Cronofy Limited

ISO/IEC 27001:2013
Stage 2 Report

June 18, 2020

Table of Contents

SECTION 1: STAGE 2 AUDIT REPORT **1**

Company Background *2*
Overview *2*
Audit Findings *2*
Audit Conclusion *2*
Audit Objectives *2*
Audit Criteria *3*
Audit Scope *3*
Audit Method *3*
Audit Process *4*
Internal Audit *5*
Management Reviews *5*
Conformity Level *5*
Nonconformity Remediation Status *5*
Confidentiality Statement *5*
Distribution List *6*

SECTION 2: CONFORMANCE TESTING **7**

ISO 27001:2013 Clauses *8*
ISO 27001:2013 Annex A *18*

SECTION 3: NONCONFORMITY SUMMARY **24**

SECTION 1: STAGE 2 AUDIT REPORT

Cronofy Limited
Karl Bagci
Head of Operations
4th Floor, 1 Broadway,
Nottingham, NG1 1PR

June 18, 2020

Company Background

Cronofy Limited ("Cronofy" or the "Company") was founded in 2014 to address the needs of people wanting to schedule time with organizations, teams, and other people. The core service is delivered as a software as a service (SaaS) application programming interface (API) designed to allow a software developer to interact with an end-user's calendar data and drive scheduling workflows with it. For those who don't want to code against an API, Cronofy offers embeddable and stand-alone scheduling products, built on top of the core API.

Cronofy's serves software vendors providing solutions to a wide variety of industries, including human resources, finance, healthcare, labor marketplaces, education and customer relationship management (CRM).

Overview

To demonstrate the Company's dedication to information security, Cronofy 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, maintaining an ISMS. A-LIGN Compliance and Security Inc. (A-LIGN) was engaged by Cronofy to perform the initial certification audit to validate conformity and certify the Company's ISMS against the ISO 27001 standard.

The initial certification audit is conducted in two stages: stage 1 and stage 2. A stage 1 audit is performed to review the documented ISMS information, obtain necessary information regarding the scope of the ISMS, and determine the preparedness for stage 2. The remote stage 1 was performed on April 23, 2020.

The stage 2 audit was conducted to evaluate the implementation, including effectiveness, of the Company's ISMS. Stage 2 was performed between June 1, 2020 and June 3, 2020.

A-LIGN analyzed all information and audit evidence gathered during stage 1 and stage 2, reviewed the audit findings, and agreed on the audit conclusion.

Audit Findings

No non-conformities were identified during the stage 2 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 certification as of the date of this report.

Audit Objectives

The stage 2 audit was conducted to accomplish the following:

- Determine the conformity of the Company's ISMS, or parts of it, with the audit criteria
- Determine the ability of the Company's ISMS to meet applicable statutory, regulatory, and contractual requirements
- Determine the effectiveness of the Company's ISMS to achieve specified objectives
- Identify areas of potential improvement of the Company's ISMS, as applicable

Audit Criteria

A-LIGN performed the stage 2 audit to determine conformity to the requirements of ISO 27001 and the defined processes and procedures of the Company's ISMS. Statement of applicability version 1.4, dated June 2, 2020, 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 purpose of this document is to provide a record of the scope of the Information Security Management System (ISMS). Cronofy is committed to protecting all data, employee and customer. To achieve this goal, the company has implemented an Information Security Management System in accordance with the standard. Cronofy's ISMS protects all information and data assets for the delivery of all Cronofy functions, services and activities. The assets protected are electronic data, software, and physical IT hardware. Supporting technology includes cloud-based servers, which are within the control of Cronofy. The ISMS applies to all functions, services, activities and data information assets of Cronofy."

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:

- Examine and verify the structure, policies, processes, procedures, records, and related documents of the client relevant to the ISMS
- Determine that these met all the requirements relevant to the intended scope of certification
- Determine that the processes and procedures were established, implemented, and maintained effectively, to provide a basis for confidence in the Company's ISMS
- Communicate to the client, for its action, any inconsistencies between the Company's policy, objectives, and targets

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

Evidence description	Version / Date
Scope of ISMS	4.0 5/27/2020
Information security policy	6.0 5/29/2020
Information security risk assessment methodology	7.0 6/1/2020
Information security risk treatment methodology	7.0 6/1/2020
Statement of applicability	1.4 6/2/2020
Information security objectives	Various
Evidence of competence	7.0 5/29/2020

Evidence description	Version / Date
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	5/28/2020
Information security risk treatment plan	5/28/2020
Evidence of monitoring and measuring results	1.0 6/1/2020
Internal audit program	3.0 5/18/2020
Internal audit report	6/2/2020
Management reviews	Various
Nonconformities and subsequent action(s) taken	Ongoing
Correction(s) and corrective action(s)	Various
ISMS roles and responsibilities	4.0 5/20/2020
Asset inventory	Various
Acceptable use policy	4.0 5/29/2020
Operating procedures for IT management	Various
Secure system(s) engineering principles	Various
Vendor security policy	2.0 5/18/2020
Incident management procedures	7.0 5/29/2020
Business continuity procedures	3.0 5/19/2020
Statutory, regulatory, and contractual requirements	6.0 5/29/2020
Logs of user activities, exceptions, and security events	Various

Audit Process

An opening meeting occurred at approximately 1:00 PM GMT on June 1, 2020. In attendance were Karl Bagci (Head of Operations, Cronofy); Garry Shutler (CTO and Co-founder, Cronofy); Aleksandar Ivanov (Lead Auditor, A-LIGN); and Eric Bruning (Auditor, A-LIGN). An opening meeting agenda and audit plan was communicated.

The audit was performed over 3 days, between June 1, 2020 and June 3, 2020, which consisted of 3 remote auditing days. Teleconferencing and screen-sharing technology were utilized during the stage 2 audit. 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 GMT on June 3, 2020. In attendance were Chris Taylor (Senior Site Reliability Engineer, Cronofy); Karl Bagci (Head of Operations, Cronofy); Garry Shutler (CTO and Co-founder, Cronofy); Aleksandar Ivanov (Lead Auditor, A-LIGN); and Eric Bruning (Lead Auditor, A-LIGN). An agenda was provided as well as version 1 of the stage 2 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 June 2020 by internal employees hand-picked to ensure objectivity and impartiality, identified 9 nonconformities. Results of this internal audit, including any nonconformities, and corrective actions were reviewed and approved by the ISMS Board in June 2020, 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 ISMS Board, were scheduled to occur quarterly. The ISMS Board was composed of:

- CTO
- Head of Operations

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 ISMS Board.

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:

- Garry Shutler, CTO and Co-Founder, Cronofy
- Karl Bagci, Head of Operations, Cronofy
- Steve Simmons, EVP Compliance Services, A-LIGN
- Arti Lalwani, ISO Practice Lead, A-LIGN
- Adam Lubbert, Senior Manager, A-LIGN
- Aleksandar Ivanov, Lead Auditor, A-LIGN
- Eric Bruning, Auditor, A-LIGN

SECTION 2: CONFORMANCE TESTING

	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

	ISO 27001:2013 Clauses	Conformity Level
5.3.b	Reporting on the performance of the information security management system to top management.	Conforms
	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

	ISO 27001:2013 Clauses	Conformity Level
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
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

	ISO 27001:2013 Clauses	Conformity Level
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
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

	ISO 27001:2013 Clauses	Conformity Level
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
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

	ISO 27001:2013 Clauses	Conformity Level
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
	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

	ISO 27001:2013 Clauses	Conformity Level
	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
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

	ISO 27001:2013 Clauses	Conformity Level
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
9.3.c	Feedback on the information security performance, including trends in: 1) Non-conformities 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 non-conformities 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

	ISO 27001:2013 Clauses	Conformity Level
10.1.e	Make changes to the information security management system, if necessary.	Conforms
Corrective actions shall be appropriate to the effects of the non-conformities 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	Conforms
6.1.2	Segregation of duties	Conforms
6.1.3	Contact with authorities	Conforms
6.1.4	Contact with special interest groups	Conforms
6.1.5	Information security in project management	Not applicable
6.2 Mobile devices and teleworking		
6.2.1	Mobile device policy	Conforms
6.2.2	Teleworking	Conforms
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

ISO 27001:2013 Annex A		Conformity Level
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
8.3 Media handling		
8.3.1	Management of removable media	Not applicable
8.3.2	Disposal of media	Conforms
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	Conforms
9.2 User access management		
9.2.1	User registration and de-registration	Conforms
9.2.2	User access provisioning	Conforms
9.2.3	Management of privileged access rights	Conforms
9.2.4	Management of secret authentication information of users	Conforms
9.2.5	Review of user access rights	Conforms
9.2.6	Removal or adjustment of access rights	Conforms
9.3 User responsibilities		
9.3.1	Use of secret authentication information	Conforms
9.4 System and application access control		
9.4.1	Information access restriction	Conforms
9.4.2	Secure log-on procedures	Conforms
9.4.3	Password management system	Conforms
9.4.4	Use of privileged utility programs	Conforms
9.4.5	Access control to program source code	Conforms
A.10 - Cryptography		
10.1 Cryptographic controls		
10.1.1	Policy on the use of cryptographic controls	Conforms
10.1.2	Key management	Conforms

ISO 27001:2013 Annex A		Conformity Level
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
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	Conforms
11.2.7	Secure disposal or re-use of equipment	Conforms
11.2.8	Unattended user equipment	Conforms
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

ISO 27001:2013 Annex A		Conformity Level
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
A.13 - Communications Security		
13.1 Network security management		
13.1.1	Network controls	Conforms
13.1.2	Security of network services	Conforms
13.1.3	Segregation in networks	Not applicable
13.2 Information transfer		
13.2.1	Information transfer policies and procedures	Conforms
13.2.2	Agreements on information transfer	Conforms
13.2.3	Electronic messaging	Conforms
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	Conforms
14.1.2	Securing application services on public networks	Conforms
14.1.3	Protecting application services transactions	Conforms
14.2 Security in development and support processes		
14.2.1	Secure development policy	Conforms
14.2.2	System change control procedures	Conforms
14.2.3	Technical review of applications after operating platform changes	Conforms
14.2.4	Restrictions on changes to software packages	Conforms
14.2.5	Secure system engineering principles	Conforms
14.2.6	Secure development environment	Conforms
14.2.7	Outsourced development	Not applicable
14.2.8	System security testing	Conforms

ISO 27001:2013 Annex A		Conformity Level
14.2.9	System acceptance testing	Conforms
14.3 Test data		
14.3.1	Protection of test data	Not applicable
	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	Conforms
15.1.3	Information and communication technology supply chain	Conforms
15.2 Supplier service delivery management		
15.2.1	Monitoring and review of supplier services	Conforms
15.2.2	Managing changes to supplier services	Conforms
	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	Conforms

ISO 27001:2013 Annex A		Conformity Level
18.1.3	Protection of records	Conforms
18.1.4	Privacy and protection of personally identifiable information	Conforms
18.1.5	Regulation of cryptographic controls	Conforms
18.2 Information security reviews		
18.2.1	Independent review of information security	Conforms
18.2.2	Compliance with security policies and standards	Conforms
18.2.3	Technical compliance review	Conforms

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
1.	No nonconformities found during the Stage 2 Audit.				