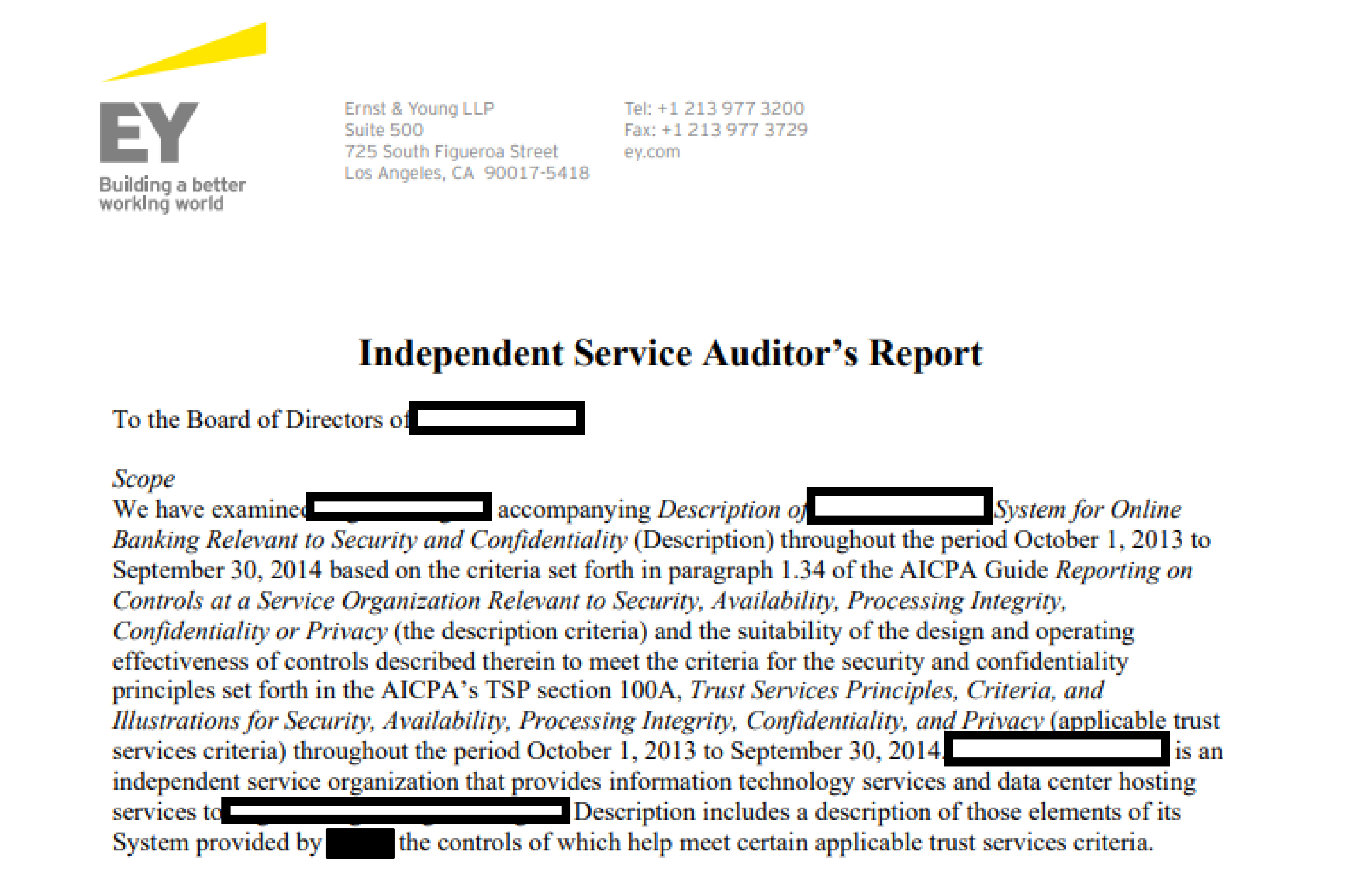
SOC Quick Guide

- Auditor
- Review dates
- Scope/Exclusions
- SOC 1, 2 or 3 and Sections of SOC 2
- Type 1 or 2
- Opinion/Qualification
- Complementary User Entity Controls
- Subservice Organizations

SOC Quick Guide

- Critical controls:
  - Perimeter Security (often outsourced)
  - Operating System/DB level security
  - User Access Administration
  - Software Development (test, test, test)
- Response to findings:
  - Substantive Testing/Explaining Away
  - Fixing of Individual Items Identified
  - Process Changes

SOC Quick Guide



Building a better working world

Ernst & Young LLP
Suite 500
725 South Figueroa Street
Los Angeles, CA 90017-5418

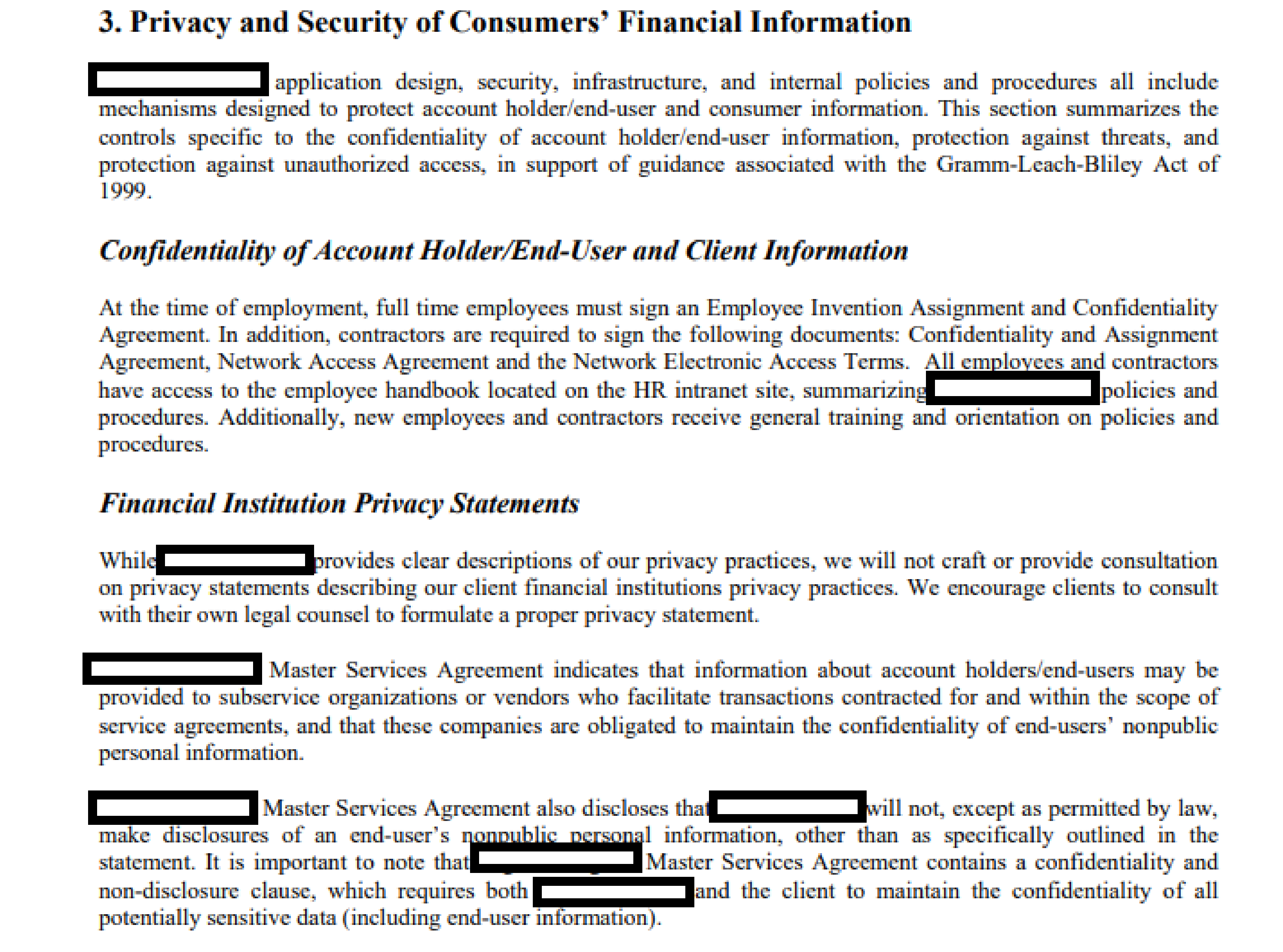
Tel: +1 213 977 3200
Fax: +1 213 977 3729
ey.com

Independent Service Auditor's Report

To the Board of Directors of [redacted]

Scope
We have examined [redacted] accompanying *Description of* [redacted] *System for Online Banking Relevant to Security and Confidentiality* (Description) throughout the period October 1, 2013 to September 30, 2014 based on the criteria set forth in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and confidentiality principles set forth in the AICPA's TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) throughout the period October 1, 2013 to September 30, 2014. [redacted] is an independent service organization that provides information technology services and data center hosting services to [redacted] Description includes a description of those elements of its System provided by [redacted] the controls of which help meet certain applicable trust services criteria.

SOC Quick Guide



3. Privacy and Security of Consumers' Financial Information

[redacted] application design, security, infrastructure, and internal policies and procedures all include mechanisms designed to protect account holder/end-user and consumer information. This section summarizes the controls specific to the confidentiality of account holder/end-user information, protection against threats, and protection against unauthorized access, in support of guidance associated with the Gramm-Leach-Bliley Act of 1999.

Confidentiality of Account Holder/End-User and Client Information

At the time of employment, full time employees must sign an Employee Invention Assignment and Confidentiality Agreement. In addition, contractors are required to sign the following documents: Confidentiality and Assignment Agreement, Network Access Agreement and the Network Electronic Access Terms. All employees and contractors have access to the employee handbook located on the HR intranet site, summarizing [redacted] policies and procedures. Additionally, new employees and contractors receive general training and orientation on policies and procedures.

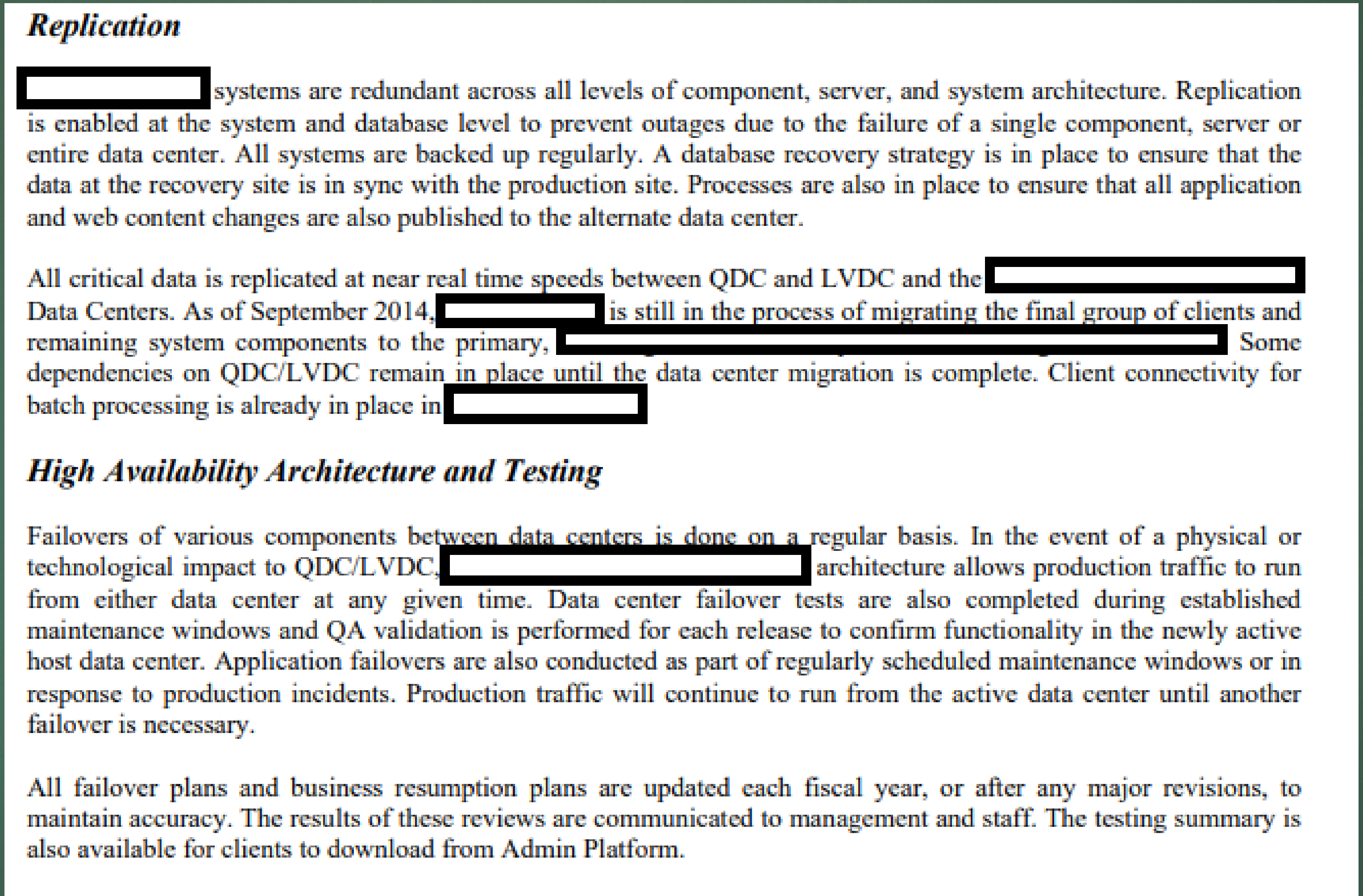
Financial Institution Privacy Statements

While [redacted] provides clear descriptions of our privacy practices, we will not craft or provide consultation on privacy statements describing our client financial institutions privacy practices. We encourage clients to consult with their own legal counsel to formulate a proper privacy statement.

[redacted] Master Services Agreement indicates that information about account holders/end-users may be provided to subservice organizations or vendors who facilitate transactions contracted for and within the scope of service agreements, and that these companies are obligated to maintain the confidentiality of end-users' nonpublic personal information.

[redacted] Master Services Agreement also discloses that [redacted] will not, except as permitted by law, make disclosures of an end-user's nonpublic personal information, other than as specifically outlined in the statement. It is important to note that [redacted] Master Services Agreement contains a confidentiality and non-disclosure clause, which requires both [redacted] and the client to maintain the confidentiality of all potentially sensitive data (including end-user information).

SOC Quick Guide



Replication

[redacted] systems are redundant across all levels of component, server, and system architecture. Replication is enabled at the system and database level to prevent outages due to the failure of a single component, server or entire data center. All systems are backed up regularly. A database recovery strategy is in place to ensure that the data at the recovery site is in sync with the production site. Processes are also in place to ensure that all application and web content changes are also published to the alternate data center.

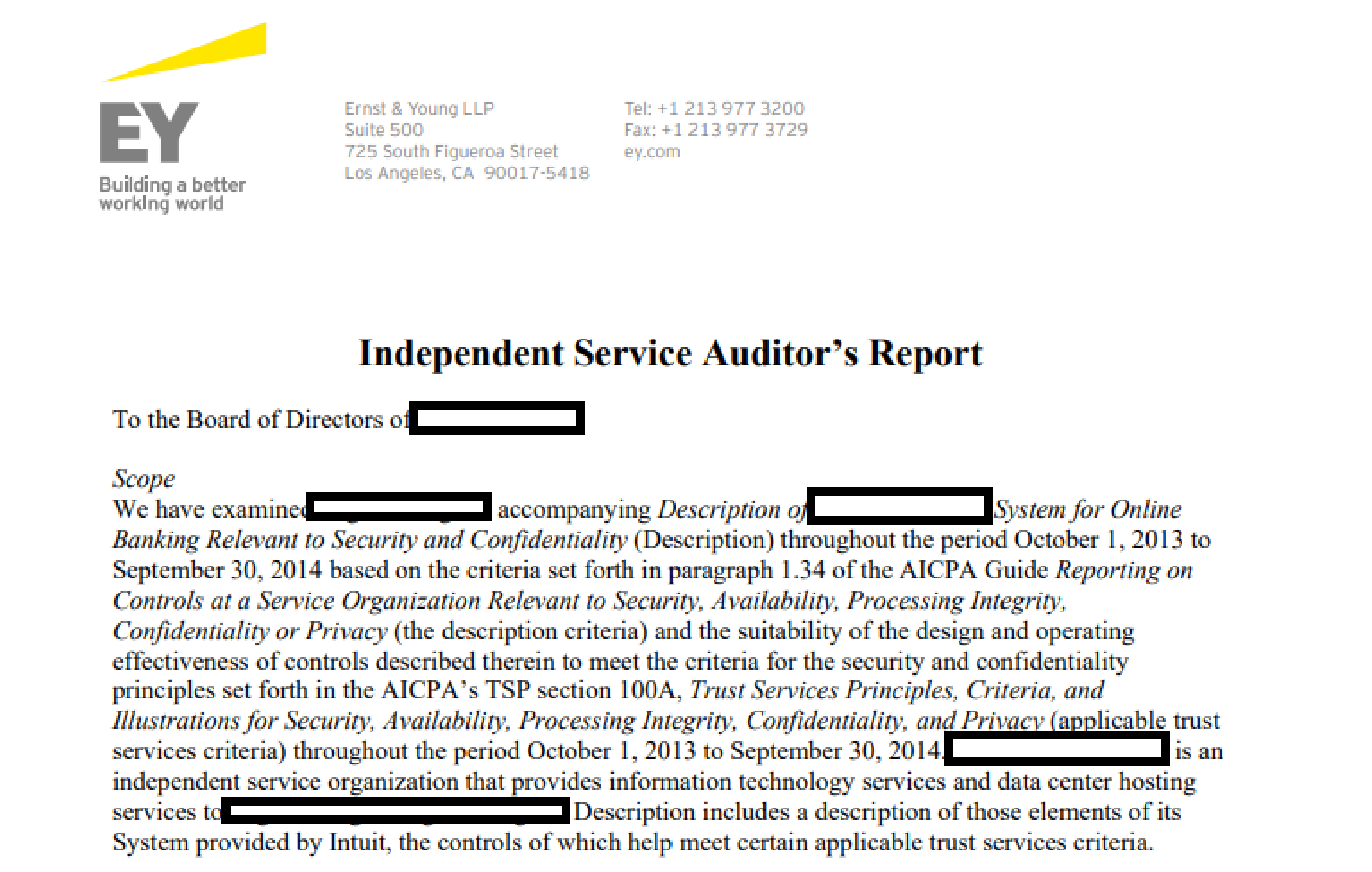
All critical data is replicated at near real time speeds between QDC and LVDC and the [redacted] Data Centers. As of September 2014, [redacted] is still in the process of migrating the final group of clients and remaining system components to the primary, [redacted] Some dependencies on QDC/LVDC remain in place until the data center migration is complete. Client connectivity for batch processing is already in place in [redacted]

High Availability Architecture and Testing

Failovers of various components between data centers is done on a regular basis. In the event of a physical or technological impact to QDC/LVDC, [redacted] architecture allows production traffic to run from either data center at any given time. Data center failover tests are also completed during established maintenance windows and QA validation is performed for each release to confirm functionality in the newly active host data center. Application failovers are also conducted as part of regularly scheduled maintenance windows or in response to production incidents. Production traffic will continue to run from the active data center until another failover is necessary.

All failover plans and business resumption plans are updated each fiscal year, or after any major revisions, to maintain accuracy. The results of these reviews are communicated to management and staff. The testing summary is also available for clients to download from Admin Platform.

SOC Quick Guide



EY
Building a better
working world

Ernst & Young LLP
Suite 500
725 South Figueroa Street
Los Angeles, CA 90017-5418

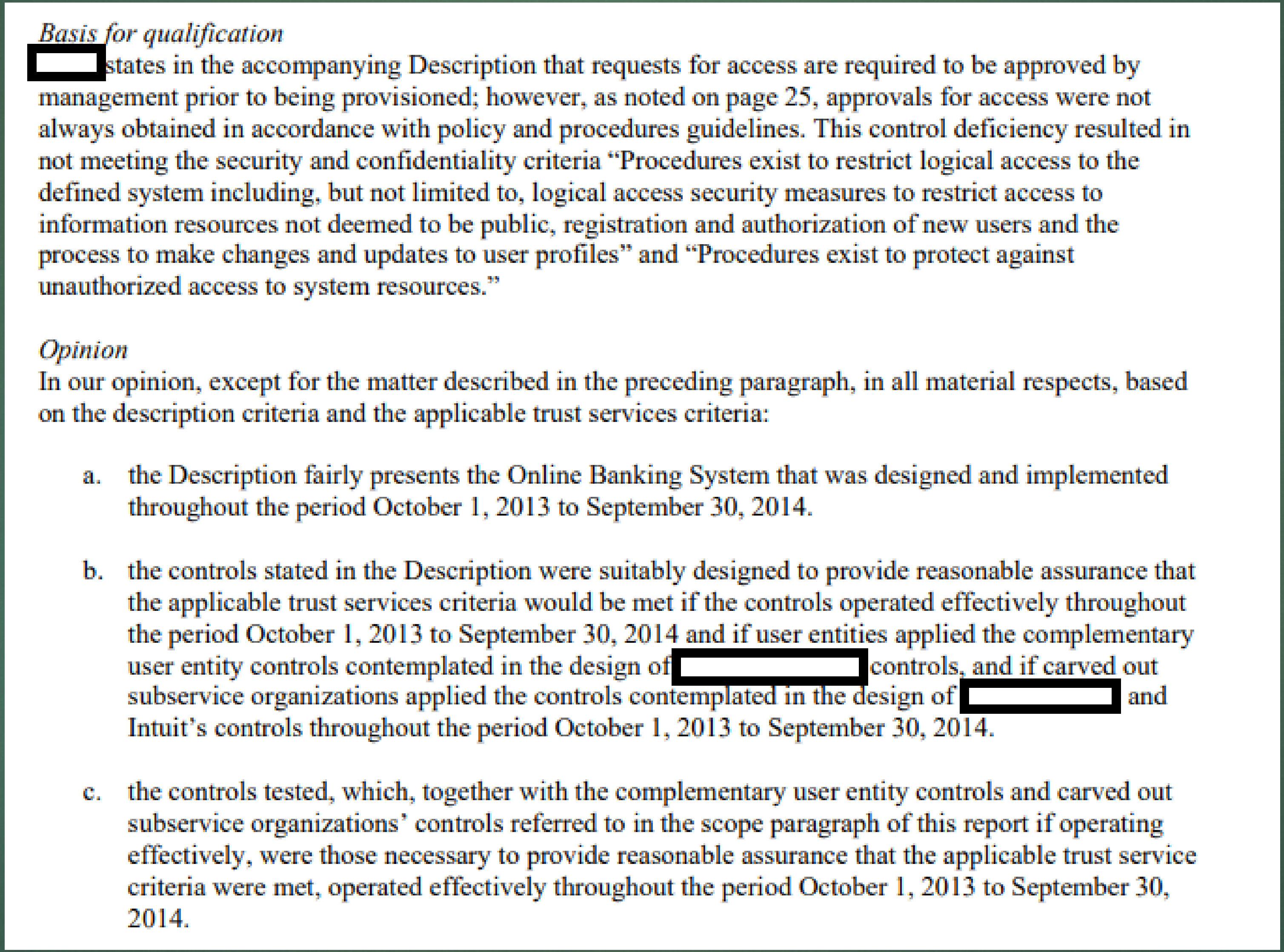
Tel: +1 213 977 3200
Fax: +1 213 977 3729
ey.com

Independent Service Auditor's Report

To the Board of Directors of [redacted]

Scope
We have examined [redacted] accompanying *Description of* [redacted] *System for Online Banking Relevant to Security and Confidentiality* (Description) throughout the period October 1, 2013 to September 30, 2014 based on the criteria set forth in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and confidentiality principles set forth in the AICPA's TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) throughout the period October 1, 2013 to September 30, 2014. [redacted] is an independent service organization that provides information technology services and data center hosting services to [redacted] Description includes a description of those elements of its System provided by Intuit, the controls of which help meet certain applicable trust services criteria.

SOC Quick Guide



Basis for qualification

[redacted] states in the accompanying Description that requests for access are required to be approved by management prior to being provisioned; however, as noted on page 25, approvals for access were not always obtained in accordance with policy and procedures guidelines. This control deficiency resulted in not meeting the security and confidentiality criteria "Procedures exist to restrict logical access to the defined system including, but not limited to, logical access security measures to restrict access to information resources not deemed to be public, registration and authorization of new users and the process to make changes and updates to user profiles" and "Procedures exist to protect against unauthorized access to system resources."

Opinion

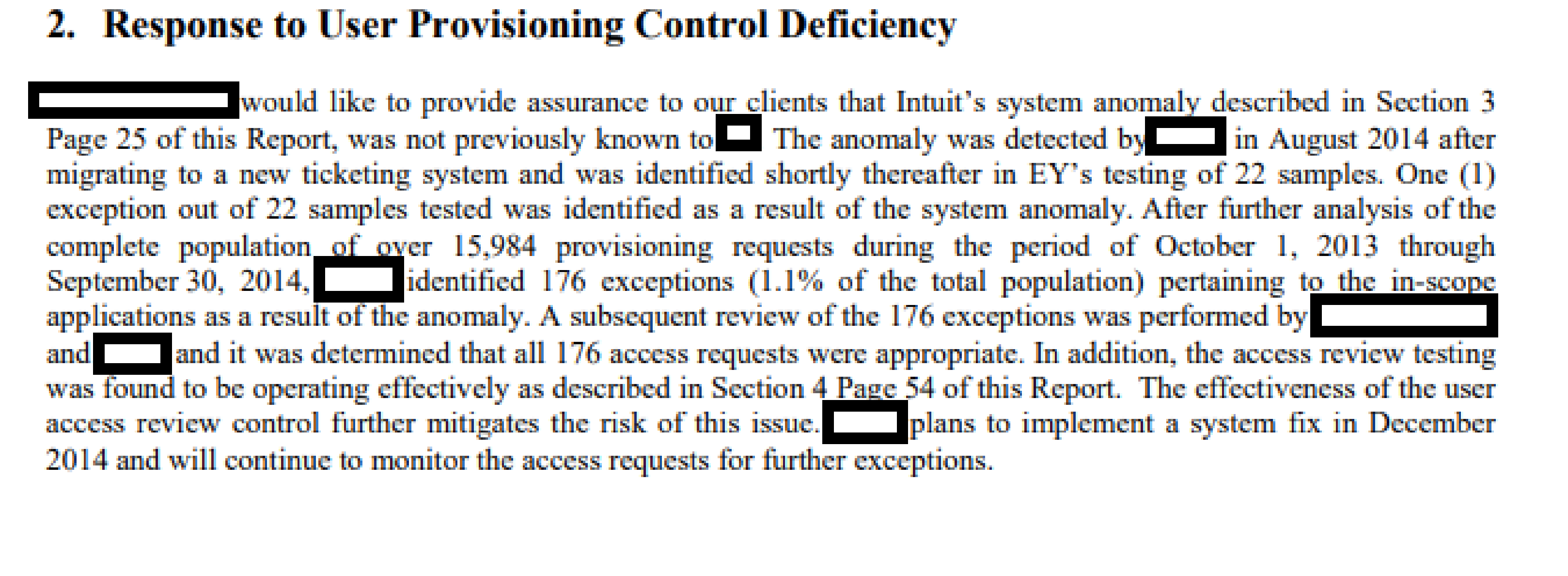
In our opinion, except for the matter described in the preceding paragraph, in all material respects, based on the description criteria and the applicable trust services criteria:

a. the Description fairly presents the Online Banking System that was designed and implemented throughout the period October 1, 2013 to September 30, 2014.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period October 1, 2013 to September 30, 2014 and if user entities applied the complementary user entity controls contemplated in the design of [redacted] controls, and if carved out subservice organizations applied the controls contemplated in the design of [redacted] and Intuit's controls throughout the period October 1, 2013 to September 30, 2014.

c. the controls tested, which, together with the complementary user entity controls and carved out subservice organizations' controls referred to in the scope paragraph of this report if operating effectively, were those necessary to provide reasonable assurance that the applicable trust service criteria were met, operated effectively throughout the period October 1, 2013 to September 30, 2014.

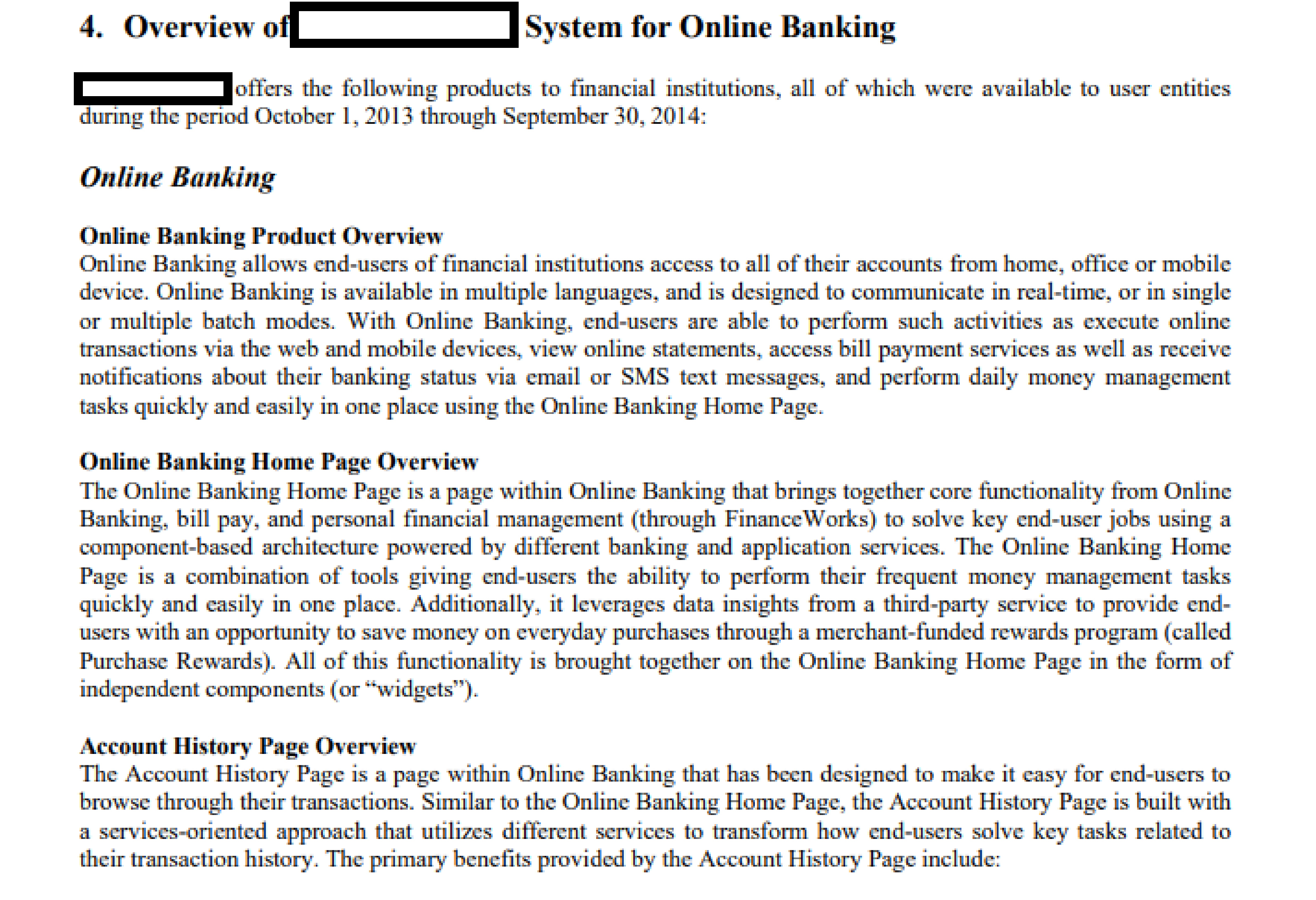
SOC Quick Guide



2. Response to User Provisioning Control Deficiency

[redacted] would like to provide assurance to our clients that Intuit's system anomaly described in Section 3 Page 25 of this Report, was not previously known to [redacted] The anomaly was detected by [redacted] in August 2014 after migrating to a new ticketing system and was identified shortly thereafter in EY's testing of 22 samples. One (1) exception out of 22 samples tested was identified as a result of the system anomaly. After further analysis of the complete population of over 15,984 provisioning requests during the period of October 1, 2013 through September 30, 2014, [redacted] identified 176 exceptions (1.1% of the total population) pertaining to the in-scope applications as a result of the anomaly. A subsequent review of the 176 exceptions was performed by [redacted] and [redacted] and it was determined that all 176 access requests were appropriate. In addition, the access review testing was found to be operating effectively as described in Section 4 Page 54 of this Report. The effectiveness of the user access review control further mitigates the risk of this issue. [redacted] plans to implement a system fix in December 2014 and will continue to monitor the access requests for further exceptions.

SOC Quick Guide



4. Overview of [redacted] System for Online Banking

[redacted] offers the following products to financial institutions, all of which were available to user entities during the period October 1, 2013 through September 30, 2014:

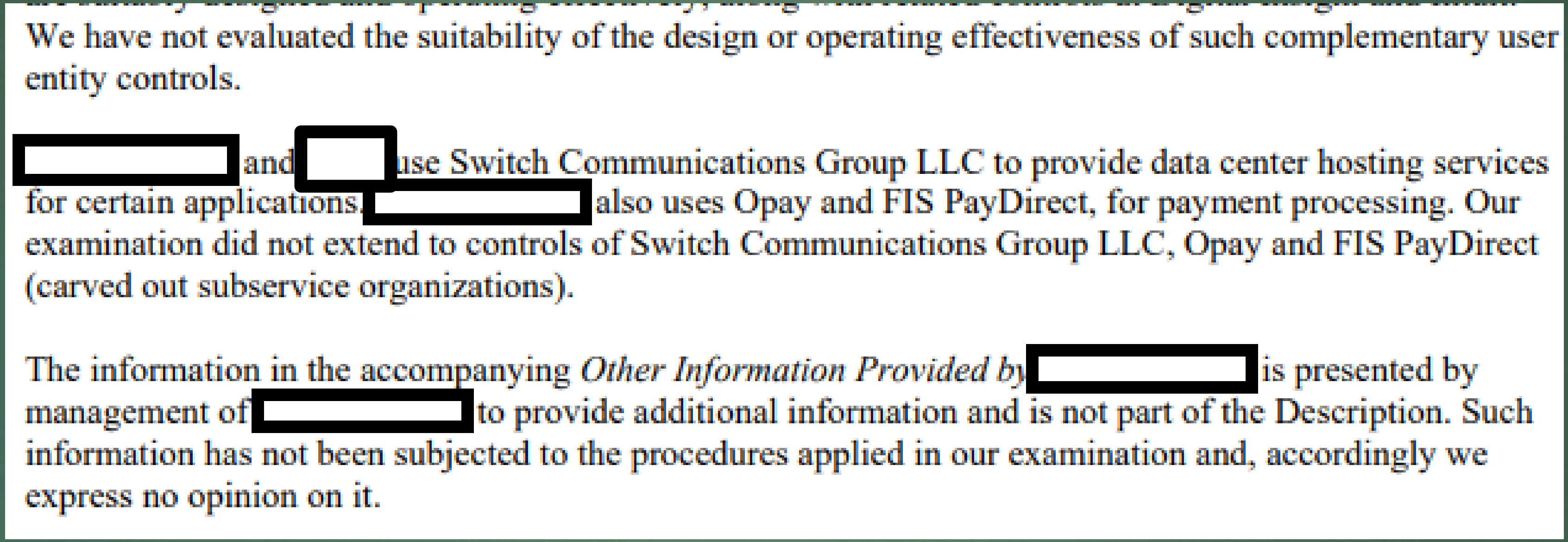
Online Banking

Online Banking Product Overview
Online Banking allows end-users of financial institutions access to all of their accounts from home, office or mobile device. Online Banking is available in multiple languages, and is designed to communicate in real-time, or in single or multiple batch modes. With Online Banking, end-users are able to perform such activities as execute online transactions via the web and mobile devices, view online statements, access bill payment services as well as receive notifications about their banking status via email or SMS text messages, and perform daily money management tasks quickly and easily in one place using the Online Banking Home Page.

Online Banking Home Page Overview
The Online Banking Home Page is a page within Online Banking that brings together core functionality from Online Banking, bill pay, and personal financial management (through FinanceWorks) to solve key end-user jobs using a component-based architecture powered by different banking and application services. The Online Banking Home Page is a combination of tools giving end-users the ability to perform their frequent money management tasks quickly and easily in one place. Additionally, it leverages data insights from a third-party service to provide end-users with an opportunity to save money on everyday purchases through a merchant-funded rewards program (called Purchase Rewards). All of this functionality is brought together on the Online Banking Home Page in the form of independent components (or "widgets").

Account History Page Overview
The Account History Page is a page within Online Banking that has been designed to make it easy for end-users to browse through their transactions. Similar to the Online Banking Home Page, the Account History Page is built with a services-oriented approach that utilizes different services to transform how end-users solve key tasks related to their transaction history. The primary benefits provided by the Account History Page include:

SOC Quick Guide

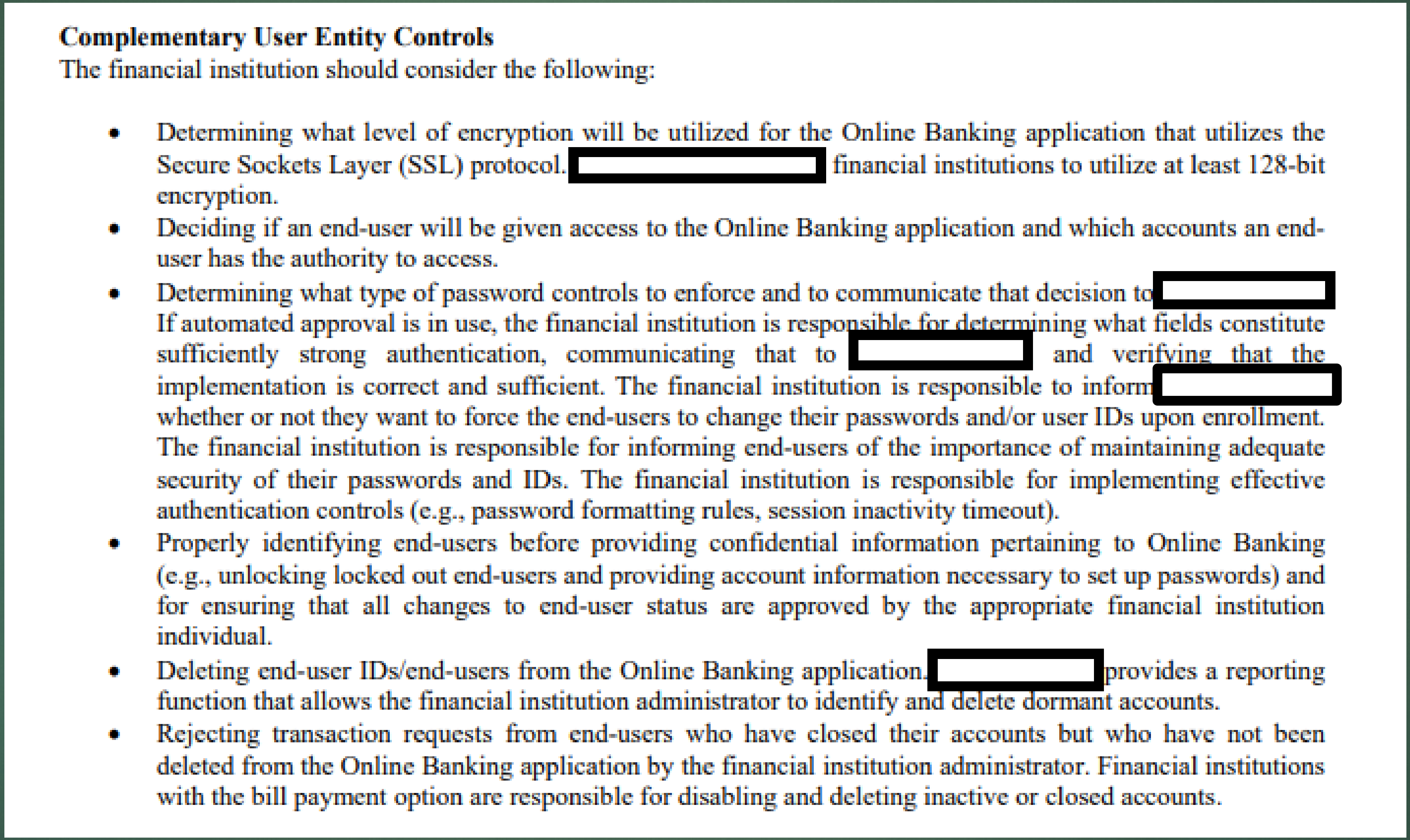


We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

[redacted] and [redacted] use Switch Communications Group LLC to provide data center hosting services for certain applications. [redacted] also uses Opay and FIS PayDirect, for payment processing. Our examination did not extend to controls of Switch Communications Group LLC, Opay and FIS PayDirect (carved out subservice organizations).

The information in the accompanying *Other Information Provided by* [redacted] is presented by management of [redacted] to provide additional information and is not part of the Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

SOC Quick Guide

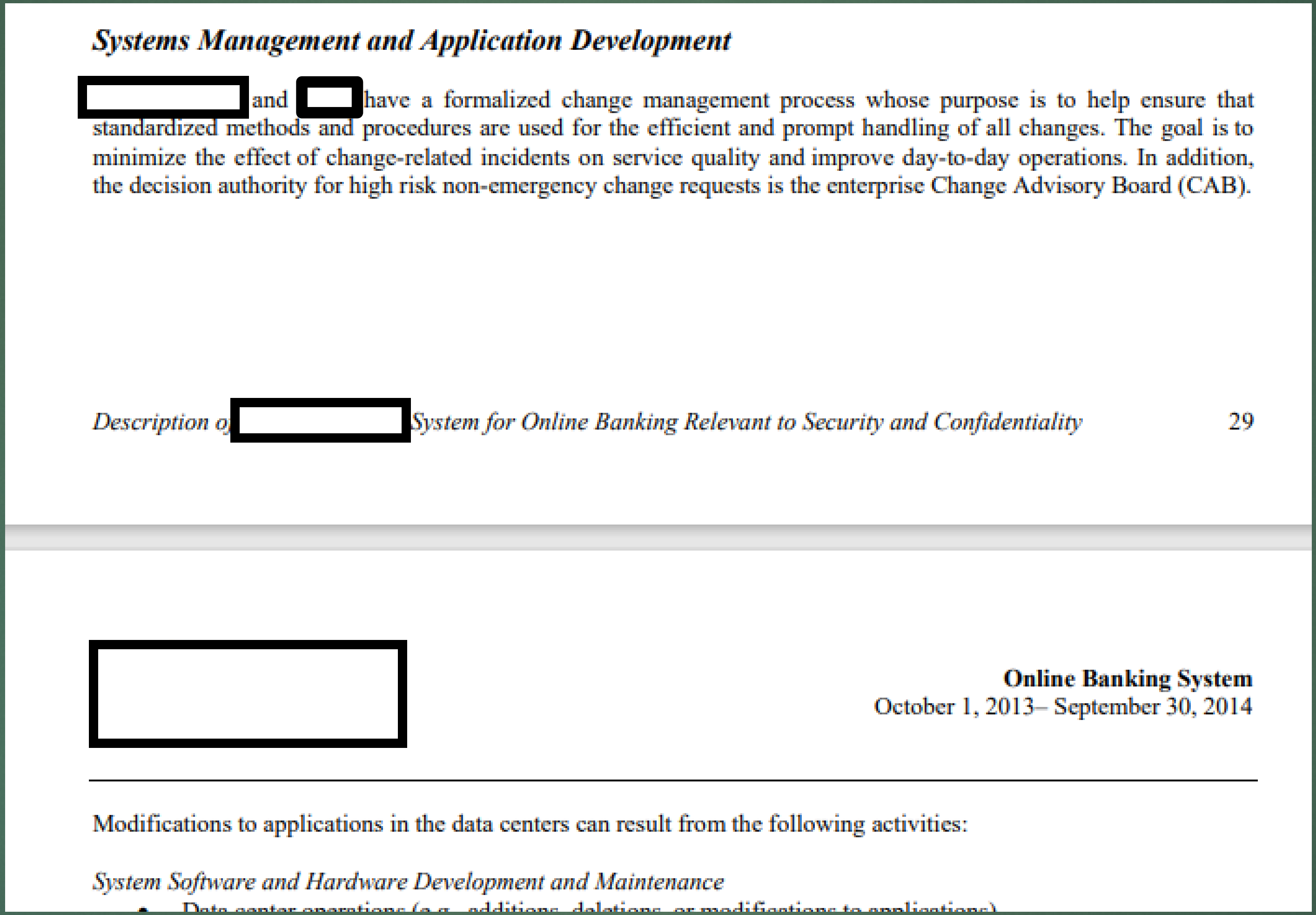


Complementary User Entity Controls

The financial institution should consider the following:

- Determining what level of encryption will be utilized for the Online Banking application that utilizes the Secure Sockets Layer (SSL) protocol. [redacted] financial institutions to utilize at least 128-bit encryption.
- Deciding if an end-user will be given access to the Online Banking application and which accounts an end-user has the authority to access.
- Determining what type of password controls to enforce and to communicate that decision to [redacted] If automated approval is in use, the financial institution is responsible for determining what fields constitute sufficiently strong authentication, communicating that to [redacted] and verifying that the implementation is correct and sufficient. The financial institution is responsible to inform [redacted] whether or not they want to force the end-users to change their passwords and/or user IDs upon enrollment. The financial institution is responsible for informing end-users of the importance of maintaining adequate security of their passwords and IDs. The financial institution is responsible for implementing effective authentication controls (e.g., password formatting rules, session inactivity timeout).
- Properly identifying end-users before providing confidential information pertaining to Online Banking (e.g., unlocking locked out end-users and providing account information necessary to set up passwords) and for ensuring that all changes to end-user status are approved by the appropriate financial institution individual.
- Deleting end-user IDs/end-users from the Online Banking application. [redacted] provides a reporting function that allows the financial institution administrator to identify and delete dormant accounts.
- Rejecting transaction requests from end-users who have closed their accounts but who have not been deleted from the Online Banking application by the financial institution administrator. Financial institutions with the bill payment option are responsible for disabling and deleting inactive or closed accounts.

SOC Quick Guide



Systems Management and Application Development

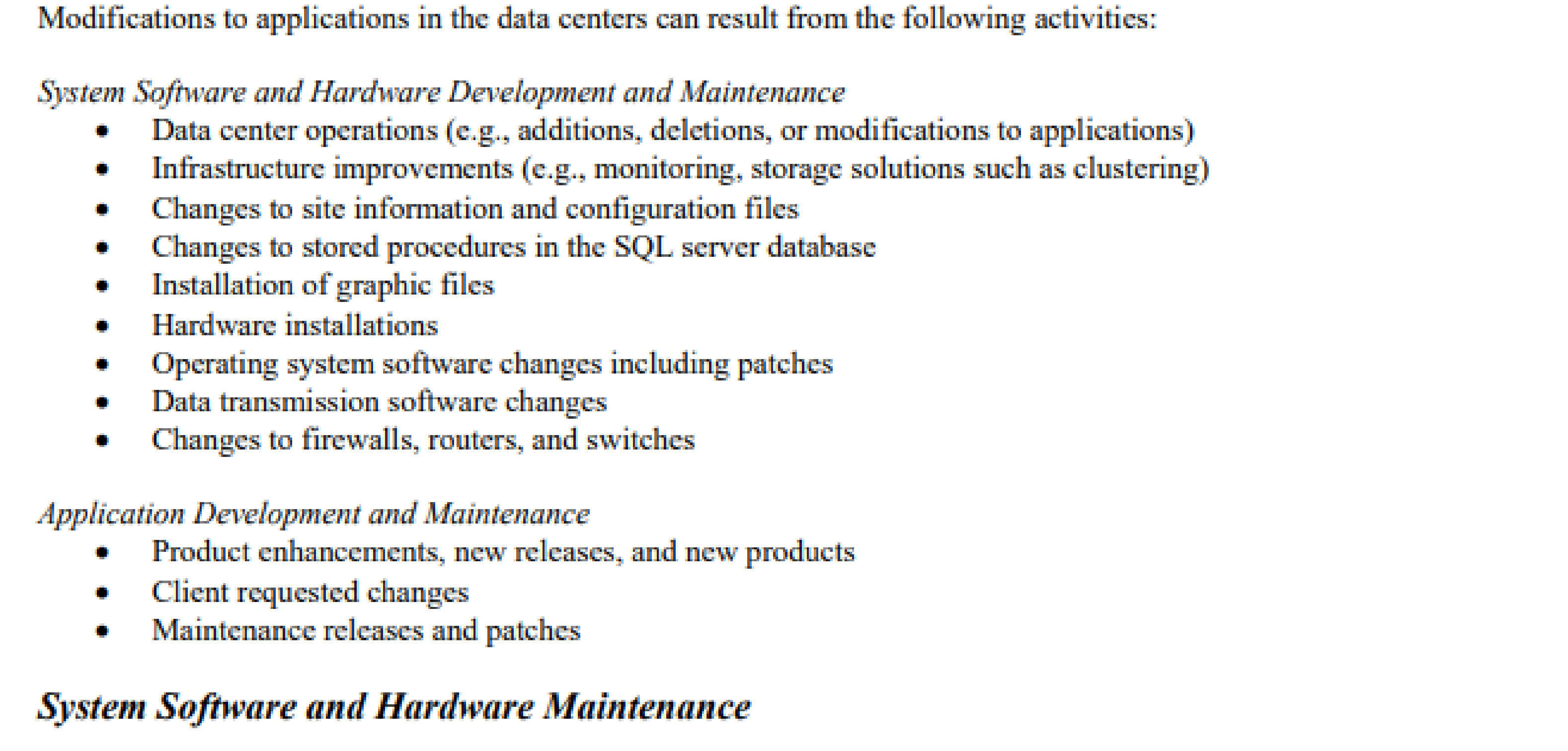
[redacted] and [redacted] have a formalized change management process whose purpose is to help ensure that standardized methods and procedures are used for the efficient and prompt handling of all changes. The goal is to minimize the effect of change-related incidents on service quality and improve day-to-day operations. In addition, the decision authority for high risk non-emergency change requests is the enterprise Change Advisory Board (CAB).

Modifications to applications in the data centers can result from the following activities:

System Software and Hardware Development and Maintenance

- Data center operations (e.g., additions, deletions, or modifications to applications)

SOC Quick Guide



Modifications to applications in the data centers can result from the following activities:

System Software and Hardware Development and Maintenance

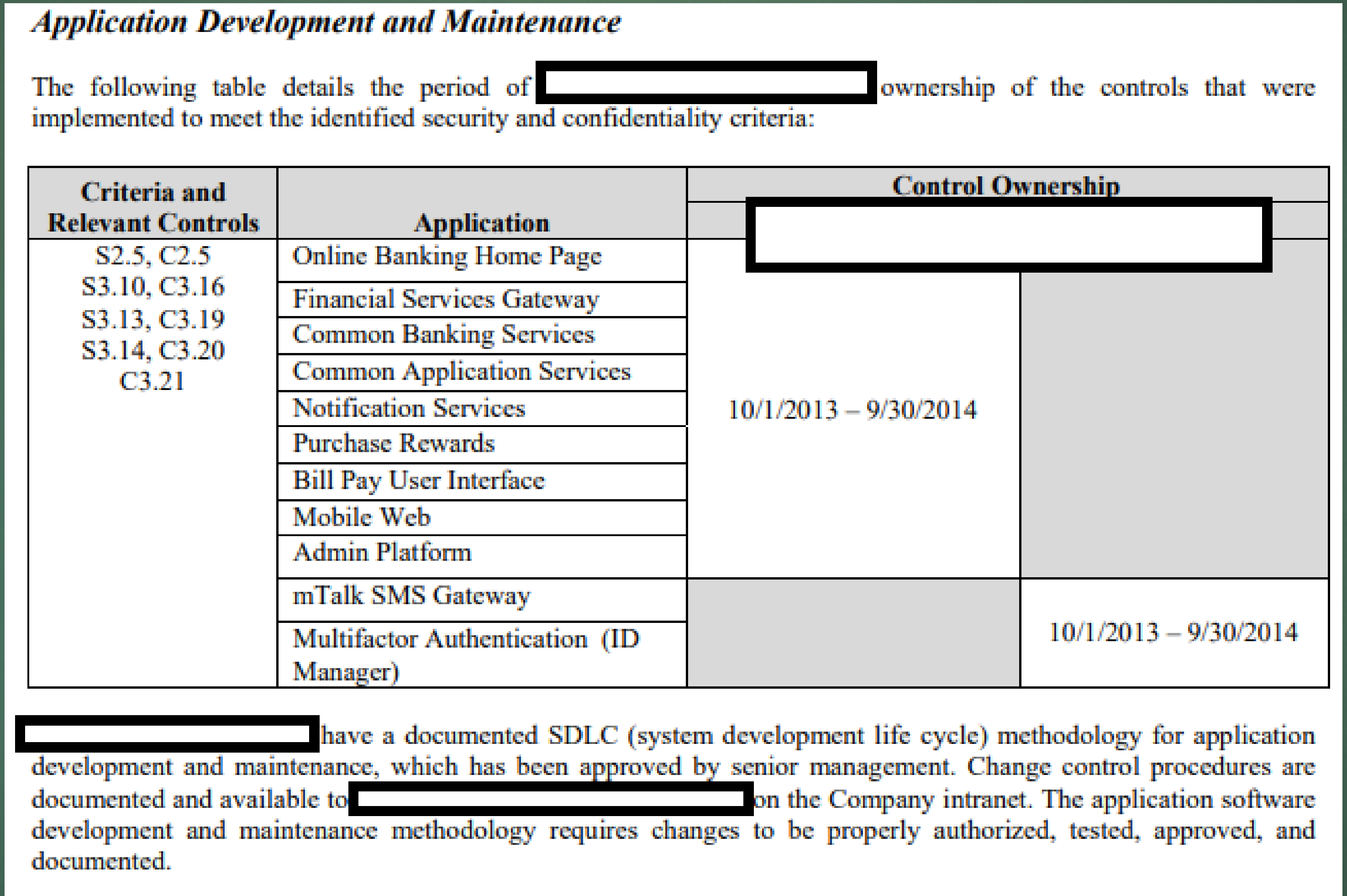
- Data center operations (e.g., additions, deletions, or modifications to applications)
- Infrastructure improvements (e.g., monitoring, storage solutions such as clustering)
- Changes to site information and configuration files
- Changes to stored procedures in the SQL server database
- Installation of graphic files
- Hardware installations
- Operating system software changes including patches
- Data transmission software changes
- Changes to firewalls, routers, and switches

Application Development and Maintenance

- Product enhancements, new releases, and new products
- Client requested changes
- Maintenance releases and patches

System Software and Hardware Maintenance

SOC Quick Guide



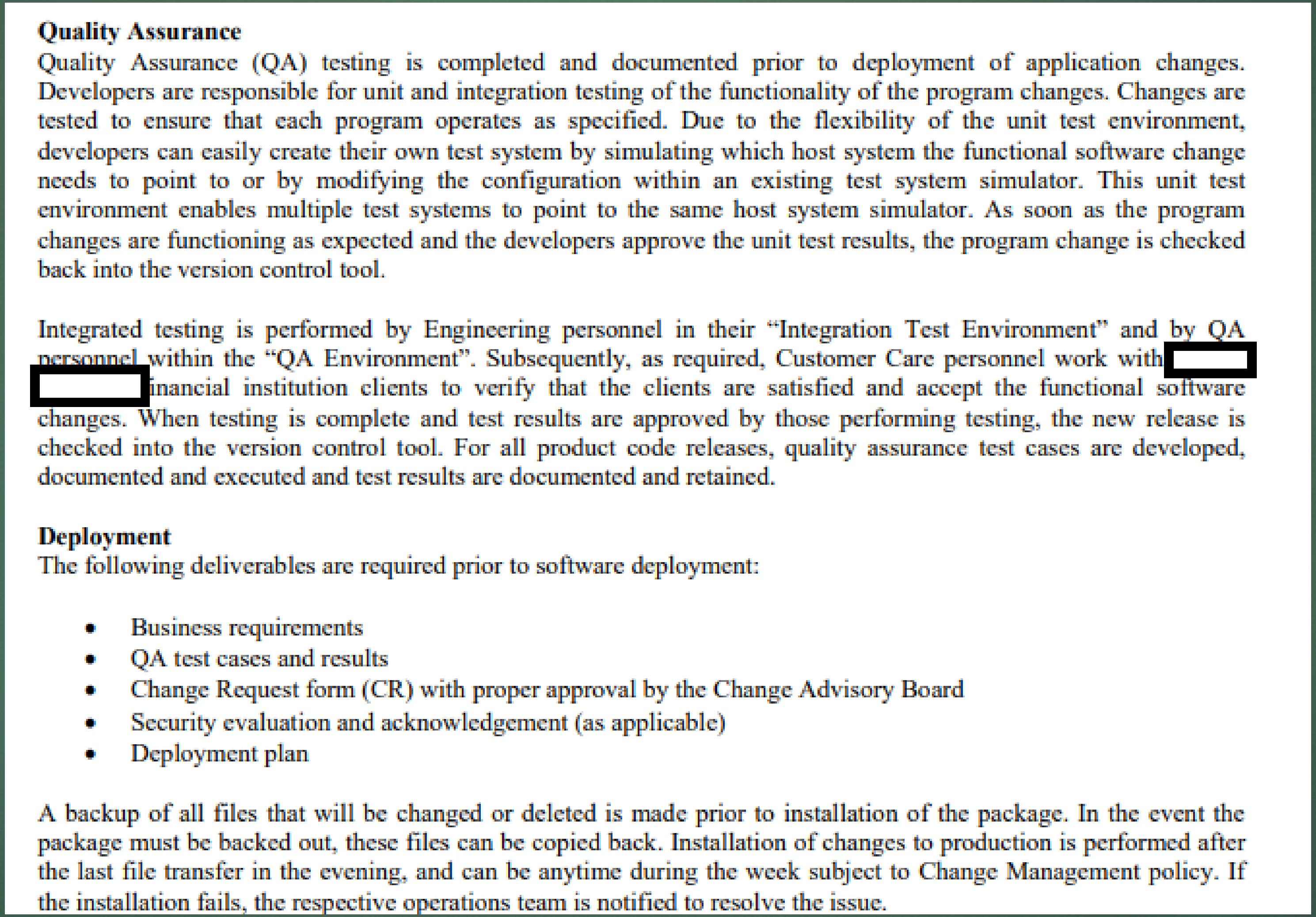
Application Development and Maintenance

The following table details the period of [redacted] ownership of the controls that were implemented to meet the identified security and confidentiality criteria:

Criteria and Relevant Controls	Application	Control Ownership	
		[redacted]	[redacted]
S2.5, C2.5 S3.10, C3.16 S3.13, C3.19 S3.14, C3.20 C3.21	Online Banking Home Page	10/1/2013 – 9/30/2014	
	Financial Services Gateway		
	Common Banking Services		
	Common Application Services		
	Notification Services		
	Purchase Rewards		
	Bill Pay User Interface		
	Mobile Web		
	Admin Platform		
	mTalk SMS Gateway		10/1/2013 – 9/30/2014
	Multifactor Authentication (ID Manager)		

[redacted] have a documented SDLC (system development life cycle) methodology for application development and maintenance, which has been approved by senior management. Change control procedures are documented and available to [redacted] on the Company intranet. The application software development and maintenance methodology requires changes to be properly authorized, tested, approved, and documented.

SOC Quick Guide



Quality Assurance

Quality Assurance (QA) testing is completed and documented prior to deployment of application changes. Developers are responsible for unit and integration testing of the functionality of the program changes. Changes are tested to ensure that each program operates as specified. Due to the flexibility of the unit test environment, developers can easily create their own test system by simulating which host system the functional software change needs to point to or by modifying the configuration within an existing test system simulator. This unit test environment enables multiple test systems to point to the same host system simulator. As soon as the program changes are functioning as expected and the developers approve the unit test results, the program change is checked back into the version control tool.

Integrated testing is performed by Engineering personnel in their "Integration Test Environment" and by QA personnel within the "QA Environment". Subsequently, as required, Customer Care personnel work with [redacted] [redacted]inancial institution clients to verify that the clients are satisfied and accept the functional software changes. When testing is complete and test results are approved by those performing testing, the new release is checked into the version control tool. For all product code releases, quality assurance test cases are developed, documented and executed and test results are documented and retained.

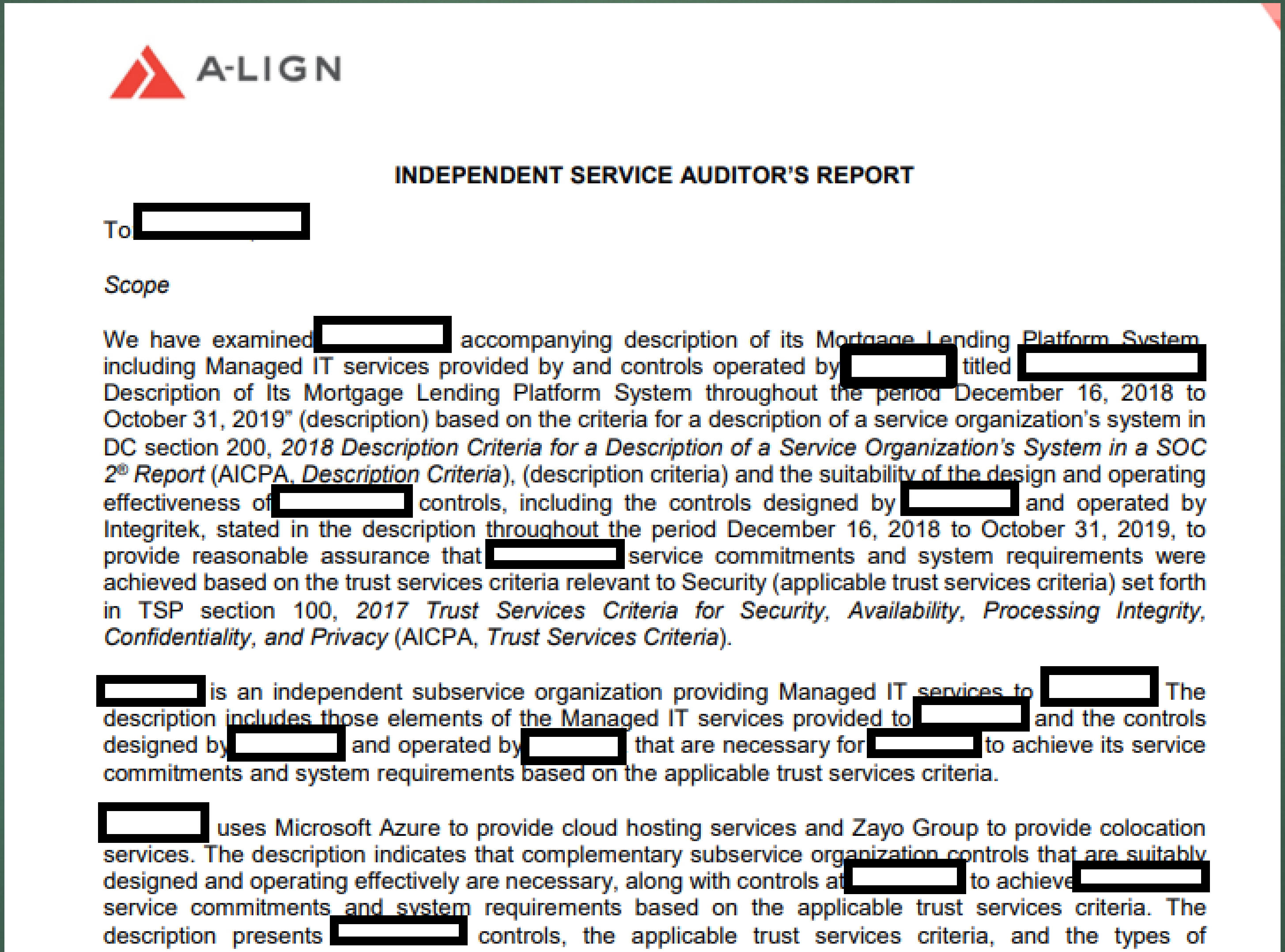
Deployment

The following deliverables are required prior to software deployment:

- Business requirements
- QA test cases and results
- Change Request form (CR) with proper approval by the Change Advisory Board
- Security evaluation and acknowledgement (as applicable)
- Deployment plan

A backup of all files that will be changed or deleted is made prior to installation of the package. In the event the package must be backed out, these files can be copied back. Installation of changes to production is performed after the last file transfer in the evening, and can be anytime during the week subject to Change Management policy. If the installation fails, the respective operations team is notified to resolve the issue.

Homework: Lending Platform



A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To [redacted]

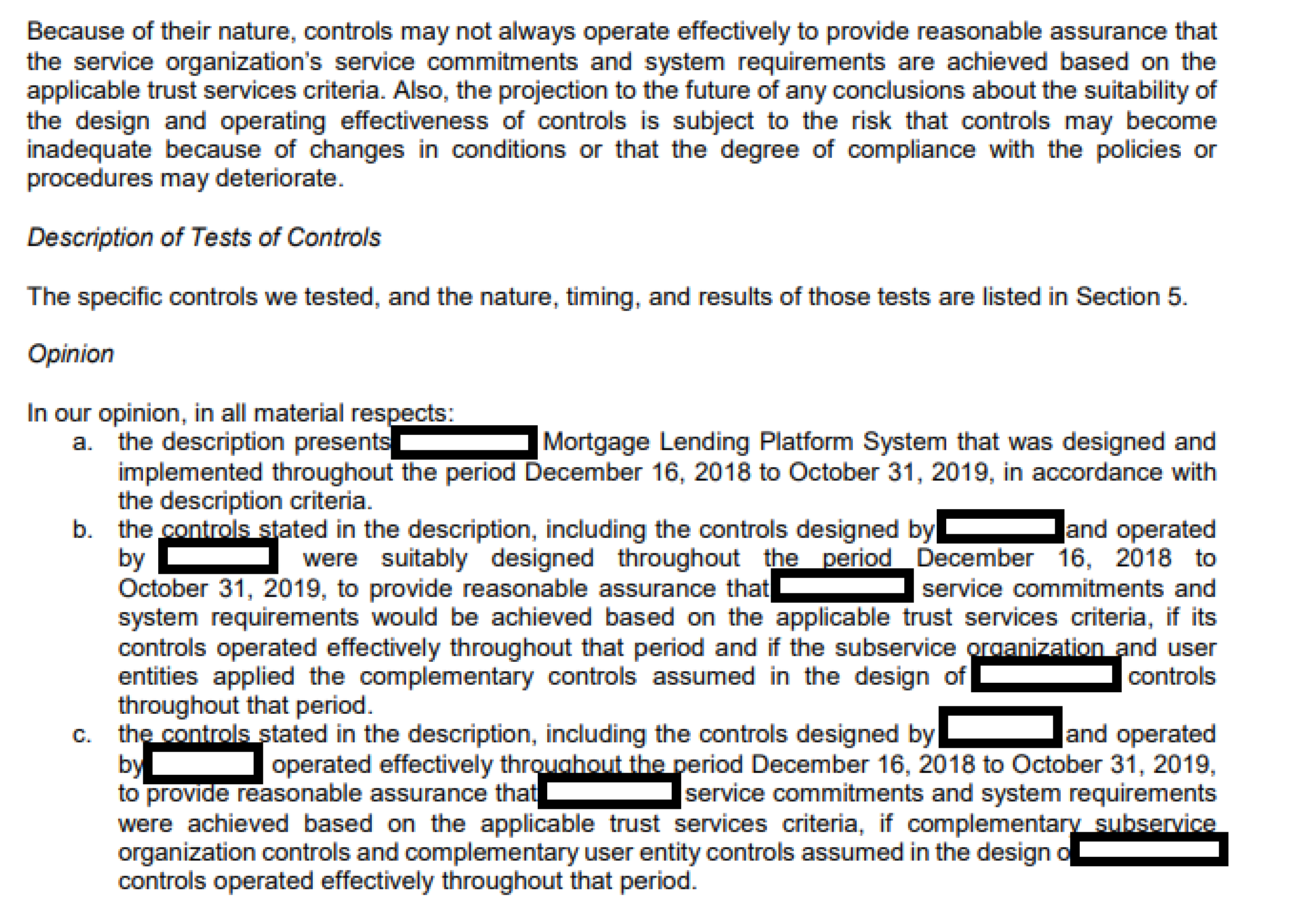
Scope

We have examined [redacted] accompanying description of its Mortgage Lending Platform System including Managed IT services provided by and controls operated by [redacted] titled [redacted] Description of Its Mortgage Lending Platform System throughout the period December 16, 2018 to October 31, 2019” (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 [redacted] controls, including the controls designed by [redacted] and operated by Integritek, stated in the description throughout the period December 16, 2018 to October 31, 2019, to provide reasonable assurance that [redacted] 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*).

[redacted] is an independent subservice organization providing Managed IT services to [redacted] The description includes those elements of the Managed IT services provided to [redacted] and the controls designed by [redacted] and operated by [redacted] that are necessary for [redacted] to achieve its service commitments and system requirements based on the applicable trust services criteria.

[redacted] uses Microsoft Azure to provide cloud hosting services and Zayo Group to provide colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at [redacted] to achieve [redacted] service commitments and system requirements based on the applicable trust services criteria. The description presents [redacted] controls, the applicable trust services criteria, and the types of

Homework: Lending Platform



Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 5.

Opinion

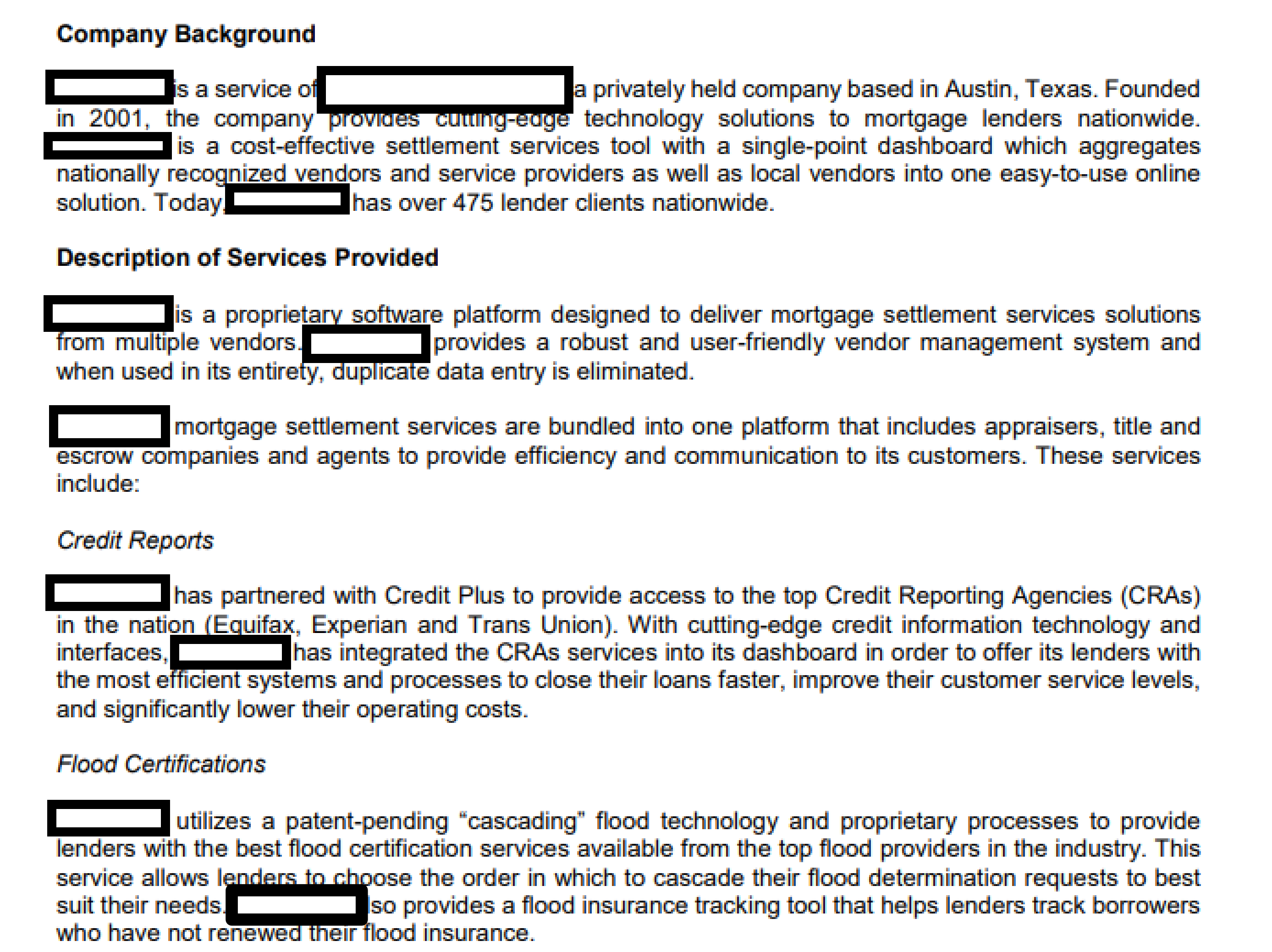
In our opinion, in all material respects:

a. the description presents [redacted] Mortgage Lending Platform System that was designed and implemented throughout the period December 16, 2018 to October 31, 2019, in accordance with the description criteria.

b. the controls stated in the description, including the controls designed by [redacted] and operated by [redacted] were suitably designed throughout the period December 16, 2018 to October 31, 2019, to provide reasonable assurance that [redacted] service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of [redacted] controls throughout that period.

c. the controls stated in the description, including the controls designed by [redacted] and operated by [redacted] operated effectively throughout the period December 16, 2018 to October 31, 2019, to provide reasonable assurance that [redacted] 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 o[redacted] controls operated effectively throughout that period.

Homework: Lending Platform



Company Background

[redacted] is a service of [redacted] a privately held company based in Austin, Texas. Founded in 2001, the company provides cutting-edge technology solutions to mortgage lenders nationwide. [redacted] is a cost-effective settlement services tool with a single-point dashboard which aggregates nationally recognized vendors and service providers as well as local vendors into one easy-to-use online solution. Today, [redacted] has over 475 lender clients nationwide.

Description of Services Provided

[redacted] is a proprietary software platform designed to deliver mortgage settlement services solutions from multiple vendors. [redacted] provides a robust and user-friendly vendor management system and when used in its entirety, duplicate data entry is eliminated.

[redacted] mortgage settlement services are bundled into one platform that includes appraisers, title and escrow companies and agents to provide efficiency and communication to its customers. These services include:

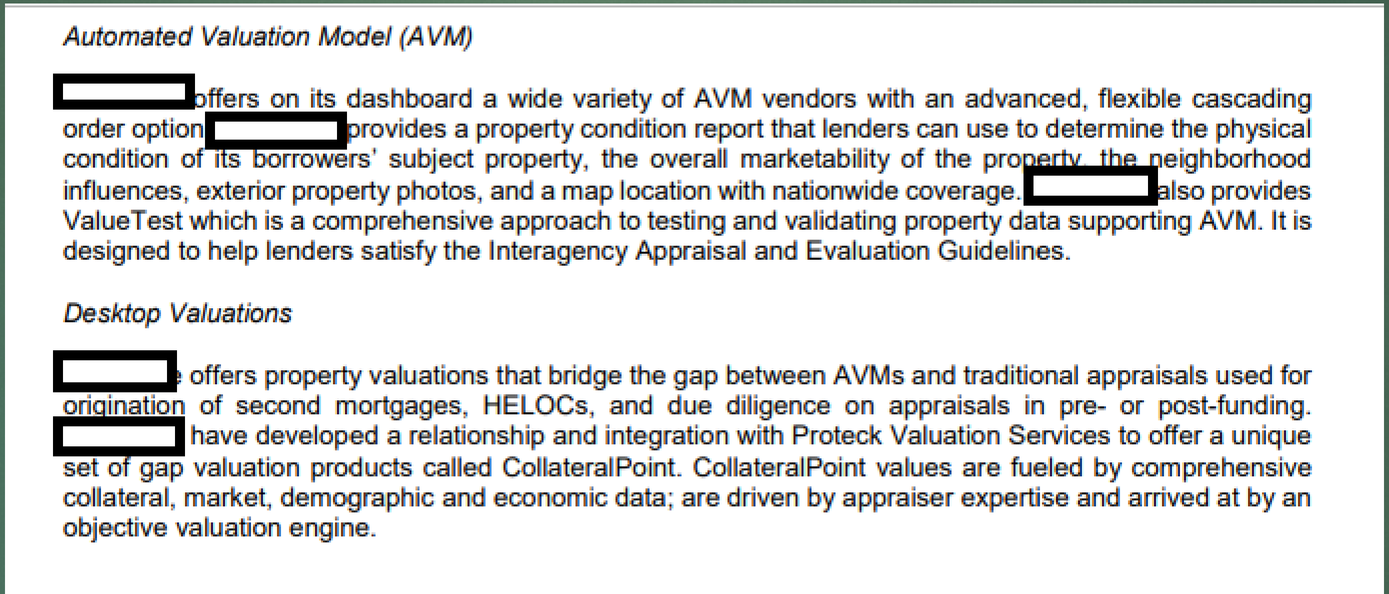
Credit Reports

[redacted] has partnered with Credit Plus to provide access to the top Credit Reporting Agencies (CRAs) in the nation (Equifax, Experian and Trans Union). With cutting-edge credit information technology and interfaces, [redacted] has integrated the CRAs services into its dashboard in order to offer its lenders with the most efficient systems and processes to close their loans faster, improve their customer service levels, and significantly lower their operating costs.

Flood Certifications

[redacted] utilizes a patent-pending "cascading" flood technology and proprietary processes to provide lenders with the best flood certification services available from the top flood providers in the industry. This service allows lenders to choose the order in which to cascade their flood determination requests to best suit their needs. [redacted] so provides a flood insurance tracking tool that helps lenders track borrowers who have not renewed their flood insurance.

Homework: Lending Platform



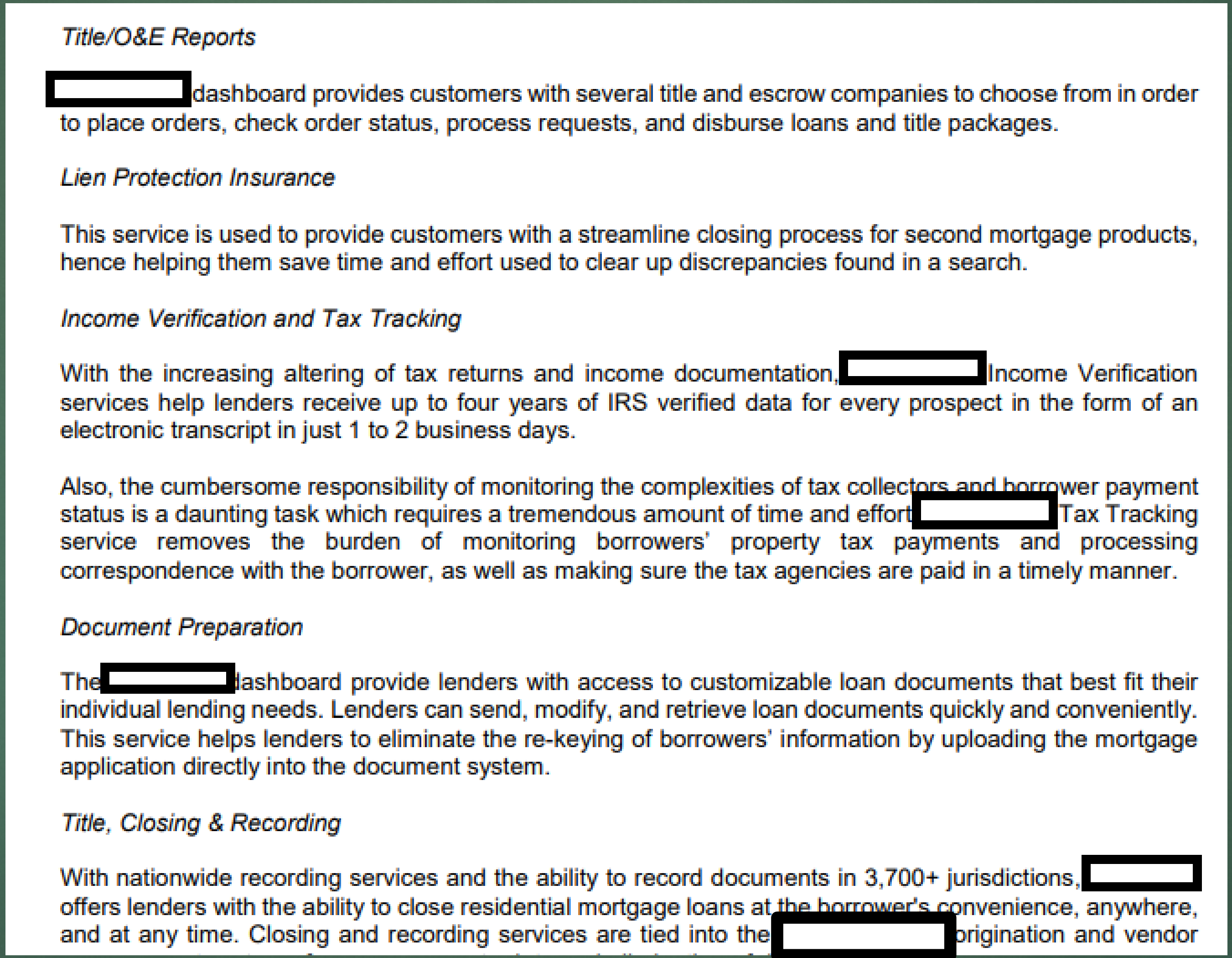
Automated Valuation Model (AVM)

[redacted] offers on its dashboard a wide variety of AVM vendors with an advanced, flexible cascading order option [redacted] provides a property condition report that lenders can use to determine the physical condition of its borrowers' subject property, the overall marketability of the property, the neighborhood influences, exterior property photos, and a map location with nationwide coverage. [redacted] also provides ValueTest which is a comprehensive approach to testing and validating property data supporting AVM. It is designed to help lenders satisfy the Interagency Appraisal and Evaluation Guidelines.

Desktop Valuations

[redacted] offers property valuations that bridge the gap between AVMs and traditional appraisals used for origination of second mortgages, HELOCs, and due diligence on appraisals in pre- or post-funding. [redacted] have developed a relationship and integration with Proteck Valuation Services to offer a unique set of gap valuation products called CollateralPoint. CollateralPoint values are fueled by comprehensive collateral, market, demographic and economic data; are driven by appraiser expertise and arrived at by an objective valuation engine.

Homework: Lending Platform



Title/O&E Reports

[redacted] dashboard provides customers with several title and escrow companies to choose from in order to place orders, check order status, process requests, and disburse loans and title packages.

Lien Protection Insurance

This service is used to provide customers with a streamline closing process for second mortgage products, hence helping them save time and effort used to clear up discrepancies found in a search.

Income Verification and Tax Tracking

With the increasing altering of tax returns and income documentation, [redacted] Income Verification services help lenders receive up to four years of IRS verified data for every prospect in the form of an electronic transcript in just 1 to 2 business days.

Also, the cumbersome responsibility of monitoring the complexities of tax collectors and borrower payment status is a daunting task which requires a tremendous amount of time and effort [redacted] Tax Tracking service removes the burden of monitoring borrowers' property tax payments and processing correspondence with the borrower, as well as making sure the tax agencies are paid in a timely manner.

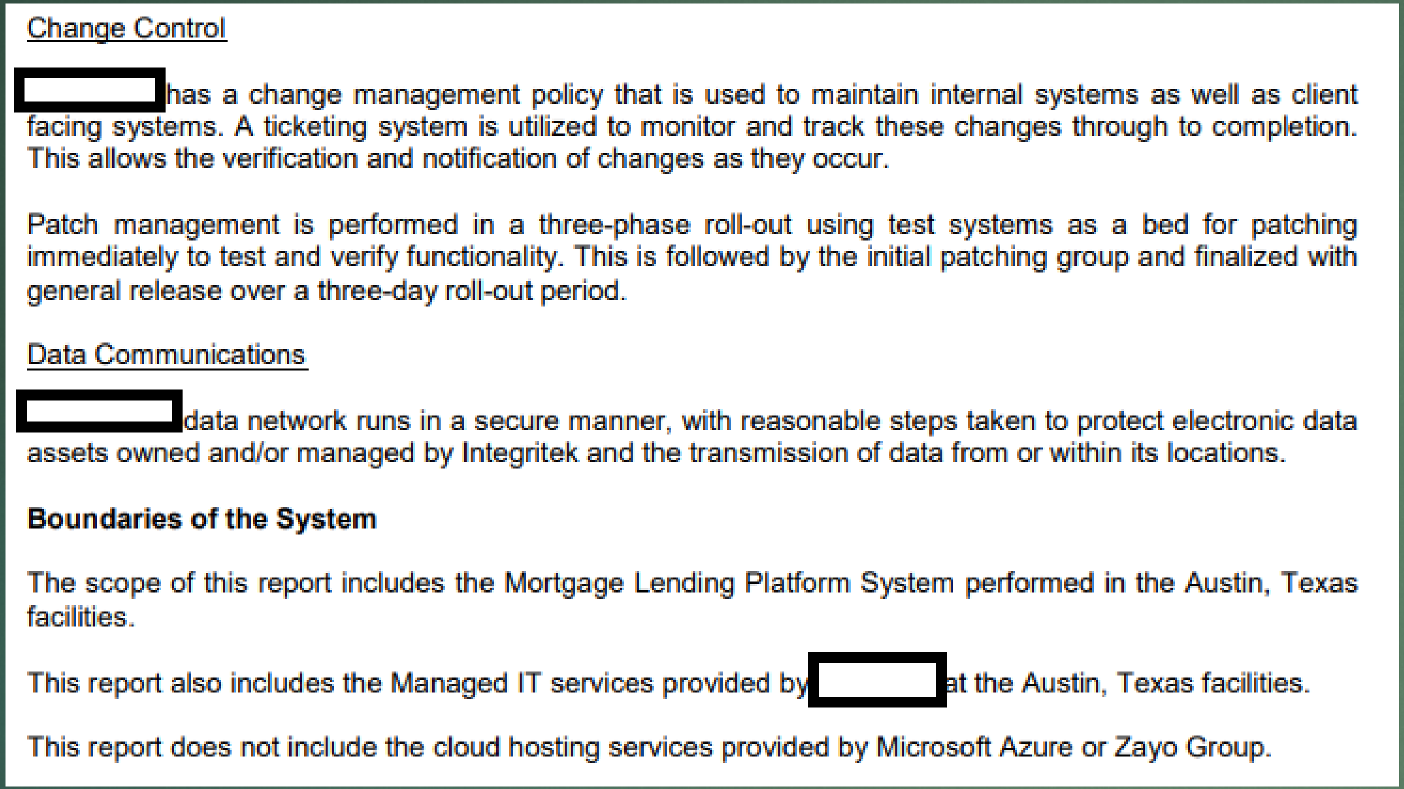
Document Preparation

The [redacted] dashboard provide lenders with access to customizable loan documents that best fit their individual lending needs. Lenders can send, modify, and retrieve loan documents quickly and conveniently. This service helps lenders to eliminate the re-keying of borrowers' information by uploading the mortgage application directly into the document system.

Title, Closing & Recording

With nationwide recording services and the ability to record documents in 3,700+ jurisdictions, [redacted] offers lenders with the ability to close residential mortgage loans at the borrower's convenience, anywhere, and at any time. Closing and recording services are tied into the [redacted] origination and vendor

Homework: Lending Platform



Change Control

[redacted] has a change management policy that is used to maintain internal systems as well as client facing systems. A ticketing system is utilized to monitor and track these changes through to completion. This allows the verification and notification of changes as they occur.

Patch management is performed in a three-phase roll-out using test systems as a bed for patching immediately to test and verify functionality. This is followed by the initial patching group and finalized with general release over a three-day roll-out period.

Data Communications

[redacted] data network runs in a secure manner, with reasonable steps taken to protect electronic data assets owned and/or managed by Integritek and the transmission of data from or within its locations.

Boundaries of the System

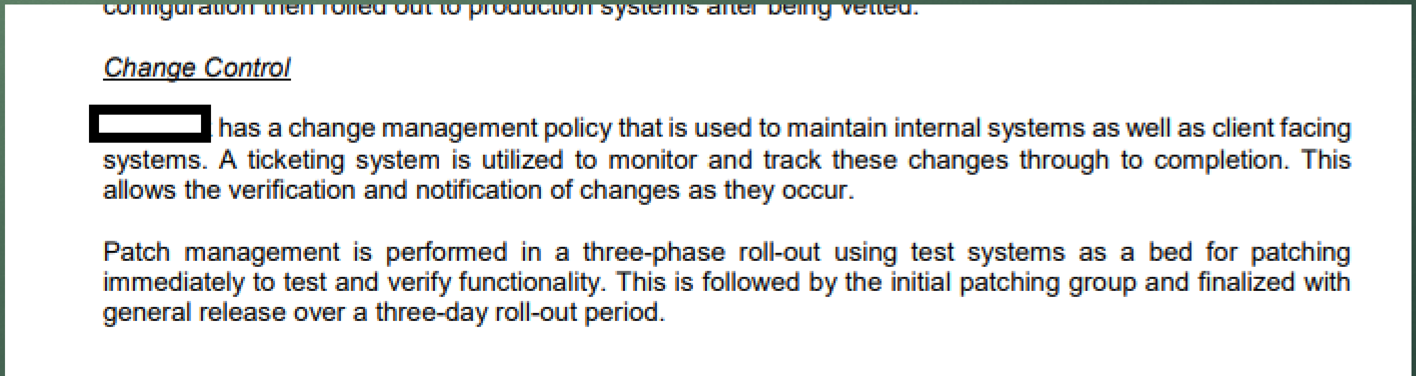
The scope of this report includes the Mortgage Lending Platform System performed in the Austin, Texas facilities.

This report also includes the Managed IT services provided by [redacted] at the Austin, Texas facilities.

This report does not include the cloud hosting services provided by Microsoft Azure or Zayo Group.

Primary Vendor

Secondary Vendor



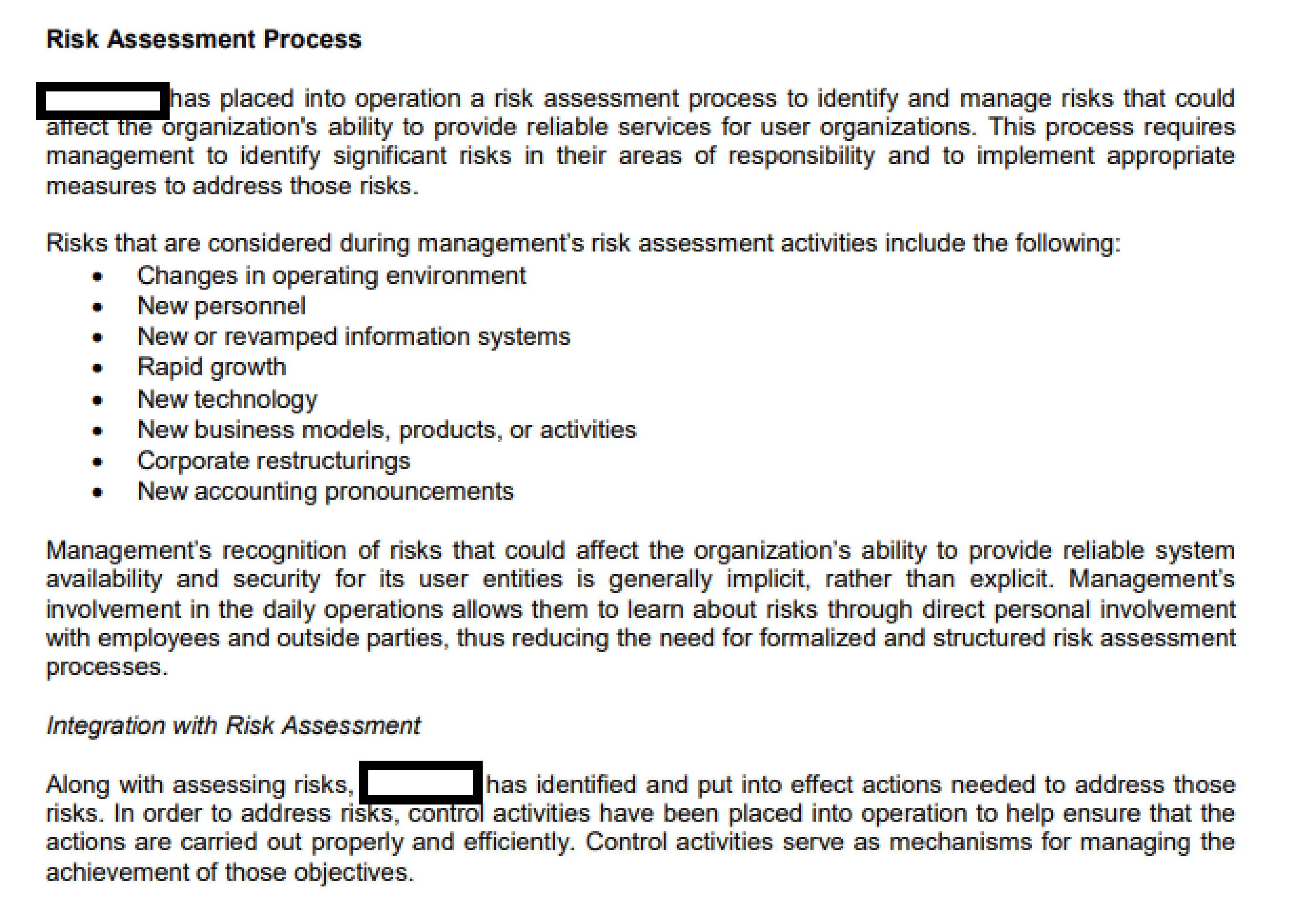
configuration then rolled out to production systems after being vetted.

Change Control

[redacted] has a change management policy that is used to maintain internal systems as well as client facing systems. A ticketing system is utilized to monitor and track these changes through to completion. This allows the verification and notification of changes as they occur.

Patch management is performed in a three-phase roll-out using test systems as a bed for patching immediately to test and verify functionality. This is followed by the initial patching group and finalized with general release over a three-day roll-out period.

Homework: Lending Platform



Risk Assessment Process

[redacted] has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable services for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks.

Risks that are considered during management's risk assessment activities include the following:

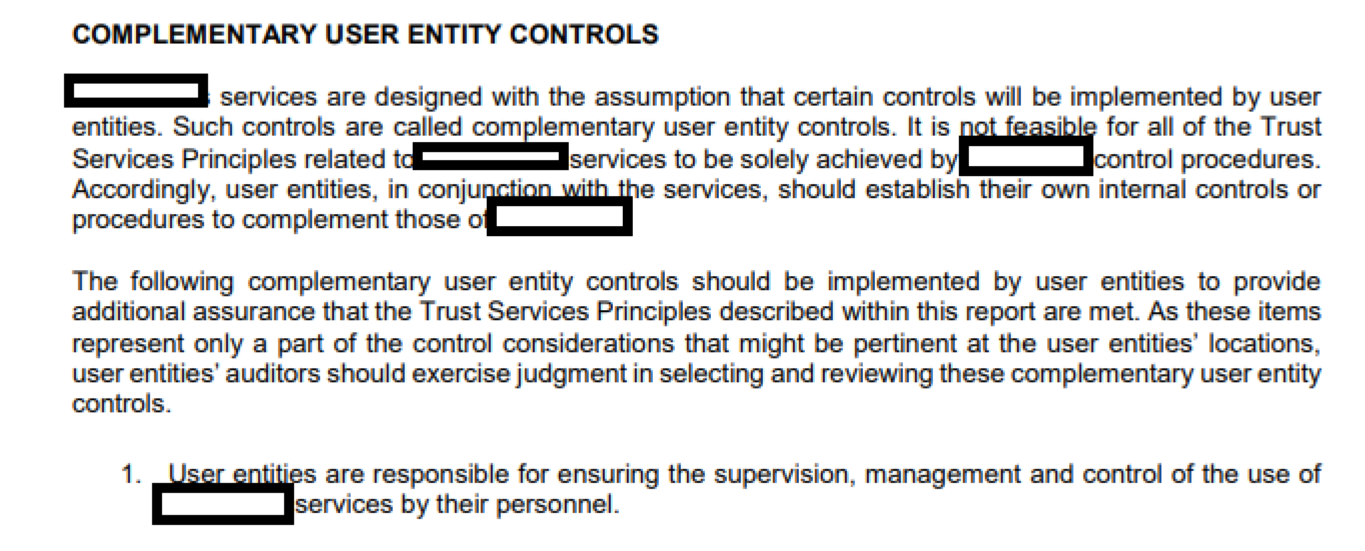
- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New business models, products, or activities
- Corporate restructurings
- New accounting pronouncements

Management's recognition of risks that could affect the organization's ability to provide reliable system availability and security for its user entities is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

Integration with Risk Assessment

Along with assessing risks, [redacted] has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Homework: Lending Platform

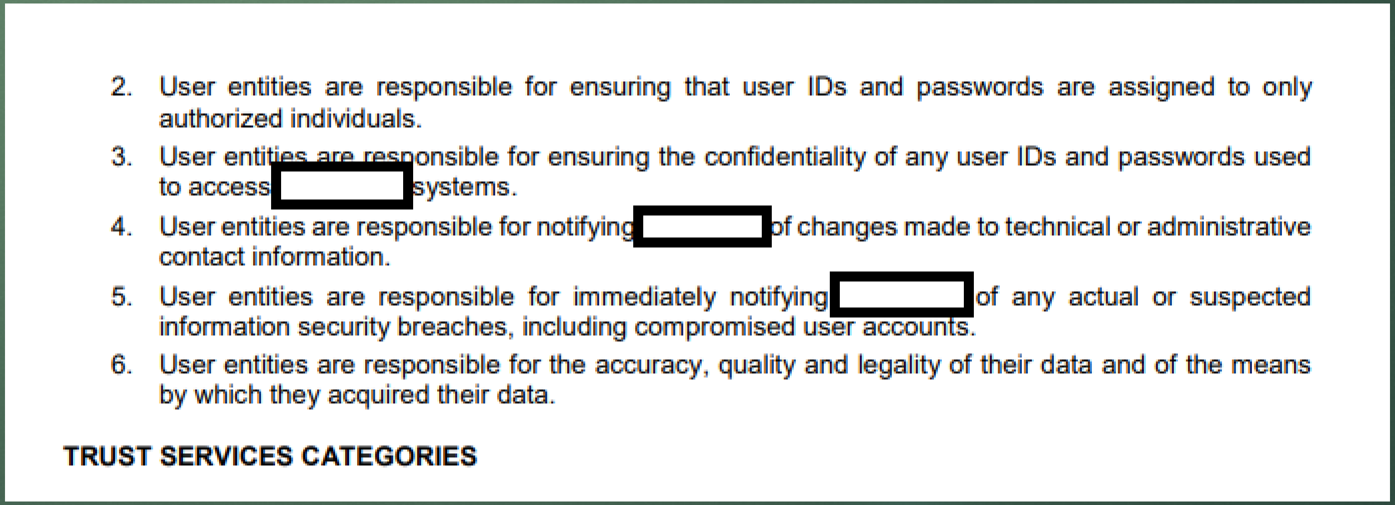


COMPLEMENTARY USER ENTITY CONTROLS

[redacted] services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to [redacted] services to be solely achieved by [redacted] control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of [redacted]

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

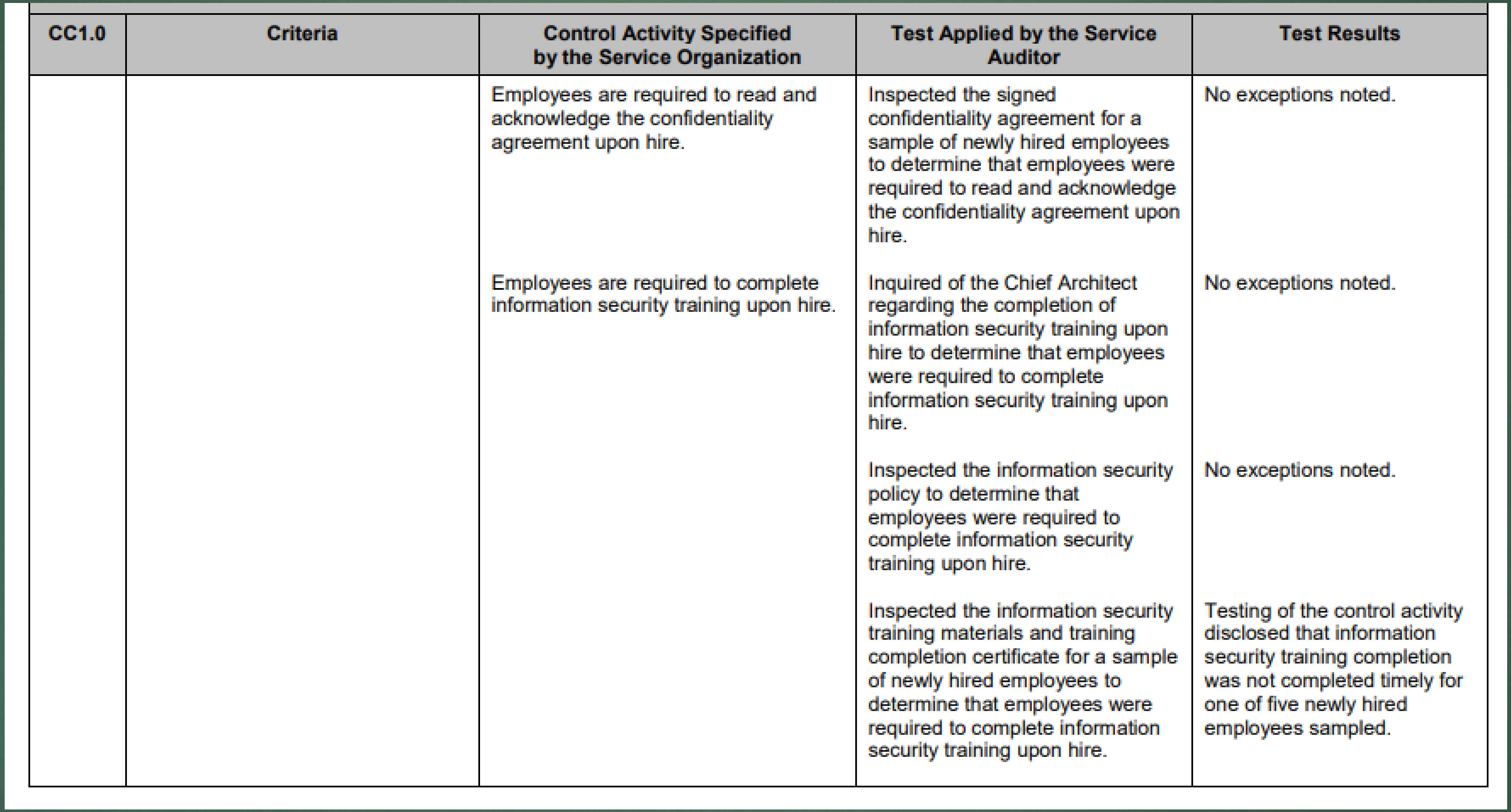
1. User entities are responsible for ensuring the supervision, management and control of the use of [redacted] services by their personnel.



2. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
3. User entities are responsible for ensuring the confidentiality of any user IDs and passwords used to access [redacted] systems.
4. User entities are responsible for notifying [redacted] of changes made to technical or administrative contact information.
5. User entities are responsible for immediately notifying [redacted] of any actual or suspected information security breaches, including compromised user accounts.
6. User entities are responsible for the accuracy, quality and legality of their data and of the means by which they acquired their data.

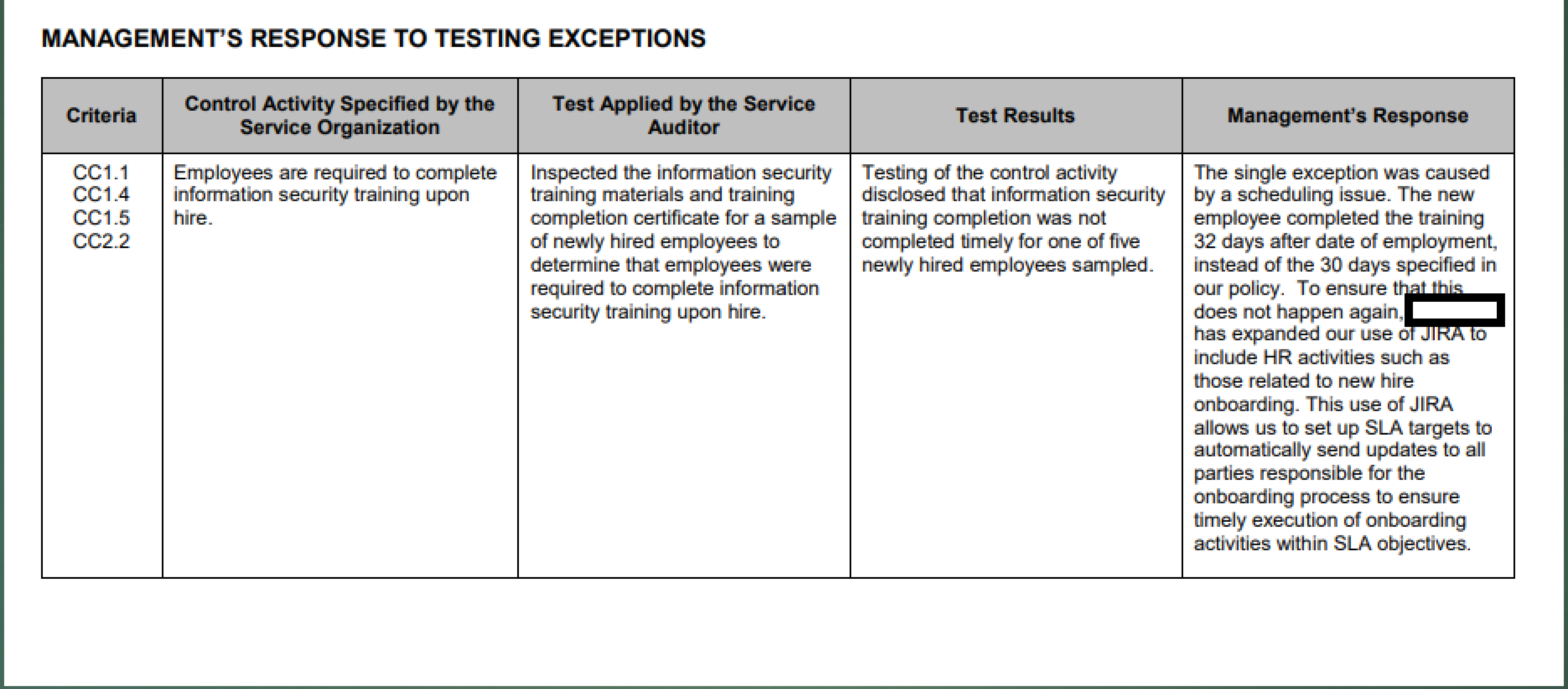
TRUST SERVICES CATEGORIES

Homework: Lending Platform



CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Employees are required to read and acknowledge the confidentiality agreement upon hire.	Inspected the signed confidentiality agreement for a sample of newly hired employees to determine that employees were required to read and acknowledge the confidentiality agreement upon hire.	No exceptions noted.
		Employees are required to complete information security training upon hire.	Inquired of the Chief Architect regarding the completion of information security training upon hire to determine that employees were required to complete information security training upon hire.	No exceptions noted.
			Inspected the information security policy to determine that employees were required to complete information security training upon hire.	No exceptions noted.
			Inspected the information security training materials and training completion certificate for a sample of newly hired employees to determine that employees were required to complete information security training upon hire.	Testing of the control activity disclosed that information security training completion was not completed timely for one of five newly hired employees sampled.

Homework: Lending Platform



MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1 CC1.4 CC1.5 CC2.2	Employees are required to complete information security training upon hire.	Inspected the information security training materials and training completion certificate for a sample of newly hired employees to determine that employees were required to complete information security training upon hire.	Testing of the control activity disclosed that information security training completion was not completed timely for one of five newly hired employees sampled.	The single exception was caused by a scheduling issue. The new employee completed the training 32 days after date of employment, instead of the 30 days specified in our policy. To ensure that this does not happen again, [redacted] has expanded our use of JIRA to include HR activities such as those related to new hire onboarding. This use of JIRA allows us to set up SLA targets to automatically send updates to all parties responsible for the onboarding process to ensure timely execution of onboarding activities within SLA objectives.