Report on Warren Averett's Description of Its Technology Department Services and Connect Platform and the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to the Security, Availability, and Confidentiality Categories Throughout the Period June 1, 2023 to May 31, 2024

System and Organization Controls (SOC) 3 Report
Prepared in Accordance with AICPA Attestation Standards

HANCOCK ASKEW & CO LLP
ACCOUNTANTS & ADVISORS

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Warren Averett Management

Scope

We have examined Warren Averett management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of its Controls over the Technology Department Services and Connect Platform Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Warren Averett's (the "Company") controls over the Technology Department Services and Connect Platform (System) were effective throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Warren Averett's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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)*.

Warren Averett uses subservice organizations for internal/external communications, data storage and classification, collaboration tools, tax preparation software, audit confirmations, accounting servicing platform, marketing tools, servers and proxy services, email archives, for data retention and email spam services, and electronic signature devices. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Warren Averett, to achieve Warren Averett's service commitments and system requirements based on the applicable trust services criteria. The description presents Warren Averett's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Warren Averett'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.

Management's Responsibilities

Warren Averett's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Warren Averett's service commitments and system requirements were achieved. Warren Averett management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, 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 obtain reasonable assurance about whether management's assertion is fairly stated, in all material aspects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtained an understanding of Warren Averett's relevant security policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Warren Averett's cybersecurity risk management program. Accordingly, we do not express an opinion on any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Warren Averett and to meet our ethical responsibilities, as applicable for examination engagements set forth in the Preface Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Warren Averett's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Warren Averett's controls over the System were effective throughout the period June 1, 2023 to May 31, 2024 to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Hancock Askew & Co., LLP

Peachtree Corners, Georgia
August 12, 2024

SECTION 2

ASSERTION OF WARREN AVERETT MANAGEMENT

Assertion of Warren Averett Management

We, as management of, Warren Averett, are responsible for:

- Identifying the Warren Averett Technology Department Services and Connect Platform and describing the boundaries of the System, which are presented in Section 3
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of our principal service commitments and system requirements that are the objectives of our system, which are presented in Section 3
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust service categories and associated criteria that are the basis of our assertion

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that the service commitments and system requirements were achieved based on the criteria relevant to security set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*

Very truly yours,

Warren Averett

SECTION 3

WARREN AVERETT'S DESCRIPTION OF ITS TECHNOLOGY DEPARTMENT SERVICES AND CONNECT PLATFORM THROUGHOUT THE PERIOD JUNE 1, 2023 TO MAY 31, 2024

Overview of Operations

Warren Averett is a private organization that provides tax, audit, accounting and consulting services to clients in all sectors and businesses across the Southeastern United States. The Company, established in 1972, is headquartered in Birmingham, Alabama and operates from locations in Georgia, Florida, and Alabama.

The company recognizes that the services it delivers rely heavily on our commitments, integrity, focus on the client and their businesses, and information technology. Relying on information technology so heavily, we understand the exposure to increasing levels of risk from external threats. A custom portal designed and implemented called Warren Averett Connect helps facilitate interactions of sharing and distributing documents such as filed tax returns, financial statements and sensitive documents. These documents are transmitted and stored securely and available 24/7 in the Connect portal infrastructure.

Warren Averett provides several tailored service solutions under the tax and accounting services, audit and assurance services, and consulting umbrella.

Tax and Accounting Services – Warren Averett has built a team of professionals with specialized expertise to ensure its clients employ sophisticated strategies that make the most of business opportunities. These professionals are experts in important areas such as mitigating taxes on operations, mergers and acquisitions, business succession planning, maximizing after tax enterprise value, state and local tax, international tax and tax controversy assistance.

Audit & Assurance Services – Warren Averett offers audit and assurance services, including: Internal Audits, Audit Review and Compilations, Specialized Audits, Review and Assurance, SEC and IFRS Reporting.

Consulting Services – Warren Averett provides a broad range of innovative solutions and strategic guidance around some of the most challenging business circumstances and opportunities.

Description of Services Provided

The scope of this report covers internal controls within the Warren Averett Information Technology Department as well as Warren Averett Connect, the secure document management and delivery system, applicable to the Security, Availability and Confidentiality Trust Services Criteria. Warren Averett utilizes certain third parties which are considered subservice organizations. The activities performed by these subservice organizations are not within the scope of this report.

Warren Averett Connect – Designed, Implemented, and supported by Warren Averett. Each client is provided with access. Offers a dedicated storage area for sharing and interactions with documents securely 24 hours a day 7 days a week.

The Warren Averett Connect Portal is accessed via a web browser. The system utilizes a Secure Sockets Layer (SSL) encrypted communication stream to protect data in transit. The data at rest is also protected by encryption down to the hardware layer. To ensure ultimate accountability, an audit trail logs all activity in the system by username and IP address. The Connect Portal is accessible from almost all internet connected smart devices and computers.

Principal Service Commitments and System Requirements

Warren Averett makes service commitments to its clients and has established system requirements as part of its core services. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Warren Averett 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 Warren Averett's service commitments and system requirements are achieved.

Service commitments to clients are documented and communicated in Terms of Engagement Letters, End User Agreements, Business Associate Agreements and in the description of the services offered as provided on Warren Averett's website. Service commitments include, but are not limited to, the following:

- Security: Warren Averett has made commitments related to securing client data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, logical security and other relevant security controls.
- Availability: Warren Averett has made commitments related to availability for its Warren Averett Connect Portal as well as commitments related to terms of engagements.
- Confidentiality: Warren Averett has made commitments related to maintaining the confidentiality of client data through data classification policies, data encryption and other relevant security controls.

Warren Averett has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Warren Averett's system policies and procedures, system design documentation, and contracts with clients. 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 various Warren Averett services.

Components of the System Used to Provide the Services
This system description covers the Warren Averett services, and it is comprised of the following areas:

1. Infrastructure
2. Software
3. People
4. Processes & Procedures
5. Data

Infrastructure

Physical Locations

Offices: The Headquarters (HQ) is located at 2500 Acton Road, Birmingham, Alabama. Access points to the facilities are secured by a Radio-Frequency Identification (RFID) card key entry system. Visitors enter through the main entrances and obtain a visitor's badge and are escorted throughout the building. All unmonitored entry and exit points are self-closing and auto-locking when closed.

- Birmingham, Alabama – Acton Road Office (HQ)
- Homewood, Alabama – University Park Office
- Anniston, Alabama – Anniston Office
- Huntsville, Alabama – Huntsville Office
- Cullman, Alabama – Cullman Office
- Montgomery, Alabama – Montgomery Office
- Foley, Alabama – Foley Office
- Mobile, Alabama – Mobile Office

- Atlanta, Georgia – Atlanta Office
- Pensacola, Florida – Pensacola Office
- Fort Walton Beach, Florida – Ft. Walton Office
- Destin, Florida – Destin Office
- Panama City, Florida – Panama City Office
- Tampa, Florida – Tampa Office

The facilities are protected by a monitored smoke and fire suppression and detection system, which automatically communicates to the fire department in case of an emergency.

Data Centers: Warren Averett utilizes two data centers that are geographically separated. Each data center is secured via access controls and monitored via video.

Warren Averett's primary data center is located at 2500 Acton Road, Birmingham, Alabama. The facility is setup with recorded video surveillance. Access to the facility is controlled by RFID card key entry systems. The facility is protected by cooling systems, two generator backups, communication lines and fire detection / suppression systems.

Warren Averett's secondary data center is located at 101 Monroe St NW, Huntsville Alabama. The secondary data center is secured via electronic card key access, and recorded video surveillance. The secondary data center is in use and is also used as a functioning office serving the surrounding clients of Montgomery, Alabama.

Access requests to the data centers require a documented access request and manager approval prior to access being provisioned. Access is reviewed quarterly by management. Each data center has un-interruptible power supplies, generators, and primary and secondary internet connectivity. Warren Averett deploys a combination of storage level replication and server snapshotting to transfer data between data centers automatically.

The following equipment is used to deliver, maintain and provide access to Warren Averett Connect, CCH Axcess, Office365 Core, Azure, Mimecast, Intacct, Confirmation.com, Hubspot, and DocuSign systems:

Primary Data Center (Birmingham, Alabama)

Item	Description
Palo Alto Firewalls	Firewall
Cisco Catalyst 9500	Core Switching/Storage
Cisco Catalyst 3750 Switch	Core Switching
Cisco Catalyst 2960 Switch	Endpoint Switching
Cisco ISR 4431	Routing
HP GEN 10 DL360 Servers	Server Cluster (Hyper-v)
HP NetAPP AF250 SAN	Storage

Secondary Data Centers (Huntsville, Alabama) (In Commission on 12/8/2023):

Item	Description
Palo Alto Firewalls	Firewall
Cisco Catalyst 4500	Core Switching
Cisco ISR 4331	DR Routing
Cisco Catalyst 2960 Switch	Endpoint Switching
Cisco ISR 4431	Routing
Lenovo 3550 Servers	Server Cluster (Hyper-v)
HP 3PAR 8400 SAN	Storage
HP NetApp SAN	Storage
Cisco Nexus 3000	Server Switches
Brocade FC Switches	Server Storage Switches

Secondary Data Center Montgomery, AL (Out of Commission on 12/8/2023):

Item	Description
Palo Alto Firewalls	Firewall
Cisco Catalyst 4500	Core Switching
Cisco ISR 4331	Routing
Cisco 2950	Endpoint Switching
Netapp SAN	Storage
Solidfire SAN	Storage
Cisco Fabric Interconnects	Switch Interconnects
Cisco UCS Chassis	Server Blade Chassis
Cisco UCS Blades	Server Blades(Hyper-V)

Change management controls exist to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled information technology infrastructure to minimize the number and impact of any related incidents upon service.

System Maintenance

As part of Warren Averett's standard maintenance process, all operating system software is updated, and security patches applied on a scheduled and regular basis. Critical systems, such as the virus protection database, utilize automated processes to download and perform updates in real time. Logs are maintained documenting system maintenance and updates.

System changes are derived from internal and client requests and internal monitoring and planning processes. A ticketing/change management system is used to track network and system changes.

Network Security

Warren Averett utilizes Palo Alto firewalls, Carbon Black, Applocker, CyberARK, and Windows Defender. Firewalls provide an intrusion detection system (IDS), real-time data analysis, and web virus protection. Carbon Black, Windows Defender, CyberARK and Applocker provide a complete layer of defense against threats against endpoints. Updates to the virus databases are published by Palo Alto, Carbon Black, and Microsoft and are downloaded and implemented in real-time. All firewall notifications, IDS alerts, and virus notifications are logged. Critical notifications and alerts are emailed to Warren Averett IT employees. Follow-up and escalation procedures are in place to notify management and clients in the event of a serious breach.

Third party software is utilized to conduct a perimeter scan and vulnerability assessments of the network on an ad-hoc basis. Results are reviewed by information security analysts and senior management and appropriate changes are implemented as considered necessary.

Backup and Recovery Systems

Warren Averett utilizes a combination of hardware and software level replication and backup systems to ensure client data availability. Hyper-V virtual servers are replicated to the secondary datacenter. Snapshots via snapshotting technology is stored on a HP NetAPP storage area network (SAN) and taken daily located in the primary data center.

Software

Warren Averett's suite for software to be able to meet the service commitments, consists of a suite of proprietary, non-proprietary, as well as third-party software packages. All virtual servers and supporting servers are built on a combination VMWare's hypervisor software and Microsoft's HyperV hypervisor software.

Item	Description
Carbon Black	Virus & Malware Protection
Confirmation.com	Transaction Confirmation Service (SaaS)
CCH Axcess	Engagement Management Binder Software
Confirmation.com	Bank Statement confirmations
CyberARK	Application Whitelisting, Admin Restriction
Hubspot	CRM, Annual Revenue Projections
Hyper-V	HyperVisor
Intacct	Tax Prep Software
Live Action	Network Performance Monitoring
ManageEngine ServiceDesk	Ticketing and Support, System Inventory, Process/Change Control & Approval
Microsoft Applocker	Application Blacklist/Whitelist

Item	Description
Office365 Core	Email and Office Applications/Servers, SharePoint, Teams
SCCM	Endpoint management and compliance
Mimecast	Email Archiving, Spam Filter (New Spam/Archive)
Splunk / Microsoft Sentinel	Security Information and Event Management (SIEM), System Performance Monitoring
Team Foundation Server	CodeBase Storage for WA Connect
Windows Defender	Virus & Malware Protection
Windows Server	Virtual & Physical Servers

Only authorized system administrators can install software on system devices. Unauthorized use or installation of software is explicitly covered in the personnel and policy guide.

People

Hiring

Warren Averett has formal hiring practices designed to ensure that new employees are qualified to carry out their job responsibilities. All job requirements within the company are documented. Hiring policies require that criminal and credit background checks and employment verifications are conducted for each new prospective employee. New employees are required to submit a written confirmation that they have read the Personnel and Policy Guide. Warren Averett's policies include non-disclosure and confidentiality agreements. The agreement contains clear guidelines of the employee's role in protecting client information. The personnel and policy guide is provided to all new employees and contains policies and sections on confidentiality, disclosure of information, code of conduct and ethical standards, office security, and use of Warren Averett equipment. Employees are notified of changes to the personnel and policy guide as they occur.

Training

Management establishes requisite skillsets for personnel, whether an employee, contractor, or vendor employee, and provides continued training about its commitments and requirements for personnel to support the achievement of objectives. Personnel are trained through outside seminars, educational material, in-house courses, and on-job training. Employees are required to participate in periodic training regarding information security, including review of internal policy and procedures, industry standards, and best practices. A security awareness program exists to educate employees about potential threats, and how to safeguard information.

Specific training is conducted as necessary. Employees are required to participate in training regarding applicable legal and compliance issues regarding the protection of sensitive data and information. Attendance logs are maintained to document and monitor attendance for all training sessions.

The company maintains written policies and procedures necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, which are provided to personnel to carry out their responsibilities. These policies are available to all employees through Warren Averett's Knowledgebase. The CIO and Director of Network and Security are charged with establishing, maintaining, and enforcing the overall security policies and procedures.

Terminations

Documented procedures provide a checklist and guidelines for termination of employment. This includes the recovery of company property and logical and physical security access changes. Physical and logical security access is revoked immediately upon termination and the terminated employee is escorted off site. Badge access cards and any other company property are returned to Human Resources.

Processes and Procedures

Operations

Established procedures for job monitoring and documentation are in place. Daily backups ensure that backup images of critical business data and storage systems are taken and secured by disk-disk operations. Weekly and monthly backups are utilized to take snapshots of entire business applications and systems. The communication and transmission of data files to and from Warren Averett are conducted in accordance with documented security procedures. This includes the use of encryption and file transmission methods. Access is controlled by user identification and password.

Access to upload or download secured information is controlled by user identification and passwords. In accordance with documented procedures, operations personnel are responsible for monitoring and managing system activities, job execution, and system resources to ensure the successful completion of all system processing.

Data

Warren Averett treats all client data as confidential in nature and conducts the planning, design, and implementation of systems under confidentiality guidelines and policies. Formal information sharing agreements are in place with end users and vendors and include confidentiality commitments applicable to that entity. A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. Data is stored in encrypted format using software supporting the advanced encryption standard (AES).

Data Retention and Disposal

Formal data retention and disposal procedures are in place to guide the secure disposal of company and client data. Warren Averett physically destroys all media storage devices utilizing a third party that employs secure destruction confirmation and methods.

Control Environment

Control environment elements include the following, and the extent to which each element is addressed at data management is described below:

- Management Controls, Philosophy, and Operational Style
- Integrity and Ethical Values
- Standards of Conduct
- Commitment to Competence
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Security Awareness

Management Controls, Philosophy, and Operational Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security, and establishing and maintaining sound internal controls over all functional aspects of operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in client support and transactional processing.

Formal job requirements and regular departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under Warren Averett's policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring client base for trends, changes, and anomalies.

Integrity and Ethical Values

Warren Averett has programs and policies designed to promote and ensure integrity and ethical values in its environment.

Warren Averett desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Warren Averett has developed professional conduct policies that set forth policies of importance to all employees related to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violation of these polices or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

Warren Averett has implemented standards of conduct to guide all employee and contractor behavior. The code of business conduct and ethical standards are reviewed and updated at least annually and are approved by the Board of Directors or the Information Technology Steering Committee, as appropriate. All employees must read and affirm acceptance of the code of conduct and ethical standards upon hire and again when changes are made. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resource (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Warren Averett monitors personnel compliance through monitoring complaints and employs an anonymous ethics hotline. Any employee found to have violated the company's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

Warren Averett has formal requirements that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirements. Job requirements are reviewed by management on an annual basis for needed changes. Employee performance is evaluated using a bottom-up approach through the Firm's CEO of Me Program. This program allows employees to set clear goals and objectives each year that are then reviewed and adjusted by Management as deemed appropriate. Follow-up meetings are held throughout the year to measure performance against those goals and then summarized in an end of year meeting with the team members. Participation in the CEO of Me is not mandatory for all employees, however, all are encouraged to participate.

Organizational Structure

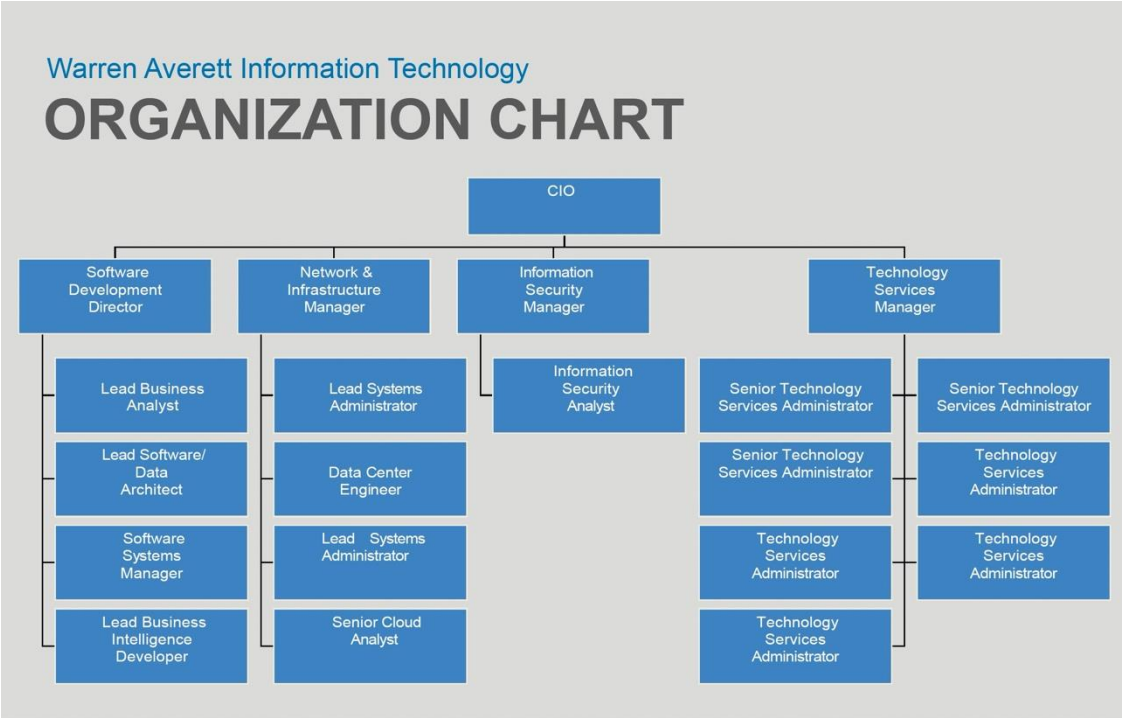
Warren Averett's organizational structure provides the framework within which its activities for achieving objectives are planned, executed, controlled and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. As a limited liability company, Warren Averett's management derives its authority from all of its Members.

Assignment of Authority and Responsibility

The Executive Committee's role is to set the strategic direction of the Firm. The Chief Executive Officer (CEO) serves as Chairperson of the Committee. Additional Members are elected to serve rotating terms on the Committee, and the Committee appoints at-large Members as deemed necessary.

The role and focus of the Operations Board is to develop, implement and maintain operational best practices that will ensure the strategic directives of the Executive Committee and CEO are met. The Board is comprised of individuals from each geographical region of the Firm. The CEO appoints the Chairperson of the Operations Board and the Chairperson appoints other members. Membership on the Board is reviewed on an annual basis and changed as deemed appropriate by the CEO and/or Board Chairperson.

Management has established the Chief Information Officer role who reports to the Chief Operating Officer (COO). This role and responsibilities are relevant to the firm's technology division as well as security.
the following organizational chart depicts Warren Averett's IT corporate structure:



Standard Operating Controls

Warren Averett's management provides guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

Warren Averett has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. Warren Averett conducts pre-employment reference checks from information provided on the employment application. In addition, prior to employment and annually thereafter, Warren Averett personnel and select senior management employees involved with or overseeing services are subject to financial and criminal background checks.

Warren Averett invests significant resources in employee development by providing on- the-job training and other learning opportunities.

Security Awareness

Warren Averett requires all new hires to attend a New Hire training program which also includes information security policies and guidelines. All employees are made aware of the security implications that revolve around their job functions and actions through ongoing annual security training.

Risk Assessment

Warren Averett has a cross functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect Warren Averett's ability to meet its contractual obligations. Risk assessment efforts include analysis of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella insurance policies. The Warren Averett Executive Committee performs a risk assessment at least annually or upon significant change to identify the information required and expected to support the internal control and achievement of its service commitments and system requirements. The assessment includes the definition of and risks surrounding the most mission-critical aspects of its service commitments, and internal and external sources of data, as well as identifying ways that fraud, misconduct, and non-compliance with laws and regulations can occur.

The Executive Committee and Operations Board identify significant risks and communicate proposed measures to management in order to mitigate those risks. Warren Averett employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated detection technology. Warren Averett strives to identify and prevent risks, including the risk of fraud, at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered through either team structure, meetings, third party reviews, or notifications. The CIO, Network and Infrastructure Manager, and the Information Security Manager assess security risks on an ongoing basis through regular meetings with IT personnel and/or the Operations Board and Executive Committee, reviewing and acting upon security event logs, performing vulnerability assessments, and through the performance of the annual risk assessment.

Warren Averett maintains security policies and communicates them to staff to ensure that individuals utilizing the Warren Averett systems understand their responsibility in reducing the risk of compromise, and exercise appropriate security measures to protect systems and data. Policy and procedure manuals are reviewed periodically by the CIO, Legal Counsel, and the CEO for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.

Information and Communication

Warren Averett uses a variety of methods for communication to ensure significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following.

- New hire training
- Ongoing training, including security specific topics
- Policy and process updates
- Meetings
- Knowledgebase announcements and articles and MS Teams Notifications
- Email communications

Warren Averett maintains systems that manage the flow of information and facilitate communication with its clients. Changes to Warren Averett's commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose services are part of the system. Warren Averett also has provided contact email and phone numbers on its website to clients, consumers, suppliers, external auditors, regulators, and others, including an anonymous administered whistle-blower hotline. Management monitors workforce member complaints reported via the hotlines, emails and phones when they occur.

Warren Averett has implemented various methods of communication to ensure that employees understand their individual roles and responsibilities related to security, confidentiality and availability requirements, and communicate significant events in a timely manner. Personnel and Policy guides are provided upon hire that communicate all relevant policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and through awareness programs. The communication system between management and operations staff includes the use of office email system, video conferencing and instant messaging. Periodic department meetings between management and staff are held to discuss new company policies and procedures and other business issues. Communication is encouraged at all levels to promote the operating efficiency of Warren Averett.

Monitoring

Management monitors internal controls as part of normal business operations. Management regularly reviews reports and/or logs, and records, and recommends mitigation or changes to management. The process for monitoring regulations, laws, or contracts is the responsibility of the CIO and internal legal counsel. The CIO and legal counsel review changes in regulations, laws, and review all contracts as a core job function. If these changes create a risk to Warren Averett, the risks are identified and integrated into Warren Averett's risk management process.

Warren Averett uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats and vulnerabilities, changing resources utilization needs, and unusual system activity. Future processing capacity demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are monitored, reviewed, and approved by management. Change requests are initiated as needed based on approved forecasts.

Vendor Monitoring

The selection of vendors (including subservice organizations) for outsourced services is performed in accordance with the organization's Vendor Management Policy. The policy is updated annually and is approved by the Chief Information Officer. Ongoing monitoring is performed to ensure the vendor is meeting, and can continue to meet, the terms of service level agreements expressed in their contracts. Monitoring also includes a Vendor Risk review which is completed for all new critical vendors as well as annually for critical vendors that may include a vendor risk assessment, review of SOC reports and other due diligence documentation.

Subservice Organizations

Warren Averett utilizes the subservice organizations listed in the table below related to its Information Technology Department. Warren Averett periodically reviews the quality of the subservice organizations' performance and manages a due diligence process through its vendor management and monitoring program as previously referenced to provide assurance over the subservice organizations' control structure. The accompanying description includes only those procedures and controls of Warren Averett and does not include controls and related control objectives of any subservice organizations.

Warren Averett's controls related to the Information Technology Department cover only a portion of overall internal control for each user entity of Warren Averett. It is not feasible for the control objectives related to Information Technology Department to be achieved solely by Warren Averett. Therefore, each user entity's control over security and confidentiality must be evaluated in conjunction with Warren Averett 's controls described in this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described in the following table.

Description of Services Rendered	Complementary Subservice Organization Controls (CSOCs)	Related Trust Services Criteria
Subservice Organization: Microsoft Office 365 Core		
Software Provider for internal/external communications, data storage and classification, and collaboration tools	• Is responsible for maintaining controls for availability, confidentiality, security of communications, data storage and collaboration platform that makes up the Software as a Service (SaaS) known as Office 365.	CC5.1- CC5.3, CC6.1, CC6.4, CC6.6, CC6.8, CC8.1, CC9.1, A1.2
Subservice Organization: CCH Axcess		
Tax Preparation Software	• Is responsible for maintaining controls for availability, confidentiality, security of communications and data storage that makes up the Software as a Service (SaaS) known as CCH Axcess. • Is responsible for developing, maintaining, updating and implementing the CCH Axcess software.	CC5.1 - CC5.3, CC6.1, CC6.4, CC6.6, CC6.8, CC8.1, CC9.1, A1.2
Subservice Organization: Confirmation.Com		
Software provider that collects confirmations for audits	• Is responsible for maintaining controls for availability, confidentiality, security of communications, data storage and services that makes up the Software as a Service(SaaS) known as confirmation.com.	CC5.1 - CC5.3, CC6.1, CC6.4, CC6.6, CC6.8, CC8.1, CC9.1, A1.2
Subservice Organization: Intacct		
Accounting Servicing Platform	• Is responsible for maintaining controls for availability, confidentiality, security of communications, data storage and services that makes up the Software as a Service(SaaS) known as Sage Intacct.	CC5.1 - CC5.3, CC6.1, CC6.4, CC6.6, CC6.8, CC8.1, CC9.1, A1.2
Subservice Organization: HubSpot		
SaaS provider for marketing tools and possible revenue streams, CRM	• Is responsible for maintaining controls for availability, confidentiality, security of communications, data storage, services that makes up the Software as a Service(SaaS) known as Hubspot.	CC5.1 - CC5.3, CC6.1, CC6.4, CC6.6, CC6.8, CC8.1, CC9.1, A1.2
Subservice Organization: Microsoft Azure		

Description of Services Rendered	Complementary Subservice Organization Controls (CSOCs)	Related Trust Services Criteria
Infrastructure provider for servers and proxy services	• Azure is responsible for maintaining controls over secure transmission, handling, and storage of data (including encryption, backups, replication, and recovery).	CC 5.3, CC6.1 CC6.8, CC7.1 - CC7.5, A1.2
Subservice Organization: Mimecast		
Infrastructure provider for servers and proxy services	• Is responsible for maintaining controls in supporting availability and storage of emails for legal compliance. • Is responsible for maintaining commitments in providing a spam scanning service.	CC 5.3, CC6.1- CC6.8, CC7.1 - CC7.5, A1.2
Subservice Organization: DocuSign		
Provider of E-Signature services in connection with Warren Averett Connect	• Is responsible for facilitating the delivery and capturing of electronic signatures securely with digital ID verification.	CC3.1 - CC3.4, CC5.1 - CC5.3, CC6.1 - CC6.8, CC7.1 - CC7.5, CC8.1, CC9.1, CC9.2, C1.1, C1.2