

Intuit Employee Management Solutions

Service Organization Control Report
Report on Controls Placed in Operation and Tests of
Operating Effectiveness
Includes Selected Controls for the Payroll Plus and
Payroll Basic Applications

For the Period
November 1, 2011, to October 31, 2012

I. Independent Service Auditor’s Report..... 1

II. Intuit Employee Management Solutions’ Assertion 4

III. Description of Intuit Employee Management Solutions’ System . 6

Company Description..... 6

 Scope..... 6

 Overview..... 6

 Services..... 6

 Summary of Payroll Services 7

Relevant Aspects of the Control Environment, Risk Management and Monitoring 8

 Control Environment..... 8

 Risk Management..... 11

 Monitoring..... 11

Information and Communication 11

Application Controls 12

 Payroll, Processing..... 12

 Authorization..... 13

 Office of Foreign Asset Control 14

General Computer Controls 15

 Computer and Network Operations 15

 Application and Systems Software and Infrastructure Acquisition, and/or Development and Maintenance 15

 Logical Access..... 18

 Physical Security and Environmental Controls..... 19

 Subservice Organizations..... 20

Complementary User Entity Controls..... 20

IV. Intuit Employee Management Solutions’ Control Objectives and Related Controls and McGladrey LLP’s Tests of Controls and Results of Tests..... 21

Control Environment, Risk Assessment and Monitoring..... 21

Logical Access 23

Systems Development and Change Management 25

Application and Business Process..... 26



I. Independent Service Auditor's Report

Management of Intuit Employee Management Solutions Service Organization
Mountain View, California

Scope

We have examined the Intuit Employee Management Solutions' description of its Payroll Basic and Payroll Plus systems for processing user entities' transactions throughout the period November 1, 2011, to October 31, 2012 (the description), and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Intuit Employee Management Solutions' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Intuit Employee Management Solutions uses Coresite, Inc. in San Jose, California, and Digital Reality, Inc. in Phoenix, Arizona, for computerized hosting facilities, including the supply of power, data connectivity and secured space. The description includes only the controls and related control objectives of Intuit Employee Management Solutions and excludes the control objectives and related controls of the subservicing organizations. Our examination did not extend to controls of these subservicing organizations.

Service Organization's Responsibilities

In Section 2 of this report, Intuit Employee Management Solutions has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Intuit Employee Management Solutions is responsible for preparing the description and for the assertion, including the completeness, accuracy and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria and designing, implementing and documenting the controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2011, to October 31, 2012.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein and the suitability criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Intuit Employee Management Solutions' assertion in Section 2 of this report:

- a) The description fairly presents the Payroll Basic and Payroll Plus systems that were designed and implemented throughout the period November 1, 2011, to October 31, 2012.
- b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the period November 1, 2011, to October 31, 2012, and user entities applied the complementary user entity controls contemplated in the design of Intuit Employee Management Solutions' controls throughout the period November 1, 2011, to October 31, 2012.
- c) The controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period November 1, 2011, to October 31, 2012.

Description of Tests of Controls

The specific controls that were tested and the nature, timing and results of those tests are listed in Section 4 of this report.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of Intuit Employee Management Solutions, user entities of Intuit Employee Management Solutions' Payroll Basic and Payroll Plus systems, during some or all of the period November 1, 2011, to October 31, 2012, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by customers themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

McGladrey LLP

January 10, 2013
San Francisco, California

II. Intuit Employee Management Solutions' Assertion

We have prepared the accompanying description of Intuit Employee Management Solutions' Payroll Basic and Payroll Plus systems for user entities of the system during some or all of the period November 1, 2011 to October 31, 2012, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- A. The description fairly presents the Payroll Basic and Payroll Plus systems made available to user entities of the systems during some or all of the period November 1, 2011 to October 31, 2012, for processing their transactions. Intuit Employee Management Solutions uses Coresite, Inc. in San Jose, California, and Digital Reality, Inc. in Phoenix, Arizona, for computerized hosting facilities, including the supply of power, data connectivity and secured space. The description includes only the controls and related control objectives of Intuit Employee Management Solutions and excludes the control objectives and related controls of the subservicing organizations. The criteria we used in making this assertion were that the accompanying description:
1. Presents how the system made available to user entities was designed and implemented to process relevant transactions, including
 - The classes of transactions processed
 - The procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary and transferred to the reports presented to user entities of the system
 - The related accounting records, supporting information and specific accounts involved in initiating, authorizing, recording, processing and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to customers of the system
 - How the system captures and addresses significant events and conditions, other than transactions
 - The process used to prepare reports or other information provided to user entities of the system
 - Specified control objectives and controls designed to achieve those objectives including complementary user entity's controls contemplated in the design of our controls
 - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that are relevant to processing and reporting transactions of user entities of the system
 2. Does not omit or distort information relevant to the scope of the Payroll Basic and Payroll Plus systems, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Payroll Basic and Payroll Plus systems that each individual user entity of the system and its auditor may consider important in its own particular environment.

3. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.
- B. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period November 1, 2011 to October 31, 2012, to achieve the control objectives stated and subservice organizations applied the controls contemplated in the design of Intuit Employee Management Solutions' controls. The criteria we used in making this assertion were that:
1. The risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization.
 2. The controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
 3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

III. Description of Intuit Employee Management Solutions' System

Company Description

Scope

The scope of this report includes the general computer controls and the business process controls related to Intuit Employee Management's Payroll Basic and Payroll Plus system.

Overview

Intuit Employee Management Solutions' (or Intuit's) Employee Management Services (EMS) division, headquartered in Mountain View, California, develops and hosts Web-based payroll management solutions targeted toward small business. The division's mission is to make payroll so easy that the Intuit Online Payroll application becomes the standard for very small businesses. Intuit's Do-It-With-You technology platform guides customers through the entire payroll process, from paychecks to W-2s, reducing the complexity and cost of payroll management. Products, Payroll Basic and Payroll Plus are delivered via the Web. In addition, the Company provides an online payroll solution for financial institutions. There are approximately 700 Intuit EMS employees globally, and more than 200,000 small businesses use Intuit Online Payroll to perform their payroll activities.

The Intuit Online Payroll application is a proprietary payroll package designed for utilization by a variety of businesses in varying industries. It allows customers the ability to manage payroll from an Internet connection, whether it is in the customer's work location, residence or other location. Intuit Online Payroll prompts customers to enter initial setup information. Then, on an ongoing basis, customers enter data to initiate payroll processing tasks. Intuit Online Payroll's functionality offers customers features for calculating hourly and salaried employee payrolls, other payments, employee expense reimbursements and third-party payment processing of nontax withholdings (e.g., garnishments, 401(k) contributions, union dues). Customers print paychecks or pay stubs using their own printing equipment. The service can also provide support for federal and state payroll tax management. Payroll tax withholding information can be transmitted for tax payment and reporting. Intuit Online Payroll also generates additional reports and has integration options for third-party accounting applications.

Customers' payroll transactions are processed at a third-party data center location in Phoenix, Arizona, with redundant, mirrored backup in San Jose, California.

Services

Intuit Online Payroll offers the following services:

Payroll Basic

Payroll Basic customers have the ability to set up their employees in the Intuit Online Payroll application and process employee payrolls, including the calculation of state, federal and local tax withholdings and voluntary deductions (such as retirement plan, insurance premiums, etc.). Paychecks and/or legal pay stubs are printed by customers at their location. Direct deposit payments are also available, as is an employee self-service website to retrieve pay stubs.

The Intuit Online Payroll application sends the customer email reminders. The emails include links directing them to the Intuit Online Payroll application to perform payday steps.

Payroll Basic has federal tax payment and filing support, including federal tax deposit and filing reminders, electronic one-click federal tax payments and the creation of signature-ready federal tax forms (941s, 940s and W-2s). Customers can also pull payroll reports from the application, including employer reports and employee detail reports, and they have the ability to drill-down into report details through the application. Intuit Online Payroll's Payroll Basic also has the ability to create one-click Microsoft Excel exports from the application along with accounting and bookkeeping software integration (e.g., Intuit QuickBooks, Microsoft Money).

Payroll Plus

In addition to those features described for Payroll Basic services, Payroll Plus adds the ability to make 1099 contractor payments. It also supports state tax management (including state tax deposit and filing email reminders), electronic one-click state tax payments, signature-ready state tax forms or guiding worksheets, signature-ready state new hire and step-by-step employer registration forms, electronic state form filing, multiple state tax payroll calculations for employees residing in a state different than the Company location, and complete federal and state payroll tax calculations for employees at additional work locations in any state.

Summary of Payroll Services

	Payroll Plus	Payroll Basic
Payday		
Payday email reminders	✓	✓
Guaranteed federal, state and local tax calculations	✓	✓
Voluntary deductions (retirement plans, insurance premiums, etc.)	✓	✓
Pay types: salary, hourly wages, multiple pay rates, overtime (OT), double OT, tips, commissions, bonuses, reimbursements, allowances and holidays	✓	✓
Vacation and sick days	✓	✓
Professional paycheck and pay stub printing from your own computer	✓	✓
Direct deposit	✓	✓
Payments to contractors	✓	
Customer Service		
Live toll-free or email support with top-rated payroll experts	✓	✓
Payroll Reports		
Eight different employer payroll reports	✓	✓
Five different employee detail reports	✓	✓
Drill-down access to report details	✓	✓
One-click Microsoft Excel export	✓	✓
Two different contractor detail reports	✓	
Accounting and Bookkeeping Software Integration		
QuickBooks, QuickBooks Online Edition, Microsoft Money, CCH ProSystems fx Write-up and the entire ATX accounting products suite	✓	✓

	Payroll Plus	Payroll Basic
Federal Payroll Taxes		
Federal tax deposit and filing email reminders	✓	✓
Electronic, one-click federal tax payments	✓	✓
Signature-ready federal forms (941s, 940s and W-2s)	✓	✓
Electronic federal form tax filings (941s, 940s and W-2s)	✓	✓
State Payroll Taxes		
State tax deposit and filing email reminders	✓	
Electronic, one-click state tax payments	✓	
Signature-ready state forms or guiding worksheets	✓	
Signature-ready state new hire and step-by-step employer registration forms	✓	
Electronic state form filings	✓	
Multiple State Withholding Calculations		
State tax payroll calculation for employees residing in a state different than company location	✓	
Additional Worksites		
Complete federal and state payroll tax calculations for employees at additional work locations in any state	✓	

Relevant Aspects of the Control Environment, Risk Management and Monitoring

Control Environment

Organization

The Intuit EMS division is part of a publicly held company of approximately 8,000 personnel at its locations in Mountain View, California, Reno, Nevada, and Arlington Heights, Illinois. The board of directors is responsible for overseeing the strategies followed by the Company and meets regularly to monitor Company progress.

The individuals comprising Intuit’s board of directors during the audit period include:

<u>Individual</u>	<u>Position</u>
Bill Campbell	Chairman of the Board
Chris Brody	Board Member
Diane Greene	Board Member
Mike Hallman	Board Member
Edward Kangas	Board Member
Suzanne Nora Johnson	Board Member
Dennis Powell	Board Member
Brad Smith	Board Member, President and Chief Executive Officer
Scott Cook	Board Member, Founder and Chairman of the Executive Committee

The EMS division's management has the primary responsibility to set the strategic direction of the Intuit Online Payroll offering and to develop, maintain and document adequate internal and compliance controls, and provides oversight to relevant Intuit operations. A formal management organizational structure exists with segregated levels of reporting and accountability. Management is responsible for directing and controlling Company operations, including establishment and communication of Company policies and procedures. The organization is designed to provide maximum oversight of control effectiveness and to verify that continuous quality feedback from Company employees and managers is incorporated into the enterprise and control environment.

The key individuals responsible for the daily operations during the audit period include:

<u>Individual</u>	<u>Position</u>
Ginny Lee	Senior Vice President and General Manager, EMS
Karen Peacock	Vice President of Marketing, EMS
Charlie Ecker	Director of Business Operations, EMS
Cameron Alder	Vice President of Customer Care
Ron Jones	Vice President of Development Management
Olivier Helleboid	Vice President of Product Management
Mike Haas	Human Resources Business Partner

Intuit's organizational structure makes certain managers can plan, execute and monitor department and individual performance. The organizational structure provides for segregation of duties, and personnel are aligned with job functions and defined responsibilities. Intuit maintains organizational charts to delineate roles and responsibilities.

The Intuit functional groups significant to the provision of customer services (affecting the control environment) are as follows:

- Management—Intuit's management supports a positive control environment and oversees operational and customer service activities. Management segregates employee responsibilities covering the areas of the Intuit Online Payroll service.
- Application operations—The application operations group supports the day-to-day operations and facilities management of the computer systems. Application operations manages systems on behalf of the customer contact center, and also manages the daily operations for Intuit Online Payroll's production environment.
- Operations—Payroll operations personnel are responsible for performing customer support (CS), data transmissions and recurring operational processes on behalf of customers. Key duties include enrolling customers in federal and state filing programs, processing authorizations from customers, and controlling routine and exception handling of money movement.
- Business development—The business development function is responsible for cultivating new business relationships with prospective partners, exploring and expanding distribution channels, and expanding relationships with existing partners.
- Product management (PM)—The PM Team manages the process of setting functional priorities for service and product development and for translating customer and business requirements into specifications for the Product Development Team. The PM Team documents and monitors multiple generations of release plans. In addition, they track and manage adherence to federal and state laws, constantly updating and adjusting application features and reference materials to help the application calculate accurately and to help customers understand and comply with relevant laws and payroll regulations.

- Product development (PD)—The PD team is responsible for designing, writing and testing the computer code for the Intuit Online Payroll software. They deliver customer and business requirements according to Product Management’s functional priorities. PD consists of three distinct roles: architecture, software engineering and quality assurance.
- Human resources (HR) services—The HR Team administers hiring, performance reviews, promotions, HR policy and staffing functions at Intuit.

Written Standards and Procedures

Intuit maintains on the intranet site policies and procedures available for employees to view. These policies and procedures include the Security Policy, Change Management Policy and Employee Handbook.

Intuit has developed the following policies, standards and procedures:

- Policies and procedures
 - Information security
 - Contract administration
 - Change management
 - Identity theft prevention
 - Employee Handbook
 - Awareness and training
 - Signature authorization
 - Data integrity
- Standards
 - Programming code standards
 - Documentation standards
 - User IDs
 - Passwords

Personnel Practices

Personnel policies and procedures are documented in the Intuit Employee Handbook and communicated to employees. Job descriptions exist that describe primary job functions and responsibilities that have been developed by management. Employee job descriptions include a position summary and describe major duties and responsibilities. Intuit performs employment screening and new employee orientation.

Criminal background checks are performed on prospective employees prior to employment for Intuit positions. Upon employment, employees receive a copy of the Employee Handbook. A policy regarding confidentiality is included in the Employee Handbook. Newly hired employees sign the Employee Invention Assignment and Confidentiality Agreement upon hire.

Intuit personnel receive on-the-job and formal training. The nature and length of this training depends on the individual's position, prior experience and educational background. Employees are cross-trained, where practical, to provide sufficient backup in the event of unexpected illness, approved long-term absences, involuntary terminations, resignation or promotion.

Terminated employees are removed from company systems by information technology (IT) personnel upon notice of termination. Passwords, keys and electronic access devices are obtained from these employees.

Segregation of Duties

The separation of functions between application operations, CS, PD and PM is designed to provide a clearly defined segregation of duties between the functions of production operations and payroll processing. Intuit maintains organizational charts to delineate roles and responsibilities. Additionally, job roles and functions are documented and communicated to employees. Intuit personnel are not responsible for the initiation, data entry, payment approval or correction of payroll information submitted by customers to Intuit for processing. However, because the Intuit Online Payroll Team is a small-sized team, instances may occur where an employee will have responsibilities in overlapping functions. Such segregation of duties conflicts are temporary in nature and are closely monitored by management.

Risk Management

Intuit reevaluates operating process strategy on an ongoing basis.

Management maintains its awareness of payroll processing industry risks by subscribing to industry publications and attending relevant seminars and training courses.

Senior management assesses the state of the control environment and related risks on at least a weekly basis. This includes the status of current customer processing and other matters of interest and concern.

Monitoring

Management evaluates the soundness, adequacy and application of accounting, financial and other operating controls; ascertains the extent of compliance with established policies, plans, procedures, laws and regulations to which the Company is subject; and assesses system application controls, customer service and account administration.

Management monitors the state of the control environment via communication with employees on a frequent and regular basis. These discussions include the status of current customer processing and other matters of interest and concern. Issues or suggestions identified by personnel are brought to the attention of management to be addressed and resolved.

Information and Communication

To help align Intuit's business strategies and goals with operating performance, management is committed to maintaining effective communication with personnel on a regular basis.

Intuit customers process payroll transactions via the Internet at Intuit's third-party data centers. The third-party data centers' servers utilize Windows and Linux as the operating system software.

The tax rates and withholding information embedded in the Intuit application are updated throughout the year. Intuit subscribes to an independent third-party tax service company that specializes in monitoring current federal, state and local tax data.

Application Controls

Application controls help to determine that transactions are valid, properly authorized, and completely and accurately processed.

Payroll, Processing

Intuit Online Payroll cash reconciliations between the ACH file transmissions and bank balances are performed daily. Variations are followed up and corrected by Intuit personnel.

Payroll Direct Deposits

Payroll direct deposits are handled through the Intuit Online Payroll application. Payroll transactions are not performed without authorization for new customers enrolling in direct deposit, state tax and/or federal tax services. Payroll transactions are not performed without automatic bank verification for a new customer's account to validate the accuracy of account information for direct deposits. Payroll is generated by Intuit Online Payroll on a daily basis. Customers are required to go online and approve direct deposits before 5:00 p.m. two days before their actual payday. The system records various dates. The first date recorded is the approval date, indicating when the customer approved the payments. The second date is referred to as the settlement date, and this is the date on which the customer wants the transaction to appear on their account. Considering the timely customer approval of payments, the Intuit online payroll application processes direct deposits and state tax payments on customer indicated settlement dates. Abnormal transactions released by the customer generate an email notification indicating the amount of the transaction and customer name for further investigation and validation.

At 5:00 p.m. daily, payroll processing is manually initiated by Intuit Online Payroll employees with ACH file transfer privileges. Once transactions are verified, the ACH file (proprietary banking format) is sent via secure File Transfer Protocol to Intuit's Online Payroll ACH processor. The processor generates a report that verifies total debits, total credits and total number of transactions. The Intuit Online Payroll employee logs into a secure website to retrieve the confirmation report, which they check against the Ops system. Once the Intuit Online Payroll employee verifies that the amounts in the confirmation report match the contents of the file transmitted, they finish processing. This final step releases emails to customers, which include information on the total amount of their transactions and the names of each employee that have been paid.

Federal Tax Deposits

The federal tax process is similar to the direct deposit process, but interfaces with a different system. Electronic Federal Tax Payment System (EFTPS) payments are set up through an Electronic Federal Tax Batch Filer System (EFTBS). After a payroll is complete, the user generates federal tax payments that are due on that specific date. The customer receives their federal tax payment information with amount due and date. Customers can decide to either pay through Intuit Online Payroll or to pay manually themselves. If the customer chooses to pay through Intuit Online Payroll, they are required to approve the payment amount at least two days prior to the due date. Considering the timely customer approval of payments, the Intuit online payroll application processes federal tax payments on customer indicated settlement dates.

At the end of each day, the Intuit Online Payroll user clicks a link for EFTPS payments on the Ops system. They navigate through a series of screens to create the payment, approve the amount and download a file by clicking Generate and Transmit EFTPS. This file is downloaded to a local folder. The file is named with a specific naming convention.

The user then opens the EFTBS software that is password-protected. Within the EFTBS system, they are required to click Import Payments, browse to the appropriate location, validate number of payment records and click Transmit Payments. A confirmation is received indicating the number of records exported. The user is then required to return to the Ops system and import the payment response. Once the file has been imported to the Ops system, the user can click Send Emails to generate email notifications to customers who incurred a federal tax payment, which includes the payment amount and date.

State Tax Payments

State tax payments are paid though the ACH process above or follow the same process as federal tax payments, but use software supplied by the state or the state's website.

Tax Calculations

The tax rates and withholding information embedded in the Intuit Online Payroll application are updated throughout the year. Intuit subscribes to Vertex, an independent third-party tax service company that specializes in providing current federal, state and local tax rate data. Changes to the tax rates are supplied to Intuit periodically.

The updates are installed following the Company's program change procedures described later in this document. Intuit does not have control over procedures employed at Vertex; however, tax rate changes are independently ascertained by Intuit personnel on a test basis.

Reporting

The online payroll system offers users a variety of reporting features. Reporting features include employer reports, employee reports, contractor reports, and paychecks and pay stub reports. The online payroll system accurately produces client reports based on input parameters form users. The Payroll system denies user input of incorrect or invalid data into the online payroll system.

Authorization

Customers process their own payrolls using the Intuit Online Payroll application. The Intuit Online Payroll application has authentication controls restricting access to those customer individuals who have been authorized by the customers to process payrolls. Customers authenticate themselves to the application upon initial signup and thereafter use the credentials they have established for future authentication.

Customers are first required to provide company and employee information for initial validation. This information is used to authorize the customers and the additional payroll information provided. The customer is then asked to provide a valid credit card number. The credit card is authorized to check its validity. Then, the customer has the option to select various features: payroll only, payroll direct deposit, electronic federal tax payments and electronic state tax payments.

If the direct deposit option is selected, the customer is required to provide appropriate account information (e.g., routing number, account number, etc.). Subsequently, customers are required to sign an authorization form that is faxed to Intuit and retained for future reference. Once received, the system generates a credit and debit transaction from \$0.01 to \$1.00 to the customer's account to test that the information is correct. The customer is then required to verify the amount of the transaction with CS or on the website. CS takes this number and enters it into the Ops system, where the number is verified. This helps verify that the customer is providing accurate account information, and Intuit Online Payroll has debit access to the account.

Office of Foreign Asset Control

Intuit has developed detailed policies and procedures to govern internal operations in complying with sanctions issued by the U.S. Treasury's Office of Foreign Asset Control (OFAC). OFAC is an office of the U.S. Treasury Department that maintains and publishes a list of countries, individuals and organizations that are hostile to the national security of the United States. Intuit has developed controls to freeze property in Intuit's possession and cooperate with financial institutions to block payment of funds to individuals and entities on the list, and to file timely any reports of such actions that may be required by OFAC. Intuit has a compliance program in place that allows them to react to frequent changes to the sanction lists and to identify accounts or transactions that would be subject to such sanctions.

The EMS Risk Management Team has the day-to-day operational responsibility for the implementation of OFAC screening procedures, which are included in Intuit's International Trade Screening Policy. Intuit's International Trade program is managed under the direction of the Ethics & Compliance Office. EMS is responsible for monitoring compliance with the requirements of OFAC and for overseeing any blocked funds. Formal compliance responsibilities have also been assigned to risk management operations and systems managers to verify that procedures are being followed.

When an Intuit customer signs up for any electronic payment services (including direct deposit, tax payments, etc.), Intuit checks the Social Security Number (SSN) against the Attus WatchDog database.

Intuit requires any employer who is applying for or adding additional electronic services to enter the principal officer's SSN. When initially selecting the electronic services option, a customer (1) enters the name of a principal officer, (2) enters the principal officer's SSN and (3) enters the principal officer's date of birth. Intuit verifies the SSN of new principal officers who sign up for electronic services against the Attus WatchDog SSN Plus database. On a daily basis, the Risk Management Operations Team will open the Ops system and run a report of the records of principal officers who sign up for e-services since the previous report was run. The Risk Management Operations Team will then access the Attus WatchDog SSN Plus database run locally on a computer, process an update file for comparison against the principal officer sign-up list, and save the results. The Attus WatchDog SSN Plus system will then return a listing of the records with expired, invalid or unissued SSN numbers. When the Risk Management Operations Team loads this Attus report back into the Ops system, the records that have cleared the SSN verification check will be marked as "passed" (meaning that the account is eligible for electronic services). If, however, a potential hit is returned on the Attus WatchDog SSN Plus report, the principal officer will be returned as "failed" once loaded into the Ops system, and the account will be denied for electronic services until Intuit can verify the identity of the principal officer.

The EMS Team is responsible for coordinating and monitoring compliance with Intuit's Ethics & Compliance Office, related rules and regulations pertaining to money laundering, and a customer identification program, including training of employees on the regulation's requirements.

On a nightly basis an ACH file review and exception report is performed to identify potential fraud or the legitimacy of transactions. For ACH files processed in a given day, an exception report is generated that identifies transactions that have met a specific set of criteria that Intuit has set up within their Ops system. The rules that have been set up in the system are business rules that Intuit has identified as appropriate to flag transactions to perform a second review.

Once the report is generated, it is reviewed to see if the companies/employees are on Intuit's internal watch list (reasons for being added to the watch list may include anything from insufficient funds for processing payroll to prior fraud), if the company attempting to process a transaction has a hold on their account or if the amount of the direct deposit transaction is large in relation to the internal rules contained within the system. A report of records of principal officers who signed up for e-services is reviewed on a daily basis by the OFAC specialist to identify and deny companies or employees on Intuit's internal watch list.

On a nightly basis an ACH file review and exception report is reviewed to identify potential fraud or the legitimacy of transactions. The risk management operations analyst reviews the report and, if after the review it is verified that a company's ACH transaction should not be processed, the employee logs back into the Ops system to manually move the payment to manual, effectively blocking the processing of the ACH transaction. The Risk Management Operations Team then sends a notification to the Application Operations Team to finish processing of the ACH file. After the file has completed processing, the total debits and credits for the file are matched to the banking site to verify that the totals were processed accurately. Additionally, the Ops system provides a notification that the ACH file has completed processing.

General Computer Controls

General computer controls include controls over computer operations, access, and systems development and maintenance. General computer controls, if suitably designed and operating effectively, provide an environment for the development and processing of applications to achieve specific application control objectives.

Computer and Network Operations

Monitoring

There are two monitoring tools that reside on a dedicated logging server and are used to measure network performance and scalability. The tools monitor two Web servers, four application servers, two operations servers, two database servers, one storage area network cluster, the service firewall and the logging server. Each is configured to generate email notifications for specific failures as configured by the IT managers, which are followed up by Intuit Online Payroll personnel.

There is also a tool used to monitor site performance over the Internet. This includes website performance and customer interactions. The tool monitors the website periodically throughout the day, and alerts generate emails, which are followed up by Intuit Online Payroll personnel.

Backups

Daily backups of the production database are performed. A backup utility is provided to schedule jobs for each server. Application, Web and database servers are imaged on-site and organized in a redundant, mirrored configuration that can be used to restore the servers when necessary. Backups are first made to disk, and then mirrored locally before they are duplicated to a separate off-site backup system.

Upon completion of backups, the utility is configured to send an email notification to the Production Operations Team. Email notifications are sent for both successful and failed backups. After the backup, recoverability is tested, and restorations are completed on an as-needed basis.

Application and Systems Software and Infrastructure Acquisition, and/or Development and Maintenance

Intuit Online Payroll software changes follow a formal change management process prior to being applied to production. Modifications are included as part of releases that take place on a monthly basis. On a weekly basis, hotfixes may be applied, which can include warm fixes and bug fixes. Monthly releases include new features, tax updates and bug fixes.

Hotfixes

Hotfixes are performed for bugs found by Intuit Online Payroll customers or Intuit Online Payroll employees. Hotfixes, in certain situations, can also be referred to as emergency fixes.

The following process is followed for hotfixes:

- Initiation: A customer will call into the CS line with issues or problems. If the CS representative is unable to resolve the problem and feels that it may be a bug within the system, an online Hypertext Markup Language-format bug form is completed. Upon submission, the form automatically generates an email that is sent to the Live Bugs Alias email group, which includes quality assurance (QA), engineering management and PM. Upon further investigation by QA, one of the following resolutions is accepted:
 - Incorrect information provided
 - Work-around provided to customer until next release
 - Certainly a bug that needs fixing (hotfix)
 - Not reproducible

Information is recorded as entries into the bug database, and the database is reviewed daily. QA assigns bugs to one member of the Engineering Team for further resolution. Changes to the bug status generate an email to the creator of the bug entry, the person who verified the bug and the assigned engineer, who verifies that bugs are monitored.

- Development—Engineers develop a resolution for the bug in the staging environment. The staging environment most closely resembles production and will provide a good basis for determining how the change will operate in the production environment. Once development is complete, the bug is marked as resolved within the database.
- Testing—QA reviews the bug database and, if the bug entry is marked as resolved, a member of QA conducts testing in an independent environment to verify that the bug has indeed been resolved. Once complete, the bug is marked as verified by QA in the database.
- Approval—Once the bug is updated within the database, an email is sent by QA indicating that the build has been successfully tested. The email is sent to one of the following to apply changes to various part of the production system: database administrator, Systems Administration Team, Production Engineering Team or director of Intuit Online Payroll engineering.
- Implementation—Prior to applying the changes to production, the bug database is checked to verify whether the bug was resolved and the resolution was verified. Once the promoter observes the proper approval as documented within the bug database ticket, the changes are applied to production.
- Post-Implementation—After production is updated with the bug fix, an email is sent indicating the build has been completed.

Software Development Life Cycle

The Intuit Online Payroll Software Development Life Cycle follows the standard change management process above. Feature changes occur as part of sprints, which allow for interactive and incremental development. Monthly releases are also managed within the same process. The following software Development Life Cycle Process is currently in place:

- **Product planning**—Each software development sprint begins with product planning. This phase includes pre-meeting preparation, product backlog review, and user story creation and prioritization. All stakeholders for the sprint are present during this phase.
- **Sprint planning**—Following product planning, sprint planning is completed. Sprint planning includes tasks such as detailed subtask definition, estimation of effort and assignment of resources, and completion of final user stories to implement.
- **Daily scrums**—Each team participates in daily scrums to track sprint progress. Each scrum involves project stakeholders, maintains sprint focus and creates visibility to both stakeholders and management.
- **Testing**—QA conducts user acceptance testing in the testing environment. CS may also go into the testing environment and attempt to become familiar with the new features.
- **Approval**—Once QA gains comfort around changes, an email containing QA approval is sent indicating the build to one of the following, who are allowed to apply changes to various part of the production system: database administrator, Systems Administration Team, Production Engineering Team or director of Intuit Online Payroll engineering.
- **Implementation**—Changes are applied to the production environment from a development server manually.
- **Demo and retrospective**—Following the completion of each sprint cycle, a demonstration of a working deliverable is reviewed, and stakeholder feedback is solicited, collected and then incorporated into the next sprint.

Version Control

Version control software is utilized in the application code change management process to support restores of previous code versions. Access to production application code within the version control software is restricted to authorized users.

Infrastructure Changes

Critical changes made to the infrastructure in production are logged in an online documentation repository or other electronic communication. In addition to the documentation, Intuit Online Payroll also relies on monitoring controls and physical security to help identify inappropriate changes so they may not be applied to the production server.

Change Monitoring

Changes made to critical files and/or configurations on production are monitored. In the event of a change, an automatic email notification is sent to the Production Operations Team. These emails are also sent to a storage email account, where they can be retrieved for future reference.

Logical Access

Access and Authentication

Access and authentication controls utilize iKey fobs with unique digital certificates and firewall authentication for internal users. The iKey requires a password for it to release the digital certificate for access. External users (customers) have access to the Intuit Online Payroll application via a Web server that requires a username and password.

Administrative accounts with access to production servers and databases are restricted to an authorized group of IT support personnel. VPN client access is accomplished with secured tokens containing Public Key Infrastructure- (PKI-) protected certificates. To access the console, the administrator gains physical access to the servers through the guards, biometric scanners, badging devices and combination cabinet locks.

Customers access and input their data regarding their company's payroll information (e.g., employees, payment amounts, tax information, etc.) in the four public servers holding input data. Intuit does not input customer payroll information for their customers. Customers access this via a Web server and log into their company accounts from the Web. Customers are restricted to their own company's payroll information, based on the username and password permissions.

Intuit Online Payroll Users

A tracking ticket is opened with when a new employee joins Intuit, which identifies the resources that an employee will need (e.g., computer, email address, desk, phone, etc.).

Internal users have a Windows account and an iKey to gain access to the Intuit Online Payroll production applications. The iKey is requested when logging into the production environment. Windows will then ask for a password to authorize the iKey to release its digital certificate and allow the user to authenticate to the system.

As identified above, VPN access is the internal service that system administrators use to make modifications to schemas, system functionality, code promotion, etc.

Internal CS and processing users gain access to the systems via a Web browser. Java 2 Platform, Enterprise Edition container-based security controls the access end users have within their Web browsers. End users are restricted to the Uniform Resource Locators (URLs) listed on the security.xml page, which defines the URLs each category of employee is allowed to access. As part of the user account administration process, end users are provided with the access specific to job requirements.

A VPN is used to restrict access to production servers. VPN access is limited to select IT support and management personnel. Granting VPN access requires documented management approval. Granting of physical tokens and related certificates requires documented manager approval. Management collects secured physical tokens from terminated employees. Certificates of terminated employees with VPN access are removed from the VPN access control list (ACL).

External Users

External users are Intuit's Online Payroll customers. They gain access to limited browser windows within the Intuit Online Payroll customer interface applications, as available, on the Internet. They input new employees and supply their own data to the Intuit Online Payroll application. Intuit Online Payroll does not alter customer account information within the system.

Access Reviews

Intuit has implemented a quarterly review process to help verify if access is granted according to job function. Intuit performs access reviews for internal users with Intuit Online Payroll system access granted through the use of secured tokens with PKI-protected certificates.

Password Policy

For the application servers, the policy defined within Windows is used as the standard password policy. Database servers reside on one domain, so the standard password policy is enforced at the domain level. The standard password policy includes a six-character minimum, password complexity requirements, required password changes and password uniqueness.

Secured tokens with PKI-protected certificates are required in addition to passwords, and are the primary control for authentication for Intuit employees. Passwords are enforced on secured tokens, production applications and the corporate domain. As described above, logical access cannot be gained to the production environment without a secured token with PKI-protected certificates.

Network Architecture and Management

The Intuit Online Payroll production network is segmented in various shared and secured zones that are protected by redundant firewalls. Firewall access and rule sets are controlled through the use of ACLs and secured tokens with PKI-protected certificates as identified above. These systems are managed by the EMS Production Operations Team.

Intrusion Detection

Administrative access to production servers and databases is controlled by a firewall. The firewall sends out an automatic notification email to personnel in the administrative group upon both successful and unsuccessful attempts to access the production environment.

Physical Security and Environmental Controls

Physical Security Access and Monitoring Procedures

Formal access procedures exist for requesting and controlling physical access to the third-party data centers. Intuit Online Payroll-authorized employees and contractors are permitted within the locked cage area containing Intuit Online Payroll hardware. Other Intuit Online Payroll employees, visitors and contractors are escorted by a member of the authorized list.

Headquarters and Customer Operations Centers

The Mountain View, Schaumburg and Reno facilities are automatically locked after hours. During operating hours, access is physically monitored and controlled by card-key readers in Mountain View, Schaumburg and Reno. After-hours, card-key access is required to access the headquarters and customer operations center facilities.

Subservice Organizations

Intuit Employee Management Solutions utilizes subservice organizations to assist in the delivery of services. The following is a high-level description of services the subservice organization provided during the audit period. This information is provided so clients and their auditors can have an understanding of the operations and how the controls at Intuit Employee Management Solutions relate to operations at subservice organization and clients. The scope of this report does not extend to the controls and related control objectives at the subservice organizations. Intuit Employee Management Solutions uses Coresite, Inc. in San Jose, California, and Digital Reality, Inc. in Phoenix, Arizona, for computerized hosting facilities, including the supply of power, data connectivity and secured space.

Subservice Organization	Service Provided
Coresite, Inc.	Co-location hosting facility
Digital Reality, Inc.	Co-location hosting facility

Complementary User Entity Controls

Intuit's Online Payroll Plus and Payroll Basic services were designed with the assumption that certain policies, procedures and controls would be in existence or implemented by user entities in order to achieve the stated control objectives. Accordingly, Intuit's user entities and their auditors should consider whether the following controls have been placed in operation at user entities:

The user entity is responsible for:

- Entering employee master data (e.g., employee expenses, withholdings, HR data) to ensure the completeness, correctness and accuracy of this data
- Entering payroll data to ensure that this data is complete, correct and accurate
- Verifying and approving payroll transactions and amounts that have been entered and processed
- Reviewing Intuit Online Payroll application report(s) and reconciling amounts to internal records
- Verifying that relevant incurred taxes are calculated independently of the Intuit Online Payroll application, such as some local and special taxes (e.g., "head" taxes), are correct
- Initiating processing functions
- Authorizing the direct deposits, federal tax payments and state tax payments
- Effectively restricting logical access to the Intuit Online Payroll application, granting access on a need-only basis and monitoring to verify that access levels are suitable for each authorized user over time
- Ensuring that user payroll duties are segregated and controlled
- Ensuring that appropriate records regarding payrolls processed on the Intuit Online Payroll application are maintained

The list of user control considerations presented above does not represent a comprehensive set of the controls that should be employed by the customer. Other controls may be required at the user organization.

IV. Intuit Employee Management Solutions' Control Objectives and Related Controls and McGladrey LLP's Tests of Controls and Results of Tests

Intuit Employee Management Solutions' control objectives and related controls are an integral part of management's description and are included in this section for presentation purposes. McGladrey LLP included the description of the tests performed to determine whether the controls were operating with sufficient effectiveness to achieve the specified control objectives and the results of tests of controls, as specified below.

Tests of the control environment, risk assessment, information and communication, and monitoring included inquiries of appropriate management, supervisory and staff personnel, observation of Intuit Employee Management Solutions' activities and operations, and inspection of Intuit Employee Management Solutions documents and records. The results of those tests were considered in planning the nature, timing and extent of McGladrey's testing of the controls designed to achieve control objectives. As inquiries were performed for substantially all of Intuit Employee Management Solutions' controls, the tests were not listed individually for every control in the tables below.

Control Environment, Risk Assessment and Monitoring

Control Objective 1: Controls provide reasonable assurance that management demonstrates through attitude, awareness and actions an atmosphere that enhances the effectiveness of specific controls.		
<i>Provided by Intuit Employee Management Solutions</i>	<i>Procedures Performed by McGladrey LLP</i>	
Control	Test Performed	Test Results
1.1 Intuit maintains a board of directors that have the relevant experience and capacity to strategically run the Company.	Inspected the list of the board of directors to verify the general composition and qualifications.	No exceptions noted.
1.2 Intuit maintains on the intranet site policies and procedures available for employees to view. These policies and procedures include the Security Policy, Change Management Policy, and Employee Handbook.	Inspected the Company intranet to verify the availability of policies and procedures regarding customer data handling, physical security, development and QA, and operations security and processing to Intuit employees.	No exceptions noted.
	Inspected a sample of written standards, such as policies and procedures, to verify the content clarity and flow, including: <ul style="list-style-type: none"> • Security policies • Change management • Employee Handbook 	No exceptions noted.
1.3 Criminal background checks are performed on prospective employees prior to employment for Intuit positions.	Inspected a sample of new employees and verified the completion of criminal background checks prior to employment.	No exceptions noted.
1.4 Newly hired employees sign the Employee Invention Assignment and Confidentiality Agreement upon new hire.	Inspected a sample of new employees and verified that the employees' Employee Invention Assignment and Confidentiality Agreements were signed and on file.	No exceptions noted.

Control Objective 1: Controls provide reasonable assurance that management demonstrates through attitude, awareness and actions an atmosphere that enhances the effectiveness of specific controls.

<i>Provided by Intuit Employee Management Solutions</i>		<i>Procedures Performed by McGladrey LLP</i>	
Control		Test Performed	Test Results
1.5	Terminated employees are removed from Company systems by IT personnel upon notice of termination.	Inspected and compared the current termination list against system user lists to verify that terminated employees did not have access.	No exceptions noted.
1.6	Intuit maintains organizational charts to delineate roles and responsibilities.	Inspected the Intuit organization charts for the designed segregation of duties to verify that definition of responsibilities exists.	No exceptions noted.

Logical Access

Control Objective 2: Controls provide reasonable assurance that logical access to the Company's networks, systems and data is restricted to authorized personnel.		
<i>Provided by Intuit Employee Management Solutions</i>		<i>Procedures Performed by McGladrey LLP</i>
Control	Test Performed	Test Results
2.1 A password-protected physical token with an encrypted PKI certificate is required to access the production environment.	Attempted to access the production environment without a password-protected physical token and verified that the system did not grant access to the production environment.	No exceptions noted.
2.2 The Intuit Online Payroll application authenticates through a Web server that requires a username and password	Inspected the Online Payroll application to verify that username and password was required.	No exceptions noted.
2.3 Customers are restricted to their own company's payroll information, based on the username and password permissions.	Inspected the Online Payroll application to verify that the username and password combination restricted the user to that company's data.	No exceptions noted.
2.4 Granting of physical tokens and related certificates requires documented manager approval.	Inspected a sample of new users with valid secured tokens and verified that manager approval was obtained before logical access was granted.	No exceptions noted.
2.5 Intuit's management performs quarterly reviews of users with production access.	Inspected a sample of quarterly secured token reviews to verify that the reviews were performed and corrective actions were taken.	No exceptions noted.
2.6 Administrative accounts with access to production servers and databases are restricted to an authorized group of IT support personnel.	Inspected a list of users with access to the production servers and databases and verified that access was restricted to authorized individuals.	No exceptions noted.
2.7 VPN access is limited to authorized IT support and management personnel and is required to access the production environment.	Inspected a list of users with access to production application code and verified that access was restricted to authorized personnel.	No exceptions noted.
	Observed and attempted to log into the production environment without a valid certificate and verified that the system did not grant access.	No exceptions noted.
2.8 Granting VPN access to production for new users requires documented management approval.	Inspected a list of newly hired users with access to the production VPN and verified that access was approved by management.	No exceptions noted.
2.9 Terminated employees with VPN access are removed from the VPN ACL.	Inspected a list of users with VPN access and a list of terminated employees and verified that VPN access was removed upon termination.	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that logical access to the Company's networks, systems and data is restricted to authorized personnel.

<i>Provided by Intuit Employee Management Solutions</i>		<i>Procedures Performed by McGladrey LLP</i>	
Control		Test Performed	Test Results
2.10	Strong password parameters are enforced on secured tokens, production applications and the corporate domain.	Inspected the Intuit paycycle password policy to verify that password requirements are defined for production applications and operating systems.	No exceptions noted.
		Inspected the password parameters on production applications and operating systems and verified that password requirements meet the Intuit password policy.	No exceptions noted.

Systems Development and Change Management

Control Objective 3: Controls provide reasonable assurance that application development and maintenance is authorized, tested, approved and documented.		
<i>Provided by Intuit Employee Management Solutions</i>		<i>Procedures Performed by McGladrey LLP</i>
Control	Test Performed	Test Results
3.1 Hotfixes or bugs identified by internal or external users are recorded in a database that is used to track the status of the bug/hotfix until resolution.	Inspected a sample of bugs and hotfixes to verify that the bugs and hotfixes were recorded and documented in a database.	No exceptions noted.
3.2 QA approvals are required for bugs and hotfixes prior to promotion to production.	Inspected a sample of bugs and hotfixes and examined supporting documentation to verify that QA approvals were obtained prior to promotion to production.	No exceptions noted.
3.3 Major changes in the form of monthly releases involving code changes and testing of those changes are documented in a ticket.	Inspected a sample of monthly releases to verify that the testing details were documented within the related deployment ticket.	No exceptions noted.
3.4 Access to production application code within the version control software is restricted to authorized users.	Inspected a list of users with access to production application code within the version control software to verify that access was restricted to authorized personnel.	No exceptions noted.

Application and Business Process

Control Objective 4: Controls provide reasonable assurance that payroll data and tax calculations are processed completely and accurately in conformity with the client specifications.		
<i>Provided by Intuit Employee Management Solutions</i>		<i>Procedures Performed by McGladrey LLP</i>
Control	Test Performed	Test Results
4.1 Payroll data, including gross and net pay, state and federal tax withholdings, expense reimbursements, garnishments, contributions and deductions are calculated completely and accurately by the Intuit application.	Set up a test account within the online payroll application and input specific employee parameter information and created a payroll run to verify that the system accurately recalculated correct payroll information.	No exceptions noted.
4.2 After each month end, the accounting manager reviews the journal entries prepared by the accountant who reconciles customer funds each business day including direct deposits and tax payments.	Inspected a sample of month-end journal entries approved by the accounting manager.	No exceptions noted.
4.3 Tax updates are applied to the payroll system as a part of the regular major releases for the system.	Inspected a sample of monthly tax updates and examined related program change documentation to verify that they were applied as part of the major releases for the system.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that reports are produced completely and accurately and available to customers.		
Provided by Intuit Employee Management Solutions		Procedures Performed by McGladrey LLP
Control	Test Performed	Test Results
5.1 The online payroll system accurately produces client reports based on input parameters form users.	Inspected a sample of reports to verify that they correctly displayed customer data inputs within the report.	No exceptions noted.

Control Objective 6: Controls provide reasonable assurance that customers are notified of rejected transactions and errors.		
Provided by Intuit Employee Management Solutions		Procedures Performed by McGladrey LLP
Control	Test Performed	Test Results
6.1 If a user enters incorrect or invalid data into the online payroll system, the user is promoted with an error message of the data validation error.	Observed the online payroll system notify users with an error message of a rejected transaction or error.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that customer tax and direct deposit transactions are processed according to the customer's instruction.		
Provided by Intuit Employee Management Solutions		Procedures Performed by McGladrey LLP
Control	Test Performed	Test Results
7.1 The Intuit online payroll application processes direct deposits and state tax payments on customer indicated settlement dates.	Inspected a sample of customers, selected a state tax payment or direct deposit transaction initiated by the customer, and verified that the payments made by Intuit were performed on customer indicated settlement dates.	No exceptions noted.
7.2 The Intuit online payroll application processes federal tax payments on customer indicated settlement dates.	Inspected a sample of customers, selected a federal tax payment transaction and verified that the federal tax payment initiation by Intuit was performed on customer indicated settlement dates.	No exceptions noted.

Control Objective 8: Controls provide reasonable assurance that the processing of customer payroll data is authorized.		
Provided by Intuit Employee Management Solutions		Procedures Performed by McGladrey LLP
Control	Test Performed	Test Results
8.1 Payroll transactions are not performed without authorization for new customers enrolling in direct deposit, state tax and/or federal tax services.	Inspected a sample of new customer accounts using direct deposit, state tax and/or federal tax services to verify that authorization was obtained for customers prior to enrollment in new services.	No exceptions noted.
8.2 Payroll transactions are not performed without automatic bank verification for a new customer's account to validate the accuracy of account information for direct deposits.	Inspected a sample of new customers' accounts enrolling in direct deposit to verify that automated bank verification was applied to each of the inspected customers' accounts to validate their account information.	No exceptions noted.

Control Objective 9: Controls provide reasonable assurance that suspicious or unusual transactions are identified by Intuit staff.		
<i>Provided by Intuit Employee Management Solutions</i>	<i>Procedures Performed by McGladrey LLP</i>	
Control	Test Performed	Test Results
9.1 On a nightly basis an ACH file review and exception report is reviewed to identify potential fraud or the legitimacy of transactions.	Observed that the operations analysts run the nightly process for the ACH file review to verify how the process was run, that it flagged unusual transactions and how the ACH file process was completed.	No exceptions noted.
	Observed the internal business rules to flag unusual transactions with the system engineer to verify the type and nature of these rules and that they flag defined transactions.	No exceptions noted.
	Inspected a sample of days to verify that the ACH exception file was reviewed by the operations analysts.	Exception noted. ACH file review confirmations were not available for the following two out of 27 sampled days: September 9, 2012; September 25, 2012. Review was performed by operations analyst for days noted as exceptions; however, the "Mark as reviewed" button was not pressed to generate a log evidencing the review.
9.2 A report of records of principal officers, who signed up for e-services is reviewed on a daily basis by the OFAC specialist to identify and deny companies or employees on Intuit's internal watch list.	Inspected a sample of days to verify that the operations team ran a report of the records of officers who signed up for e-services.	No exceptions noted.