Everything's Internet, LLC

SOC 2 Type 1 Report

completed 1st Quarter 2023

Everything's Internet, LLC
SOC 2 type 1 Report

Section 1 Auditor's Opinion

This document has been prepared by EI directly and as such does not contain an external auditor opinion.

However, this document follows the SOC 2 type 1 structure, is updated quarterly, and is ready for an external auditing firm with regards to either a SOC 2 type 1 or type 2 audit should anyone require it.

Section 2 Assertion

Everything's Internet, LLC (EI) is a freelance based company with a background that is rich and well versed in networked technology spanning voice, data, and video.

EI provides Information Technology Management Strategy plans based on the SOC trust principles in order to control infrastructure spending and to maintain a high security posture.

EI provides guidance, training, and on-boarding for integration of the SOC trust principles and Cloud based infrastructure, most noted Cloud on-boarding efforts are targeted at Microsoft Azure and Amazon EC2 Cloud platforms.

EI provides Cloud migration cost estimation services based on the client's existing voice and data networks and platforms.

EI creates and establishes a full SOC 2 type 1 report with scheduled quarterly auditing to support the report for the client in order to be prepared for a SOC 2 type 2 audit report should their clientele or business partners require it along with clearly defined ROI verification for current spending and future procurement support.

EI has published a hardback book on IT management strategies for verifying technology Return On Investments with raised security posturing based on Department of Defense standards sold at Amazon Books, Barnes and Noble Books, or direct from EI's website https://everythingsinternet.com or https://thebookextras.com

EI provides additional free and paid for material related to the book's content at the book's website https://thebookextras.com

Finally, due to personal past experience with ostomy surgery, EI provides free consulting and support to current ostomy / ileostomy patients working from home simply as a pay it forward effort for those that need it.

EI uses subservice organizations, to provide the following:

- Centris Federal Credit Union provides all traditional banking financial services
- Travelers Business Insurance Covering Error, Omissions, and Cyber Breach
- Microsoft 365 for business email service and email protections
- Microsoft Azure for Cloud Based Data Center Facilities, Virtual Desktop Computers
- Amazon EC2 for Centralized Server Hosting
- Amazon KDP Publishing and Book Distribution Services
- GoDaddy Website Hosting and Credit Card Transactions
- osTickets SaaS for managing all change or service requests and Intranet postings
- Asset Tiger SaaS for tracking technology hardware purchasing and disposal.
- Ringotel VoIP Session Border Controller for encrypted mobile telecommunications
- Vitelity Voice Over IP wholesale telephone services for public phone services

EI includes only the criteria and related controls of EI and excludes the criteria and related controls of the subservice organizations.

Section 3 System Description

Infrastructure

EI makes use of a hybrid network combining on-site platforms, the Azure Cloud platform, and SaaS programs to blend dissimilar computer systems from Microsoft, Apple and Linux into a single operational system, fully accountable and measurable, with a high level security posture.

Azure's Cloud hosted Windows computer exists for business use only. This use is for testing current NIST configurations and demo purposes to show clients an operational Cloud computer operating at security levels meeting the US Department of Defense.

User security is maintained through the use of Active Directory services at Azure where a single multi-user Windows 11 computer system is used only for business purpose.

This Windows 11 computer is joined to Azure Directory services for authentication with second factor login required. The Azure platform is fully monitored through the use of an Open Source SIEM provided by AT&T Business, maintained by EI.

The Azure cloud platform connects fully encrypted with the use of VPN to an on-premise system for local data storage and a second Active Directory server for controlling Apple McIntosh computers used for business and personal needs.

The business use of the on-site Apple computers are protected by Active Directory services isolated from a local machine account for personal needs.

All data storage is maintained on-site with a Linux based network storage unit that provides multiple journal based backup copies along with an off-site fully encrypted fail-over copy of all stored data.

There is on-premise WIFI available. However, this WIFI network is isolated from the business network through the use of VLAN technology and only used for personal needs.

EI makes use of a on-site Voice Over IP phone system that is securely exposed to the Internet. The VoIP phone system is protected and fully encrypted using a SaaS based public session border controller. This phone system has full softphone support so EI's office is not fixed and fully mobile. The only mobile device in use at the time of this audit is an Apple iPhone.

EI follows the SOC 2 trust principles with the use of SaaS platforms for maintaining change management and support tickets, along with in-house system footprint and health monitoring.

Organization and Administration

EI is a single member LLC operating under a freelance offering with oversight in place through the use of a third party legal firm and third party certified public accountants.

The legal entity meets quarterly to discuss business practice, create and enforces business policy.

The CPA firm enforces federal and state taxes are met along with the year end filings.

Communications

All internal polices and procedures are posted on the internal Intranet for EI. All work performed is under a written scope of work signed by all parties involved.

Risk Assessment

Risk assessment is easy due to the size of EI as a company. However, risk assessments are still performed and reinforced as demonstrated by this SOC 2 type 1 efforts and the stated control listing.

Monitoring of Controls

EI control effectiveness is a mainstay topic in the quarterly legal meetings.

Internal System

EI makes use of Active Directory and second factor authentication for business related systems and SaaS platform authentications.

EI utilizes footprints and health logging into AT&T's open source SIEM platform for continuous monitoring efforts. EI has an Internet Gateway Intrusion Protection System on the public connection of the Internet that provides a nightly report of all hack attempts prevented.

EI's telecommunication is VoIP based with full logging and recording capabilities.

Physical Security

EI houses on-premise networking equipment in an locked automatically cooled equipment rack. That rack is behind a locked door to the server room with real-time recorded video entrance and exit footage.

Network Security, Access to Workstations

EI uses two computer platforms for business needs. The first is the Azure Data Center for Windows 11 access, protected by Active Directory and second factor authentication. The second is Apple Mac mini desktop primarily for graphics and document development, protected by Active Directory and second factor authentication.

Data Backup

EI uses physical on-premise network data storage for both the cloud and local file safe keeping. That storage performs multiple real-time journal based backup copies along with local fail-over encrypted copies to USB drives and encrypted off-site Cloud data tape storage.

Change Management

EI makes us of osTickets as a SaaS offering, protected by second factor authentication for all change management and service ticket operations.

Summary

EI although small in head count, EI follows the practice outlined by the SOC Trust Principles along with NIST computer system hardening as an example to show the company size does not hinder the ability to operate with top notch security posturing, cost controls with ROI verification and clear future procurement statistics.

The descriptions presented here are designed to provide the reader a brief description of the activities performed by EI.

EI believes the activities are appropriate for the services provided.

EI's specific controls are designed to meet the applicable trust services criteria included in this report and are an integral part of EI's systems for business operations.

Section 4 Description of Controls

Control Environment

Principle	Points of Focus	EI Control
CC1.1 The entity demonstrates a commitment to integrity and ethical values.	Sets the Tone at the Top — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control. Considers Contractors and Vendor Employees in Demonstrating Its Commitment — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	EI although small in head count still maintains full SOC 2 Trust Principles. EI maintains full documentation, for both itself and all clients, stored in a secure SaaS platform to assure there is a full staff of people caring for that data and its backup. **Evidence provided with hard copy or data file based examples of documentation for clients and business operations.**
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations	EI is a single member LLC and does not have a board of directors but does maintain full operational company documentation, supported by an external legal staff and a fully qualified CPA **Evidence provided will be meeting minutes notes from legal meetings, copy of tax prep forms signed by EI's out source certified**

		public accountant.
Principle	**Points of Focus**	**EI Control**
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	same as CC1.2
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and out sourced service providers to support the achievement of objectives.	EI does actively recruit and maintain business partnerships for related SOC or Cloud product or service delivery based on known high integrity companies with proven performance and tenure in their field. **Evidence provided with signed agreements and email delivery of partner affiliate or dealer codes.**
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Enforces Accountability Through Structures, Authorities, and Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.	EI conducts quarterly meetings with an out source legal firm to discussion business practice and performance. **Evidence provided is meeting minutes from the legal firm quarterly meetings.**

Communications and Information

Principle	Points of Focus	EI Control
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Information systems capture internal and external sources of data.	EI uses a blend of dissimilar computer systems integrated into a single platform that all send footprint and health information into a SIEM for full accountability and reporting. **Evidence is provided through ad-hoc reporting of stored system in the SIEM.**
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Objectives and Changes to Objectives — The entity communicates its objectives and changes to those objectives to personnel in a timely manner.	EI meets quarterly with legal staff to discuss operational changes. **Evidence is provided through copies of legal meeting minutes.**
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant in-formation.	EI has a ticket system available on the public Internet where clients and business partners can freely communicate. **Evidence comes from ticket system usage reports.**

Risk Assessment

Principle	Points of Focus	EI Control
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	EI discusses risk and operational behaviors in the quarterly legal meetings. **Evidence comes from copies of legal meeting minutes.**
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.	Risk identification considers both internal and external factors and their impact on the achievement of objectives.	EI business focus is raised security posture and cost control. **Evidence is provided through meeting minutes of legal meetings and documented deployments of the same security measures and procedures used in client networks**

Monitoring Activities

Principle	Points of Focus	EI Control
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.	Establishes Baseline Understanding — The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	EI makes use of virtual computers at the Azure Data Center that can be created for testing only and destroyed upon completed testing of software or configuration changes. **Evidence will come from a formal ticket with screen shots.**
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.	Communicates Deficiencies — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	All controls, monitoring, and changes to controls are performed by myself. **Evidence comes from formal change tickets and legal meeting minutes.**

Control Activities

Principle	Points of Focus	EI Control
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Considers Entity-Specific Factors — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	EI makes use of a blended environment of cloud and real computers and networks across multiple system types all logging data to a SIEM. **Evidence comes from SIEM ad-hoc reporting.**
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	Establishes Relevant Technology Infrastructure Control Activities — Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availabilty of technology processing.	As part of technology cost control, EI uses no unnecessary computer processing. **Evidence of this comes from actual infrastructure expenses in relation to overall business overhead expense in the P&L.**
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Establishes Policies and Procedures to Support Deployment of Management's Directives — Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	EI does have established accepted use policy posted on the Intranet. **Evidence will be copies of the posted acceptable use policies.**

Logical and Physical Access Controls

Principle	Points of Focus	EI Control
CC6.1.1 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.	Identifies and Manages the Inventory of Information Assets — The entity identifies, inventories, classifies, and manages information assets.	EI makes use of Asset Tiger SaaS for equipment serial number tagging, inventory tracking, and disposals. **Evidence will come from ad-hoc reporting in the Asset Tiger database.**
CC6.1.2	Restricts Logical Access — Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	EI uses Active Directory for user access. EI also powers down all idle resources when not used. **Evidence will come from Active Directory Reporting and SIEM data verification.**
CC6.1.3	Considers Network Segmentation — Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	EI makes use of VLAN separation between business a personal resources. WIFI is alos restriocted to personal use only using VLAN addressing. **Evidence will come from screen prints and system reports.**

Principle	Points of Focus	EI Control
CC6.1.4	Manages Credentials for Infrastructure and Software — New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	EI makes use of a SaaS based ticket system to record all assigned access and removals. **Evidence comes from ticket system examples.**
CC6.1.5	Uses Encryption to Protect Data — The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.	EI makes use of VPN encryption for data passing between the cloud and local data center. Encryption is also used for all voice communications and internal text messages. Public exposure of the EI web site and store is SSL protected. **Evidence comes from system reports and screen prints.**
CC6.1.6	Protects Encryption Keys — Processes are in place to protect encryption keys during generation, storage, use, and destruction.	All encryption keys are managed by Microsoft in part of using the Azure Data Center. **Evidence will come from configuration sample data from the Azure Data Center.**

Principle	Points of Focus	EI Control
CC6.2.1 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.	Controls Access Credentials to Protected Assets — Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.	same as 6.1.4
CC6.2.2	Reviews Appropriateness of Access Credentials — The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.	EI discusses all access in the quarterly legal meetings. **Evidence will come from copies of legal meeting minutes.**

Principle	Points of Focus	EI Control
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.	Reviews Access Roles and Rules — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.	same as 6.2.2
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Reviews Physical Access — Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	same as 6.2.2

Principle	Points of Focus	EI Control
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.	Removes Data and Software From Entity Control — Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.	EI makes use a Linux based network storage for data that is joined and protected from access using Active Directory. **Evidence comes from system configuration screen prints.**
CC6.6.1 The entity implements logical access security measures to protect against threats from sources out- side its system boundaries.	Restricts Access — The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	EI protects the data center with port restricted rules in the firewalls along with nightly reports of all threats prevented. **Evidence comes from system reports and configuration reports.**
CC6.6.2	Requires Additional Authentication or Credentials — Additional authentication in- formation or credentials are required when accessing the system from outside its boundaries.	EI makes use of second factor authentication for access into web facilities and data center resources. **Evidence comes from system configurations samples.**
CC6.6.3	Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are	EI makes use of enterprise firewalls and border controllers for voice services. **Evidence comes from system configuration reports.**

	monitored to detect such attempts.	
Principle	**Points of Focus**	**EI Control**
CC6.7.1 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.	Uses Encryption Technologies or Secure Communication Channels to Protect Data — Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	same as 6.1.5
CC6.7.2	Protects Mobile Devices — Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.	Mobile devices are restricted from business data center facilities. Mobile telephone services are fully encrypted. **Evidence comes from system configuration reports.**
CC6.8.1 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Restricts Application and Software Installation — The ability to install applications and software is restricted to authorized individuals.	Computer workstations have restricted resource through the use of NIST configuration profiles and active directory role limitations. **Evidence comes from system configuration reports.**

Principle	Points of Focus	EI Control
CC6.8.2	Uses a Defined Change Control Process — A management-defined change control process is used for the implementation of software.	EI uses SaaS based osTickets for all change management and service related efforts. **Evidence comes from osTicket system reports and ticket examples.**
CC6.8.3	Uses Antivirus and Anti-Malware Software — Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.	EI uses Defender protections on Windows computers and built-in protections of macOS and Linux operating systems where used. **Evidence comes from system configuration screen prints.**

System Operations

Principle	Points of Focus	EI Control
CC7.1.1 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Uses Defined Configuration Standards — Management has defined configuration standards.	EI makes use of industry standard NIST based configurations on computer workstations. **Evidence comes from system configuration reports.**
CC7.1.2	Conducts Vulnerability Scans — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	EI conducts a vulnerable scans on data facilities and public web surfaces in June and December of each year. **Evidence comes from a copy of the external vulnerable test results.**

Principle	Points of Focus	EI Control
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.	Implements Filters to Analyze Anomalies — Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	EI makes use of an Intrusion Protection System blocking threat attempts with a nightly report of the threat events that were protected. **Evidence comes from samples of the nightly threat prevention reports and IPS configuration screen prints.**
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.	Communicates and Reviews Detected Security Events — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	This is a topic discussed in the quarterly legal meetings. **Evidence comes from sample of the legal meeting minutes.**

Principle	Points of Focus	EI Control
CC7.4 The entity responds to identified security incidents by executing a defined incident-response pro- gram to understand, contain, remediate, and communicate security incidents, as appropriate.	Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.	same as 7.2
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	Communicates Information About the Event — Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external)	same as 7.2

Change Management

Principle	Points of Focus	EI Control
CC8.1.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Designs and Develops Changes — A process is in place to design and develop system changes.	EI makes use of SaaS osTickets for all system changes. **Evidence comes from reports and samples of tickets showing planned and executed system changes.**
CC8.1.2	Tracks System Changes — A process is in place to track system changes prior to implementation.	same as 8.1.1
CC8.1.3	Configures Software — A process is in place to select and implement the configuration parameters used to control the functionality of software.	same as 8.1.1
CC8.1.4	Tests System Changes — A process is in place to test system changes prior to implementation.	EI utilizes the Azure Cloud for creating and destroying computers as needed in order to build and support a test environment as needed. **Evidence comes from screen prints and log file reports showing constructed and destroyed test computers.**

CC8.1.5	Creates Baseline Configuration of IT Technology — A baseline configuration of IT and control systems is created and maintained.	EI makes use of industry standard NIST based system configurations. **Evidence comes from screen prints and system configuration reports.**

Risk Mitigation

Principle	Points of Focus	EI Control
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.	EI makes use of industry standards, NIST configurations, the SOC principles and outside support of legal and SaaS to meet all security requirements and maintain a high level of security posturing. **Evidence comes from platform screen prints and formal meeting minutes.**
CC9.2.1 The entity assesses and manages risks associated with vendors and business partners.	Establishes Communication Protocols for Vendors and Business Partners — The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	EI maintains a ticket system recording activities with vendors and out sourcing. **Evidence comes from ticket system examples and reports.**
CC9.2.2	Assesses Vendor and Business Partner Performance — The entity periodically assesses the performance of vendors and business partners.	EI performs a vendor management review at year end using the data collected in the ticket system. **Evidence comes from the evaluation data at year end.**
CC9.2.3	Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.	same as 9.2.2 with the addition of a formal ticket to track vendor relationship ends. **Evidence comes from ticket system reports**.

Management Letter

In all fairness, if I completed this SOC 2 Type 1 audit on another company I would complete it with a management letter stating areas of improvement that have been identified in the audit. Based on the data provided, the first item of improvement would be the addition of DLP for your email and when additional users are added, a second item is a network file audit trail, the third item would be the supporting control count.

1. DLP stands for Data Loss Prevention. This is a SaaS based system that gets placed in front of your email services. It works for both in-house email systems and hosted email systems such as Microsoft 365 email services. The DLP system checks all incoming and outgoing email for threats. It has capabilities that detects the structure of an account number or social security number and will block any outgoing emails that match a list of unapproved items you want to be assured is never emailed outside the company.

2. A Network file monitor system keeps track of who touches any file on the network shared file system. When you have many employees this system provides you the ability to look back and know what employee touched a file and what they did to that file.

3. If this assembly was targeted to support a full SOC 2 Type 2 external audit the number of controls needs increased. In a SOC 2 type 2 audit the minimum number of controls per the stated principle criteria should be three to assure the control meets evidence expectations should one control fail to cover the evidence of the targeted principle's criteria.

Management Letter Response

Item 1 is not in place due to the added expense. As a freelance company there are not multiple users of the email system creating risk requiring this level of monitoring. The expense, as of this audit date, is $6,000.00 annually. Should company growth warrant it, the system will be installed. Until such time this is considered a manageable and acceptable risk.

Item 2 is not warranted due to EI being a freelance company where all files are currently touched by only me. Should the time arrive where others touch saved file, the system will be installed as that will make this an unacceptable risk.

Item 3 is expected due to company size and that this audit is targeted for accountably and cost controls. The technology assembly and SOC 2 type 1 report does produce a fully accountable network, with controlled technology risk and spending, including verifiable ROI.

The purpose is also to demonstrate how the benefits of accountable networks and the SOC principles can raise your security posture plus financially benefit any size company.

Everything's Internet, LLC

Certificate of Completion

Everything's Internet, LLC

for successful completion

2023 1st Quarter Technology Audit

3.14.2023

Date

EI Audit Team

Signature