A-LIGN

TokenEx, Inc.

ISO/IEC 27001:2013
First Surveillance Audit Report

April 8, 2022

A-LIGN.COM

Table of Contents

SECTION 1: SURVEILLANCE AUDIT REPORT

TokenEx, Inc.
Marc Phillips
GRC Manager
5314 S Yale Ave. Ste. 850
Tulsa, Oklahoma 74135
United States

April 8, 2022

Company Background

TokenEx, Inc. or "the Company" combats data theft while helping organizations reduce the costs associated with Payment Card Information (PCI) compliance. What started as a method of replacing payment card data with undecipherable tokens, evolved into a strategic platform as a service (PaaS) for data security, integrating four key technologies tokenization, encryption, data vaulting, and key management with highly secure cloud-computing.

Overview

To demonstrate the Company's dedication to information security, TokenEx, Inc. implemented an information security management system (ISMS) to conform to the requirements of ISO/IEC 27001:2013 (ISO 27001). ISO 27001 was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to standardize the process for establishing, implementing, operating, monitoring, reviewing, and maintaining an ISMS. A-LIGN Compliance and Security, Inc. ("A-LIGN") was engaged by TokenEx, Inc. to perform the surveillance audit to validate conformity and certify the Company's ISMS against the ISO 27001 standard.

The surveillance audits are once a calendar year audits, but are not necessarily full system audits, performed so that the certification body can maintain confidence that the Company's certified ISMS continues to fulfill requirements between recertification audits. The first surveillance audit was performed between March 21, 2022 and March 25, 2022.

A-LIGN analyzed all information and audit evidence gathered during the surveillance audit, reviewed the audit findings, and agreed on the audit conclusion.

Audit Findings

Zero (0) major nonconformities and zero (0) minor nonconformities was identified during the surveillance audit.

Audit Conclusion

A-LIGN considered the audit evidence with respect to the certification requirements, the scope of certification, and changes to the Company and the ISMS to reach its decision. A-LIGN concludes that the ISMS met the requirements of the audit criteria established, and therefore, recommends continued certification as of the date of this report.

Audit Objectives

The surveillance audit was conducted to verify that the certified ISMS continued to be implemented, to consider the implications of changes to that system initiated as a result of changes in the Company's operations and to confirm continued compliance with certification requirements.

Audit Criteria

A-LIGN performed the surveillance audit to determine continuing conformity to the requirements of ISO 27001 and the defined processes and procedures of the Company's ISMS. Statement of applicability version 1.2, dated February 9, 2022, was used as the basis for the audit, which derived controls and control objectives from ISO 27001 Annex A.

Audit Scope

The scope of certification was defined as:

> "The ISMS supporting the confidentiality, integrity, and availability of systems and customer data as related to TokenEx's tokenization platform and services."

The scope of certification covered the Company's location in Tulsa, OK.

Locations sampled this audit: Tulsa, OK.

A-LIGN deemed the scope of certification to be appropriate based on audit evidence obtained.

Audit Method

During the audit, A-LIGN obtained information relevant to the audit objectives, scope, and criteria. Methods to obtain information included, but was not limited to interviews, observation of processes and activities, and reviews of documentation and records. The audit result also relied upon sampling procedures of the available information, which does not provide absolute assurance of the operation of the controls across the population.

A-LIGN applied the audit methods to address:

- Internal audits and management reviews
- Actions taken for nonconformities identified during previous audits
- Complaints handling
- Effectiveness of the ISMS with regard to achieving the objectives and the intended results of the ISMS
- Progress of planned activities aimed at continual improvement
- Continual operational control
- Review of any changes
- Use of marks and/or any other reference to certification

Audit evidence either examined or observed during the surveillance audit consisted of, but was not limited to:

Evidence description	Version / Date
Scope of ISMS	Various 3/11/2022
Information security policy	Various 2/28/2022
Information security risk assessment methodology	2.0 2/28/2022
Information security risk treatment methodology	2.0 2/28/2022
Statement of applicability	1.2 2/9/2022
Information security objectives	Various

Evidence description	Version / Date
Evidence of competence	Various
Documented information determined by the organization as being necessary for the effectiveness of the ISMS	Various
Operations planning and control	Various
Information security risk assessment	Various 3/11/2022
Information security risk treatment plan	Various 3/11/2022
Evidence of monitoring and measuring results	Various
Internal audit program	Various 2/3/2022
Internal audit report	Various 2/3/2022
Management reviews	Various 3/11/2022
Nonconformities and subsequent action(s) taken	Various
Correction(s) and corrective action(s)	Various
ISMS roles and responsibilities	1.4 3/14/2021
Asset inventory	Various
Acceptable use policy	3.6 3/8/2021
Operating procedures for IT management	4.3 2/15/2021
Secure system(s) engineering principles	3.3 1/22/2022
Vendor security policy	1.5 2/28/2022
Incident management procedures	2.4 4/21/2021
Business continuity procedures	2.5 3/23/2022
Statutory, regulatory, and contractual requirements	Various
Logs of user activities, exceptions, and security events	Various

Audit Process

An opening meeting occurred at approximately 9:00 AM ET on March 21, 2022. In attendance Marc Phillips (GRC Manager, TokenEx), Jon Clemenson (Director of IT Security, TokenEx), Chase Neumayer (Lead Auditor, A-LIGN), Deborah Yadidi (Auditor, A-LIGN), Darian Ramroop (Auditor, A-LIGN), and John Bowman (Auditor, A-LIGN). An opening meeting agenda and the surveillance audit plan was communicated.

The audit was performed over 5 days, between March 21, 2022 and March 25, 2022, which consisted of 5 remote auditing days. Teleconferencing and screen-sharing technology were utilized during the surveillance audit. The on-site audit was conducted at the Company’s location in Tulsa, OK. No significant changes to the ISMS were identified since prior year audits. No significant issues were identified that would impact the audit program.

Upon completion of the audit activities a closing meeting occurred at approximately 5:00 PM ET on March 25, 2022. In attendance were Marc Phillips (GRC Manager, TokenEx), Jon Clemenson (Director of IT Security, TokenEx), Chase Neumayer (Lead Auditor, A-LIGN), Deborah Yadidi (Auditor, A-LIGN), Darian Ramroop (Auditor, A-LIGN). An agenda was provided as well as version 1.0 of the surveillance audit plan. All audit objectives were completed as planned.

Internal Audit

A-LIGN examined the audit program for the objectives, scope, criteria of internal audits. Internal audits were to be performed annually. The most recent internal audit, completed in January 2022 by internal employees hand-picked to ensure objectivity and impartiality, identified 0 nonconformities. Results of this internal audit, including any nonconformities, and corrective actions were reviewed and approved by the GRC Committee in March 2022, and documented in the meeting minutes.

Based on audit evidence gathered, A-LIGN concluded that the internal audit objectives, scope, and criteria were appropriate, and the internal audit could ensure that the ISMS was effectively implemented and managed.

Management Reviews

Management reviews, in the form of meetings of the GRC Committee, were scheduled to occur annually. The GRC Committee was composed of:

- CEO
- DPO
- Chief Legal Counsel
- GRC Manager
- Director of Information Security
- CTO
- VP of IT Operations
- Staff Attorney

A-LIGN examined the management review results and approvals for the risk assessment and risk treatment plan, monitoring and measurement results, internal audit, nonconformities, and corrective actions in the meeting minutes of the GRC Committee, which were examined during the surveillance audit.

Based on audit evidence gathered, A-LIGN concluded that management could be relied upon to ensure continued suitability, adequacy, and effectiveness of the ISMS.

Conformity Level

A-LIGN has classified the level of conformity to the requirements in relation to the audit criteria as defined below:

- Conforms - Requirement(s) were fulfilled
- Nonconformity - Requirement(s) were not fulfilled:
    - Major - A nonconformity that affects the capability of the ISMS to achieve the intended results
    - Minor - A nonconformity that does not affect the capability of the ISMS to achieve the intended results
- Not Applicable - Requirement was excluded on the Statement of Applicability
- Not Selected - Requirement was excluded based on the audit program

Nonconformity Remediation Status

A remediation status has been assigned for each nonconformity identified based on the criteria defined below:

- Open - Status assigned when neither the correction or corrective action has been reviewed and approved by A-LIGN
- Plan for correction and corrective action accepted - Status assigned when the corresponding correction and corrective action has been reviewed and approved by A-LIGN
- Resolved - Status assigned when the correction and corrective action was reviewed, approved, and verified by A-LIGN

Confidentiality Statement

The information included in this report is to be treated as confidential. The report is intended to be for the use of those parties included in the distribution list below and should not be relied upon by any other parties.

Distribution List

The report has been distributed to the following persons:

- Marc Phillips, GRC Manager, TokenEx
- Jon Clemenson, Director of IT Security, TokenEx
- Petar Besalev, EVP of Cybersecurity and Compliance Services, A-LIGN
- Adam Lubbert, Associate Director, A-LIGN
- Chase Neumayer, Lead Auditor, A-LIGN
- Deborah Yadidi, Auditor, A-LIGN

SECTION 2: CONFORMANCE TESTING

ISO 17021 / ISO 27006 Surveillance requirements	Conformity Level
Communications from external parties	Conforms
Changes to the documented system	Conforms
Areas subject to change	Conforms
Action taken on nonconformities identified during the last audit	Conforms
Appropriate use of the certificate /mark	Conforms
Appeals and complaints	Conforms
Continual improvement	Conforms

	ISO 27001:2013 Clauses	Conformity Level
	Clause 4 - Context of the Organization	
4.1	**Understanding the Organization and its Context**	
4.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	Conforms
4.2	**Understanding the Needs and Expectations of Interested Parties**	
4.2.a	The organization shall determine: Interested parties that are relevant to the information security management system; and	Conforms
4.2.b	The organization shall determine: The requirements of these interested parties relevant to information security.	Conforms
4.3	**Determining the scope of the Information Security Management System**	
The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider:		
4.3.a	The external and internal issues referred to in 4.1;	Conforms
4.3.b	The requirements referred to in 4.2; and	Conforms
4.3.c	Interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	Conforms
4.4	**Information Security Management System**	
4.4	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	Conforms
	Clause 5 - Leadership	
5.1	**Leadership and Commitment**	
Top management shall demonstrate leadership and commitment with respect to the information security management system by:		
5.1.a	Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;	Conforms
5.1.b	Ensuring the integration of the information security management system requirements into the organization’s processes;	Conforms

ISO 27001:2013 Clauses		Conformity Level
5.1.c	Ensuring that the resources needed for the information security management system are available;	Conforms
5.1.d	Communicating the importance of effective information security management and of conforming to the information security management system requirements;	Conforms
5.1.e	Ensuring that the information security management system achieves its intended outcome(s);	Conforms
5.1.f	Directing and supporting persons to contribute to the effectiveness of the information security management system;	Conforms
5.1.g	Promoting continual improvement; and	Conforms
5.1.h	Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	Conforms
5.2	**Policy**	
Top management shall establish an information security policy that:		
5.2.a	Is appropriate to the purpose of the organization;	Conforms
5.2.b	Includes information security objectives (see 6.2) or provides the framework for setting information security objectives;	Conforms
5.2.c	Includes a commitment to satisfy applicable requirements related to information security; and	Conforms
5.2.d	Includes a commitment to continual improvement of the information security management system.	Conforms
The information security policy shall:		
5.2.e	Be available as documented information;	Conforms
5.2.f	Be communicated within the organization; and	Conforms
5.2.g	Be available to interested parties, as appropriate.	Conforms
5.3	**Organizational Roles, Responsibilities, and Authorities**	
Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for:		
5.3.a	Ensuring that the information security management system conforms to the requirements of this International Standard; and	Conforms
5.3.b	Reporting on the performance of the information security management system to top management.	Conforms

ISO 27001:2013 Clauses		Conformity Level
	Clause 6 - Planning	
6.1	**Actions to Address Risks and Opportunities**	
6.1.1	**General**	
When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:		
6.1.1.a	Ensure the information security management system can achieve its intended outcome(s);	Conforms
6.1.1.b	Prevent, or reduce, undesired effects; and	Conforms
6.1.1.c	Achieve continual improvement.	Conforms
The organization shall plan:		
6.1.1.d	Actions to address these risks and opportunities; and	Conforms
6.1.1.e	How to: 1) Integrate and implement the actions into its information security management system processes; and 2) Evaluate the effectiveness of these actions.	Conforms
6.1.2	**Information Security Risk Assessment**	
The organization shall define and apply an information security risk assessment process that:		
6.1.2.a	Establishes and maintains information security risk criteria that include: 1) The risk acceptance criteria; and 2) Criteria for performing information security risk assessments;	Conforms
6.1.2.b	Ensures that repeated information security risk assessments produce consistent, valid, and comparable results;	Conforms
6.1.2.c	Identifies the information security risks: 1) Apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the information security management system; and 2) Identify the risk owners;	Conforms
6.1.2.d	Analyzes the information security risks: 1) Assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) Assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) Determine the levels of risk; and	Conforms

ISO 27001:2013 Clauses		Conformity Level
6.1.2.e	Evaluates the information security risks: 1) Compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) Prioritize the analyzed risks for risk treatment.	Conforms
6.1.3	**Information Security Risk Treatment**	
The organization shall define and apply an information security risk treatment process to:		
6.1.3.a	Select appropriate information security risk treatment options, taking account of the risk assessment results;	Conforms
6.1.3.b	Determine all controls that are necessary to implement the information security risk treatment option(s) chosen; (Note: Organizations can design controls as required or identify them from any source)	Conforms
6.1.3.c	Compare the controls determined in 6.1.3.b above with those in Annex A and verify that no necessary controls have been omitted;	Conforms
6.1.3.d	Produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;	Conforms
6.1.3.e	Formulate an information security risk treatment plan; and	Conforms
6.1.3.f	Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	Conforms
6.2	**Information Security Objectives and Planning to Achieve Them**	
The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:		
6.2.a	Be consistent with the information security policy;	Conforms
6.2.b	Be measurable (if practicable);	Conforms
6.2.c	Take into account applicable information security requirements, and results from risk assessment and risk treatment;	Conforms
6.2.d	Be communicated; and	Conforms
6.2.e	Be updated as appropriate.	Conforms
The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine:		
6.2.f	What will be done;	Conforms

	ISO 27001:2013 Clauses	Conformity Level
6.2.g	What resources will be required;	Conforms
6.2.h	Who will be responsible;	Conforms
6.2.i	When it will be completed; and	Conforms
6.2.j	How the results will be evaluated.	Conforms
	Clause 7 - Support	
7.1	**Resources**	
7.1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the information security management system.	Conforms
7.2	**Competence**	
The organization shall:		
7.2.a	Determine the necessary competence of person(s) doing work under its control that affects its information security performance;	Conforms
7.2.b	Ensure that these persons are competent on the basis of appropriate education, training, or experience;	Conforms
7.2.c	Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and	Conforms
7.2.d	Retain appropriate documented information as evidence of competence.	Conforms
7.3	**Awareness**	
Persons doing work under the organization’s control shall be aware of:		
7.3.a	The information security policy;	Conforms
7.3.b	Their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and	Conforms
7.3.c	The implications of not conforming with the information security management system requirements.	Conforms
7.4	**Communication**	
The organization shall determine the need for internal and external communications relevant to the information security management system including:		
7.4.a	On what to communicate;	Conforms
7.4.b	When to communicate;	Conforms
7.4.c	With whom to communicate;	Conforms

ISO 27001:2013 Clauses		Conformity Level
7.4.d	Who shall communicate; and	Conforms
7.4.e	The processes by which communication shall be effected.	Conforms
7.5	**Documented Information**	
7.5.1	**General**	
The organization's information security management system shall include:		
7.5.1.a	Documented information required by this International Standard; and	Conforms
7.5.1.b	Documented information determined by the organization as being necessary for the effectiveness of the information security management system.	Conforms
7.5.2	**Creating and Updating**	
When creating and updating documented information the organization shall ensure appropriate:		
7.5.2.a	Identification and description (e.g. a title, date, author, or reference number);	Conforms
7.5.2.b	Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	Conforms
7.5.2.c	Review and approval for suitability and adequacy.	Conforms
7.5.3	**Control of Documented Information**	
Documented information required by the information security management system and by this International Standard shall be controlled to ensure:		
7.5.3.a	It is available and suitable for use, where and when it is needed; and	Conforms
7.5.3.b	It is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	Conforms
For the control of documented information, the organization shall address the following activities, as applicable:		
7.5.3.c	Distribution, access, retrieval, and use;	Conforms
7.5.3.d	Storage and preservation, including the preservation of legibility;	Conforms
7.5.3.e	Control of changes (e.g. version control); and	Conforms
7.5.3.f	Retention and disposition.	Conforms

ISO 27001:2013 Clauses		Conformity Level
Clause 8 - Operation		
8.1	**Operational Planning and Control**	
	The organization shall plan, implement, and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.	Conforms
8.2	**Information Security Risk Assessment**	
	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	Conforms
8.3	**Information Security Risk Treatment**	
	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	Conforms
Clause 9 - Performance Evaluation		
9.1	**Monitoring, Measurement, Analysis, and Evaluation**	
The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:		
9.1.a	What needs to be monitored and measured, including information security processes and controls;	Conforms

ISO 27001:2013 Clauses		Conformity Level
9.1.b	The methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results;	Conforms
9.1.c	When the monitoring and measuring shall be performed;	Conforms
9.1.d	Who shall monitor and measure;	Conforms
9.1.e	When the results from monitoring and measurement shall be analyzed and evaluated; and	Conforms
9.1.f	Who shall analyze and evaluate these results.	Conforms
9.2	**Internal Audit**	
The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:		
9.2.a	Conforms to: 1) The organization’s own requirements for its information security management system; and 2) The requirements of this International Standard; and	Conforms
9.2.b	Is effectively implemented and maintained.	Conforms
The organization shall:		
9.2.c	Plan, establish, implement, and maintain an audit program, including the frequency, methods, responsibilities, planning requirements and reporting. The audit program shall take into consideration the importance of the processes concerned and the results of previous audits;	Conforms
9.2.d	Define the audit criteria and scope for each audit;	Conforms
9.2.e	Select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	Conforms
9.2.f	Ensure that the results of the audits are reported to relevant management; and	Conforms
9.2.g	Retain documented information as evidence of the audit program and the audit results.	Conforms
9.3	**Management Review**	
Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. The management review shall include consideration of:		
9.3.a	The status of actions from previous management reviews;	Conforms
9.3.b	Changes in external and internal issues that are relevant to the information security management system;	Conforms

ISO 27001:2013 Clauses		Conformity Level
9.3.c	Feedback on the information security performance, including trends in: 1) Nonconformities and corrective actions; 2) Monitoring and measurement results; 3) Audit results; and 4) Fulfilment of information security objectives;	Conforms
9.3.d	Feedback from interested parties;	Conforms
9.3.e	Results of risk assessment and status of risk treatment plan; and	Conforms
9.3.f	Opportunities for continual improvement.	Conforms
The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.		
	Clause 10 - Improvement	
10.1	**Nonconformity and Corrective Action**	
When a nonconformity occurs, the organization shall:		
10.1.a	React to the nonconformity, and as applicable: 1) Take action to control and correct it; and 2) Deal with the consequences;	Conforms
10.1.b	Evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) Reviewing the nonconformity; 2) Determining the causes of the nonconformity; and 3) Determining if similar nonconformities exist, or could potentially occur;	Conforms
10.1.c	Implement any action needed;	Conforms
10.1.d	Review the effectiveness of any corrective action taken; and	Conforms
10.1.e	Make changes to the information security management system, if necessary.	Conforms
Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:		
10.1.f	The nature of the non-conformities and any subsequent actions taken; and	Conforms
10.1.g	The results of any corrective action.	Conforms
10.2	**Continual Improvement**	
	The organization shall continually improve the suitability, adequacy, and effectiveness of the information security management system.	Conforms

ISO 27001:2013 Annex A		Conformity Level
A.5 - Information Security Policies		
5.1 Management director for information security		
5.1.1	Policies for information security	Conforms
5.1.2	Review of the policies for information security	Conforms
A.6 - Organization of Information Security		
6.1 Internal organization		
6.1.1	Information security roles and responsibilities	Not selected
6.1.2	Segregation of duties	Not selected
6.1.3	Contact with authorities	Not selected
6.1.4	Contact with special interest groups	Not selected
6.1.5	Information security in project management	Not selected
6.2 Mobile devices and teleworking		
6.2.1	Mobile device policy	Not selected
6.2.2	Teleworking	Not selected
A.7 - Human Resource Security		
7.1 Prior to employment		
7.1.1	Screening	Conforms
7.1.2	Terms and conditions of employment	Conforms
7.2 During employment		
7.2.1	Management responsibilities	Conforms
7.2.2	Information security awareness, education, and training	Conforms
7.2.3	Disciplinary process	Conforms
7.3 Termination and change of employment		
7.3.1	Termination or change of employment responsibilities	Conforms
A.8 - Asset Management		
8.1 Responsibility for assets		
8.1.1	Inventory of assets	Conforms
8.1.2	Ownership of assets	Conforms
8.1.3	Acceptable use of assets	Conforms
8.1.4	Return of assets	Conforms
8.2 Information classification		
8.2.1	Classification of information	Conforms
8.2.2	Labeling of information	Conforms
8.2.3	Handling of assets	Conforms

ISO 27001:2013 Annex A		Conformity Level
8.3 Media handling		
8.3.1	Management of removable media	Conforms
8.3.2	Disposal of media	Not applicable
8.3.3	Physical media transfer	Not applicable
A.9 - Access Control		
9.1 Business requirements of access control		
9.1.1	Access control policy	Conforms
9.1.2	Access to network and network services	Not selected
9.2 User access management		
9.2.1	User registration and de-registration	Not selected
9.2.2	User access provisioning	Not selected
9.2.3	Management of privileged access rights	Not selected
9.2.4	Management of secret authentication information of users	Not selected
9.2.5	Review of user access rights	Not selected
9.2.6	Removal or adjustment of access rights	Not selected
9.3 User responsibilities		
9.3.1	Use of secret authentication information	Not selected
9.4 System and application access control		
9.4.1	Information access restriction	Not selected
9.4.2	Secure log-on procedures	Not selected
9.4.3	Password management system	Not selected
9.4.4	Use of privileged utility programs	Not selected
9.4.5	Access control to program source code	Not selected
A.10 - Cryptography		
10.1 Cryptographic controls		
10.1.1	Policy on the use of cryptographic controls	Conforms
10.1.2	Key management	Conforms
A.11 - Physical and Environmental Security		
11.1 Secure areas		
11.1.1	Physical security perimeter	Not applicable
11.1.2	Physical entry controls	Not applicable
11.1.3	Securing offices, rooms, and facilities	Not applicable
11.1.4	Protecting against external and environmental threats	Not applicable
11.1.5	Working in secure areas	Not applicable

ISO 27001:2013 Annex A		Conformity Level
11.1.6	Delivery and loading areas	Not applicable
11.2 Equipment		
11.2.1	Equipment siting and protection	Not applicable
11.2.2	Supporting utilities	Not applicable
11.2.3	Cabling security	Not applicable
11.2.4	Equipment maintenance	Not applicable
11.2.5	Removal of assets	Not applicable
11.2.6	Security of equipment and assets off-premises	Not applicable
11.2.7	Secure disposal or re-use of equipment	Not applicable
11.2.8	Unattended user equipment	Not applicable
11.2.9	Clear desk and clear screen policy	Not applicable
A.12 - Operations Security		
12.1 Operational procedures and responsibilities		
12.1.1	Documented operating procedures	Conforms
12.1.2	Change management	Conforms
12.1.3	Capacity management	Conforms
12.1.4	Separation of development, testing and operational environments	Conforms
12.2 Protection from malware		
12.2.1	Controls against malware	Conforms
12.3 Backup		
12.3.1	Information backup	Conforms
12.4 Logging and monitoring		
12.4.1	Event logging	Conforms
12.4.2	Protection of log information	Conforms
12.4.3	Administrator and operator logs	Conforms
12.4.4	Clock synchronization	Conforms
12.5 Control of operational software		
12.5.1	Installation of software on operational systems	Conforms
12.6 Technical vulnerability management		
12.6.1	Management of technical vulnerabilities	Conforms
12.6.2	Restrictions of software installation	Conforms
12.7 Information systems audit considerations		
12.7.1	Information systems audit controls	Conforms

ISO 27001:2013 Annex A		Conformity Level
A.13 - Communications Security		
13.1 Network security management		
13.1.1	Network controls	Not selected
13.1.2	Security of network services	Not selected
13.1.3	Segregation in networks	Not selected
13.2 Information transfer		
13.2.1	Information transfer policies and procedures	Not selected
13.2.2	Agreements on information transfer	Not selected
13.2.3	Electronic messaging	Not selected
13.2.4	Confidentiality or non-disclosure agreements	Conforms
A.14 - Systems Acquisition, Development, and Maintenance		
14.1 Security requirements of information systems		
14.1.1	Information security requirements analysis and specification	Not selected
14.1.2	Securing application services on public networks	Not selected
14.1.3	Protecting application services transactions	Not selected
14.2 Security in development and support processes		
14.2.1	Secure development policy	Not selected
14.2.2	System change control procedures	Not selected
14.2.3	Technical review of applications after operating platform changes	Not selected
14.2.4	Restrictions on changes to software packages	Not selected
14.2.5	Secure system engineering principles	Conforms
14.2.6	Secure development environment	Not selected
14.2.7	Outsourced development	Not applicable
14.2.8	System security testing	Not selected
14.2.9	System acceptance testing	Not selected
14.3 Test data		
14.3.1	Protection of test data	Not selected
A.15 - Supplier Relationships		
15.1 Information security in supplier relationships		
15.1.1	Information security policy for supplier relationships	Conforms
15.1.2	Addressing security within supplier agreements	Not selected
15.1.3	Information and communication technology supply chain	Not selected

ISO 27001:2013 Annex A		Conformity Level
15.2 Supplier service delivery management		
15.2.1	Monitoring and review of supplier services	Not selected
15.2.2	Managing changes to supplier services	Not selected
A.16 - Information Security Incident Management		
16.1 Management of information security incidents and improvements		
16.1.1	Responsibilities and procedures	Conforms
16.1.2	Reporting information security events	Conforms
16.1.3	Reporting information security weaknesses	Conforms
16.1.4	Assessment of and decision on information security events	Conforms
16.1.5	Response to information security incidents	Conforms
16.1.6	Learning from information security incidents	Conforms
16.1.7	Collection of evidence	Conforms
A.17 - Information Security Aspects of Business Continuity Management		
17.1 Information security continuity		
17.1.1	Planning information security continuity	Conforms
17.1.2	Implementing information security continuity	Conforms
17.1.3	Verify, review and evaluate information security continuity	Conforms
17.2 Redundancies		
17.2.1	Availability of information processing facilities	Conforms
A.18 - Compliance		
18.1 Compliance with legal and contractual requirements		
18.1.1	Identification of applicable legislation and contractual requirements	Conforms
18.1.2	Intellectual property rights	Not selected
18.1.3	Protection of records	Not selected
18.1.4	Privacy and protection of personally identifiable information	Not selected
18.1.5	Regulation of cryptographic controls	Not selected
18.2 Information security reviews		
18.2.1	Independent review of information security	Not selected
18.2.2	Compliance with security policies and standards	Not selected
18.2.3	Technical compliance review	Not selected

SECTION 3: NONCONFORMITY SUMMARY

Nonconformities from the current certification cycle, including the current year, if any, are listed below:

	CONTROL	CONTROL OBJECTIVE	JUSTIFICATION	NOTED	STATUS
There were no nonconformities identified in this surveillance audit.					