e3 TECHNOLOGY

Allixo

NIST 800-171and HIPAA
Security Risk Assessment (SRA)
Technical Controls Review Attestation Memo

October 2019

Prepared By:

Stuart Chontos-Gilchrist, Principal Consultant
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Ethical Hacker (CEH)
Information Systems Security Management Professional (ISSMP)
Certified Authorization Professional (CAP)
Certified in Risk and Information Systems Control (CRISC)
Bachelor of Science, Computer Science (BSCS)

Executive Summary

E3 Technology, Inc. (E3) has examined the managerial, operational, and technical security controls in place at Allixo in Mount Vernon, WA. As part of the scope of work, E3 performed an internal vulnerability analysis, HIPAA Security Risk Assessment, NIST 800-171 Security Risk Assessment, and an external penetration test.

Our examination included a review of all relevant policies, procedures, and systems to obtain reasonable assurance about whether the controls in place for Allixo's systems are adequate and if they meet NIST 800-171 and HIPAA standards and if those controls were complied with satisfactorily.

In our opinion, the accompanying description of the controls within Allixo's network systems presents fairly in all material respects, the relevant aspects of the controls that had been placed in operation during the period August 2018 to September 2019.

Testing Objectives

The primary objectives of this review were to evaluate the security controls relating to the all servers and workstations, the network that the systems reside on, and other miscellaneous equipment that provide services to the organization that aid in the operation of the relevant systems.

Scope and Approach

Testing was performed using the following general procedures:

- An evaluation of the Allixo network's current security stance (including relevant networking equipment), as well as policies, procedures, and technical, physical, and logical security measures based upon standard security guidelines.
- A series of controlled Internet vulnerability and penetration tests using a reliable set of automated tools and manual methods in August 2018.

Additionally, our procedures included interviews with key personnel, review of available documentation and information security procedures, inspection, evaluation, and testing of controls surrounding and provided by the technical systems. In addition, a physical security review of primary Mount Vernon facility was conducted.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to tests of operating effectiveness of specified controls described below, our procedures included tests of the relevant elements of the Allixo control environment, including the relevant organizational structure and approach to segregation of duties and management control methods.

Our tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved as of September 2019.

Control Objective	Testing performed by E3	Results of Tests
1. Internal Vulnerability Assessment		
1.1 Port Scans Port scans are run using automated tools to determine which ports answer to incoming requests and help to determine which systems are on and available on the network.	*E3 ran Nmap against all the internal IP ranges and determined which ports and systems where alive. Scans were conducted in December 2016.*	E3 scanned all subnets and found all live nodes. All nodes and ranges were scanned.
1.2 Vulnerability Scans Use of automated tools to scan the internal network for open ports that exhibit certain characteristics that are vulnerable to attack. Classes of vulnerabilities typically fall into four different categories: (1) patches, (2) poor configuration, (3) legacy systems and services, and (4) unauthorized software	*E3 ran Nessus Professional against all relevant internal systems and examined the results. Some medical and EMR systems were included in-scope. Scans were ran over a period starting in August 2018 and completing in June 2019*	While multiple patch, configuration, and legacy issues were noted in the scans, high and medium risk issues were remediated. An internal vulnerability management program has been instituted to conduct ongoing scans by internal staff.
1.3 Exploiting Vulnerabilities Where reasonable and if the risk of disabling a system is low, E3 attempted to exploit vulnerabilities.	*E3 ran Nessus professional and hand tested multiple 'Safe" vulnerabilities to validate if the organization has exploitable vulnerabilities*	Some safe vulnerabilities were exploited with suitable evidence provided to staff. All high-risk issues were corrected.
1.4 Internal monitoring Allixo staff should be notified of scanning and exploit activity on the internal network in a reasonable period of time after the attack occurs.	*E3 worked with internal staff to validate that monitoring systems were working as intended and alerts were received in a reasonable time period.*	An extensive monitoring program is in place at the organization to detect a wide variety of events including recon scans and exploit events.
2. External Penetration Test		

Control Objective	Testing performed by E3	Results of Tests
2.1 External Vulnerability Testing External vulnerability testing uses automated tools to scan IP addresses over the internet to find open ports that are vulnerable to attack.	*E3 used Nessus professional to scan all 65535 possible open TCP and UDP ports and look for vulnerabilities. Some limited denial of service testing was run. Testing was completed in August 2018*	E3 scanned all external IP addresses. All high risk issues were remediated upon conclusion of the scans.
2.2 Penetration Testing Attempts to exploit a system should be run to validate if vulnerabilities are real.	*E3 used Nessus professional, Hand testing, and brute force login attempts to try to gain access to systems.*	No exploitable vulnerabilities were discovered
2.3 External monitoring Allixo staff should be notified of scanning and exploit activity on the external network in a reasonable period of time after the attack occurs.	*E3 worked with internal staff to validate that monitoring systems were working as intended and alerts were received in a reasonable time period.*	A extensive monitoring program is in place at Allixo. Detection methods for external scans were validated.
3 NIST 800-171 and HIPAA Security Review		
3.1 Review of 800-171 and HIPAAA Security A review of written controls utilizing NIST 800-171 and HIPAA Security	*E3 reviewed relevant documentation and interviewed staff to determine the adequacy of in-place controls. The initial review was completed in August 2018 with follow up in June 2019 determine current status.*	Allixo has provided a large number of documents that were reviewed and compared to the NIST 800-171 and HIPAA standards. No critical issues were noted during the review. All high and most Medium risk issues have been remediated as of September 2019.
3.2 Physical Security Review Access to patient data and sensitive areas of the organization should be controlled through secure access techniques and the confidentiality, integrity, and availability of systems should be protected at all times.	*E3 reviewed the physical security controls of the organization by conducting a walkthrough of the data center and general organization in August 2018 and September 2019.*	Data center and general organization controls meet relevant standards.

Control Objective	Testing performed by E3	Results of Tests
3.3. Risk Assessment and Business Impact Analysis Review A risk assessment process that meets HIPAA and NIST SP 800-30 guidelines is essential to understanding areas that the organization has weaknesses that need to be addressed.	*E3 reviewed the organization's in-place risk assessment processes. E3 worked with staff in the June 2019 to September 2019 period to make improvements in the Risk Assessment and Business Impact Analysis*	The organization has an in-place Business Impact Analysis and Risk Assessment process. The documents and processes used follow relevant NIST guidelines.
3.4 Encryption Control Review Encryption of sensitive data at rest and in motion is essential to safeguard corporate and client data that is processed, transmitted, or stored on organization systems.	*E3 reviewed Allixo's use of encryption tools used to protect sensitive data.*	E3 determined that all sensitive data is protected using suitable tools to encrypt all data at rest and in motion are in place and working as intended. A strong encryption policy exists in reviewed written materials.