ZOCCAM

Information Systems General Controls and Security Review

April 1, 2016

I. PROJECT BACKGROUND

A. BACKGROUND

Security of technology assets is an important priority within the financial industry. As threats to data and systems have evolved, so have the requirements for safeguarding client and organization information. The processes and people that support the security of technology are the key components in protecting these valuable business assets. Likewise, it is important to measure the security of technology assets to understand the ability to defend against threats.

B. OBJECTIVE OF THIS PROJECT

The primary objective was to perform the information systems (IS) general controls and security review of ZOOCAM's internally managed and third-party managed applications.

The management of ZOCCAM is responsible for establishing and maintaining internal controls. The objective of this review is to provide management an assessment on the design of their internal controls. In establishing controls related to IS, estimates and judgments by management are required to assess the expected benefits and related costs of controls.

Because of inherent limitations in any controls, errors or fraud may occur and not be detected. Also, projection of any evaluation of the controls to future periods is subject to the risk that the controls may become inadequate because of changes in the control environment, or that the degree of compliance with the controls may deteriorate.

C. SCOPE

The IS general controls and security review included reviewing requested documentation and interviewing ZOOCAM personnel to assess IS general controls and security related to the ZOOCAM environment.

The applications considered in the scope of the review included the following:

Managed by ZOCCAM

Active Directory	ZOCCAM Application

Third-Party Managed

Jack Henry ProfitStars	Microsoft Azure

D. APPROACH

To accomplish the objective of this engagement, ZOCCAM controls were assessed to determine design appropriateness and 3rd party SOC reports were reviewed to determine if those reports were qualified in nature, or contained any significant control deficiencies which could impact ZOCCAM's customers or clients.

II. EXECUTIVE SUMMARY

Our IS general controls and security review was designed to answer the following questions for ZOCCAM:

- **What is the assessment of ZOCCAM IS general controls?**

  Based on a review of the results of our activities, I believe overall, your Information Security Program and IS general controls are **satisfactory** as of the date of the review.

  A **satisfactory** designation indicates that while there may be control improvements identified, ZOOCAM appears to have taken appropriate action to ensure IS general controls are designed appropriately. The projection of any evaluation of these controls to future periods is subject to the risk that the controls may become inadequate because of changes in the control environment or that the degree of compliance with the controls may deteriorate.

No review of controls or security can ever provide total assurance or 100 percent protection against possible control failures or security intrusions on your systems. The potential effectiveness of specific controls and security measures is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, information networks, applications and control environments are extremely dynamic in nature and our examination of your control and security methods and procedures are conducted and documented as of the following specific period in time:

Assessment Service	Start Date	End Date
IS General Controls and Security Review	03/28/2016	04/01/2016

As a result, the projection of any conclusions, based on our examination, to future periods is subject to the risk that (1) changes are made to the systems or controls; (2) changes are made in processing requirements; (3) changes are required because of the passage of time; or (4) new security exploits are discovered that may alter the validity of such conclusions. Therefore, I take no responsibility for any lack of specific controls, control failures, breach of security, or other errors or fraud related to any part of your business environment. Any subsequent control or security issues that may arise within those areas examined or any control or security issues that are present at the time of this examination, but that are outside the scope of the examination, are solely the responsibility of ZOCCAM.

III. ZOCCAM BACKGROUND

A. PRODUCT PLATFORM DESCRIPTION

Zoccam's payment services platform consist of four major components laid out in a three-tier architecture: (1) the mobile application, (2) the web application, (3) the web services, and (4) the database.

1. Mobile Application (tier 1)

The mobile application runs on the end-users mobile device. We first identify the end user through realtor license number of invitation code from another user and a device identification code sent to the mobile number they provide. The user creates a PIN for subsequent login to the application. User registrations are manually reviewed and accounts are disabled when the user requests termination of service.

As its primary function, the mobile application captures real estate contract metadata and images of the check to be deposited as part of the real estate transaction and passes this information securely to the ZOCCAM web services, but never stores this information on the mobile device.

As payment for the transaction, the user provides a credit card number and expiration date which the app passes to ZOCCAM web services for authentication and processing.

No personal identifying information, payment information, or financial transaction information is ever stored on the device.

2. Web Application (tier 1)

For some functions, users access the ZOCCAM application website. All access to the website is secured with 2048 bit high-encryption SSL. No user name/password is required for access to static product information. One-time-use codes are issued through notifications for reference to transaction information and access to the site functions is only allowed with these code.

The application website is the user-facing tier of the application besides the mobile application. It is hosted on Microsoft Azure Platform-as-a-Service (PaaS) where Microsoft maintains the physical security of the servers, the currency and digital security of the platform, and Internet protocol security (IPSec) of the application, platform, and servers.

No application or user information is stored in the web application. All information is maintained and processed by the second tier, the secure Web Services.

3. Web Services (tier 2)

The mobile and web applications leverage the second tier, Web Services, to manage all business logic processing and persistent data access. This component provides an intermediary to access information and provide any core platform processing.

The web services are also hosted on Microsoft Azure PaaS where Microsoft maintains full currency of the underlying hardware and software, physical and IP security, and

transparent geo-physical redundancy and recovery in the case of underlying hardware failure or even data center disaster.

Access to the web services is secured using 2048 bit high-encryption SSL connections and programmatically authenticated with a token issued upon user authentication in the mobile app with either mobile phone identification (SMS code) or user ID & PIN combination. The web services (not directly accessible by end users) comprise the only software component with direct access to the platform database. This tier also mediates secure connections to other service provider including Jack Henry ProfitStars EPS (check processing), JetPay payment services (credit card processing), Google web services (geo calculations and maps), Mandrill for email, and Twilio for SMS. Access to each of these other services is secured with SSL and authenticated with private access keys that prevent misuse of ZOCCAM services accounts. The private access keys are stored securely in the Azure services portal where they are programmatically accessed. Keys are rotated every six months or according to the service provider policies, whichever is more frequent, by the ZOCCAM administrator.

4. Database (tier 3)

The ZOCCAM database is the final logical component and the third tier in the three-tier architecture. The database houses ZOCCAM user and application information and run in a Microsoft SQL Azure deployment with full automatic backup and geo-replication for disaster resiliency. The SQL Azure platform is fully maintained by Microsoft just as their other PaaS products are.

Access to the database is limited to application and administrative accounts via ID/password that are not shared with anyone outside of key ZOCCAM personnel. Direct database access is only used for special data inspection or manipulation for customer support purposes. All access to the database is logged automatically with the SQL Azure Audit Logs feature. Audit event data is stored in a separate Azure Storage Table and retained for 365 days. SQL Azure also employs a white-list security model where even authorized users cannot access the database from unknown IP addresses.

B. OPERATIONS PLATFORM DESCRIPTION

1. Business Platform

The ZOCCAM business employs a number of software-as-a-service (SaaS) products to operate efficiently. Each is managed by the ZOCCAM principals and maintained as needed to grant/revoke end-user permissions to other ZOCCAM representatives. The following is a non-exhaustive list.

- *GoDaddy.com* for domain hosting and SSL certificate issuance
- *Microsoft Office 365* for business productivity software, email hosting, document management, etc.
- *Weebly* for website hosting
- *ZenDesk* for customer support functions
- *PhoneBooth* for VOIP telephony & answering service

- *MailChimp* for email marketing
- *Microsoft Azure* for hosting the product/platform and collecting analytics

2. Product Development Platform

a. Software Development Lifecycle (SDLC)

The ZOCCAM product development team follows an agile Scrum method for planning and tracking work. In Scrum, work to be accomplished is first listed in a prioritized backlog, then decomposed into tasks that are tracked through stages of work and completion. The ZOCCAM product team grooms the backlog and plans work for each iteration on a weekly basis.

b. Tools and External Sevices

The ZOCCAM technology team uses some key tools and services to deliver its product. Each of these services is administered by ZOCCAM principals with end-user access granted to/revoked from other ZOCCAM personnel as required by business processes. Note that publishing functions are accessed exclusively by ZOCCAM principals.

- *Microsoft Visual Studio Team Services* (VSTS) for work item management, source control, and team communication. VSTS provides web access with limited permissions where the ZOCCAM product manager updates the product backlog during planning, developers and the product manager together create tasks to track work, and developers check code into source control where each "commit" is associated with a task for review and auditing purposes.
- *Microsoft Developer Network* (MSDN) for access to development tools and knowledge base
- *Apple Developer Console* for creation and distribution of publishing certificates
- *Apple iTunes Connect* for publishing iOS application binaries
- *Google Play Developer Console* for publishing Android application binaries
- *Microsoft Azure* for publishing web application and service binaries

Product publishing procedures (without passwords) are documented in Microsoft OneNote files stored in the ZOCCAM Office 365 SharePoint document management portal.

All service account administration user IDs and passwords are stored securely in Lastpass password management tool in a managed folder only accessible by ZOCCAM principals.

IV. CONTROL DESCRIPTIONS

ZOCCAM Controls:

Backup and recovery controls:

- Control Objective—BK1: Data has been backed-up and is recoverable.

  Control Description BR-1: All product, operational, and development information stored in SaaS systems with frequent cyclical backup procedures.

Operational controls:

- Control Objective—OP1: Physical access to computer hardware is limited to appropriate individuals.

  Control Description PS-1: Personal computers are kept in locked offices. Developer laptops employ full-hard drive encryption.

- Control Objective—OP2: Database access is monitored.

  Control Description PS-2: All access to the database is logged automatically. Audit event data is stored and retained for 365 days.

SDLC:

- Control Objective—SD1: Changes are authorized.

  Control Description CM-1: Change requests are initiated and approved by appropriate members of management.

- Control Objective—SD2: Changes are tested.

  Control Description CM-2: All changes made to production programs, configurations and data are tested.

- Control Objective—SD3: Changes are approved.

  Control Description CM-3: All changes made to production programs, configurations and data are approved by appropriate members of management before being promoted to production.

Access controls:

- Control Objective—AC1: Segregation of duties/access to production programs.

  Control Description AM-1: Access to application configuration parameters and data restricted to authorized personnel.

- Control Objective—AC1: Segregation of duties/access to production programs.

  Control Description AM-2: Access to databases is limited appropriate members of IT.

- Control Objective—AC3: Access to privileged IT functions is limited to appropriate individuals.

  Control Description AM-3: Access rights of terminated employees are disabled on a timely basis.

- Control Objective—AC4: Access to privileged IT functions is limited to appropriate individuals.

  Control Description AM-4: The number of people with administrator privileges is limited appropriately.

- Control Objective—AC5: User access is authorized and appropriately established

  Control Description AM-5: Access rights of users and IT personnel are documented and approved by appropriate members of management.

- Control Objective—AC6: Logical access process is monitored.

  Control Description AM-6: User and IT personnel access rights are periodically reviewed and approved by management.

- Control Objective—AC7: User access is monitored.

  Control Description AM-7: User registrations are manually reviewed and accounts are disabled when the user requests termination of service

3rd Party SOC Reports:

- Jack Henry and Associates, Inc. – Report on JHA's Description of its Systems related to Enterprise Payment Solutions Systems and the Suitability of the Design and Operations Effectiveness of Controls for the period from October 1, 2014 or September 30, 2015.

- Microsoft Azure – Independent Service Auditor's Report for the period from January 15, 2015 to July 31, 2015.

Reporting

We kept you informed of our progress throughout the engagement through periodic formal and informal status reports and meetings as appropriate. Upon completion of the review, we prepared this written report of our findings and recommendations.

V. RESULTS

ZOCCAM Controls:

- IT general controls listed above were found to be designed appropriately as of April 1, 2016.

3rd Party SOC Report Review:

- Jack Henry – The SOC report for the period tested was reviewed and found to be unqualified in nature and contained no exceptions noted for any of the control objectives tested by the independent auditor.

- Microsoft Azure - The SOC report for the period tested was reviewed and found to be unqualified in nature. The independent auditor noted that for the period tested, reasonable assurance was provided that
    - The system was protected against unauthorized access, use or modification,
    - The system was available for operation and use as committed or agreed,
    - Information within the system, designated as confidential, was protected as committed or agreed, and
    - The system processing was complete, valid, accurate, timely, and authorized

April 1, 2016

Ashley Cook, CEO
ZOCCAM
5950 Berkshire Lane, Suite 1460
Dallas, Texas 75225

Dear Ms. Cook:

This report contains the results related to the information technology (IS) general controls and security review performed for ZOCCAM.

No assessment of controls or security can ever provide total assurance or 100 percent protection against possible control failures or security intrusions on your systems. The potential effectiveness of specific controls and security measures is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, information networks, applications and control environments are extremely dynamic in nature and our examination of your control and security methods and procedures are conducted and documented as of the following specific period in time:

Assessment Service	Start Date	End Date
IS General Controls and Security Review	03/28/2016	04/01/2016

As a result, the projection of any conclusions, based on our examination, to future periods is subject to the risk that (1) changes are made to the systems or controls; (2) changes are made in processing requirements; (3) changes are required because of the passage of time; or (4) new security exploits are discovered that may alter the validity of such conclusions. Therefore, I take no responsibility for any lack of specific controls, control failures, breach of security, or other errors or fraud related to any part of your business environment. Any subsequent control or security issues that may arise within those areas examined or any control or security issues that are present at the time of this examination, but that are outside the scope of the examination, are solely the responsibility of ZOCCAM.

This report is intended solely for use by the management of ZOCCAM.

I appreciate the courtesies and cooperation extended to me during this project and the opportunity to be of service to ZOCCAM. Please contact Matthew Sargent at +1 214 585 6939 if you have any questions regarding this report.

Sincerely,

Matthew Sargent, CFE, CISSP, CISA, CRISC