

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and _____ ("Service Provider") on _____ ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Section I: General - All Data *(Continued)*

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.
Agree: Yes No

5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
Agree: Yes No

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
Agree: Yes No

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
Agree: Yes No

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).
Agree: Yes No

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.
Agree: Yes No

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Agree: Yes No

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Agree: Yes No

3. Vendors cannot sell student information.

Agree: Yes No

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Agree: Yes No

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Agree: Yes No

6. Vendors must delete district-controlled student information when requested by the District.

Agree: Yes No

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

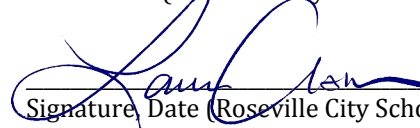
Print Name



Signature, Date

Laura Assem

Print Name (Roseville City School District)

 4/8/2023

Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Section 1.7: Internal Security

Section II.2: Exporting of Student-Created Content

Section II.4: Review and Correcting Personally Identifiable Information (PII)

EXHIBITS

Section II.5: Securing Student Data

Section II.6: Disclosure Notification

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Section III.5: How Student Data is Protected:

Compliance with FERPA:

The Federal Education Rights and Privacy Act (FERPA) requires educators to protect the privacy of students and safeguard the confidentiality of their records. As our platform is anonymous and “un-rostered” we avoid some of the direct PII points of contact and categories of data that are typically protected under FERPA. Unlike some other “rostered” or “registered” ARS platforms STOPit Solutions does not require registration (and a User cannot register) to initiate a report on our platform, and thus no personally identifiable information is captured (no name, email, phone number, or student ID, etc.). Still, there are ways that PII can creep into a dataset through self-identification or through every day use by a reporter or administrator, and information from student reports can contain sensitive information. Because of the general sensitivity of the information flowing through our platform, we take great care in safeguarding access and data security. We have a multi-tiered permissions process allowing only those with designated permissions and appropriate role assignments to view such data. We also apply significant resources to 5 generally recognized security areas, in order to comply with FERPA including:

- We own, host and maintain all of our technology and data entirely within the United States, using redundant facilities and industry standard DR protocols
- Encryption – Incident data is encrypted in motion and at rest using advanced encryption standards (AES)
- Vulnerability and Penetration Testing - We regularly undergo third party security audits which provide vulnerability testing and results which are promptly remediated where necessary
- Compliance Monitoring Mechanisms – We utilize industry standard monitoring processes and tools to ensure performance and identify threats and vulnerabilities
- SOC2 Audit – we are one of the few anonymous reporting platforms to have undergone SOC2 data security requirements and annual independent SOC 2 audits – we can make our latest SOC2 report available, upon request

In terms of access to and control of incident information, the school district is the ultimate custodian of this data and the district controls to whom it is released, if at all. Any exceptions to this would be:

- Our “super admins” which are designated customer experience individuals in our organization empowered with full-access level viewing rights so that they may help organizations with support and / or crisis needs
- Our crisis center team members (our trained and certified Incident Response Specialists) which are empowered by school districts, in certain situations (predefined with districts prior to launch), to intervene in emergencies and act on a district’s behalf
- In response to a lawfully issued subpoena, in which case, we always act in accordance with the law

Safe Handling of Inappropriate Content:

This is a large area of concern among administrators and we have taken significant precautions around handling inappropriate content according to best practices provided to us by school administrators and law enforcement. Specifically:

- Both images and videos can be uploaded as evidence on our platform and attached to a reported incident.
- We utilize a product called “AWS ReKognition” which specifically screens all images for inappropriate content (its accuracy rates tend to be 98% or higher).
- Upon programmatically identifying inappropriate content, our platform “Hides” the image from viewing so that administrators cannot access.
- “ReKognition” is trained to pick up certain categories of inappropriate content according to our instructions (we have refined this categorization over the years)
- Video hiding is performed through an automated message which asks a reporter to indicate whether or not it contains inappropriate content. Video hiding will be automated using “ReKognition” in the near future, similar to the above automated procedure for images
- Our Data Privacy team can “Un-Hide” these images upon request from law enforcement so that users appropriately permissioned on our platform can view a piece of evidence. We do not take these instructions from non-law enforcement school personnel



Service Organization Control 2 (SOC 2®) Type 2 Report

Report on Inspirit Group, LLC, dba STOPit Solutions description of its Anonymous Reporting System and on the suitability of the design and operating effectiveness of controls relevant to Security for the period March 15, 2021 to December 31, 2021



Attestation & Advisory Services



This report is intended solely for use by the management of Inspirit Group, LLC, dba STOPit Solutions and the specified parties, and is not intended and should not be used by anyone other than these parties.



Table of Contents

Section I	1
Inspirit Group, LLC, dba STOPit Solutions's Management Assertion	2
Section II	4
Independent Service Auditor's Report	5
Section III	10
Purpose and Scope of Report	11
Principal Service Commitments and System Requirements	12
Components of the System Used to Provide the Services	12
Infrastructure	12
Software	14
People	15
Policies, Processes & Procedures	15
Data	16
Significant Changes to the System Throughout the Examination Period	17
Control Environment	17
Risk Assessment	20
In-Scope Trust Service Categories	21
Trust Service Criteria and Related Control Activities	22
Information and Communication	22
Monitoring	23
Control Activities	24
Complementary Subservice Organization Controls	28
Complementary User Entity Controls	29
Section IV	31
Trust Service Criteria, Related Controls and Tests of Controls	32



Section I

Inspirit Group, LLC, dba STOPit Solutions's Management Assertion



Inspirit Group, LLC, dba STOPit Solutions's Management Assertion

We have prepared the attached description titled "Inspirit Group, LLC, dba STOPit Solutions's Description of its Anonymous Reporting System" throughout the period March 15, 2021 to December 31, 2021 ("description") based on the criteria for a description of a service organization's system in DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide users with information about the Anonymous Reporting System that may be useful when assessing the risks arising from interactions with Inspirit Group, LLC, dba STOPit Solutions's Anonymous Reporting System, particularly information about system controls that Inspirit Group, LLC, dba STOPit Solutions has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, *Trust Services Criteria*).

Inspirit Group, LLC, dba STOPit Solutions uses subservice organizations to provide cloud infrastructure services. The description indicates that complementary subservice organization controls that are suitably designed and implemented are necessary, along with controls at Inspirit Group, LLC, dba STOPit Solutions, to achieve Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements based on the applicable trust services criteria. The description presents Inspirit Group, LLC, dba STOPit Solutions's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and implemented are necessary, along with controls at Inspirit Group, LLC, dba STOPit Solutions, to achieve Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements based on the applicable trust services criteria. The description presents Inspirit Group, LLC, dba STOPit Solutions controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls.



We confirm, to the best of our knowledge and belief, that:

1. The description presents Inspirit Group, LLC, dba STOPit Solutions's Anonymous Reporting System that was designed and implemented throughout the period March 15, 2021 to December 31, 2021 in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period March 15, 2021 to December 31, 2021 to provide reasonable assurance that Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls throughout the period March 15, 2021 to December 31, 2021.
3. The controls stated in the description operated effectively throughout the period March 15, 2021 to December 31, 2021, to provide reasonable assurance that Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls, operated effectively throughout the period March 15, 2021 to December 31, 2021.

DocuSigned by:

CBF7C2C253A8496...

Jai Prakash Pandu, CTO
Inspirit Group, LLC, dba STOPit Solutions
January 24, 2022



Section II

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Inspirit Group, LLC, dba STOPit Solutions:

Scope

We have examined Inspirit Group, LLC, dba STOPit Solutions's attached description titled "Inspirit Group, LLC, dba STOPit Solutions's Description of its Anonymous Reporting System" throughout the period March 15, 2021 to December 31, 2021, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 15, 2021 to December 31, 2021, to provide reasonable assurance that Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Inspirit Group, LLC, dba STOPit Solutions uses subservice organizations to provide cloud infrastructure services. The description indicates that complementary subservice organization controls that are suitably designed and implemented are necessary, along with controls at Inspirit Group, LLC, dba STOPit Solutions to achieve Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements based on the applicable trust services criteria. The description presents Inspirit Group, LLC, dba STOPit Solutions's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and implemented are necessary, along with controls at Inspirit Group, LLC, dba STOPit Solutions, to achieve Inspirit Group, LLC, dba STOPit Solutions's service

commitments and system requirements based on the applicable trust services criteria. The description presents Inspirit Group, LLC, dba STOPit Solutions's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

Service organization's responsibilities

Inspirit Group, LLC, dba STOPit Solutions is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements were achieved. In Section I, Inspirit Group, LLC, dba STOPit Solutions has provided the accompanying assertion titled "Inspirit Group, LLC, dba STOPit Solutions's Management Assertion" ("assertion"), about the description and the suitability of the design of controls stated therein. Inspirit Group, LLC, dba STOPit Solutions is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

Service auditors' responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with the Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other Than

Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance* and with attestation standards established by the American Institute of Certified Public Accountants (AICPA). These standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description
- Performing such other procedures as we considered necessary in the circumstances

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects,

- a. The description presents Inspirit Group, LLC, dba STOPit Solutions's Anonymous Reporting System that was designed and implemented throughout the period March 15, 2021 to December 31, 2021 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period March 15, 2021 to December 31, 2021 to provide reasonable assurance that Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls throughout the period March 15, 2021 to December 31, 2021.
- c. The controls stated in the description operated effectively throughout the period March 15, 2021 to December 31, 2021 to provide reasonable assurance that

Inspirit Group, LLC, dba STOPit Solutions's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Inspirit Group, LLC, dba STOPit Solutions's controls, operated effectively throughout the period March 15, 2021 to December 31, 2021.

Restricted use

This report, is intended solely for the information and use of Inspirit Group, LLC, dba STOPit Solutions; user entities of Inspirit Group, LLC, dba STOPit Solutions's Anonymous Reporting System throughout the period March 15, 2021 to December 31, 2021, business partners of Inspirit Group, LLC, dba STOPit Solutions subject to risks arising from interactions with the Anonymous Reporting System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

DocuSigned by:

MHM Professional Corporation

4F227774372B4BC...

Chartered Professional Accountant

Calgary, Alberta

January 24, 2022



Section III

Inspirit Group, LLC, dba STOPit Solutions's Description of its Anonymous Reporting System



Purpose and Scope of Report

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of Inspirit Group, LLC, dba STOPit Solutions's ("STOPit Solutions") controls that may be relevant to a user organization's internal control structure, based on the criteria to meet the security categories as set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). The purpose of this report is to provide information on the internal controls of STOPit Solutions as they relate to the STOPit Solutions Anonymous Reporting System. Specifically, this report pertains to the security controls regarding the STOPit Solutions Platform.

This report is intended to assist user entities in determining the adequacy of the internal controls that are outsourced to STOPit Solutions and are relevant to their internal control structures as it relates to security risks.

Company Overview

STOPit Solutions is a privately held technology company founded in 2014 and headquartered in Holmdel, NJ. The Anonymous Reporting System allows victims and bystanders who witness incidents of bullying, violence, and other issues to anonymously report to administrators in their organization, who can provide assistance and resolution through a mobile app available on mobile phones and computers in school and workplace settings.

Services Provided

STOPit Solutions ARS provides users within a client's community a platform to anonymously report their concerns via an app or web interface to those that may be able to help. During the incident submission process, users are able to submit media, photos, videos, or documents to aid in reporting their concern. STOPit Solutions allows client organizations the ability to administer incidents and communicate with their communities through various technologies like Messenger, a two way chat service. The STOPit Solutions ARS is a SaaS solution that includes a mobile phone (Android and iOS) app and web-based user interface for allowing client's user communities to download, enroll and submit incidents to the ARS platform. Client entities have the ability to utilize STOPit Solutions Incident Management Service (IMS) to intercept and manage time critical incidents in real-time and escalate severe events to the Client's



crisis or incident response teams for resolution. The platform serves to anonymize the connection of communications between App User and Administrator to allow for a free flow of information and communication between the parties. It also allows administrators of the service to manage, administer and escalate incidents as needed within their organization.

Principal Service Commitments and System Requirements

STOPit Solutions designs its processes and procedures related to its Anonymous Reporting System to meet its objectives. Those objectives are based on the service commitments that STOPit Solutions makes to user entities related to security, regulations that govern SaaS providers, and the financial, operational, and compliance requirements that STOPit Solutions has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Anonymous Reporting System that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.

STOPit Solutions establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in STOPit Solutions system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Anonymous Reporting System.

Components of the System Used to Provide the Services

Infrastructure



STOPit Solutions ARS is a SaaS-multi-tenant client-server application hosted in Amazon Web Services. All customers receive their own account within the STOPit Solutions ARS Platform, and their data is logically separated and not accessible to other tenants to prevent unauthorized access. Client data locations and data flows are outlined in the diagram below along with the security measures in place to protect this data.

The STOPit Solutions application runs within Amazon Web Services VPCs using the US East-1 region as the primary region, with US West-2 serving as the secondary region. The application runs on a combination of EC2 systems running Amazon Linux as the operating system. There are several layers of architecture of the application with the backend API written in Python/Django, a middle tier of application logic in Python, and the frontend written in Django, Foundation CSS Frameworks. Apache Web server is utilized as the web server with an Elastic Load Balancer with an autoscaling group to serve the HTTP/S requests.

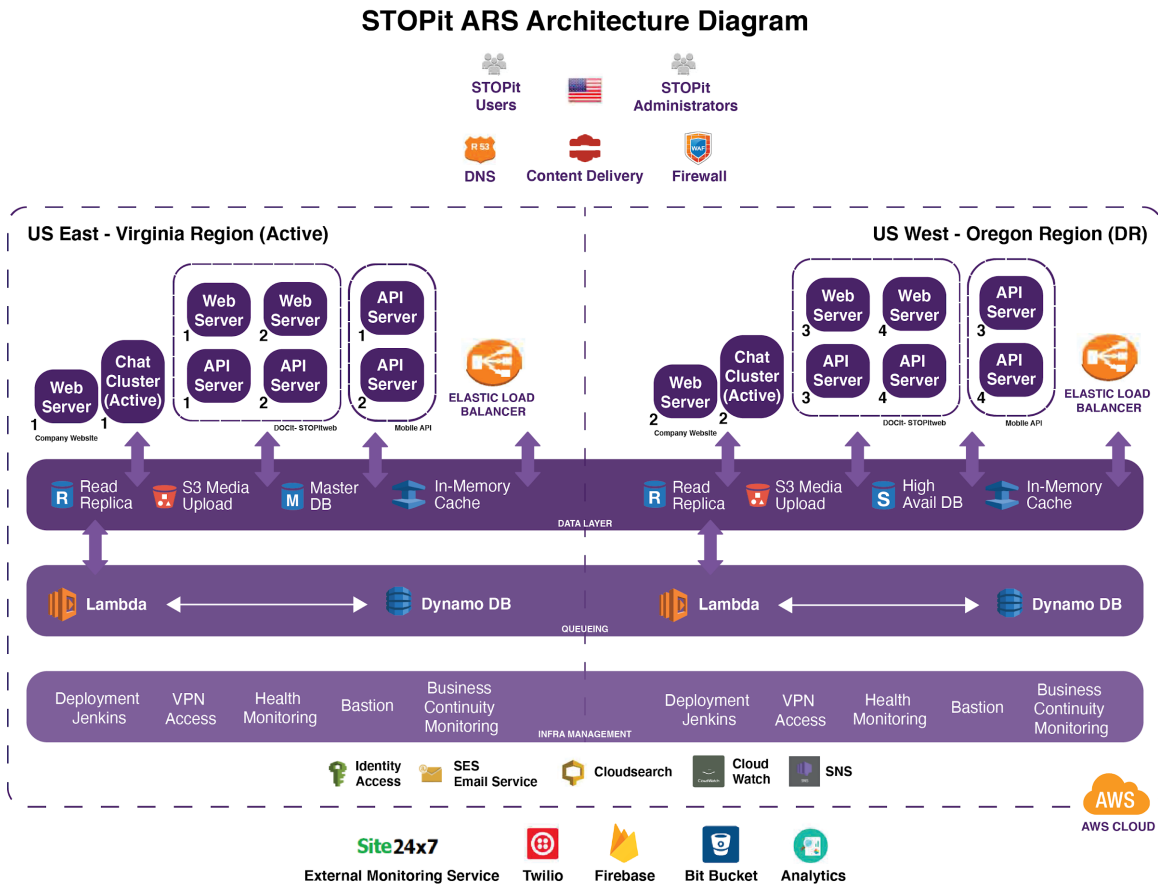
The database supporting the application utilizes Amazon Web Services' Aurora running MySQL. The primary database is replicated real-time into a secondary database in the US West-2 region for backup and redundancy purposes. Amazon Web Services S3 Buckets are used to store user uploaded files and are replicated real-time between the primary and secondary regions. Amazon Web Services REDIS is used for session management. Amazon Web Services Cloud Watch is used for log storage and AWS CloudWatch and Site247 are used for monitoring purposes.

The ARS platform allows for five types of access as follows:

- App Users (includes usage of appweb.stopitsolutions.com) for the submission of incidents to the platform into a client entity's account within STOPit Solutions ARS platform.
- Client Account Admin accounts, which there are levels of permissions available for user configuration, each allowing the client management team to manage incidents from their App Users
- IMC Agents, a STOPit Solutions user type that administers a 24/7/365 operations and incident management center to allow (if subscribed) any App Users incidents to be managed proactively as a supplemental administrator to an enrolled client account.
- STOPit Super Admin, held by internal STOPit Solutions team members for providing configuration, technical support and other functions to the STOPit Solutions ARS Platform
- Engineering Admin Accounts are provided solely to the Engineering team responsible for managing, maintaining and ensuring the ARS platform is

operational at all times. These accounts are tightly controlled by the CTO at STOPit Solutions.

The following diagram identifies the virtual design of the solution, including all places where customer data resides, all data flows and how it is secured by STOPit Solutions:



Software

The following provides a summary of software systems used to deliver STOPit Solutions ARS:

- AWS Cloud Watch – used for the monitoring of production systems and log storage.
- Amazon Web Services CloudWatch / Site24x7.com – used for enterprise monitoring of availability and capacity.

- Qualys – used for web application vulnerability scanning.
- Bitbucket – used for source code version control.
- Amazon Linux – operating systems to support operation of the system.
- Python/Django – programming language used to write the backend API of the web application.
- Android Development Environment Library - Java
- iOS xCode using Swift
- Amazon Web Services SES - used for sending application email
- Amazon Web Services Serverless framework to handle notifications

People

STOPit Solutions has a defined organizational structure with specific roles, responsibilities, and appropriate lines of reporting required to support the STOPit Solutions Platform. It is comprised of, and supported by, the following teams who are responsible for the delivery and management of the system:

- Executive Committee – responsible for providing the overall direction, strategic vision, and management of STOPit Solutions.
- Product Development Committee – Comprising Engineering leadership and company Executive Committee Members, this committee is responsible for guiding the overall direction of the product roadmap including usability, enhancements, and new features.
- Engineering – responsible for front and back-end development of the in-scope applications and services. Also, responsible for oversight of software and data engineering, IT Infrastructure, and all IT related activities.
- Operations – responsible for day-to-day operations such as document processing and office functions.
- Sales – responsible for development of new business related to the STOPit Solutions services.
- Customer Success - responsible for successful onboarding of customers on STOPit Solutions platform and act as advocates for the continued success of the platform. They are responsible for product support issues, customer engagement and growth.

The teams and associated initiatives, workstreams, and functions are led by the executive management leads.

Policies, Processes & Procedures

Management has developed and communicated to employees and contractors a set of policies, processes, and procedures in several operational areas which support the security objectives of the ARS. As part of the wider Information Security Management Program, STOPit Solutions has developed and organized the following policies and procedure documents that are used to support the ARS Platform.

The following policies and procedures are available to employees and contractors:

- Access Control
- Remote Access
- Key Management and Cryptography
- Server Security
- Technology Equipment Handling and Disposal
- IT Asset Management
- Internal Audit
- Customer Support and SLA
- Business Continuity and Disaster Recovery
- Information Classification
- Workstation Security
- Network Security
- Information Security
- Personnel Security
- Acceptable Use
- Corporate Ethics
- Risk Assessments
- Vendor Management
- Software Development
- Incident Management
- Vulnerability Management
- Change Management
- Diversity and Inclusion

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. STOPit Solutions has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved



when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

Data is securely submitted through the client web application and sent to the application servers via REST calls to the API over HTTPS. The data is processed and written to the RDS instance. Data transmission is secured using TLS 1.2 , PBKDF 2, SHA-256 with RSA Encryption, and does not leave the VPC. Data replication channels are also encrypted and transmitted via the private Amazon Web Services connection. All data access requests require an ACL context which contains both the authenticated user and the organization that is requesting the data. These requests are validated via the STOPit Solutions permissions system to exclude the possibility of cross-client data leakage. All data at rest is encrypted using AES-256 encryption.

Significant Changes to the System Throughout the Examination Period

During the examination period, STOPit Solutions has incorporated a full scale LMS into it's client onboarding process and has enabled all new users of the platform to be fully trained and skill tested before launching the STOPit ARS platform. The new LMS includes training videos, settings and configuration training and facilitated setup as well as skills based testing to ensure client administrators are fully trained and have setup the system for their needs.

Control Environment

The control environment is determined by the control consciousness of an organization, which sets the tone of an organization and the way personnel conduct their activities, influencing how they carry out their control functions. This is the foundation for all other components of internal control providing discipline and structure for the business operations.

STOPit Solutions control environment establishes the basis for organizational processes, and influences control procedures and discipline of employees. Controls are designed to meet relevant trust criteria. The control environment at STOPit Solutions begins with management's philosophy and operating style as well as the priorities and direction provided by the Executive Management team. STOPit Solutions' entire organization is dedicated to delivering the highest level of customer service. The company has created a corporate culture that supports this mission.



Commitment to Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people, who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership's example.

STOPit Solutions understands the importance of integrity and ethical values and implements, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior to all employees and contractors. STOPit Solutions has formalized an equality and diversity policy that is available and acknowledged by all the employees.

In addition, STOPit Solutions has established an employee handbook outlining requirements on the code of conduct, acceptable usage and confidentiality commitments which are reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions. Third-party contractors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

STOPit Solutions assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job and has a process in place to evaluate the competency of employees on an annual basis. STOPit Solutions reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Management's Philosophy and Operating Style



Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions for the security and confidentiality of information. STOPit Solutions management takes a relatively conservative approach to information processing and risk associated with new business ventures.

STOPit Solutions management team is customer-driven and tightly focused on providing value to customers. Security is recognized as a key component of the value proposition of the ARS service offering. Controls over security are recognized as key enablers for delivery of value to the customer.

Oversight responsibility of the board of directors

STOPit Solutions Board of Directors is ultimately accountable for oversight of STOPit Solutions operations and their responsibilities are defined and documented and acknowledged by the Board on an annual basis. The Board of Directors comprises non-executive directors independent from management with expertise relevant to security aspects. The Board meets on a quarterly basis to provide oversight on internal controls, operations and business objectives supporting the ARS.

The responsibilities of key positions within STOPit Solutions are clearly defined and communicated to personnel. Individuals that hold key positions are knowledgeable and experienced within the industry. STOPit Solutions organizational structure supports communication of information both up to leadership as well as down to support staff. STOPit Solutions organizational structure consists of seven primary business units that work together to deliver STOPit Solutions services and applications. The business units supporting the ARS consist of the following departments also described in the People section above: Management, Product, Engineering, Operations, Sales, Customer Success, and Labs.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes. To support this, management has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and operations of its services. The organization structure is reviewed and updated in case of significant changes. In addition, Job descriptions that document the objectives of the role, responsibilities, reporting lines,



employee qualifications and other requirements are made available to the employees and are reviewed and updated annually or in case of significant changes.

Management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. In addition, the executive team meets on a weekly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.

As mentioned above, STOPit Solutions has defined job responsibilities and clear communication channels to disseminate information within the organization enabling STOPit Solutions to react to market and regulatory changes and to meet its goals and objectives. STOPit Solutions is appropriately staffed to support its operations, particularly with respect to critical areas such as software development, implementation, customer support, and information technology system support

Human Resource Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counselling, and remedial action. Standards for hiring qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior demonstrate. All new employees and contractors are subjected to reference checks prior to joining the organization.

STOPit Solutions commitment to hiring and retaining only highly competent and trustworthy people. Personnel career growth and reward of meeting expectations are driven by periodic performance feedback and demonstrate STOPit Solutions commitment to advance qualified personnel to higher levels of responsibility. Personnel who work for STOPit Solutions are required to read and acknowledge the company's internal policies and confidentiality requirements as well as the confidentiality of customer managed information.

Risk Assessment

STOPit Solutions Executive Management performs annual risk assessments, which requires STOPit Solutions to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. STOPit Solutions management reevaluates the risk assessment at least annually to both update the previous results and to identify any new potential areas of concern. The risk assessment process assesses risks related to security, fraud, regulatory and

technology changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.

The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
- Monitoring – The monitoring phase includes the performance of monitoring activities by STOPit Solutions management team to evaluate whether the processes, initiatives, functions, and/or activities are mitigating the risk as designed.

Prior to engaging with new vendors and on an annual basis, management assesses the risk (and ongoing performance) of working with that vendor taking into account considerations such as the role of the vendor and their access to in-scope systems and data. A process is in place to remove access to systems and data when the vendor relationship has been terminated.

In-Scope Trust Service Categories

The table below provides the Trust Service Categories within the scope of this report. The controls designed and implemented to meet the applicable trust service criteria have been included in Section IV.

Trust Service Categories	Definition
--------------------------	------------

Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect STOPit Solutions’s ability to achieve its service commitments and system requirements.
----------	--

Security

Security refers to the protection of:

- i. Information during its collection or creation, use, processing, transmission, and storage and;
- ii. Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust Service Criteria and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, STOPit Solutions management has identified and put into effect the necessary actions to address those risks. To address these risks, control activities have been placed into operation to help ensure that the actions are carried out in a competent and efficient manner. Control activities serve as mechanisms for managing the achievement of the security categories and applicable criteria.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in Section IV of this report, to eliminate the redundancy that would result from listing the items in this section as well. Although the control activities are included in Section IV, they are, nevertheless, an integral part of STOPit Solutions description of its Anonymous Reporting System. Any applicable TSC that are not addressed by control activities at STOPit Solutions are also described within Section IV.



The description of the service auditors' tests of operating effectiveness and the corresponding results are also presented in the testing matrices, adjacent to the service organization's control procedures. The description and results of such tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Information and Communication

Information Systems

STOPit Solutions ARS is maintained in a virtualized environment on the Amazon Web Services Cloud platform. STOPit Solutions relies on the applicable physical and logical security controls in place at the corresponding Amazon Web Services facility to ensure equipment and information is protected from unauthorized access.

Confidential data transmitted through the ARS is secured and protected using various access control and encryption technologies. Other information systems are used internally by STOPit Solutions to communicate information throughout the organization, such as secure/encrypted email and manual or automated processes for recording and reporting internal decision support information.

Internal communication of information that supports internal controls

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. STOPit Solutions management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and, appropriately addressed.

Internal policies and procedure documents relating to security are maintained and made available to employees through Tugboat Logic platform.

External communication regarding internal controls

During the onboarding process, designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities. STOPit Solutions has developed system documents and user guides that describe relevant system components as well as the



purpose and design of the system. These documents are made available to internal and external users and updated on an as needed basis.

Customers are communicated with on the security commitments as part of terms of service which is required to be accepted by customers during initial access to the ARS. Any changes or Incidents that may affect the security of the ARS are communicated to internal and external users, through system notifications that are advertised to platform users in advance of the planned changes.

Monitoring

The ongoing monitoring of the control environment is achieved through active, hands-on management, including regularly scheduled meetings to discuss business and operational issues. STOPit Solutions utilizes a risk-based approach to monitor business units and other entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed on a priority basis. Results from the risk assessment are documented in formal communications to Executive Management and other relevant parties as appropriate. Internal controls are periodically assessed during the year in addition to:

- Vulnerability scans are performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.
- An external penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.

Controls that STOPit Solutions assumes will be implemented by applicable subservice organizations are evaluated through an assessment of the subservice organization's SOC2 or other relevant compliance report. These evaluations consider the appropriateness of scope, impact of identified exceptions and the implementation of applicable complementary user entity controls.

Controls that STOPit Solutions assumes will be implemented by applicable subservice organizations are evaluated through an assessment of the subservice organization's SOC2 or other relevant compliance report. These evaluations consider the appropriateness of scope, impact of identified exceptions and the implementation of applicable complementary user entity controls.

Control Activities

Identity and Access Management

Information system accounts (commonly referred to as admin accounts) are required to access the ARS and supporting infrastructure. These consist of all necessary account types that allow users to perform their essential roles and responsibilities. Each user account and associated username is unique and is identifiable to an individual user. IT Operations team accounts i.e. the accounts that are required to access the Amazon Web Services production and non-production environments, system administrator accounts and the accounts required to manage the Platform, are only granted to internal users after authorization from management. Also, access to generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on job responsibilities.

For internal users that are required to access the Platform or supporting infrastructure, access rights to perform certain operations are assigned based on business need. In addition, management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review and/or anytime a user's role changes. For instance, terminated internal users with access to ARS and supporting infrastructures are disabled or removed in a timely manner.

Authentication Management

STOPit Solutions enforces access to the ARS Incident Management Platform and its supporting infrastructure through a combination of password and multi-factor authentication mechanisms to production environments. In order to minimize the risk of unauthorized access, unique ID and password are required in order to gain access to the ARS and Amazon Web Services portal. Password standards have been established that define the appropriate password length, complexity and lockout threshold (as appropriate). These are enforced globally for all internal users and external users.

Incident reporting access - through the STOPit Solutions iOS and Android apps - called "STOPit" are accessed through an access code or, in some cases, directory lookup, depending on client agreement and their connections are secured through an Intellicode generated by the ARS and assigned to the device app installation for purposes of maintaining an anonymous connection to the device being used. App Users that use the app in this way allows, for example, a student in a client school



district, to use the STOPit App to report an incident to their school administrators anonymously, without revealing their identity.

Platform Access

The STOPit Solutions Platform is accessible to all approved user organizations and internal users and to meet the security commitments, all client sessions to the ARS are encrypted through TLS/HTTPS. All sessions are logged and monitored, and the Firewall rules are reviewed on an annual basis.

STOPit Solutions has implemented strong encryption technologies to protect communications and transmission of data. Confidential data transmitted through the ARS is secured and protected using various access control and encryption technologies.

Client Data Segregation

To ensure confidentiality of data within the ARS, customers are prevented from accessing other customers' data through appropriate segmentation controls. All customers receive their own tenant of the STOPit Solutions ARS and their data is logically separated and not accessible to other tenants to prevent unauthorized access. Data hosted and stored in the Platform databases are encrypted through the use of the Amazon Web Services provided and managed encryption keys to encrypt data at rest.

Secure Data Disposal

STOPit Solutions has defined policies that specify the data back-up and retention period, and process to follow for the secure disposal of confidential or sensitive information stored within the ARS. As part of terms of service which is required to be accepted by customers during initial access to the ARS and includes requirement on disposal and return of confidential information on termination or expiration of contract.

Anti-Virus and Malware Protection

STOPit Solutions has anti-virus software installed on all corporate laptops and workstations and is configured to force updates to definitions on a minimum of a daily basis and to perform file-level scans during any read/write operations to prevent or detect and act upon the introduction of unauthorized or malicious software.

Change Management



STOPit Solutions has developed a formal SDLC methodology that governs the development, acquisition, implementation, and maintenance of application development. For the ARS, there are separate logical environments that are used to segregate access and between Development, Testing and Production instances. These environments are used to support a consistent code release and change management workflow in order to ensure product enhancements and bug fixes are efficiently and accurately reviewed, prioritized, scheduled, tested, signed-off and approved by senior management before being released into the production environment.

STOPit Solutions has established a formal change management process that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed. In accordance to this process, changes to the application(s) and supporting infrastructure are documented, tested and approved by authorized personnel prior to implementation into the production environment and Access to promote changes to production is restricted to authorized personnel based on job responsibilities.

STOPit Solutions change management process also covers emergency changes. Such changes intended to repair, resolve or prevent a live operational issue that is impacting (or is about to impact) the business to a high degree and/or is to protect the organization from a threat and must be introduced as soon as possible. Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.

Data Backup and Recovery

Customer data and user activity are recorded within the ARS via Amazon Web Services Amazon Web Services Aurora snapshots and also replicated to an additional Amazon Web Services regions for redundancy. Backup procedures are in place to help ensure that backup media is secure, available, and verified for the integrity of data to help ensure recovery in the event of a primary production system failure.

Backups are taken in the form of global replication to S3 buckets in the global repositories and made available to all AWS regions used by STOPit Solutions. Additionally we synchronize replicas of all DynamoDB and MySQL Aurora instances to multiple regions for availability in our disaster recovery solution and business continuity solution. In addition, STOPit Solutions performs failover and DR testing for purposes of restoration testing on a quarterly basis to test the integrity and



completeness of back-up information. The incident management process is invoked for anomalies.

Disaster recovery plans have been developed and are tested annually. Test results are reviewed, and contingency plans are updated.

System Monitoring

STOPit Solutions employs a variety of tools to monitor the performance and security of the Anonymous Reporting System and associated production infrastructure.

- STOPit Solutions employs various tools to monitor and manage its ARS. The tools are used in combination to monitor the overall health of all resources configured within the Production and non-production Amazon Web Services environments.
- Logging is enabled to monitor the following events at the IT infrastructure level:
 - Administrator activities
 - System errors
 - Data deletions

These tools automatically generate alerts for key activities that may require attention. Support teams are immediately notified of these alerts and they are actioned in a timely manner. System logs are retained for forensic purposes and interrogated as needed.

Complementary Subservice Organization Controls

STOPit Solutions’s controls related to the Anonymous Reporting System cover only a portion of the overall internal control structure for each user entity of STOPit Solutions’s services. It is not feasible for the control objectives related to the Anonymous Reporting System to be achieved solely by STOPit Solutions. Therefore, each user entity's internal controls must be evaluated in conjunction with STOPit Solutions's controls described in Section IV of this report, taking into account the related complementary subservice organization controls (CSOCs) expected to be implemented at the subservice organization as described below.

Control Activities Expected to be Implemented by AWS	Applicable Trust Criteria
---	----------------------------------

AWS is responsible for restricting logical and physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC9.2
AWS is responsible for identifying changes that could significantly impact the system of security controls, including the effects, both positive and negative, on its clients.	CC3.4, CC8.1
AWS is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC6.8, CC7.5, CC9.2
AWS is responsible for maintaining segregation of client's environment(s) from other AWS clients.	CC6.1, CC6.6
AWS is responsible for maintaining the integrity of system logs and their associated configurations.	CC5.3, CC7.1, CC7.2
AWS is responsible for evaluating the impact of a security incident, communicating the incident to impacted clients, remediating against incidents, and working towards prevention of future incidents.	CC7.2, CC7.3, CC7.4, CC7.5, CC9.1
AWS is responsible for the management of any third-party vendors with access to customer environments.	CC9.1, CC9.2

Complementary User Entity Controls

The control activities performed by STOPit Solutions cover only a portion of the overall internal control structure of Anonymous Reporting System. Therefore, each user entity's internal control structure must be evaluated in conjunction with STOPit Solutions's control policies and procedures described in this report and certain of the following controls at the user entity assumed to be in place and operating effectively.

- Clients are responsible for verifying the completeness and accuracy of policy configuration and customer data entered into the Suite.
- Clients are responsible for notifying STOPit Solutions of actual or suspicious events or breaches of the ARS and providing assistance as necessary, to permit problem resolution.

- Clients are responsible for reviewing and taking action upon notification of STOPit Solutions communication in regards to system changes, maintenance windows or other matters impacting the availability of the system
- Clients are responsible for monitoring the use of the STOPit Solutions ARS Platform and the information contained therein to confirm that users are using the system and information for the right purpose.
- Clients are responsible for confirming that end users are managing information from ARS in accordance with their information security and other internal policies.
- Client administrators are responsible for confirming that end users' access to ARS is authorized, set up appropriately (ie username and password), revoked within a timely manner upon users leaving the client organization and maintaining the confidentiality of login credentials.
- Client administrators are responsible for periodically reviewing end users' access to ARS for validity and appropriateness and making corrective changes within a timely manner.
- User entities are responsible for demonstrating a commitment to integrity, ethical values and action, and confidentiality. User entities hold individuals at all levels within their organization accountable for control responsibilities in pursuit to business objectives and security.
- User entities are responsible for deploying security controls related to their operation to both protect against and detect security incidents, in addition to acting upon security incidents be it suspected or actual.

Section IV

Trust Service Criteria, Related Controls and Tests of Controls

Trust Service Criteria, Related Controls and Tests of Controls

Testing Approach

The objective of the auditor’s controls testing is to determine the operating effectiveness of the controls specified by STOPit Solutions’s management throughout the examination period of March 15, 2021 to December 31, 2021. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved throughout the examination period. The nature of the tests conducted took into consideration the type of testing and the evidential matter that is available to perform a test to determine the operating effectiveness.

Types of Tests Performed

1. Inquiry: tests include the corroboration of relevant personnel to verify the knowledge and understanding of the described control activity.
2. Observation: tests include the physical observation of the implementation, application of, or, existence of specific controls.
3. Inspection: tests include the physical validation of documents, records, configuration, or settings.
4. Re-performance: includes reprocessing transactions, procedures, & calculations to ensure the accuracy and completeness of the description.

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by STOPit Solutions:

Control Type & Frequency	Minimum Number of Items to Test
Transaction / Occurrence based	10% up to 25
Manual control performed monthly	1-2
Manual control performed quarterly	1-2
Manual control performed annually	1
Application / Programmed control	1 application of each programmed control



Control Number	Description of STOPit Solutions Controls	Service Auditor Test	Test Results
Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
OM4	The organization has defined a Code of Conduct and Ethics and reviews them annually.	1. Inspect that the code of conduct has been reviewed within the past year.	No exceptions noted
OM5	The organization has established an employee Handbook outlining requirements on the Code of Conduct, acceptable usage and confidentiality commitments which is reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions.	1. Inspect that the employee handbook includes components of code of conduct, acceptable use and confidentiality responsibilities and has been reviewed by management within the past year. 2. For a sample of employees hired during the period, inspect that they have signed-off on the handbook. 3. For a sample of existing employees inspect that they have signed off on the handbook where significant revisions were made to the handbook during the period.	No exceptions noted
OM9	The organization has established communication channels that allow employees to confidentially report issues related to fraud, harassment and other issues	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted

	impacting the organization's ethical and integrity requirements.		
VM1	Third-party contractors/vendors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.	1. For a sample of 3rd party vendors/contractors, inspect that they have signed their agreement to company's code of conduct, security and confidentiality requirements.	No exceptions noted
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
OM2	The Board of Directors comprises of non-executive directors independent from management and meets on a quarterly basis for oversight on internal controls, operations and business objectives.	1. Inspect that the Board of Directors membership includes non-executive directors and that it meets on a quarterly basis. 2. Inspect that a sample of board meeting minutes includes oversight of security/compliance.	No exceptions noted
OM3	The oversight responsibilities of the Data Compliance Committee are defined, documented and acknowledged by its members on an annual basis.	1. Inspect that the Data Compliance Committee contains details of each member's oversight responsibilities and that each member has reviewed and signed-off within the past year.	No exceptions noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			

HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	<p>1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities.</p> <p>2. For a sample of new contractors, inspect that their employment agreement is signed and contains details of security responsibilities.</p>	No exceptions noted
HR2	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.	<p>1. Inspect a sample of job descriptions for review in the past year and that it is stored in a location accessible to employees.</p> <p>2. Inspect a sample of job descriptions and validate that it includes the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements.</p>	No exceptions noted
HR3	Organization has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services. The organization structure is reviewed and updated in case of significant changes.	1. Inspect that the current organization chart includes roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services and has been reviewed if any significant organization changes occurred during the audit period.	No exceptions noted
OM6	The organization's executive team meets on a monthly to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted

CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policy and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	<ol style="list-style-type: none"> 1. Inspect information security policies for review by management within the past year. 2. Inspect that information security policies are posted on a platform that is accessible by employees 	No exceptions noted
AT2	Employees are required to complete an information security and awareness training annually.	<ol style="list-style-type: none"> 1. Inquire of management as to how security awareness training is conducted and attested to by employees. 2. For a sample of employees, inspect that they have completed training. 	No exceptions noted
HR2	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.	<ol style="list-style-type: none"> 1. Inspect a sample of job descriptions for review in the past year and that it is stored in a location accessible to employees. 2. Inspect a sample of job descriptions and validate that it includes the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements. 	No exceptions noted
HR4	The organization has a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	<ol style="list-style-type: none"> 1. Inspect that a performance evaluation was performed in accordance with process for a sample of employees. 	No exceptions noted

HR5	The organization has a formal training plan in place for the employees and meets annually to identify relevant training needs to support in scope-systems.	1. Inspect the annual training plan has been communicated to employees and reviewed within the past year	No exceptions noted
HR6	New employees are subjected to a background and reference checks prior to joining the organization.	1. Inspect that the employment hiring policy requires background/reference checks prior to new employees being hired. 2. For a sample of new employees, inspect evidence that background/reference check was performed.	No exceptions noted
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis. 2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.	No exceptions noted
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			

HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	<p>1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities.</p> <p>2. For a sample of new contractors, inspect that their employment agreement is signed and contains details of security responsibilities.</p>	No exceptions noted
HR4	The organization has a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	1. Inspect that a performance evaluation was performed in accordance with process for a sample of employees.	No exceptions noted
OM5	The organization has established an employee Handbook outlining requirements on the Code of Conduct, acceptable usage and confidentiality commitments which is reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions.	<p>1. Inspect that the employee handbook includes components of code of conduct, acceptable use and confidentiality responsibilities and has been reviewed by management within the past year.</p> <p>2. For a sample of employees hired during the period, inspect that they have signed-off on the handbook.</p> <p>3. For a sample of existing employees inspect that they have signed off on the handbook where significant revisions were made to the handbook during the period.</p>	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an	<p>1. Inquire of management as to how internal controls are periodically assessed.</p> <p>2. Inspect the internal controls assessment document for performance/sign-off within the</p>	No exceptions noted

	annual basis and identified deficiencies are remediated in a timely manner.	last 12 months, identification of exceptions, and evidence of remediation.	
OM9	The organization has established communication channels that allow employees to confidentially report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted
Information and Communication			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
AT3	Designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.	1. Inspect that the onboarding process includes functional training for customer focused employees. 2. Inspect that new employees are trained on the relevant applications.	No exceptions noted
AT4	The organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to internal and external users and updated on an as needed basis.	1. Inspect that documentation and user guides exist that describe relevant system components as well as the purpose and design of the system. 2. Inspect evidence to determine that the documents and user guides are made available to internal and external users.	No exceptions noted

		3. Inspect evidence to determine that the documentation and user guide have been reviewed and updated as required.	
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	<p>1. Inquire of management as to how internal controls are periodically assessed.</p> <p>2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.</p>	No exceptions noted
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policy and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	<p>1. Inspect information security policies for review by management within the past year.</p> <p>2. Inspect that information security policies are posted on a platform that is accessible by employees</p>	No exceptions noted
AT2	Employees are required to complete an information security and awareness training annually.	<p>1. Inquire of management as to how security awareness training is conducted and attested to by employees.</p> <p>2. For a sample of employees, inspect that they have completed training.</p>	No exceptions noted

AT4	The organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to internal and external users and updated on an as needed basis.	<p>1. Inspect that documentation and user guides exist that describe relevant system components as well as the purpose and design of the system.</p> <p>2. Inspect evidence to determine that the documents and user guides are made available to internal and external users.</p> <p>3. Inspect evidence to determine that the documentation and user guide have been reviewed and updated as required.</p>	No exceptions noted
CM4	Changes that affect the functionality and security of the system components are communicated to internal and external users.	1. For a sample of system changes, inspect that the functionality and/or security changes were communicated (e.g. release notes) to affected parties in accordance with the change management process.	No exceptions noted
HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	<p>1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities.</p> <p>2. For a sample of new contractors, inspect that their employment agreement is signed and contains details of security responsibilities.</p>	No exceptions noted
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted

	reviewed by management on an annual basis and updated as required.		
OM2	The Board of Directors comprises of non-executive directors independent from management and meets on a quarterly basis for oversight on internal controls, operations and business objectives.	<ol style="list-style-type: none"> 1. Inspect that the Board of Directors membership includes non-executive directors and that it meets on a quarterly basis. 2. Inspect that a sample of board meeting minutes includes oversight of security/compliance. 	No exceptions noted
OM5	The organization has established an employee Handbook outlining requirements on the Code of Conduct, acceptable usage and confidentiality commitments which is reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions.	<ol style="list-style-type: none"> 1. Inspect that the employee handbook includes components of code of conduct, acceptable use and confidentiality responsibilities and has been reviewed by management within the past year. 2. For a sample of employees hired during the period, inspect that they have signed-off on the handbook. 3. For a sample of existing employees inspect that they have signed off on the handbook where significant revisions were made to the handbook during the period. 	No exceptions noted
OM6	The organization's executive team meets on a monthly to discuss operations, issues relating to internal controls and delivery on key performance metrics.	<ol style="list-style-type: none"> 1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery 	No exceptions noted

		on key performance metrics and actions agreed to by the executives were discussed.	
OM9	The organization has established communication channels that allow employees to confidentially report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted
VM1	Third-party contractors/vendors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.	1. For a sample of 3rd party vendors/contractors, inspect that they have signed their agreement to company's code of conduct, security and confidentiality requirements.	No exceptions noted
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
AT3	Designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.	1. Inspect that the onboarding process includes functional training for customer focused employees. 2. Inspect that new employees are trained on the relevant applications.	No exceptions noted
HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities.	No exceptions noted

		2. For a sample of new contractors, inspect that their employment agreement is signed and contains details of security responsibilities.	
IM1	<p>The organization provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenge through an appropriate channel.</p> <p>Reported incidents are addressed by the organization's support staff in a timely manner.</p>	<p>1. Inquire of management as to how customer issues are recorded and actioned.</p> <p>2. For a sample of customer issues, inspect that the issue was assigned and resolved (if applicable) in a timely manner.</p>	No exceptions noted
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
OM2	The Board of Directors comprises of non-executive directors independent from management and meets on a quarterly basis for oversight on internal controls, operations and business objectives.	<p>1. Inspect that the Board of Directors membership includes non-executive directors and that it meets on a quarterly basis.</p> <p>2. Inspect that a sample of board meeting minutes includes oversight of security/compliance.</p>	No exceptions noted
OM7	The organization has formal agreements in place with customers which acknowledges their compliance on security, confidentiality and privacy commitments.	1. For a sample of customers, inspect that the customer has signed their agreement to the company's security, confidentiality and privacy commitments.	No exceptions noted

OM9	The organization has established communication channels that allow employees to confidentially report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted
OM10	New customer contracts or modifications to existing customer contracts and end-user license agreements (EULA) are reviewed annually by Management to ensure security and confidentiality commitments are met.	1. Inspect that the templates (specifically the security and/or confidentiality clauses) used for customer agreements have been reviewed by management within the past 12 months.	No exceptions noted
Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year. 2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	No exceptions noted
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			

RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	<p>1. Inspect that a risk assessment exists and has been updated and reviewed within the past year.</p> <p>2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.</p>	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	<p>1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis.</p> <p>2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.</p>	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	<p>1. Inspect that a risk assessment exists and has been updated and reviewed within the past year.</p> <p>2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.</p>	No exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			

RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	<p>1. Inspect that a risk assessment exists and has been updated and reviewed within the past year.</p> <p>2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.</p>	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	<p>1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis.</p> <p>2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.</p>	No exceptions noted
Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
OM6	The organization's executive team meets on a monthly to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted

OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	<ol style="list-style-type: none"> 1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation. 	No exceptions noted
SO13	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	<ol style="list-style-type: none"> 1. Inspect the penetration test report for documentation of scope, issues analysis and remediation. Issues left unremediated should be transferred onto the risk register. 	No exceptions noted
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	<ol style="list-style-type: none"> 1. For a sample of vulnerability scans, inspect that scope of the scan was documented and that issues are analyzed and remediated in a timely manner. 	No exceptions noted
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	<ol style="list-style-type: none"> 1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable. 	No exceptions noted

CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	<p>1. Inquire of management as to how internal controls are periodically assessed.</p> <p>2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.</p>	No exceptions noted
Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
OM6	The organization's executive team meets on a monthly to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	<p>1. Inquire of management as to how internal controls are periodically assessed.</p> <p>2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.</p>	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			

OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	<ol style="list-style-type: none"> 1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation. 	No exceptions noted
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policy and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	<ol style="list-style-type: none"> 1. Inspect information security policies for review by management within the past year. 2. Inspect that information security policies are posted on a platform that is accessible by employees 	No exceptions noted
OM6	The organization's executive team meets on a monthly to discuss operations, issues relating to internal controls and delivery on key performance metrics.	<ol style="list-style-type: none"> 1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed. 	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an	<ol style="list-style-type: none"> 1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the 	No exceptions noted

	annual basis and identified deficiencies are remediated in a timely manner.	last 12 months, identification of exceptions, and evidence of remediation.	
Logical and Physical Access			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
AA1	<p>Unique user IDs and passwords are required in order to gain access to the infrastructure supporting the application (i.e. Active Directory, server and database accounts). The following password policies are enforced for user accounts:</p> <ul style="list-style-type: none"> - Minimum password length: 10 characters - Password complexity: Enabled - Password History - 5 Passwords - Maximum Password Age - 90 days - MFA 	1. Inspect the password parameters for each in scope infrastructure element and validate they align to the control description.	No exceptions noted
AA2	<p>Unique user IDs and passwords are required in order to gain access to the application production environment. The following password policies are enforced globally for user accounts:</p> <ul style="list-style-type: none"> - Minimum password length: 8-15 characters - Password complexity: Enabled 	1. Inspect the password parameters for each in scope application and validate they align to the control description.	No exceptions noted

	- Lockout attempts: 5 attempts		
AA3	Multi-factor authentication (MFA) is enforced for user accounts with administrative access to the organization's production platform.	1. Inspect authentication parameters and validate that Multi Factor Authentication is required for admin/generic access to production.	No exceptions noted
AC1	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	1. Inquire of management as to the access management policy, procedures performed and individuals authorized to grant access to systems. 2. For a sample of new users, inspect the access request document and validate that approval was obtained from an authorized individual prior to access being provisioned on the system.	No exceptions noted
AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed and access is revoked for terminated employees in a timely manner.	1. Inquire of management as to the access management procedures performed to remove access for terminated individuals. 2. For a sample of terminated employees, inspect that a termination checklist documenting all logical access removed was completed and approved by management and that logical access was removed from the systems in a timely manner.	No exceptions noted

AC5	System components are configured such that the organization and its customers' access is appropriately segmented from other tenant users.	<p>1. Inquire of management as to how customer data is segmented within the applications and databases.</p> <p>2. Inspect system configuration settings and validate that they restrict access to customer data.</p>	No exceptions noted
OM1	The organization maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.	1. Inspect the IT asset inventory document includes details on asset ownership, data classification and location; and that it has been reviewed and approved within the last 12 months.	No exceptions noted
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	<p>1. Inspect the encryption and key management policy and validate that key management system is used in accordance with policy.</p> <p>2. Inspect that the individuals with access to encryption keys are authorized.</p>	No exceptions noted
SO5	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.	<p>1. Inquire of management as to what tools are used to ensure data in databases is encrypted.</p> <p>2. Inspect system configurations for evidence that data at rest is encrypted .</p>	No exceptions noted
SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	1. Inquire of management as to what tools are used to ensure data in transit is encrypted.	No exceptions noted

		2. Inspect system configurations for evidence that data in transit is encrypted .	
SO11	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	1. Inspect the network diagram for description of protection mechanisms in place. 2. Inspect the network diagram for review within the past year.	No exceptions noted
WS2	Disk encryption and system passwords are enabled across all organization workstations.	1. Inspect that system password parameters and disk encryption are enabled for a sample of workstations.	No exceptions noted
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
AC1	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	1. Inquire of management as to the access management policy, procedures performed and individuals authorized to grant access to systems. 2. For a sample of new users, inspect the access request document and validate that approval was obtained from an authorized individual prior to access being provisioned on the system.	No exceptions noted

AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed and access is revoked for terminated employees in a timely manner.	<p>1. Inquire of management as to the access management procedures performed to remove access for terminated individuals.</p> <p>2. For a sample of terminated employees, inspect that a termination checklist documenting all logical access removed was completed and approved by management and that logical access was removed from the systems in a timely manner.</p>	No exceptions noted
AC4	Management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.	1. Select a sample of user reviews and inspect for evidence of review, sign-off and remediation.	<p>Exception noted</p> <p>While management provided details of the user review activities performed, their documentation doesn't fully describe the reviews performed or the remedial actions taken.</p> <p>Management Response: The documentation of account reviews has been upgraded to fully describe the review, parameters and process.</p>

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

AC1	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	<p>1. Inquire of management as to the access management policy, procedures performed and individuals authorized to grant access to systems.</p> <p>2. For a sample of new users, inspect the access request document and validate that approval was obtained from an authorized individual prior to access being provisioned on the system.</p>	No exceptions noted
AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed and access is revoked for terminated employees in a timely manner.	<p>1. Inquire of management as to the access management procedures performed to remove access for terminated individuals.</p> <p>2. For a sample of terminated employees, inspect that a termination checklist documenting all logical access removed was completed and approved by management and that logical access was removed from the systems in a timely manner.</p>	No exceptions noted
AC3	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.	1. Inquire of management as to the process for managing access privilege/administrative accounts (end user, generic and system/service) accounts on the in-scope servers and databases.	No exceptions noted

		2. Inspect list of all administrative/privilege accounts on the in- scope systems to determine that access to these accounts are restricted to authorized and appropriate personnel.	
AC4	Management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.	1. Select a sample of user reviews and inspect for evidence of review, sign-off and remediation.	Exception noted While management provided details of the user review activities performed, their documentation doesn't fully describe the reviews performed or the remedial actions taken. Management Response: The documentation of account reviews has been upgraded to fully describe the review, parameters and process.
AC6	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	1. Inspect system list of all users with access to deploy changes to production and confirm that users with access do not have development responsibilities. 2. For a sample of changes made to production, confirm that the individual who promoted the change into the production	No exceptions noted

		environment is different from the user who developed the change.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
DS4	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of information.	1. Inspect that data retention & disposal policies and procedures are in place and approved by management.	No exceptions noted
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	1. Inspect the encryption and key management policy and validate that key management system is used in accordance with policy. 2. Inspect that the individuals with access to encryption keys are authorized.	No exceptions noted

SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	<ol style="list-style-type: none"> 1. Inquire of management as to what tools are used to ensure data in transit is encrypted. 2. Inspect system configurations for evidence that data in transit is encrypted . 	No exceptions noted
SO11	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	<ol style="list-style-type: none"> 1. Inspect the network diagram for description of protection mechanisms in place. 2. Inspect the network diagram for review within the past year. 	No exceptions noted
SO15	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.	<ol style="list-style-type: none"> 1. Inspect that firewall rules are configured on the application gateway and production network and have been reviewed within the past year. 	No exceptions noted
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
DS3	Production data is not used in testing or development environments.	<ol style="list-style-type: none"> 1. Inquire with IT management on how production data is not be copied into or used in testing or development environments. 	No exceptions noted
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	<ol style="list-style-type: none"> 1. Inspect the encryption and key management policy and validate that key management system is used in accordance with policy. 2. Inspect that the individuals with access to encryption keys are authorized. 	No exceptions noted

SO5	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.	<p>1. Inquire of management as to what tools are used to ensure data in databases is encrypted.</p> <p>2. Inspect system configurations for evidence that data at rest is encrypted .</p>	No exceptions noted
SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	<p>1. Inquire of management as to what tools are used to ensure data in transit is encrypted.</p> <p>2. Inspect system configurations for evidence that data in transit is encrypted .</p>	No exceptions noted
WS2	Disk encryption and system passwords are enabled across all organization workstations.	1. Inspect that system password parameters and disk encryption are enabled for a sample of workstations.	No exceptions noted
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
AC3	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.	<p>1. Inquire of management as to the process for managing access privilege/administrative accounts (end user, generic and system/service) accounts on the in-scope servers and databases.</p> <p>2. Inspect list of all administrative/privilege accounts on the in- scope systems to determine that access to these accounts are restricted to authorized and appropriate personnel.</p>	No exceptions noted

CM1	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.	1. Inspect that the change management process was reviewed by IT management within the past year.	No exceptions noted
SO3	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.	1. Inspect the configuration management tool for evidence of baseline configurations being stored. 2. Inspect that baseline configurations are updated after significant system changes are made.	No exceptions noted
WS1	Security software (firewall, Antivirus and anti-spam) is installed and enabled on all workstations.	1. Inspect that firewalls and anti-virus/anti-malware are enabled on a sample of workstations. 2. Inspect that anti-virus/anti-malware definitions are configured to remain current.	No exceptions noted
System Operations			
<i>CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</i>			
SO3	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.	1. Inspect the configuration management tool for evidence of baseline configurations being stored.	No exceptions noted

		2. Inspect that baseline configurations are updated after significant system changes are made.	
SO9	A log management process has been formalized to make sure that access to change the log configuration and access to modify logs is restricted.	<p>1. Inquire of management as to the log management process (configuration & retention).</p> <p>2. Inspect the log configuration and validate that only authorized individuals have access to modify the log settings and the log files.</p>	No exceptions noted
SO13	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	1. Inspect the penetration test report for documentation of scope, issues analysis and remediation. Issues left unremediated should be transferred onto the risk register.	No exceptions noted
SO14	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	<p>1. Inspect logging configurations and validate that key activities are included.</p> <p>2. Inspect notification/alert settings and validate that alerts are enabled for all key activities and personnel set up to receive alerts are appropriate.</p> <p>3. For a sample of alerts, inspect back-up documentation and validate that actions were taken to resolve the issue in accordance with log management process.</p>	No exceptions noted

SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	1. For a sample of vulnerability scans, inspect that scope of the scan was documented and that issues are analyzed and remediated in a timely manner.	No exceptions noted
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved. 2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	No occurrence of the control There we no security incidents during the period per management.
SO2	Infrastructure has been configured to automatically scale the capacity and performance needs of the systems.	1. Inspect configuration showing that infrastructure automatically scales based on capacity and performance needs.	No exceptions noted

SO14	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	<ol style="list-style-type: none"> 1. Inspect logging configurations and validate that key activities are included. 2. Inspect notification/alert settings and validate that alerts are enabled for all key activities and personnel set up to receive alerts are appropriate. 3. For a sample of alerts, inspect back-up documentation and validate that actions were taken to resolve the issue in accordance with log management process. 	No exceptions noted
SO15	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.	<ol style="list-style-type: none"> 1. Inspect that firewall rules are configured on the application gateway and production network and have been reviewed within the past year. 	No exceptions noted
SO16	IT team continuously monitors system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Incident management process is invoked for confirmed events and anomalies.	<ol style="list-style-type: none"> 1. Inspect logging configurations and validate that performance related measures are included. 2. Inspect notification/alert settings and validate that alerts are enabled for all key measures and personnel set up to receive alerts are appropriate. 3. For a sample of alerts, inspect back-up documentation and validate that actions were taken to resolve the issue in accordance with log management process. 	No exceptions noted

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
IM2	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments.	1. Inspect that the incident management process contains details of notifying affected parties in case of a data breach. 2. For a sample of data breaches, inspect that notification was provided to affected parties in accordance with incident management process.	No occurrence of the control Per management, no data breaches occurred during the period.
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved. 2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	No occurrence of the control There we no security incidents during the period per management.

IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	<ol style="list-style-type: none"> 1. Inspect that incident management process contains details of performing a post-mortem on closed incidents. 2. For a sample of incidents, inspect the incident response documentation for evidence of a post-mortem being performed. 	<p>No occurrence of the control</p> <p>There we no security incidents during the period per management therefore there are no lessons learned documents.</p>
<i>CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</i>			
CR2	Daily system back-ups are performed using an automated system and replicated to an offsite location. Backups are monitored for failure using an automated system.	<ol style="list-style-type: none"> 1. Inspect the backup schedule and configuration on the backup tool and confirm that the system is configured for taking weekly full and daily incremental backups of the application and databases. 2. Inspect backup system configuration and confirm that data backups are replicated to an offsite location. 3. Inspect backup configuration and confirm that the system is setup to notify the relevant personnel in the event of failures and that the persons set up to receive the notifications have responsibilities over the backup process. 	No exceptions noted

		4. For a sample of backup failures, inspect evidence that failures were resolved within a timely manner.	
CR6	Disaster recovery plans (including restoration of backups) have been developed and tested annually. Test results are reviewed and consequently contingency plans are updated.	<p>1. Inspect the DRP for management review within the last year.</p> <p>2. Inspect test results for evidence of review and follow-up.</p>	No exceptions noted
IM2	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments.	<p>1. Inspect that the incident management process contains details of notifying affected parties in case of a data breach.</p> <p>2. For a sample of data breaches, inspect that notification was provided to affected parties in accordance with incident management process.</p>	<p>No occurrence of the control</p> <p>Per management, no data breaches occurred during the period.</p>
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	<p>1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved.</p> <p>2. For a sample of incidents during the period, inspect that the incidents were analyzed,</p>	<p>No occurrence of the control</p> <p>There we no security incidents during the period per management.</p>

		communicated and resolved according to the process.	
IM5	Management has established defined roles and responsibilities to oversee implementation of security policies including incident response.	1. Inspect the Information Security policy (and Incident Management process if necessary) for defined roles and responsibilities for implementing and operating key security functions (including incident response).	No exceptions noted
IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	1. Inspect that incident management process contains details of performing a post-mortem on closed incidents. 2. For a sample of incidents, inspect the incident response documentation for evidence of a post-mortem being performed.	No occurrence of the control There we no security incidents during the period per management therefore there are no lessons learned documents.
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	1. For a sample of vulnerability scans, inspect that scope of the scan was documented and that issues are analyzed and remediated in a timely manner.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved.	No occurrence of the control

		2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	There we no security incidents during the period per management.
IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	<p>1. Inspect that incident management process contains details of performing a post-mortem on closed incidents.</p> <p>2. For a sample of incidents, inspect the incident response documentation for evidence of a post-mortem being performed.</p>	<p>No occurrence of the control</p> <p>There we no security incidents during the period per management therefore there are no lessons learned documents.</p>
SO12	A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. In addition, production servers are scanned to test patch compliance on a quarterly basis.	<p>1. Inspect the patch management process and validate that operating system vulnerabilities are addressed in a timely manner.</p> <p>2. For a sample of quarterly scan results on production servers, inspect the results to validate management has assessed the level of compliance.</p>	No exceptions noted
WS3	A patch management process exists to confirm that operating system level vulnerabilities for workstations are remediated in a timely manner. In addition, workstations are scanned to test patch compliance on a quarterly basis.	<p>1. Inspect the patch management process and validate that operating system vulnerabilities are addressed in a timely manner.</p> <p>2. For a sample of quarterly scan results on workstations, inspect the results to validate</p>	No exceptions noted

		management has assessed the level of compliance.	
Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
AC6	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	<p>1. Inspect system list of all users with access to deploy changes to production and confirm that users with access do not have development responsibilities.</p> <p>2. For a sample of changes made to production, confirm that the individual who promoted the change into the production environment is different from the user who developed the change.</p>	No exceptions noted
CM1	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.	1. Inspect that the change management process was reviewed by IT management within the past year.	No exceptions noted
CM2	Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.	1. For a sample of emergency system changes made during the year, inspect that the changes were documented, tested and approved prior to implementation and in accordance with the change management process.	No exceptions noted

CM3	A formal system development life cycle (SDLC) methodology is established that governs the development, acquisition, implementation, and maintenance of application development and enhancement projects.	1. Inspect that a formal system development life cycle (SDLC) is in place that governs the development, acquisition, implementation, and maintenance of application development and enhancement projects.	No exceptions noted
CM4	Changes that affect the functionality and security of the system components are communicated to internal and external users.	1. For a sample of system changes, inspect that the functionality and/or security changes were communicated (e.g. release notes) to affected parties in accordance with the change management process.	No exceptions noted
CM5	Changes to the application(s) and supporting infrastructure are documented, tested and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	1. For a sample of system changes made during the year, inspect that the changes were documented, tested and approved prior to implementation and in accordance with the change management process.	No exceptions noted
CM6	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.	1. For a sample of changes to the production environment, inspect change documentation and validate that the changes were tested in a segregated environment.	No exceptions noted
DS3	Production data is not used in testing or development environments.	1. Inquire with IT management on how production data is not be copied into or used in testing or development environments.	No exceptions noted
SO3	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.	1. Inspect the configuration management tool for evidence of baseline configurations being stored.	No exceptions noted

		2. Inspect that baseline configurations are updated after significant system changes are made.	
Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
RM1	Management maintains insurance coverage through an external service provider against major financial risks for overall business.	1. Inspect that an insurance certificate/policy exists with a 3rd party that covers major financial risks.	No exceptions noted
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year. 2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted

VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	<p>1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis.</p> <p>2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.</p>	No exceptions noted
VM4	Vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.	<p>1. Inspect that the vendor management process includes security procedures in the event agreements are terminated (e.g. data destruction or recovery, separation of APIs, etc).</p> <p>2. For a sample of vendor terminations, confirm that access to programs and/or data was removed per the process</p>	<p>No occurrence of the control</p> <p>No vendors were terminated during the period per management.</p>