were achieved. Enchant, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Enchant, LLC is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Enchant, LLC's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Enchant, LLC's service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the

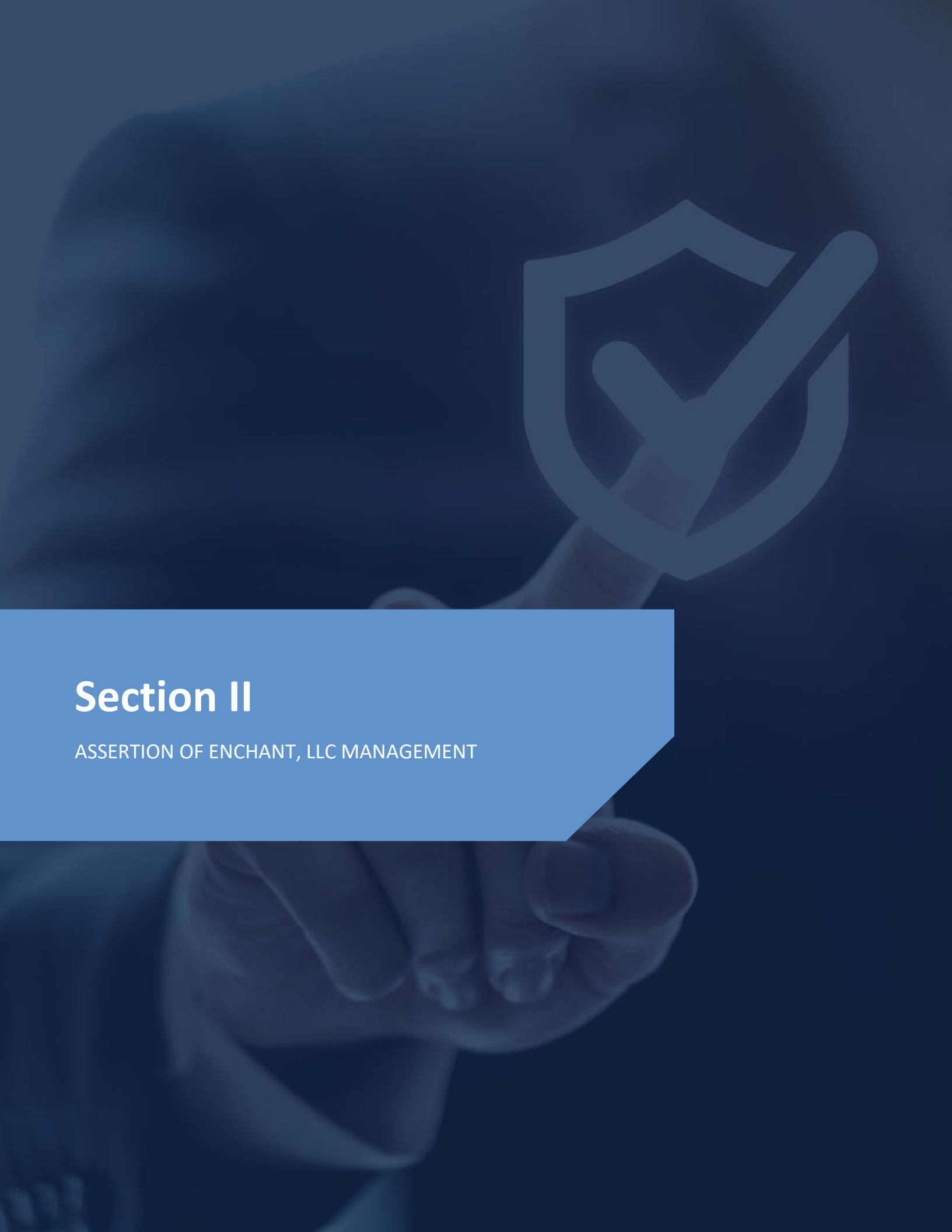
future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Enchant, LLC's Follow Up Boss system were effective throughout the period January 28, 2023, to April 28, 2023, to provide reasonable assurance that Enchant, LLC service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
December 8, 2023



Section II

ASSERTION OF ENCHANT, LLC MANAGEMENT

We have prepared the accompanying description of Enchant, LLC's "Description of Follow Up Boss" for the period January 28, 2023 to April 28, 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 Enchant, LLC's Follow Up Boss (system) that may be useful when assessing the risks arising from interactions with Enchant, LLC's system, particularly information about system controls that Enchant, LLC 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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA, Trust Services Criteria).*

We are responsible for designing, implementing, operating, and maintaining effective controls within Enchant, LLC's Follow Up Boss system (system) throughout the period January 28, 2023 to April 28, 2023, to provide reasonable assurance that Enchant, LLC's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Follow Up Boss" and identifies the aspects of the system covered by our assertion.

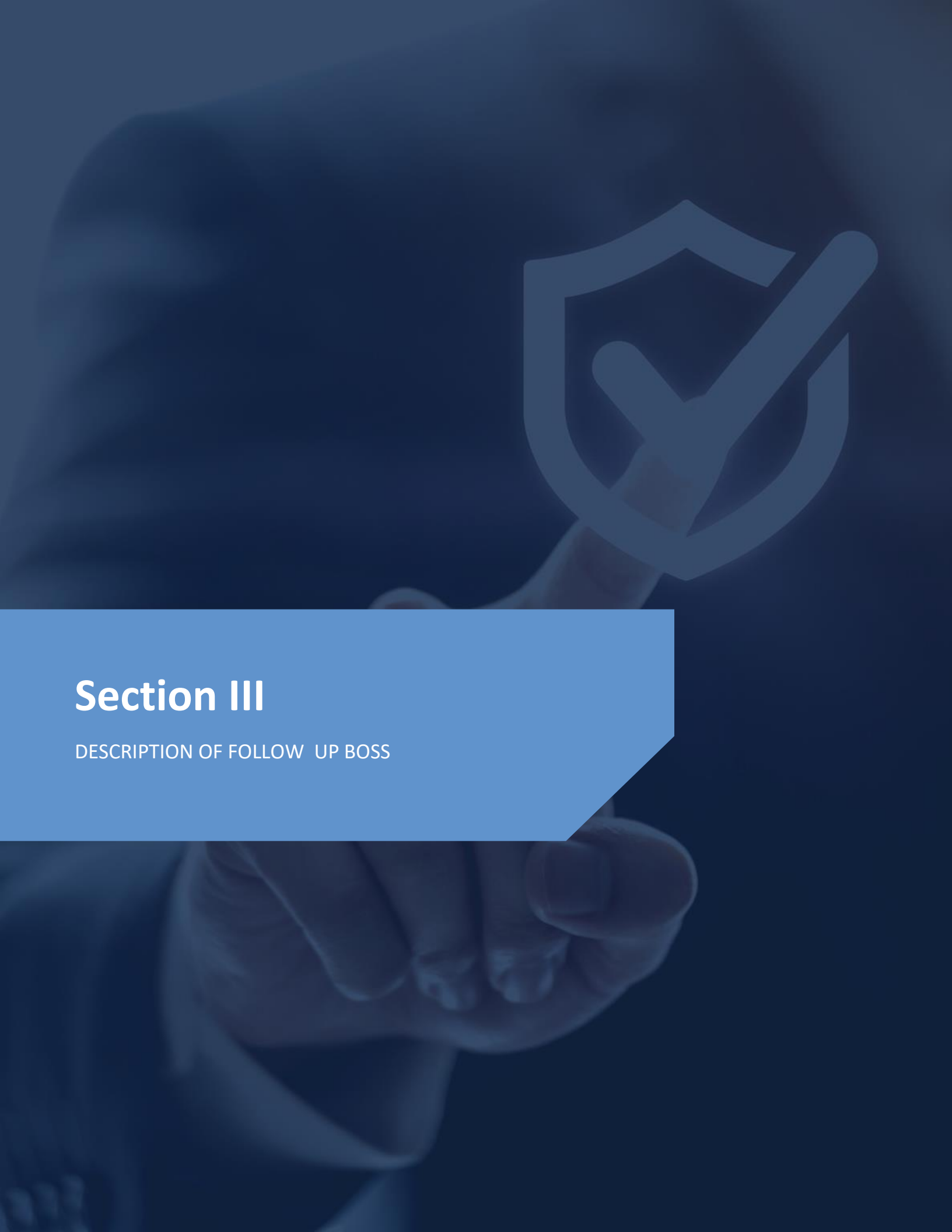
We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 28, 2023 to April 28, 2023, to provide reasonable assurance that Enchant, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Enchant, LLC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 28, 2023 to April 28, 2023, to provide reasonable assurance that Enchant, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Enchant, LLC Management
December 8, 2023



Section III

DESCRIPTION OF FOLLOW UP BOSS

COMPANY BACKGROUND

Enchant, LLC dba Follow Up Boss ("FUB" or the "Company") optimizes core sales activities for real estate agents and teams to help them set more appointments and close more deals with their leads, past clients, and sphere of influence.

The first line of code for Follow Up Boss was written WAY back in April 2011. It stemmed from an interview with our very first customer who told us a story about how he couldn't even sit down to watch a movie with his kids because he had to stay on his phone, manually forwarding leads out to his agents that came into his email.

Fast forward 11 years, and we're now a team of 90+ (and growing), serving thousands of brokers, team leaders, and solo agents just like him, helping to solve the many challenges around the fast-paced, always-on, relentless business of real estate sales.

Dan Corkill has spent over 10+ years personally working with top-producing agents and teams, discovering what drives their success and developing tools to help them expand their business with less effort. He often offers his knowledge of lead conversion, real estate technology, and entrepreneurship on webinars, panels, and online forums.

SERVICES PROVIDED

The Follow Up Boss application makes it incredibly easy for real estate teams and operators to manage their clients/contacts/relationships in a single platform as well as tools to communicate directly with those contacts (email, phone, and text). Follow Up Boss is delivered as a web and mobile application; it automatically syncs with a customer's email and calendar system.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Follow Up Boss designs its processes and procedures related to its platform to meet its objectives for providing CRM to its clients. Those objectives are based on the service commitments that FUB makes to user entities, the laws and regulations that govern the provision of FUB's services, and the financial, operational, and compliance requirements that FUB has established for the services. The SaaS services of FUB are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which FUB operates.

Security commitments to user entities are documented and communicated in the Terms of Service, Privacy Policy, and any Service Level Agreements (SLAs) or other customer agreements, as well as in the description of the service offering provided online.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Follow Up Boss platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use encryption technologies to protect customer data both at rest and in transit.

Follow Up Boss (FUB) establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in FUB's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the 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 Follow Up Boss platform.

COMPONENTS OF THE SYSTEM

Infrastructure

Follow Up Boss system infrastructure is supported by cloud platform technologies, including application and database hosting, networking tools, and cloud storage.

Software

Follow Up Boss software is developed for web browsers, iOS and Android platforms.

Follow Up Boss web browser application is delivered via a single-page application architecture that interfaces with Follow Up Boss APIs.

iOS and Android applications are natively developed and interface with Follow Up Boss APIs.

People

Follow Up Boss has a current staff of 95 employees and contractors organized into the following functional areas:

Product: Individuals who are responsible for understanding customer needs, creating new features, and working with our internal team to bring them to market. Besides choosing what to build, they communicate the benefits and measure the performance of the product.

Development | Engineering: Engineers who design and maintain the Follow-Up Boss product, including the web interface, the proprietary sync engine, infrastructure, and all debugging tools. This team designs and implements new functionality, and assesses and remediates any issues or bugs found in the product.

People + Operations: Individuals who are responsible for the day-to-day management and operation of the company. This team handles all of the business administration of systems, equipment, people, and processes needed to make the organization function. People Operations is a strategic business function that focuses on putting the employee first by humanizing impersonal systems and continuously improving employee engagement, development, and retention.

Advocacy: The customer success team is central to our business as this role helps our customers set up and implement strategies to drive more business for them and their teams. Our Customer Support Experts are the helping hand that our users count on; internally they serve as the pulse of our users and customer experts.

Marketing: The internal team that drives the promotional engine of a business. Responsible for increasing brand awareness, while also driving potential and recurring customers to a company's products or services.

Sales: Our sales team works directly with prospective customers to understand their business, and their goals, and demonstrate the value Follow Up Boss will provide.

Data

Follow Up Boss classifies its data to ensure appropriate security measures are implemented to protect the confidentiality, integrity, and availability of the data. The data we collect from our customers is subject to the Follow Up Boss Privacy Policy and Terms of Service.

Customer Data

Customer data is retained and deleted in line with FUB's Privacy Policy and Terms of Service.

All databases, data stores, and file systems are encrypted according to Follow Up Boss's Encryption Policy.

PROCESSES AND PROCEDURES

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Follow Up Boss (FUB) policies and procedures that define how services should be delivered. These are located in the Company's handbook and can be accessed by any Follow Up Boss team member.

Physical Security

All data is hosted by cloud technology providers.

Logical Access

Follow Up Boss (FUB) applies role-based access controls, follows principles of least privilege, and performs periodic user access reviews.

Follow Up Boss (FUB) uses single sign on and multi-factor authentication.

The management team is responsible for onboarding new employees. A background check must be performed prior to hire, and once hired, the employee is responsible for reviewing and accepting Follow Up Boss (FUB)'s policies and completing security training. Employees perform all work duties on FUB company-managed device with full-disk encryption and endpoint protection.

When an employee is terminated, access to systems is removed and company-owned devices are collected in accordance with the company's Asset Management Policy.

Computer Operations – Backups

Customer data is backed up by Enchant, LLC dba Follow Up Boss (FUB) regularly to ensure continuation and continuity of service. Enchant, LLC dba Follow Up Boss (FUB)'s backup processes are reviewed regularly to make sure customer data remains secure and available.

Backup infrastructure is maintained by a third-party provider with physical access restricted according to applicable policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via IAM permissions.

Computer Operations – Availability

Follow Up Boss (FUB) maintains an Incident Response Policy that gives any Follow Up Boss (FUB) employee the ability to report a potential information security event.

External parties (customers and third-party security researchers) are also given a channel to send encrypted incident reports and responsibly disclose potential issues to the Follow Up Boss (FUB) security team.

Internally, the Follow Up Boss (FUB) infrastructure team monitors the health of all applications, including the Follow Up Boss (FUB) web UI, databases, and cloud storage. Monitoring occurs 24x7 and includes the availability and performance of the web UI, the throughput and queuing latency of the job scheduler, and any faults or errors encountered by users while configuring Follow Up Boss (FUB) or while their data is being synced by Follow Up Boss (FUB).

Follow Up Boss (FUB) employs vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Control

Follow Up Boss (FUB) maintains documented Software Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes through a process that is consistent and repeatable. This policy defines the high-level requirements for providing program and project stakeholders guidance to support the approval, planning, and life-cycle development of Follow Up Boss software systems, including change requirements, test procedures and results, change approval and release notification.

Data Communications

Data is replicated across multiple availability zones within cloud infrastructure providers for redundancy and disaster recovery.

Follow Up Boss (FUB) engages an external security firm to perform annual vulnerability scans and annual testing to look for unidentified vulnerabilities, and the product/engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Services performed by Follow Up Boss (FUB). This report does not include the data center hosting services provided by our cloud hosting providers.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
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 removals of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Follow Up Boss (FUB)'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Follow Up Boss (FUB)'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Follow Up Boss (FUB)'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Follow Up Boss (FUB)'s management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Follow Up Boss (FUB) can help customers build workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Follow Up Boss (FUB) to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Follow Up Boss is currently organized in a simple, flat structure in which all employees report directly to the CEO, COO, and CTO. As the team grows, management will elect to build an organizational structure that ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting upward and downward in the organizational hierarchy.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Follow Up Boss's success is founded on and reinforced by a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensures the organization operates at maximum efficiency. Follow Up Boss's human resources policies and practices relating to employee hiring, onboarding, role-specific training, evaluation, coaching, promotion, compensation, and disciplinary activities.

Specific control activities that the organization has implemented in this area are described below:

- New employees are required to sign a non-disclosure agreement prior to their first day of employment.
- Evaluations for each employee are performed on an annual basis on their work anniversaries.
- 1:1 coaching sessions take place at least every 3 months
- Employees are sent our employee handbook that details our policies, procedures, benefits, and career path progression on their first day of employment
- Employee termination procedures are in place to guide the termination process and are documented in an offboarding checklist.

RISK ASSESSMENT PROCESS

Follow Up Boss (FUB)'s risk assessment process identifies and manages risks that could potentially affect FUB's ability to provide reliable

and secure services to our customers. As part of this process, Follow Up Boss (FUB) maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks. The risk register is reevaluated annually, and tasks are incorporated into the regular Follow Up Boss (FUB) product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Follow Up Boss (FUB)'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Follow Up Boss (FUB) addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Follow Up Boss (FUB)'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATIONS SYSTEMS

Information and communication are integral components of FUB's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

FUB uses several information and communication channels internally to share information with management, employees, contractors, and customers. FUB uses chat systems and email as the primary internal and external communication channels. FUB maintains policies for the appropriate use of electronic communications by FUB personnel. These policies set restrictions on use of electronic communications, disclosure of privileged information, public representations, spam, and intellectual property. In addition, FUB communicates with customers via customer support applications.

Structured data is communicated internally via our SaaS applications and our project management tools. Finally, FUB uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. FUB's management and security teams perform monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Follow Up Bosses (FUB)'s management conducts quality assurance monitoring on a regular basis and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in FUB's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any

control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of FUB's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM IN THE LAST 12 MONTHS

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

INCIDENTS IN THE LAST 12 MONTHS

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant Common Criteria/Security trust services criteria were applicable to the Follow Up Boss (FUB) Services system.

COMPLEMENTARY USER ENTITY CONTROLS

Follow Up Boss (FUB) services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Follow Up Boss's services to be solely achieved by Follow Up Boss (FUB) control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Follow Up Boss (FUB).

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Follow Up Boss.
2. User entities are responsible for notifying Enchant, LLC dba Follow Up Boss (FUB) of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Enchant, LLC dba Follow Up Boss (FUB) services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Enchant, LLC dba Follow Up Boss (FUB) services.
6. User entities are responsible for immediately notifying Enchant, LLC dba Follow Up Boss (FUB) of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.