DEA 1311.205 Compliance Report for Pharmacy Application Providers as of April 29, 2019

ASSURANCE CONCEPTS

A SKODA MINOTTI ADVISORY FIRM

Table of Contents

SECTION 1: Independent Auditors Report on Applying Agreed-Upon Procedures

To Management of WENO Exchange, LLC.:

We have performed the procedures described below, which were agreed to by WENO Exchange, LLC. ("WENO" or the "Company"); solely to assist in the identification of Compliance Assessment for DEA Part 1311.205 controls that were in place as of April 29, 2019, as set forth in the accompanying Schedule A. The maintenance of these controls is solely the responsibility of WENO. Consequently, we make no representation regarding the sufficiency of the controls as a whole for WENO as described below either for the purpose for which this report has been requested or for any other purpose.

The controls and associated findings are as follows:

1. Compared WENO' controls implemented in the pharmacy application WENO to applicable controls specified by the DEA Part 1311.205 pharmacy application requirements. Reviewed application operations and processes to verify that controls were in place and operating as of April 29, 2019 (SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices).
   No exceptions were found as a result of this comparison.
2. Reviewed WENO' controls implemented in the information security environment for the production system of WENO' electronic prescription application services. Reviewed information security controls and processes to verify that controls were in place and operating as of April 29, 2019 (SECTION 3: Schedule B | DEA Part 1311.205 Testing Matrices).
   No exceptions were found as a result of this comparison.

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on the controls set forth in the accompanying Schedule A. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported.

The description of controls at WENO is as of April 29, 2019, and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at WENO is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of WENO' controls, individually or in the aggregate.

This report is intended solely for the information of potential customer, existing customers, regulatory agencies and use by the management of WENO and is not intended to be and should not be used by anyone other than these specified parties.

Assurance Concepts, LLC

April 29, 2019

SECTION 2: WENO Pharmacy Application System Description

Company Overview and Services Provided

Weno Exchange LLC (WENO) is an electronic Prescribing (ePrescribing) network which routes standard ePrescribing messages, including controlled substances, between healthcare providers, payers, and pharmacies. This is accomplished when electronic health record (EHR) systems connect to WENO's network or when a healthcare provider uses WENO's web based ePrescribing application.

WENO is the only known competitor of Surescripts. WENO's super niche technology is focused on making ePrescribing easy and affordable for all. WENO is headquartered in Austin, Texas.

WENO has been hailed as an innovative competitor in an otherwise dominated e-prescribing network and benefit service market.

Information Systems Overview

WENO information systems were built to facilitate the electronic prescriptions processes for controlled substances used by a DEA registrant. Information systems retain all prescription and dispensing information required by DEA regulations, digitally signatures of the records of the prescription that is sent to pharmacy and maintain an internal audit trail of any required auditable events. WENO's information systems are comprised of internal and external third party managed services.

WENO's custom developed application that healthcare providers utilize to process electronic prescriptions for controlled substance resides in a third party managed IT infrastructure service provider for Enterprise Hosting Services. WENO's third party managed IT infrastructure service provider (Liquid Web) goes under a reoccurring SOC 2 Type II audit every year. The SOC 2 Type II audit reports on the suitability and operating effectiveness of the Third Party Enterprise Hosting Services; where WENO deployed their electronic prescription application for their DEA Part 1311.120 compliance for hosted application service providers. WENO manages access to their electronic prescription application via a formal authorization process and limits the access to the application and data that resides in their systems to WENO personnel and clients. Physical security to the application service provider is maintain and monitored by the third party and therefore is not included in this report.

Scope and Summary of Report

This report describes the control structure under the guidance of DEA Part 1311.205 for WENO as it relates to application and information security standards for their Electronic Pharmacy Application Services at the Austin, Texas facilities. It is intended to assist WENO' customers and potential customers in determining the adequacy of WENO' internal controls. The scope of this assessment included the evaluation of the DEA Part 1311.205 Pharmacy Application Requirements as it applies to WENO' hosted instance and processing integrity of the supporting system infrastructure. "SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices" of this report describes the procedures performed to verify WENO' application features and information security of their hosted application. Physical security was not included in the scope of this report as all production systems reside at Liquid Web and are supported by their current SOC 2 Type II report.

SECTION 2: WENO Pharmacy Application System Description

Pharmacies are required to adhere to requirements described in DEA Part 1311.200; this information can be access via http://www.deadiversion.usdoj.gov/21cfr/cfr/1311/subpart_c100.htm#200. Although WENO provides pharmacy application requirements to their customers described in DEA 1311.205 and throughout the remainder of this report, pharmacies still have requirements to be evaluated under DEA 1311.200. Additionally, there are certain parts of the application services provided to pharmacies that WENO alone is not able to provide by itself, which users of the system are required to assess the User Control Considerations defined Throughout Section 3 of this report.

SECTION 2: WENO Pharmacy Application System Description

DEA 1311.205 Pharmacy Applications Control Specifications:

Sec. 1311.205 Pharmacy Application Requirements are specified by the DEA and are required to be met, where applicable, to the system under review. The pharmacy application was evaluated for the following control specifications referenced in (a) and (b) 1 through 18:

(a) The pharmacy may only use a pharmacy application that meets the requirements in paragraph (b) of this section to process electronic controlled substance prescriptions.

(b) The pharmacy application must meet the following requirements:

(1) The pharmacy application must be capable of setting logical access controls to limit access for the following functions:

(i) Annotation, alteration, or deletion of prescription information.

(ii) Setting and changing the logical access controls.

(2) Logical access controls must be set by individual user name or role.

(3) The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.

(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in §1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in §1311.08.

(iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in §1311.08.

(iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

(v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(5) The pharmacy application must verify a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).

(6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application must either:

(i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or

(ii) Display the field for the pharmacist's verification.

(7) The pharmacy application must read and retain the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe controlled substances by the hospital or other institution as provided in §1301.22(c) of this chapter.

(8) The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.

(9) The pharmacy application must read and store in full the information required under §1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.

(10) The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing:

(i) Number of units or volume of drug dispensed.

(ii) Date dispensed.

(iii) Name or initials of the person who dispensed the prescription.

(11) The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.

(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.

(13) The pharmacy application must maintain an audit trail of all actions related to the following:

(i) The receipt, annotation, alteration, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.

(iii) Auditable events as specified in **§1311.215**.

(14) The pharmacy application must record within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(15) The pharmacy application must conduct internal audits and generate reports on any of the events specified in **§1311.215** in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.

(16) The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.

(17) The pharmacy application must back up the controlled substance prescription records daily.

(18) The pharmacy application must retain all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of **§1311.305**

§1311.210 Archiving the initial record.

(a) Except as provided in paragraph (c) of this section, a copy of each electronic controlled substance prescription record that a pharmacy receives must be digitally signed by one of the following:

(1) The last intermediary transmitting the record to the pharmacy must digitally sign the prescription immediately prior to transmission to the pharmacy.

(2) The first pharmacy application that receives the electronic prescription must digitally sign the prescription immediately on receipt.

(b) If the last intermediary digitally signs the record, it must forward the digitally signed copy to the pharmacy.

(c) If a pharmacy receives a digitally signed prescription that includes the individual practitioner's digital signature, the pharmacy application must do the following:

(1) Verify the digital signature as provided in FIPS 186–3, as incorporated by reference in **Section 1311.08**.

(2) Check the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.

(3) Archive the digitally signed record. The pharmacy record must retain an indication that the prescription was verified upon receipt. No additional digital signature is required.

§1311.215 Internal audit trail.

(a) The pharmacy application provider must establish and implement a list of auditable events. The auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.

(2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the pharmacy application.

(4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The pharmacy application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) The pharmacy must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the pharmacy application service provider, if applicable, and the Administration within one business day.

User Control Considerations:

- Users of the pharmacy applications are responsible to verify all prescription information fields received when filling prescriptions.
- Users of the pharmacy application are required to maintain security of their own premise systems, network and hardware.
- Users of the pharmacy application are required to restrict logical access to their own internal networks.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

Schedule A – Electronic Pharmacy Application Testing Matrices

Control Objective 1: Control activities provide reasonable assurance that the electronic prescription application that processes the dispensing of received electronic prescriptions for controlled substances (EPCS) used by dispensing agents retains prescription and dispensing information required by DEA Part 1311.205.

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.1	(1) The pharmacy application must be capable of setting logical access controls to limit access for the following functions: (i) Annotation, alteration, or deletion of prescription information. (ii) Setting and changing the logical access controls.	Inspected the pharmacy application to verify that the application was capable of user security to enforce the following permissions: ➢ Annotation ➢ Alteration ➢ Deletion of prescription information ➢ User security administration	No exceptions noted.
1.2	(2) Logical access controls must be set by individual user name or role.	Inspected the pharmacy application to verify that during user account creation, the application defaulted to a low privileged role and the system administrator could only accept the default role or select another role during user creation. The application only allows rolls to be assigned to user accounts and then additional security is available to limit certain functions within specific rolls. Role based privileges can only be modified by WENO.	No exceptions noted.
1.3	(3) The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.	Observed the application receive a prescription without a digital signature to verify that the prescription was digitally signed by the application, attached to the record and archived.	No exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.4	(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements: (i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in §1311.08. (ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in §1311.08. (iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in §1311.08. (iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key. (v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.	Inspected the deployed software module for digital signatures to verify that the deployed cryptographic module with a FIPS 140-2 Validation Certificate and FIPS 186-3 and FIPS 180-3 compliant hash functions were valid and approved and during the creation of the digital signature the prescription information (name and address of the patient, the drug name, strength, dosage form, quantity prescribed, directions for use, and the name, address and registration number of the practitioner) was included when signing. Inspected the time clock implemented in the application to ensure that a synchronization clock, approved from the National Institute of Standards and Technology, time source was utilized.	No exceptions noted.
1.5	(5) The pharmacy application must verify a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).	Inspected that the pharmacy application does not accept digital signatures.	No exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.6	(6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application must either: (i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or (ii) Display the field for the pharmacist's verification.	Inspected prescriptions sent through the application with no digital signature to verify that the application checked for the signature indicator flag to verify the prescription was signed. Inspected prescriptions sent through the application with no digital signature and no signature indicator field to verify that prescriptions received with no digital signature or a signature indicator flag were rejected.	No exceptions noted.
1.7	(7) The pharmacy application must read and retain the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe controlled substances by the hospital or other institution as provided in §1301.22(c) of this chapter.	Inspected prescriptions sent through the application to verify that the full DEA number and other internal codes were captured with the prescription.	No exceptions noted.
1.8	(8) The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.	Inspected the pharmacy application to verify that for each prescription the following was capable of being displayed and stored: ➢ full name and address of the patient ➢ the drug name, strength dosage form ➢ quantity prescribed ➢ directions for use ➢ name, address and registration number of the practitioner. WENO' Pharmacy Application does not have transferring capabilities at this time.	No exceptions noted.
1.9	(9) The pharmacy application must read and store in full the information required under §1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.	Inspected the pharmacy application receive, store and display prescriptions to verify that the following was available for the pharmacist's verification: ➢ full name and address of the patient ➢ the drug name, strength dosage form ➢ quantity prescribed ➢ directions for use ➢ name, address and registration number of the practitioner. Inspected the pharmacy application code to verify that the application performs checks for each item listed above and will reject the sent prescription if any of the fields are empty.	No exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.10	(10) The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing: (i) Number of units or volume of drug dispensed. (ii) Date dispensed. (iii) Name or initials of the person who dispensed the prescription.	Inspected the pharmacy application and a sample of dispensed prescriptions via the dispense log to verify that the following was linked in read only logs to the dispensed prescription records: ➢ Description (included the type of drug and the number of units or volume dispensed) ➢ Date/Time that drug was dispensed by pharmacy user ➢ User (unique identifier for person that dispensed the prescription)	No exceptions noted.
1.11	(11) The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.	Inspected the pharmacy application search and reporting features to verify that a query and retrieval was capable for each of the following attributes: ➢ practitioner name ➢ patient name ➢ drug name ➢ date dispensed	No exceptions noted.
1.12	(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.	Observed the application's report export functionality to verify that reports were exportable to a .csv file.	No exceptions noted.
1.13	(13) The pharmacy application must maintain an audit trail of all actions related to the following: (i) The receipt, annotation, alteration, or deletion of a controlled substance prescription. (ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions. (iii) Auditable events as specified in §1311.215.	Inspected the audit trail logs for a sample of prescriptions in the application to verify that the following were available, where applicable: ➢ the receipt, annotation, alteration, or deletion of a controlled substance prescription. ➢ any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions. (iii) Auditable events as specified in 1311.215.	No exceptions noted.
1.14	(14) The pharmacy application must record within each audit record the following information: (i) The date and time of the event. (ii) The type of event. (iii) The identity of the person taking the action, where applicable. (iv) The outcome of the event (success or failure).	Inspected the audit logs for a sample of transactions in the application to verify that the following were recorded, where applicable: ➢ the date and time of the event. ➢ the type of event. ➢ the identity of the person taking the action, where applicable. ➢ the outcome of the event (success or failure).	No exceptions noted.

SECTION 3: Schedule A | DEA Part 1311.205 Testing Matrices

#	Control Activity Specified by DEA Part 1311.205	Procedures Performed by the Independent Accountant	Results
1.15	(15) The pharmacy application must conduct internal audits and generate reports on any of the events specified in §1311.215 in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.	Inspected the audit reports to verify that daily reports were available, auditable events listed in 1311.215 applicable to the pharmacy application and were presented in a readable structure.	No exceptions noted.
1.16	(16) The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.	Inspected the pharmacy application and audit records to verify that audit records were read only through the application user interface.	No exceptions noted.
1.17	(17) The pharmacy application must back up the controlled substance prescription records daily.	Inspected the backup configuration and logs of completed backups to verify that the controlled substance prescription records were backed up daily.	No exceptions noted.
1.18	(18) The pharmacy application must retain all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of §1311.305.	Inspected the pharmacy application prescription records and verified that the records were available for a minimum of two years prior to the day of that the records were verified as available.	No exceptions noted.

SECTION 3: Schedule B | DEA Part 1311.205 Testing Matrices

Schedule B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
IS.1	Formal information security policies and procedures are in place to establish organizational information security standards.	Inquired of the CEO to verify that information security policies and procedures were in place to establish organizational information security standards. Inspected the information security policies and procedures to verify that organizational information security standards were documented. No relevant exceptions noted.
IS.2	IT access requests are approved prior to granting access to production systems.	Inquired of the CEO to verify that an approved IT access request was required prior to granting access to production systems. Inspected IT authorization procedures for new production system accounts to verify that production system access was required to be authorized. No relevant exceptions noted.
IS.3	<u>Windows Operating System Access</u> Server operating system authentication is restricted via unique user account and passwords that required: ➢ Minimum length of eight characters ➢ Maximum age of 180 days ➢ Password history requirement of three ➢ Complexity requirement ➢ Lockout threshold of five consecutive failed attempts	Inquired of the CEO to verify that server operating system authentication user account passwords required the following characteristics: ➢ Minimum length of eight characters ➢ Maximum age of 180 days ➢ Password history requirement of three ➢ Complexity requirement ➢ Lockout threshold of five consecutive failed attempts Inspected the application password authentications to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length of eight characters ➢ Maximum age of 180 days ➢ Password history requirement of three ➢ Complexity requirement ➢ Lockout threshold of five consecutive failed attempts No relevant exceptions noted.
IS.4	Administrative access to the server operating system is restricted to personnel with administration job responsibilities.	Inquired of the CEO to verify that administrative access to the server operating system was restricted to personnel with administrative job responsibilities. Inspected users with administrative access to the server operating system to verify that administrative access was restricted to IT personnel with administrative job responsibilities. No relevant exceptions noted.

SECTION 3: Schedule B | DEA Part 1311.205 Testing Matrices

Schedule B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
IS.5	User access to server operating systems is revoked upon notification of termination.	Inquired of the CEO to verify that operating system accounts assigned to terminated personnel were deactivated upon notification of termination. No relevant exceptions noted.
		Inspected user with access to the operating system to verify that access was only assigned to current authorized personnel. No relevant exceptions noted.
IS.6	Operating System Logging The operating system audit settings are configured to log specific events.	Inquired of the CEO to verify that the operating system audit settings were configured to log specific events. Inspected the operating system audit settings to verify that certain operating system events were logged. No relevant exceptions noted.
IS.7	Database Access Database authentication is restricted via unique user account, service accounts and data center hosting accounts and based on windows authentication.	Inquired of the CEO to verify that database authentication was restricted to unique user account, service accounts and data center hosting accounts and based on windows authentication. Inspected the application password authentications to verify that database authentication was based on windows authentication. No relevant exceptions noted.
IS.8	Access to the database is restricted via authorized application, administrator accounts, and data center hosting accounts.	Inquired of the CEO to verify that access to the database was restricted via authorized application, administrator accounts, and data center hosting accounts. Inspected the database user accounts and roles permissions to verify that access to the databases was restricted to IT personnel with administrative job responsibilities. No relevant exceptions noted.
IS.9	Database access privileges are revoked as a component of the termination process.	Inquired of the CEO to verify that database access privileges were revoked upon notification of termination. Inspected the database user access to verify that access of terminated personnel was revoked. No relevant exceptions noted.
IS.10	Database Logging The database records certain user account activity that is available for ad hoc review.	Inquired of the CEO to verify that the database logs record certain user activity that was available for adhoc review.

SECTION 3: Schedule B | DEA Part 1311.205 Testing Matrices

Schedule B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
		Inspected the database configurations and email alert notification to verify that database logs records certain user account activity that was available for ad hoc review. No relevant exceptions noted.
IS.11	Application Authentication Application authentication is restricted via unique user account and passwords that required: ➢ Minimum length of six characters ➢ Alpha and numeric ➢ Complexity requirements of one number and one symbol	Inquired of the CEO to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length of six characters ➢ Alpha and numeric ➢ Complexity requirements of one number and one symbol Inspected the application password authentications to verify that application authentication user account passwords required the following characteristics: ➢ Minimum length of six characters ➢ Alpha and numeric ➢ Complexity requirements of one number and one symbol No relevant exceptions noted.
IS.12	Application Access Controls Access to administer the application is limited to personnel based on their job responsibilities.	Inquired of the CEO to verify that access to administer the application was limited to certain personnel with application administration responsibilities. Inspected the application access user listing to verify that access to administer the application was limited to certain IT personnel based on their job responsibilities. No relevant exceptions noted.
IS.13	Application Logging Controls The application is configured to log certain user account application activities and is available for ad hoc review purposes.	Inquired of the CEO to verify that the application was configured to log certain user account application activities and was available for ad hoc review purposes. Inspected a sample of application logs to verify that application activities were logged and available for ad hoc review. No relevant exceptions noted.
IS.14	Firewall Administration A firewall and web application firewall are in place to help prevent unauthorized access.	Inspected the firewall and web application firewall settings to verify they were in place. No relevant exceptions noted.

SECTION 3: Schedule B | DEA Part 1311.205 Testing Matrices

Schedule B - Information Security

Control Objective 2: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals and to foster system processing is complete, accurate, timely and authorized.

Control #	Control Activity	Testing Procedures and Results
IS.15	Firewall rulesets and configurations have documented business justifications and changes to firewall rules required management approval.	Inquired of the CEO to verify that fire rulesets and configurations had documented business justifications and changes to rules required management approval. No relevant exceptions noted.
		Inspected the documented business justifications and change control procedures to verify that firewall rulesets and configurations were documented and changes required management approval. No relevant exceptions noted.
IS.16	Remote Access Customer web sessions are encrypted using a certification authority.	Inquired of the CEO to verify that customer web sessions were encrypted. Inspected the approved certificates to verify web sessions were encrypted. No relevant exceptions noted.
IS.17	Remote access is performed over encrypted protocols to help ensure the privacy and integrity of the data passing over the public network.	Inquired of the CEO to verify that encrypted protocols were utilized for remote access to help ensure the privacy and integrity of the data passing over the public network. Inspected the encryption settings to verify that remote access was encrypted. No relevant exceptions noted.