VTEX BRASIL TECNOLOGIA PARA E-COMMERCE LTDA.

Service Organization Control (SOC) 3 for Service Organizations Report
for the period from January 1, 2022, to December 31, 2022

Report of Independent Service Auditors issued by
Grant Thornton Auditoria e Consultoria Ltda.

Contents

Grant Thornton Auditoria e Consultoria Ltda.

Av. Eng. Luiz Carlos Berrini, 105 - 12º andar, Itaim Bibi, São Paulo (SP) Brasil

T +55 11 3886-5100

www.grantthornton.com.br

I. Report of Independent Auditors

To the Management and the Board of Directors of VTEX Brasil Tecnologia para E-commerce Ltda.:

Scope
We have examined VTEX Brasil Tecnologia para E-Commerce Ltda. ("the Company or "VTEX") accompanying assertion titled Assertion of "VTEX Brasil Tecnologia para E-Commerce Ltda." (assertion) that the controls within VTEX Cloud Platform (system) were effective throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that VTEX's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (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).*

Service organization's responsibilities
VTEX is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that VTEX's service commitments and system requirements were achieved. VTEX has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, VTEX is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditor's responsibilities
Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by American Institute of Certified Public Accounts (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve VTEX's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve VTEX's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations
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 provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness 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.

Opinion
In our opinion, management's assertion that the controls within VTEX's system were effective throughout the period January 1, 2022 through December 31, 2022, to provide reasonable assurance that VTEX's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

São Paulo, Brazil
January 31, 2023

Grant Thornton Auditoria e Consultoria Ltda.
CRC 2SP-034.766/O-0

II. VTEX Brasil Tecnologia para E-commerce Ltda. Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within II. VTEX Brasil Tecnologia para E-commerce Ltda. (the "system") throughout the period January 1,2022, to December 31, 2022, to provide reasonable assurance that VTEX' service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that VTEX's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy ("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).* VTEX's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Attachment A – VTEX Cloud Commerce Platform

A. About VTEX

VTEX provides a highly customizable platform that supports several commerce operations of different natures, from B2C to B2B, from grocery to services. It means that not all the aspects of each store are purely defined by VTEX, but by the tenants themselves.

Solutions Overview

This report describes the control structure of VTEX Brasil Tecnologia para E-Commerce Ltda. (“the Company or “VTEX”) as it relates to its provided services for the Security, Availability, Processing Integrity, Confidentiality, and Privacy with Trust Services Criteria.

System Overview

Functional Services:

- VTEX ID
- License Manager
- Catalog
- Master Data
- PCI Gateway
- Logistics
- Channel
- Rates & Benefits
- OMS
- Conversation Tracker
- Message Center
- CMS
- Billing
- Bridge
- Suggestions
- Insights
- Credit Control
- Pricing

Supporting Services:

- Janus
- Pachamama
- DeLorean
- Slack
- Splunk
- GitHub

Infrastructure Providers:

- Amazon Web Services
- Microsoft Azure
- Google Mail

Shared Responsibility

The service provided by VTEX is a highly customizable platform that supports several commerce operations of different natures, from B2C to B2B, from grocery to services. It means that not all of the aspects of each store are purely defined by VTEX, but by the tenants themselves.

For that reason, complying with the Trust Services Criteria is a task that sometimes relies on VTEX, and others must be taken care of by the tenant, supported or not by features or characteristics of the platform.

B. SOFTWARE

FUNCTIONAL SERVICES

VTEX ID

VTEX ID is a VTEX authentication service. It is responsible for identifying platform users, both administrators and store clients, while keeping store clients isolated from admin users. It natively offers some authentication methods:

- Temporary one-time-use token sent to the email to be authenticated.
- Google ID.
- Email + password.

For administrative users, it enforces the use of two-factor authentication.

It can be extended by any external Identity Provider that implements either OAuth 2 or SAML 2.0.

License Manager

Service responsible for the authorizing users of the platform. A store starts with one single user, the master user, and they will use License Manager to delegate permissions by defining roles and assigning those roles to administrative users or integrated systems.

Using the License Manager, one can also manage different hostnames used by a given account. This allows an account to be either single or multi-domain.

Catalog

Every web store has their products, whatever the kind, to physically deliverable items to digital products or services. The Catalog service is where the products of the store are registered for selling.

The basic structure of the product catalog comprises Categories, Products, and SKUs.

Category is a container for products. It not only contains products under it, but also defines its data model. The administrator will determine which are the fields to be filled in a product contained by a Category. Each field will be set, amongst other things, as required, searchable, used as a search facet.

A hierarchy exists and can go as deep as three levels, so that a Category will inherit the structure of its ancestral line.

Products are what the store offers to their customers and hold the information that is sufficient for the client to identify and decide for the purchase.

SKUs are the variations of a product. Examples of variations of the same product are colors, sizes, voltage, etc.

Master Data

This service allows the tenant to model and implement their own data entities, both structure and some behavior. The customization of data may happen with the creation of fully new entities or the extension of native data entities, like the Client entity.

Master Data entities may be consumed and modified, as well as their structure, using the UI of the module or its API.

PCI Gateway

The PCI Gateway has two main goals:

- Encapsulate all processing and storage of payment card information, limiting the scope of the PCI DSS certification assessment.
- Work as a normalization interface between the rest of the platform, especially the Checkout services, and the different payment providers integrated to VTEX.

The service processes, stores, and tokenizes payment card information to serve VTEX Smart Checkout with payment services.

Logistics

Logistics module allows our tenants to keep record of their sellable items inventory, distribution center locations and docks availability, and courier services used for final delivery. This allows this service to provide both the availability of goods offered in the web store as well as simulate shipment to calculate price and date of delivery to the consumer.

Channel

Channel module provides an interface between our tenants and marketplaces that are able to offer their products to different audiences. Using the tools provided by Channels, tenants acting as sellers on those marketplaces are able to see the integration of products and orders.

Rates & Benefits

This module is called Rates & Benefits because it is responsible to model taxes (rates), discounts and gifts (benefits) to be offered to consumers. Each store can set up combinations of causes and consequences to be applied to orders. Attributes existing today allow for highly customizable scenarios with combinations that count to more than three thousand.

OMS

Order Management System (OMS) gives access and management tools to orders received from all the different channels available in the store. Orders can be searched, listed and orders lists can be filtered by different attributes, as well as individually detailed. Status management is also available, and changes can be made to orders in accordance to proper business conditions.

Conversation Tracker

This module intermediates all the e-mail communication related to an order, granting that every message is trackable along the order timeline in the OMS. The implementation is made in a way that even the eventual email communication between an external seller and the end consumer is trackable in the OMS of the marketplace where the order was first placed.

Message Center

Message Center module provides a way to set templates and delivery configuration for transactional email messages sent by the platform.

CMS

CMS component is VTEX's rendering system for web store pages. It holds page templates for hot sites, landing pages, search pages, categories, and product pages. It provides an extended HTML markup for highly customizable pages, leveraging components that accelerate the inclusion of information taken from the data available in the web store, like product catalog, prices, promotions, and so on.

Billing

Billing module is responsible for calculating the value for each invoice owed by the store. This calculation is made based on the orders received by the store, using the commercial conditions given by edition and vouchers defined in contract.

Bridge

Module that is responsible for integrating VTEX platform with market leader marketplaces supported natively by VTEX.

Suggestions

Suggestion's module helps with receiving product suggestions to a marketplace's product catalog from external sellers that want to offer them there. Here a marketplace catalog administrator is able to map categories, product attributes, modify attribute values, accept and refuse product suggestions.

Insights

As implied by its name, this module gives management insights to store administrators to help to achieve better commercial performance. Insights given by the tool are actionable items like, for example, alerting about highly demanded products that are about to become unavailable.

Credit Control

The Credit Control module lets the store give and manage credit to consumers. This credit can then be used during Checkout to pay for order fully or in part. The credit lines managed by the module may be used for any business situation conceived by the store administrators.

Pricing

The Pricing module helps the store to define prices for their offered products and/or services for several different contexts, from B2B to B2C experiences, distinct sales channels, or even several physical stores.

INTERNAL SUPPORTING SERVICES

Janus

It is our set of internal edge services, comprising specific components responsible for throttling, security aspects, and request routing.

Pachamama

This is a VTEX continuous deployment solution.

DeLorean

DeLorean supports our engineering teams in the publication or rollback of specific versions of their services.

EXTERNAL SUPPORTING SERVICES

Slack

Corporate instant messaging system. It's also an important tool in the communication of messages generated by automated operational processes, like our monitoring systems.

Splunk

Concentrates all system logs. Is the core of our SIEM solution.

GitHub

The tool used by VTEX as its VCS.

C. INFRASTRUCTURE

Amazon Web Services - AWS is the cloud provider for the platform provided as a service by VTEX.

Microsoft Azure - Hosts VTEX's corporate Identity Provider and Federation.

D. PEOPLE

For all this process, that employee has made all onboarding processes verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks, or limited by the applicable law. The VTEX is led by the Chief Executive Officer who reports directly to the Execute Officer. VTEX Enterprise Architecture Office is responsible for building the security defense ecosystem, designing, developing, operating, managing the system operations, and keeping compliance with the best security practices.

E. DATA

Data should be classified considering confidentiality, integrity, and availability impacts as high, moderate, and low. This framework will result in one of three classifications, respectively: restricted, confidential, or public. Any other data that belongs to the scope of a tenant's account is classified at least as confidential, as it is owned by the tenant, and not by VTEX, which determines that it should not be available to anyone that is not explicitly supposed to have access to it. Personal data, being considered restricted data, must always be encrypted not only in transit, but at rest as well.

F. PROCESS AND PROCEDURES

VTEX has established policies, processes, and procedures to formulate control activities and support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. These processes and procedures cover the following areas:

- Data Security Management
- Change Management
- Security Incident Management
- Business Continuity Management
- Identity and Access Management

Attachment B – Principle Service Commitments and System Requirements

VTEX designs its processes and procedures related to user entities to meet its objectives for its VTEX Cloud Commerce Platform. Those objectives are based on the service commitments that VTEX makes to user entities; the laws and regulations that govern the provision of the VTEX system; and the financial, operational, and compliance requirements that VTEX has established for the services. The security commitments and Service Level Agreement (SLA) to user entities are documented and communicated in contracts and other agreements. VTEX's principal service commitments include, but are not limited to, the following:

1. Protection of user entities' information against unauthorized access, modification, or disclosure;
2. Providing for the availability of services supporting user accounts;
3. Use of encryption technologies to protect customer data both at rest in transit; and
4. Conduct standards dictating security, availability, and privacy standards.

VTEX establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in VTEX's 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.