MCCRACKEN FINANCIAL SOLUTIONS CORPORATION

Report on McCracken Financial Solutions Corporation's Description of Its Information Technology General Control System for the Application Service Provider Hosting Environment and on the Suitability of the Design and Operating Effectiveness of Controls throughout the period October 1, 2019 to September 30, 2020

Prepared Pursuant to AICPA AT-C Section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*

TABLE OF CONTENTS

SECTION I

REPORT OF INDEPENDENT SERVICE AUDITORS

Report of Independent Service Auditors

To the Management of McCracken Financial Solutions Corporation

Scope

We have examined McCracken Financial Solutions Corporation's description of its information technology general control system for the Application Service Provider ("ASP") hosting environment (the "system") entitled "McCracken Financial Solutions Corporation's Description of Its Information Technology General Control System for the Application Service Provider Hosting Environment" throughout the period October 1, 2019 to September 30, 2020 (the "description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in McCracken Financial Solutions Corporation's Assertion (the "assertion"). The controls and control objectives included in the description are those that management of McCracken Financial Solutions Corporation believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

The description of the system does not include control objectives related to business process controls, automated application controls, or key reports produced by the Application Service Provider hosting environment. Therefore, our examination did not extend to control objectives related to business process controls, automated application controls, or key reports produced by the Application Service Provider hosting environment.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of McCracken Financial Solutions Corporation's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

In Section II McCracken Financial Solutions Corporation has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. McCracken Financial Solutions Corporation is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and the 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 stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditors' 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.

Our examination was conducted 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, based on the criteria in management's assertion, 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 October 1, 2019 to September 30, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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 based on the criteria in management's assertion.
- 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.
- testing the operating effectiveness of those controls management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion in Section II

Inherent limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization or a subservice organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions by the system. 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 or a subservice organization may become ineffective.

Description of tests of controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in McCracken Financial Solutions Corporation's Assertion in Section II,

a. the description fairly presents the system that was designed and implemented throughout the period October 1, 2019 to September 30, 2020.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2019 to September 30, 2020 and user entities applied the complementary controls assumed in the design of McCracken Financial Solutions Corporation's controls throughout the period October 1, 2019 to September 30, 2020.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2019 to September 30, 2020 if complementary user entity controls assumed in the design of McCracken Financial Solutions Corporation's controls operated effectively throughout the period October 1, 2019 to September 30, 2020.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of McCracken Financial Solutions Corporation, user entities of the system during some or all of the period October 1, 2019 to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and 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. This report is not intended to be, and should not be, used by anyone other than these specified parties. If report recipients are not user entities that have contracted for services with McCracken Financial Solutions Corporation for the period October 1, 2019 to September 30, 2020 or their independent auditors (herein referred to as a "non-specified user") and have obtained this report, or have access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

November 19, 2020

SECTION II

MCCRACKEN FINANCIAL SOLUTIONS CORPORATION'S ASSERTION

8 Suburban Park Drive, Unit #2, Billerica, MA 01821-3903
978.439.9000: Main Number 978.439.9068: Fax Number
www.mccrackenfs.com

McCracken Financial Solutions Corporation's Assertion

We have prepared the description of McCracken Financial Solutions Corporation's information technology general control system for the Application Service Provider ("ASP") hosting environment (the "system") entitled "McCracken Financial Solutions Corporation's Description of Its Information Technology General Control System for the Application Service Provider Hosting Environment" throughout the period October 1, 2019 to September 30, 2020 (the "description") for user entities of the system during some or all of the period October 1, 2019 to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and 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 misstatement of user entities' financial statements.

The description of the system does not include control objectives related to business process controls, automated application controls, or key reports produced by the Application Service Provider hosting environment. Therefore, the examination did not extend to control objectives related to business process controls, automated application controls, or key reports produced by the Application Service Provider hosting environment.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of McCracken Financial Solutions Corporation's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. the description fairly presents the system made available to user entities of the system during some or all of the period October 1, 2019 to September 30, 2020 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

(1) the types of services provided, including, as appropriate, the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

(3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the system during the period covered by the description.

iii. does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2019 to September 30, 2020 to achieve those control objectives if user entities applied the complementary controls assumed in the design of McCracken Financial Solutions Corporation's controls throughout the period October 1, 2019 to September 30, 2020. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

SECTION III

MCCRACKEN FINANCIAL SOLUTIONS CORPORATION'S DESCRIPTION OF ITS INFORMATION TECHNOLOGY GENERAL CONTROL SYSTEM FOR THE APPLICATION SERVICE PROVIDER HOSTING ENVIRONMENT

A. Scope of the Report

This report describes certain application service provider (ASP) controls at McCracken Financial Solutions Corporation ("McCracken" or "MFS") and is designed to provide information for use by McCracken's ASP customers, and their independent auditors. This report has been prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants' AT-C Section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting ("AT-C 320")*.

This report is structured into five main sections:

- **Section I** contains the report of PricewaterhouseCoopers LLP ("PricewaterhouseCoopers" or "PwC").
- **Section II** contains McCracken's written assertion.
- **Section III** contains McCracken's description, including an overview of operations and description of the Information Technology General Control system for the ASP hosting environment.
- **Section IV** details the control objectives and related controls performed by McCracken, PwC's tests of operating effectiveness and the results of testing performed by PwC.

This report is intended to focus on elements that may be relevant to the internal controls of ASP operations to support client accounts. The scope of this report is limited to the Strategy[SM] application, including all client and web modules, and the relevant underlying technology components.

This report does not encompass all aspects of the services provided or procedures followed by McCracken for various types of clients. The scope of this report, including the description of the system, the related control objectives and tests of controls, is limited to McCracken's ASP operations. The following areas are not included within the scope of the report:

- The management of client specific routers that are contracted for as an additional service by certain clients.
- The functionality of the Customer Support team and their response and resolution to client issues.
- The software development and maintenance of McCracken's Strategy[SM] application and other McCracken developed applications.
- The functionality of the Strategy[SM] application (e.g. automated application controls, automated calculations, and other functionality within or facilitated by the system).
- The validation of outputs and reporting generated from the Strategy[SM] application.

B. Overview of Operations

McCracken Financial Solutions Corporation

McCracken Financial Solutions Corporation is a leading provider of software solutions for the commercial finance industry. From the corporate headquarters in Billerica, Massachusetts, McCracken provides servicing solutions for streamlining all aspects of the loan lifecycle. Clients include some of the leading commercial finance companies in the world: mortgage bankers, banks, insurance companies, thrifts, and government agencies. McCracken customers service nearly $2 trillion in loans worldwide.

Clients have been using McCracken applications since 1986 with the McCracken Application Service Provider maintaining a hosting environment since 1999.

McCracken Financial Solutions Corporation, ASP Division

The McCracken Application Service Provider (ASP) maintains a hosting environment for the IBM Power 9 series platform. Since 1999, McCracken has offered full service outsourcing and hosting solutions by acting as an

Application Service Provider. McCracken hosts Strategy[SM], its loan servicing system, for 28 customers.

C. Control Environment

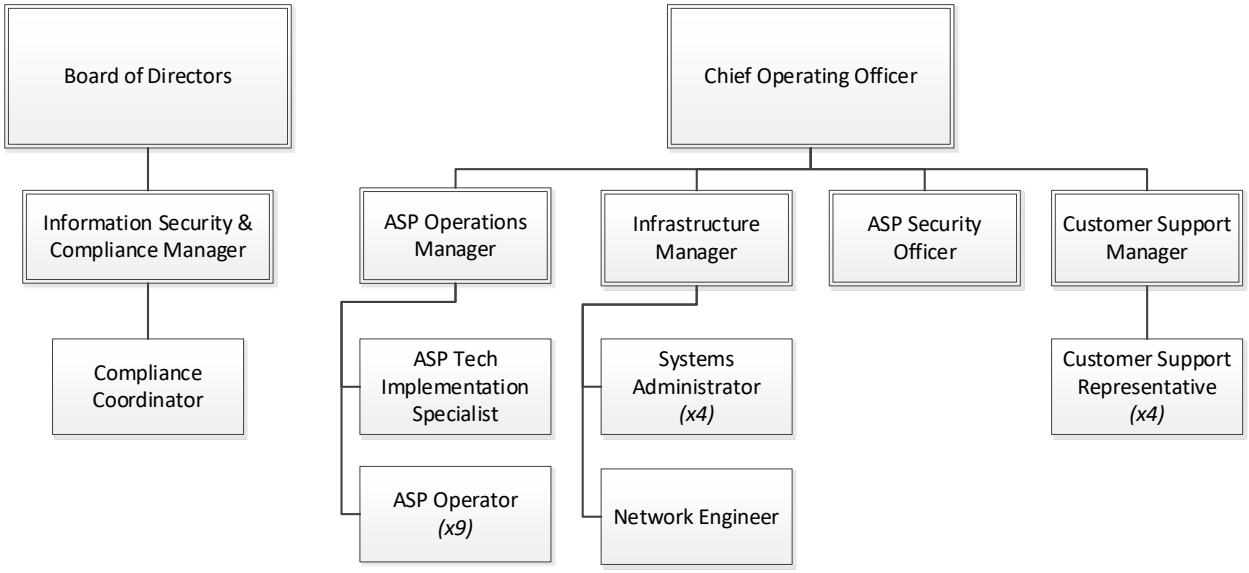
Organizational Structure

The ASP Business Unit is under the direction of the Chief Operating Officer, who reports to the President and Chief Executive Officer of McCracken.

Figure A provides an organization chart for the management structure at McCracken and **Figure B** provides an organization chart for the ASP operations.

Figure A – McCracken Organization Chart

Figure B – McCracken ASP Organization Chart



Please also note that the Information Security & Compliance Manager reports twice a year to the Board of Directors regarding all security and compliance activities and matters affecting the company.

McCracken ASP Roles and Responsibilities

The roles and responsibilities within ASP operations are as follows:

- The Chief Operating Officer is responsible for the management of the ASP organization and the McCracken Customer Support group as well as the Consulting, Infrastructure Development and Test groups.

- The Infrastructure Manager is responsible for managing the system infrastructure and for the oversight of system changes. Management of the relationship between the third party hardware, network, and off-site storage providers, and ASP business continuity planning are responsibilities of the Infrastructure Manager.

- The ASP Operations Manager schedules shifts for the Systems Operators and is responsible for the management of daily activities for ASP Operations. Managing ASP installations, coordinating with third party applications, and working with Customer Support and Implementation are among the Manager's duties.

- The ASP Technical Implementation Specialist establishes new customer environments and restructures existing customer environments, when necessary. The Implementation Specialist works with third party applications, acts as a backup for the approval of delivery requests, and is also a backup for ASP operations.

- The iSeries Operators are responsible for the support of the iSeries operating systems and processing of the Strategy[SM] application day-ends and transmissions. These individuals manage operational job schedules and batch processing and perform daily backups. They are responsible for addressing client requests and questions, and are on-call 24 hours a day, 7 days a week.

- The ASP Security Officer is responsible to define, enforce, and monitor security models for all iSeries environments except for certain dedicated logical partitions or dedicated iSeries clients who manage this responsibility.

- The Systems Administrators are responsible for tape management, and performance monitoring. These individuals manage maintenance procedures and perform library maintenance. Physical security of the building and data center and data recovery are areas in which the Systems Administrators are responsible.

- The Network Engineer is responsible for all network security, firewall and routers. This includes ASP connectivity to clients and the Internet. Other responsibilities include ASP client network problem resolution and network server maintenance.

- The Information Security & Compliance Manager is responsible for understanding the ASP environment and its associated processes as they relate to compliance. When changes occur, this individual assesses the potential impact to established procedures and to the ASP control environment. Coordinating efforts for the annual SOC 1 examination and responding to individual customers' compliance assessment requests is another responsibility of the Information Security & Compliance Manager.

- The Compliance Coordinator is responsible for maintaining ASP processes and preparing associated documentation. The coordinator ensures that documented change control processes are effective and are adhered to on a regular basis to meet control objectives. The Compliance Coordinator also tracks operational and monitoring activities, and gathers evidence for the annual SOC 1 examination.

McCracken Customer Support

The McCracken Customer Support Group is responsible for application support and the resolution of application issues. When application errors arise, or application support is requested by ASP customers, the issue is forwarded to the Customer Support Group, where it is logged and addressed. The Customer Support Group notifies ASP of issue receipt and communicates with the customer.

Personnel Policies and Procedures

McCracken provides a cooperative and progressive working environment through the adherence to, and understanding of, comprehensive human resources policies and procedures. This practice promotes integrity, fairness, participation and a high degree of accomplishment. It is through the ethical and socially responsible conduct of each employee that business can be conducted to the highest standards.

Hiring
McCracken follows formal hiring practices. Qualified candidates are interviewed, references are verified, and final hiring approval is given by the hiring manager or supervisor for the business group. Appropriate screening, including credit and criminal background checks are performed.

Hiring decisions are based on qualifications and essential functions are described in the job descriptions. Selections are made by evaluating the skills, experience, and other characteristics of candidates to determine the person most qualified to fill a job opening. McCracken is committed to filling job openings with the best-qualified candidates.

Personnel Training
McCracken is committed to providing support and learning opportunities to employees by assessing the needs of individual departments and providing training where appropriate. Training goals are aligned with business goals and objectives. Training and development opportunities include on-the-job training, cross training between teams and shifts, new technology training, vendor-provided training, conferences, and certifications.

Information Security Awareness
McCracken requires all employees to follow information security policies and procedures. Employees are required to attend an annual Information Security Awareness session, at which time the Information Security Program is reviewed. The Information Security Program is also reviewed upon initial hire. This program includes incident

handling procedures, media destruction policies, and other specifics with regard to information security practices.

Employee Termination
A formal process is followed upon employee termination. The following tasks are performed in this process:

- Return of confidential documentation, coordination with payroll, and communication of benefit information to the employee.
- Return of access badges and removal of access from internal systems (e-mail, iSeries, corporate network, etc.).
- Access from the ASP network is removed, if applicable.
- ASP iSeries access is removed, if applicable.

Oversight Responsibility

ASP Status Meeting
ASP holds a weekly ASP Status meeting, which includes personnel from management, Operations, and Infrastructure. Discussions include the previous week's activities, a review of any reported issues, and planning for upcoming events.

Management Operations
The President of the company has an open door policy and participates daily with management and other personnel to understand current issues and determine action plans.

Weekly operations meetings are held by the Chief Operating Officer with all department managers to review projects and give status updates.

Management Monitoring

At an operational level, recurring tasks and monitoring tasks are managed through a Microsoft Office task list specifically for ASP. The Compliance Coordinator maintains and oversees a master task list and ensures that the operational and monitoring activities are completed by the assigned resources. A weekly ASP Status meeting is held to review prior week activities and issues as well as upcoming plans and activities. It is the responsibility of the ASP Operations Manager to report to the Chief Operating Officer any exceptions or problems in ASP processes or operations. Annual surveys are sent to ASP customers to solicit feedback on operational effectiveness and general customer satisfaction.

Risk Assessment

The CFO prepares budgets, monthly financial statements, monitors actual to projected performance and prepares what-if models. The CFO reports and reviews company performance monthly and at interim periods with the President. The departments within the organization are reviewed. The company's financials are audited by an independent CPA firm.

The President receives monthly reports from the CFO and meets with the CFO regularly in order to discuss and review progress and status on current company objectives.

Transaction, Enterprise and IT Risk Assessment

McCracken recognizes the importance of risk awareness and the proper use of resources and controls to reduce and manage vulnerabilities that are exploitable by threats both internal and external, and support ongoing determinations of the effectiveness of these controls. Three Assessments are performed.

- An IT risk assessment is completed annually on all of the technologies. If new technologies are added during the year, a separate risk assessment is performed. A risk assessment summary is produced annually.
- A Transaction Risk Assessment is completed annually on all of the business functions.
- The Enterprise risk assessment includes the assessing of each risk category for each product and service within Organization.

The results of the annual assessments are reviewed by the McCracken senior management. Annually, the Compliance Manager presents the Transaction, Enterprise and IT Risk Assessment summary to the Board of Directors or when a new technology of high risk is identified.

Physical Access

The ASP data center is located in the McCracken corporate headquarters in Billerica, Massachusetts. The entrances to the building are locked and entry is restricted by card access. There are no loading docks for the building. Security cameras monitor the outside of the building, exterior doors and the ASP data center 24 hours a day, 7 days a week. Visitors to the building are required to sign in and wear badges. Entry into the data center is by authorized card access only with dual authentication. Access to the data center is granted subsequent to management approval, and is reviewed on a monthly basis to ensure that access remains restricted to authorized personnel on the basis of job role.

Control Objectives and Related Controls

McCracken has specified the control objectives and identified the controls that are designed to achieve the related control objectives. McCracken's specified control objectives and related controls are included in the accompanying Section IV of this report to eliminate the redundancy that would result from listing within Section III. Although McCracken's specified control objectives and related controls are included in Section IV, they are, nevertheless, an integral part of the organization's description of its information technology general control system for the ASP hosting environment. The description that follows outlines the processes and controls that are performed by McCracken for its customers and should be read in conjunction with the detailed control objectives and control activities described in Section IV that are intended to be incorporated herein.

D. INFORMATION TECHNOLOGY GENERAL CONTROLS

Hosting Service Environments

The ASP infrastructure includes unique system components. ASP clients may specifically contract to host either McCracken developed applications or an application developed by a third-party. Additionally, McCracken may provide the above-mentioned ASP hosting services to a single client who has specifically contracted for a separate network with its own unique infrastructure.

Customers can contract to be hosted in one of three ways:

- Private: The customer has their own IBM i Database and Linux or Windows Application Server environment. They connect to the McCracken data center through their own separate network infrastructure.

- Dedicated: The customer has a dedicated (or multiple dedicated) logical partition(s) on an IBM i Database and a unique instance on shared Linux Application Server environment. A dedicated virtual Linux application Server is an add-on, if required. Connections to the McCracken data center may be through a shared network.

- Shared: Customers leverage a shared logical partition on an IBM i Database and a unique instance running

on a shared Linux Server environment. Connections to the McCracken data center are through the shared network.

Private and dedicated customers can maintain a significant amount of control over their iSeries environment and Application Server and may not rely solely upon McCracken for controls in this area.

ASP System Software Maintenance and Network Security

Modifications to the operating system and network infrastructure are maintained and managed by the ASP Systems Administrators as well as by one Network Engineer (who all report to the Infrastructure Manager). Their role is to develop and maintain technology architecture concepts for the ASP customers. These individuals are responsible for virus management, firewall and router configurations, and monitoring network traffic and activity. Authentication to the McCracken network, sterile network, web and application (Linux) servers, and the VPN client is enforced via unique user ID and password combinations. Additionally, ASP Systems Administrators maintain and manage hardware and infrastructure changes for ASP. An annual calendar is released to each customer informing them of the four quarterly maintenance weekends. In addition to maintenance work, operating system and hardware changes are completed when necessary. Activities are approved by the Infrastructure Manager, prior to completion. Network access is reviewed by the Infrastructure Manager on a quarterly basis to ensure access is restricted to current McCracken employees and remains commensurate to job role.

Data Center and Environmental Controls

The McCracken data center has been structured to include a variety of physical and environmental controls to protect the assets resident therein. The ASP clients' system components are all maintained in the same physical and environmental control environment. The McCracken data center can be accessed through only one inside door equipped with a dual authentication magnetic card reader system. The Data Center has raised flooring, redundant air conditioning units, water sensors, and is protected by an FM-200 fire suppression system. Furthermore, a Caterpillar diesel generator and universal power supply systems provide uninterrupted electrical power.

ASP Operations and System Security

The ASP Operations group maintains and manages the McCracken production environment. ASP Operations consists of ten iSeries Operators including the ASP Operations Manager (as described in the Organizational Charts on pages 10 and 11). The iSeries Operators perform computer operation functions, oversee logical access to the systems, perform manual job requests, respond to customer operational issues, and coordinate application moves to production.

iSeries system security, for the shared customer environments, is defined and managed by the ASP Security Officer. The ASP Security Officer establishes security standards and procedures along with ASP management and performs compliance and monitoring of these standards on a defined basis, including monitoring of system level access on all IBM i logical partitions ("LPARs"). ASP Operations has also implemented a security incident and event management (SIEM) tool to log and monitor access to the Linux environment. System level access is reviewed by the ASP Operations Manager on a monthly basis to ensure access is restricted to current McCracken employees and remains commensurate to job role.

Strategy^{SM} Application Development

The Strategy^{SM} application automates the commercial loan servicing process. Modules include adjustable loan processing, investor reporting, transaction and escrow processing, asset management, as well as providing solutions for other collateral associated workflow processing.

The development of the Strategy^{SM} application is managed and maintained within a distinct business unit at

McCracken outside of the ASP Department. The development controls in place at McCracken are under the control of the Product Development Department, reporting to the Chief Operating Officer, and application changes are tested by the customer (refer to the Complementary User Entity Controls on page 16). Strategy[SM] application development is not included in the scope of this report (refer to Scope of the Report on page 9).

ASP Application Maintenance

The McCracken development organization builds, tests, and packages Strategy[SM] releases and upgrades. Product releases and upgrades are published on the McCracken website. It is at the customer's discretion whether to install these releases and upgrades. ASP customers make requests through the Customer Support group to schedule the install of a release or upgrade (or individual fix) into their ASP test environment. Upon completion of customer testing, the customer notifies Customer Support (who maintains record of approval from the customer) who coordinates and creates the delivery request to implement the release, perform the upgrade, or enter the fix into the customer's production environment. The job delivery document is submitted to ASP Operations from Customer Support to schedule the move to production. ASP Operations marks the delivery request as completed, which notifies Customer Support that the job is completed. Customer Support then notifies the customer that the move has been completed.

E. COMPLEMENTARY USER ENTITY CONTROLS

McCracken's controls relating to ASP operations cover only a portion of the overall controls for each client. Customers also need to implement and maintain effective internal control in conjunction with McCracken's controls that are summarized in Section IV of this report. Each customer's internal control depends upon the nature of the transactions processed, the degree of interaction of controls, and the terms of agreement with McCracken.

This section highlights those control responsibilities that McCracken believes should be present for each client account. McCracken has considered complementary user entity controls in developing its controls described in this report. Each client must evaluate its own control structure to determine if the following controls are in place. Furthermore, the following list of controls is intended to address only those controls surrounding the interface and communication between each client and McCracken ASP operations. Accordingly, this list does not purport to be, and is not, a complete listing of the controls that provide a basis for the assertions underlying the financial statements of client accounts.

All customers should maintain effective controls in relation to:

- The authorization process for the set-up, modification, and deletion of user IDs (control objective 6 & 7).
- The authorization process for the set-up, modification, and deletion of access levels on the system (control objective 6 & 7).
- The testing of upgrades and application fixes to the systems and application (control objective 3 & 4).
- The authorization of changes to be applied to the Strategy[SM] application, prior to the movement of those changes into the production environment by McCracken (control objective 4).
- The review of application maintenance logs for changes to the production environment (control objective 4).
- Addressing correspondence from McCracken regarding unsuccessful production data backups (control objective 2).

Dedicated Customers

Dedicated customers who don't rely on the standard ASP Security Model should maintain effective controls in relation to:

- The definition of security parameters for their environments (control objective 6 & 7).

Private Customers

Private customers should maintain effective controls in relation to:

- The iSeries system security parameters (control objective 6).
- The review of audit journals, system logs, and monitoring of security functionality and sensitive IDs (control objective 6).
- The movement of application changes into the production environment (control objective 4).
- The Linux or Windows system security parameters for their WebSphere Application server environment (control objective 6 & 7).

SECTION IV

MCCRACKEN FINANCIAL SOLUTIONS CORPORATION'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND PRICEWATERHOUSECOOPERS' TESTS OF OPERATING EFFECTIVENESS AND TEST RESULTS

INFORMATION PROVIDED BY PRICEWATERHOUSECOOPERS LLP

This report is intended to provide McCracken's user entities and their independent auditors with information about the controls supporting the information technology general control system for the Application Service Provider ("ASP") hosting environment, as provided within McCracken's operating environment, as well as information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the internal controls at user entities, is intended to assist its independent auditors in (1) planning the audit of the user entity's financial statements and in (2) assessing control risk for assertions related to the user entity's financial statements that may be affected by controls at McCracken.

Our testing of McCracken's controls was restricted to the control objectives and the related control activities listed in Section IV of this report and were not extended to procedures or controls that may be in effect at user entities, or at subservice organizations utilized by McCracken. It is each user entity's auditor's responsibility to evaluate this information in relation to the internal controls in place at both the user entities and at the subservice organizations. If certain complementary controls are not in place at either the user entities or subservice organizations, McCracken's controls may not compensate for the resulting weaknesses.

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether the controls and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the attestation period, for each of the controls listed in the matrices below, which are designed to achieve the specified control objectives. In selecting the particular tests of operating effectiveness of controls, we considered: (1) the nature of the controls being tested; (2) the types and competence of the available evidential matter; (3) the nature of the control objectives to be achieved; (4) the assessed level of control risk; (5) the expected efficiency and effectiveness of the test; and (6) the testing of other controls within the stated control objective. Such techniques were used to evaluate the fairness of the description of the controls and to evaluate the operating effectiveness of the specified controls as indicated in the matrices below.

In addition, as required per paragraph .35 of AICPA AT-C section 205, Examination Engagements, and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence regarding the completeness and accuracy of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Environment

The control environment represents the collective effect of various elements, which establish, enhance or mitigate the effectiveness of specific controls. Elements of McCracken's ASP control environment include:

- The ASP organizational structure and approach to segregation of duties;
- Management control methods and monitoring activities;
- McCracken's personnel policies and practices; and
- Management's risk assessment process.

Our tests of the control environment included the following procedures, to the extent considered necessary:

(1) A review of the McCracken organizational structure, including the ASP division's segregation of functional responsibilities, and review of personnel policies and practices;
(2) Discussion with operations, administrative, and other management personnel who are responsible for developing and applying McCracken's control activities; and
(3) Observation of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of the testing of the operating effectiveness of controls relevant to the achievement of the control objectives.

Testing of Controls

The types of tests performed with respect to the information addressed in Section IV are briefly described below.

Test	Description
Reperformance	Reperformed application of the control activities for a sample of transactions to ensure adequacy of its application.
Inspection	Inspected a sample of documents and reports indicating performance of the control activities. This includes, among other things: • Testing of source documents to ensure transactions processed were consistent with transaction requests and that such transactions were in compliance with controls. • Inspection of source documentation and authorization to assess propriety and timeliness of transactions processed. • Testing and inspection of reconciliations and management reports that quantify reconciling items to assess whether balances and reconciling items were properly monitored, controlled, and resolved on a timely basis.
Observation	Observed application of specific control activities.
Inquiry	Inquired of the appropriate personnel of McCracken. Inquiries seeking relevant information or representation from McCracken's personnel were performed to obtain, among other things: • Knowledge and additional information regarding the control activities. • Corroborating evidence of the control activities. As inquiries were performed for substantially all McCracken's controls, this test was not listed individually for every control listed in the tables in Section IV.

SUMMARY OF CONTROL OBJECTIVES

The control objectives and related controls presented below are specified by McCracken and are an integral part of Management's description of its information technology general control system for the ASP hosting environment.

Computer Operations

Control Objective 1
Controls provide reasonable assurance that computer operations are authorized, monitored, and scheduled, and that problems are identified and resolved in a timely manner.

Control Objective 2
Controls provide reasonable assurance that production processing systems are backed up, stored at an off-site location, and are available for restoration in the event of processing errors or unexpected processing interruptions.

Change Management

Control Objective 3
Controls provide reasonable assurance that changes to system software are authorized, tested, documented, approved and implemented.

Control Objective 4
Controls provide reasonable assurance that changes to applications are authorized, documented, approved and implemented.

Physical Security

Control Objective 5
Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to authorized individuals, and that environmental controls exist.

Logical Security

Control Objective 6
Controls provide reasonable assurance that access to system software is monitored, and restricted to authorized individuals.

Control Objective 7
Controls provide reasonable assurance that access to the network is monitored, and is restricted to authorized individuals.

Control Objective 1 – Controls provide reasonable assurance that computer operations are authorized, monitored, and scheduled, and that problems are identified and resolved in a timely manner.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
Data Center Coverage			
1.1	The Data Center is operational 24 hours per day, 7 days per week. ASP Operators are scheduled to be onsite in the Data Center 24 hours per day during the business week and 8 hours per day during the weekend.	For a sample of months, inspected the monthly scheduling calendar to verify that the data center is staffed 24 hours per day on weekdays and at least 8 hours per day on weekends.	No exceptions noted.
1.2	Key personnel have backups to cover scheduled and unscheduled time off as noted on the monthly scheduling calendars.	For a sample of months, inspected the system support tree and scheduling calendar to verify scheduling of time off, shift assignments, and the existence of backups for key personnel.	No exceptions noted.
1.3	ASP customer job processing procedures for daily, monthly, and annual processes are documented in individual ASP Customer Run Books.	For a sample of ASP customers, inspected the Customer Run Books for the documentation of daily, monthly, and annual customer job processing procedures.	No exceptions noted.
Operations			
1.4	Customer end of day processing is performed by initiating scheduled jobs manually or by running automated jobs on the iSeries job scheduler. Completion of both scheduled manual jobs and automated jobs are documented and reviewed on individual Customer Day End run sheets or on the daily operations checklist.	For a sample of days, inspected a Customer Day End run sheet or daily operations checklist for evidence that both scheduled manual and automated jobs were documented and reviewed.	No exceptions noted.
1.5	ASP Operations approves delivery request forms for scheduling activity. Once the request is complete, the delivery request form status is closed within the request tracking system.	Inspected a sample of delivery request forms to verify review and approval by ASP Operations, and that the form was closed within the request tracking system upon completion.	No exceptions noted.
1.6	On a daily basis, ASP Operations monitors e-mail received from ASP customers and executes on daily operational issues. Once the issue has been resolved, the customer is e-mailed back with the resolution.	Inspected a sample of customer initiated e-mails sent to ASP Support to verify that ASP Operators monitor and respond to operational issues, and that e-mails were sent to customers to confirm resolution.	No exceptions noted.

Control Objective 1 – Controls provide reasonable assurance that computer operations are authorized, monitored, and scheduled, and that problems are identified and resolved in a timely manner.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
1.7	ASP Operations monitors e-mail received from ASP customers and follows documented escalation procedures for issues that are not operations related. ASP Operations receives notification of issue receipt from the appropriate department.	Inspected formal ASP Operations procedures have been documented to govern problem escalation and resolution activities.	No exceptions noted.
		Inspected a sample of e-mails sent to ASP Operations for non-operational issues to verify that the issues were escalated to the appropriate department.	No exceptions noted.
1.8	Daily Operations checklists are maintained and reviewed by an ASP Manager. Any identified issues are documented within the job task or on the run sheet.	For a sample of days, inspected the daily Operations checklists to verify completion and evidence of review by an ASP Manager, and that any identified issues were documented within the job task or on the run sheet.	No exceptions noted.
1.9	On a daily basis, the ASP Operators monitor the processing and performance of production systems and data through the use of various monitoring tools. Problem monitoring software is used to send automated e-mails to the ASP Operators in the event of system disk failures for the database server.	Observed the monitoring of the percentage of disk space used and the status ("Active" / "Failed") of disks in the production systems by ASP Operators.	No exceptions noted.
		For a sample of days, inspected that automated e-mails reporting of the system disk space and status were distributed to and reviewed by an ASP Operator.	No exceptions noted.
1.10	The ASP Team meets weekly to discuss operational issues and system availability.	Observed that a weekly ASP Team meeting was held to verify that operational issues and system availability were discussed.	No exceptions noted.
		For a sample of weeks, inspected minutes from the ASP Team meetings for evidence that operational and system availability issues were discussed.	No exceptions noted.

Control Objective 1 – Controls provide reasonable assurance that computer operations are authorized, monitored, and scheduled, and that problems are identified and resolved in a timely manner.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
1.11	A weekly summary of network availability and communication outages is distributed to ASP management for review.	For a sample of weeks, inspected summary e-mails that were distributed to ASP management to communicate network availability and communication outages between McCracken and/or customer locations.	No exceptions noted.
1.12	On a daily basis, ASP Technical personnel monitor the processing and performance of non- database Web and Application production systems through daily review of the disk and system status.	For a sample of days, inspected evidence of the daily review of the processing and performance of non-database Web and Application production systems to verify that the review was performed and processing and performance issues were addressed in a timely manner.	No exceptions noted.

Control Objective 2 – Controls provide reasonable assurance that production processing systems are backed up, stored at an off-site location, and are available for restoration in the event of processing errors or unexpected processing interruptions.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
Backup Activities			
2.1	Documented policies and procedures regarding the backup schedules and procedures are maintained.	Inspected that operational policies and procedures exist to govern backup procedures for the ASP environment, and that the policies were updated and approved within the period under review.	No exceptions noted.
2.2	A full network and iSeries back-up of critical programs and files is performed on a daily, weekly, and monthly basis. A daily log of backup activity is maintained, and backup tapes are sent to an off-site storage facility.	For a sample of days, weeks and months, inspected iSeries backup logs to verify that automated backup of critical programs and files was performed.	No exceptions noted.
		For a sample of days, weeks and months, inspected input manifest sheets to verify that the off-site storage facility received the items specified on the manifest.	No exceptions noted.
2.3	A daily backup log of production libraries is maintained detailing all backups that were not fully completed overnight. If the daily backup log indicates that there are non-standard backup exceptions, an e-mail is sent to the ASP group for follow-up the following day. In the event a customer's production data library is impacted, the customer is notified and an action plan is established.	For a sample of days, inspected daily backup logs to verify follow-up, resolution, and customer notification for non-standard backup exceptions, when necessary.	No exceptions noted.
Backup Storage			
2.4	All back-up tapes follow a rotation cycle and are stored off-site for a predetermined period as outlined in ASP procedures. After the period has elapsed, the back-up tapes are brought back on-site and reused. The location of backup tapes is tracked and a daily reconciliation is performed between the manifests and the vendor's inventory report.	For a sample of days and weeks inspected evidence that the daily reconciliation was performed between the input manifests and the vendor's inbound / outbound inventory report.	No exceptions noted.
		For a sample of days and weeks, reperformed the reconciliation of input manifests against the vendor's inbound / outbound inventory report.	No exceptions noted.

Control Objective 2 – Controls provide reasonable assurance that production processing systems are backed up, stored at an off-site location, and are available for restoration in the event of processing errors or unexpected processing interruptions.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
Recovery from Operational Failure			
2.5	Upon customer requests to restore back-ups, McCracken recalls the backup tape from the vendor to make data available for restoration.	For a sample of customer requests to restore back-ups, inspected for evidence that the back-up tape was returned to McCracken from the vendor to make data available for restoration.	No exceptions noted.
2.6	Only authorized employees are able to recall, receive, or release backup tapes from the off-site storage facility. ASP maintains an authorized list, and provides the listing to the off-site storage facility. This list is reviewed on a quarterly basis to determine the appropriateness of authority, and changes identified are processed.	For a sample of quarters, inspected the review of the Iron Mountain listing of authorized employees that are permitted to recall, receive or release backup tapes from the off-site storage facility, that authority was appropriate, and that any authority changes identified were processed completely and accurately.	No exceptions noted.
		For a sample of quarters, reperformed Management's review of the Iron Mountain listing of authorized employees that are permitted to recall, receive or release backup tapes from the off-site storage facility to determine if the results of testing procedures agreed to Management's conclusions.	No exceptions noted.

*Refer to **Section III E** (page 16) for the listing of Complementary User Entity Controls. Customers should maintain effective controls related to the addressing of correspondence from McCracken regarding unsuccessful data backups.*

Control Objective 3 – Controls provide reasonable assurance that changes to system software are authorized, tested, documented, approved and implemented.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
Maintenance Planning			
3.1	System Change Management and Emergency Change Management policies and procedures are documented and updated on an annual basis.	Inspected operations guidelines to verify that System Change Management and Emergency Change Management policies and procedures are documented to govern Change Management activities, and that the policies were updated and approved within the period under review.	No exceptions noted.
3.2	System upgrades (iSeries), network maintenance, and scheduled program temporary fixes (PTFs) are performed on a quarterly basis.	Inspected the Calendar of System Maintenance for the upgrades, maintenance and PTFs to verify that maintenance is scheduled on a quarterly basis.	No exceptions noted.
3.3	Back out plans for quarterly maintenance activities are created, reviewed, and approved by ASP management.	For a sample of quarters, inspected maintenance weekend documents to verify that back out plans were created, reviewed and approved by ASP management for maintenance activities.	No exceptions noted.
3.4	When iSeries or Linux Operating System (OS) upgrades are tested and installed, responsible personnel coordinate with third party vendors to ensure compatibility.	For a sample of system software changes, including upgrades, inspected Third Party Vendor Checklists and related e-mail correspondence for evidence that vendors were contacted, if applicable.	No exceptions noted.
Maintenance Approval			
3.5	All quarterly maintenance activities, including back out plans, are authorized and approved by ASP management.	For a sample of quarters, inspected system software change documentation for evidence of authorization and approval by ASP management. For a sample of system software changes, including upgrades, inspected Third Party Vendor Checklists and related e-mail correspondence for evidence of approval by ASP management.	No exceptions noted. No exceptions noted.

Control Objective 3 – Controls provide reasonable assurance that changes to system software are authorized, tested, documented, approved and implemented.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
Maintenance Notification			
3.6	E-mail notification explaining quarterly maintenance activities is sent to all customers annually and also prior to each maintenance weekend.	Inspected the annual email distributions for calendar years 2019 and 2020 to verify that all customers were notified of scheduled quarterly maintenance activities for all quarters during the period under review.	No exceptions noted.
		For a sample of quarters, inspected system software change documentation to verify that customers were notified in advance of each quarterly maintenance weekend.	No exceptions noted.
3.7	After quarterly maintenance is completed, a summary of the maintenance activity, including results and any remaining work, is sent to the client.	For a sample of quarters, inspected summary maintenance e-mails to verify that customers were notified of all activity performed, results, and any remaining work, if applicable.	No exceptions noted.

*Refer to **Section III E** (page 16) for the listing of Complementary User Entity Controls. Customers should maintain effective controls related to the testing of upgrades and application fixes to the Strategy[SM] production environment.*

Control Objective 4 – Controls provide reasonable assurance that changes to applications are authorized, documented, approved and implemented.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
Application Change Authorization			
4.1	Authorizations are received from the customer prior to implementing any changes to production. Changes include enhancements, fixes, emergency fixes, implementing upgrades, or establishing new production environments.	Inspected a sample of production application changes to verify authorization by the customer prior to production implementation.	No exceptions noted.
Application Change Completion			
4.2	A delivery request form is submitted to ASP Operations or Technical Support to perform the necessary work in production. ASP Operations approves delivery request forms for scheduling.	Inspected a sample of production application changes to verify approval of the delivery request form from ASP Operations prior to production implementation.	No exceptions noted.
Application Change Notification			
4.3	After delivery request forms are completed by ASP Operations or Technical support team, Customer Support is notified of completion via email or within the request tracking system.	Inspected a sample of production application changes to verify that the requestor was notified upon implementation in production.	No exceptions noted.

*Refer to **Section III E** (page 16) for the listing of Complementary User Entity Controls. Customers should maintain effective controls related to the testing of upgrades and application fixes, and to the authorization of movement of updated versions of Strategy[SM] into the production environment, as well as the monitoring of application maintenance logs for changes to the production environment.*

The restriction of access to the iSeries environment is addressed within Control Objective 6.

Control Objective 5 – Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to authorized individuals, and that environmental controls exist.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
Building Access			
5.1	All building entrances are secured with electronic access card readers. All building guests are required to sign in at the reception area, obtain a visitor's badge, and are supervised by a McCracken employee.	Observed that building access is restricted by use of a card reader and that all building guests are required to sign in at the reception area, and are supervised by an employee.	No exceptions noted.
5.2	The Chief Operating Officer reviews the building access card listing on a monthly basis to ensure that access to the building is restricted to authorized personnel only.	For a sample of months, inspected the building access recertifications to verify evidence of review by the Chief Operating Officer, that access was authorized and appropriate, and that any required changes in access were processed completely and accurately.	No exceptions noted.
Data Center Access			
5.3	Security cameras are located above Data Center entrances to identify unusual activity.	Observed the data center to verify security cameras were located above entrances.	No exceptions noted.
5.4	The Data Center and Operators Room entrances are secured with dual authentication electronic access card readers.	Observed the Data Center and Operators Room entrance card reader functionality to verify dual authentication is required prior to entry.	No exceptions noted.
5.5	Prior to granting access to the Data Center, an access request form is completed and authorization is obtained. The access request form is signed after completion to verify that access has been granted to the Data Center.	Inspected a listing of all employee new hires and a sample of monthly Data Center access lists to determine whether access to the Data Center had been added for any employees during the period.	No exceptions noted.
5.6	Removal of access to the Data Center is completed after authorization by ASP Management. The access request form is signed after completion to verify that access to the data center has been revoked. Access is removed on or before the day of termination.	Inspected a listing of all employee terminations and a sample of monthly Data Center access lists to determine whether access to the Data Center had been removed for any employees during the period.	No exceptions noted.

Control Objective 5 – Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to authorized individuals, and that environmental controls exist.

Provided by McCracken		Performed by PwC	
Controls		**Test Procedures**	**Results**
5.7	Vendors or contractors hired to perform certain functions within the Data Center are either supervised at all times by a McCracken employee, or, for longer term projects, are provided a temporary access card with designated hours of use and a set termination date.	Observed the visitor/guest process to ensure that vendors and contractors are supervised at all times by a McCracken employee if requiring access to the data center.	No exceptions noted.
		Inspected policy/procedure documentation to determine if McCracken has defined its requirements for escorting visitors to protected areas.	No exceptions noted.
		For a sample of months, inspected system generated listings of all users with access to the Data Center and Operators Room for vendor/contractors to verify designated hours of use and a set termination date were assigned.	No exceptions noted.
5.8	ASP management reviews system generated logs to monitor the traffic in the Data Center on a monthly basis.	For a sample of months, inspected system generated logs to verify that card access was tracked and reviewed.	No exceptions noted.
5.9	ASP management reviews the ASP access card listing on a monthly basis to ensure that access to the data center is restricted to authorized personnel only.	For a sample of months, inspected that the ASP card access listing had been reviewed by ASP management, that access was appropriate and authorized, and that any required changes in access were processed completely and accurately.	No exceptions noted.
		For a sample of months, reperformed the review conducted by management to determine if access is appropriately restricted and determine if the results of testing procedures agree to management's conclusion.	No exceptions noted.

Control Objective 5 – Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to authorized individuals, and that environmental controls exist.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
Environmental Controls			
5.10	Environmental controls are in place in the Data Center facilities to enable continued processing in the event of an interruption to services. Equipment is maintained and tested on a regular basis. This equipment includes an uninterruptible power supply, fire suppression systems, backup generator, and air conditioning units.	Observed the existence and/or operation of equipment including an uninterruptible power supply, fire suppression systems, backup generator, emergency lighting, and air conditioning units.	No exceptions noted.
		Inspected a sample of maintenance forms to verify equipment underwent regular maintenance during the period under review.	No exceptions noted.

Control Objective 6 – Controls provide reasonable assurance that access to system software is monitored, and restricted to authorized individuals.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
iSeries System Level Access and Monitoring			
6.1	The ASP Team has established ASP naming conventions in shared environments requiring that each customer user ID and library is identified by a customer-specific three letter code to comply with the iSeries system security model.	Inspected documentation to verify that policies and procedures are in-place over the naming conventions for user IDs and libraries in shared iSeries environments. Inspected iSeries reports of user profiles and customer libraries to verify that customer IDs and libraries were assigned a unique three letter prefix.	No exceptions noted. No exceptions noted.
6.2	The QSECOFR ID is a powerful iSeries user ID that is used for limited system maintenance. Access to the QSECOFR ID is restricted to individuals with legitimate business need and a daily audit journal of QSECOFR activity is reviewed by the ASP Security Officer or Infrastructure Security Specialist.	For a sample of days, inspected the QSECOFR ID logging reports to verify evidence of review by the ASP Security Officer and ASP management.	No exceptions noted.
6.3	Command Line reports from the iSeries machines are reviewed on a daily basis by the ASP Security Officer to validate that all users with command line access are authorized, that developers did not maintain access, and access was commensurate with their job responsibilities. *See 6.8 and 6.9 for monitoring controls relating to temporary access, and production program source objects and data file libraries.*	For a sample of days, inspected command line access reports from each of the iSeries LPAR machines to verify evidence of review by the ASP Security Officer, and that all users with command line access were authorized, that developers did not maintain access, and access was commensurate with their job responsibilities.	No exceptions noted.
6.4	The authentication of users for the iSeries requires unique user identification and a valid password.	For all iSeries machines, inspected the System Values Report to confirm that passwords have been configured to restrict unauthorized access, and that a unique username and password combination are required for login.	No exceptions noted.

Control Objective 6 – Controls provide reasonable assurance that access to system software is monitored, and restricted to authorized individuals.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
6.5	Anti-virus software is installed on each IBM i LPAR. Each week a review is performed to ensure that anti-virus software has been updated.	Observed all IBM i LPARs to verify the installation and updating of anti-virus software. For a sample of weeks, inspected evidence that the anti-virus software was reviewed to ensure it was up to date.	No exceptions noted. No exceptions noted.
6.6	Prior to granting access at the system level to McCracken employees, an access request form is completed, reviewed and authorized to validate the access request is commensurate with the employee's job responsibilities. The access request form is signed after completion to verify that access has been granted to the system.	For a sample of access requests to the IBM i LPARs, inspected that user access forms were completed and approved prior to granting system level access and that the access granted was commensurate with the employee's job responsibilities.	No exceptions noted.
6.7	For terminations of McCracken employees, an access request form is completed and authorization is obtained for removal of access, at the time of termination. The access request form is signed after completion to verify that system level access has been removed. Access is removed on or before the day of termination.	Inspected a listing of all terminations and a sample of monthly IBM i LPAR access lists to determine whether system level access had been removed for any employees during the period.	No exceptions noted.
6.8	Command level audit reports detail all commands by McCracken and TMP (temporary) users. Command level auditing is captured when production access to the iSeries is granted. Command level audit reports are reviewed on a daily basis by the ASP Security Officer to verify activity is appropriate.	For a sample of days, inspected the daily command level audit reports to verify evidence of review by the ASP Security Officer, and that discrepancies were researched and resolved.	No exceptions noted.

Control Objective 6 – Controls provide reasonable assurance that access to system software is monitored, and restricted to authorized individuals.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
6.9	ASP Operations monitors access settings to production program source objects and data file libraries on a daily basis to ensure access is restricted to authorized personnel.	For a sample of days, inspected system security audit reports to verify evidence of review by ASP Operations, and that discrepancies were researched and resolved.	No exceptions noted.
6.10	Access to each IBM i LPAR is reviewed by the ASP Operations Manager to ensure that it is restricted to authorized users on the basis of job role, and required changes in access are processed completely, accurately, and timely.	For a sample of months, inspected the user review for all IBM i LPARs in order to test that access for all users was reviewed for appropriateness, and that any access changes identified were processed completely, accurately and timely.	No exceptions noted.

*Refer to **Section III E** (page 16) for the listing of Complementary User Entity Controls. Customers should maintain effective controls related to the set-up, modification and deletion of user IDs and access levels on the system.*

Control Objective 7 – Controls provide reasonable assurance that access to the network is monitored, and is restricted to authorized individuals.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
7.1	The authentication of users of our sterile network, Web and Application servers (Linux Servers), and VPN client solution, requires unique user identification and a valid password.	Observed authentication into the production VPN client, the sterile network and Web and Application servers to confirm valid authentication is required.	No exceptions noted.
		Inspected the security configurations for the production VPN client, the sterile network and Web and Application servers to verify that a unique user ID and password is required to log on.	No exceptions noted.
7.2	Network password configurations have been implemented over the McCracken network.	Inspected Windows Active Directory password and account settings to verify restricted access settings have been configured and are enforced.	No exceptions noted.
7.3	Anti-virus software is installed on each network PC. The software is automatically updated on a regular basis.	Observed a network PC for installation and automatic updates of anti-virus software.	No exceptions noted.
7.4	Prior to granting direct or remote access to the network to McCracken employees, an access request form is completed, reviewed and authorized to validate the access request is commensurate with the employee's job responsibilities. The access request form is signed after completion to verify that access has been granted to the network.	Inspected a listing of all new hires and a sample of quarterly network access lists to determine whether network access had been added for any employees during the period.	No exceptions noted.

Control Objective 7 – Controls provide reasonable assurance that access to the network is monitored, and is restricted to authorized individuals.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
7.5	For terminations of McCracken employees, an access request form is completed and authorization is obtained for removal of direct or remote access, at the time of termination. The access request form is signed after completion to verify that network access has been removed. Access is removed on or before the day of termination.	Inspected a listing of all terminations and a sample of quarterly network access lists to determine whether network access had been removed for any employees during the period.	No exceptions noted.
Network Monitoring			
7.6	Detection and prevention of unauthorized access is maintained through a firewall protection technology for the McCracken Internet connection.	Observed the firewall configuration and rules to determine that firewalls are utilized to protect the internal network from external threats.	No exceptions noted.
7.7	The Technical Support team monitors daily network activity for inappropriate access or violations.	Observed the monitoring of network activity by the ASP Technical Support team.	No exceptions noted.
7.8	A weekly summary of network activity and traffic is distributed to ASP management for review.	For a sample of weeks, inspected summary e-mails that were distributed to ASP management to verify the communication of network issues.	No exceptions noted.
7.9	Access to the Linux root ID is restricted to individuals with legitimate business need, and a SIEM report is reviewed daily. Follow up is then performed by a system administrator to verify use of root was appropriate.	Observed the daily report of root activity created by management as it appeared on the daily report from the SIEM tool. For a sample of days, inspected evidence of the daily review of root logon activity to verify that the review is performed timely and root activity is appropriately reviewed and investigated, if necessary.	No exceptions noted. No exceptions noted.

Control Objective 7 – Controls provide reasonable assurance that access to the network is monitored, and is restricted to authorized individuals.

	Provided by McCracken	Performed by PwC	
Controls		**Test Procedures**	**Results**
7.10	Access to the ASP Active Directory is reviewed by the Infrastructure Manager to ensure that it is restricted to authorized users on the basis of job role, and required changes in access are processed completely, accurately, and timely.	For a sample of quarters, inspected the user review for the ASP Active Directory in order to test that access for all users was reviewed for appropriateness, and that any access changes identified were processed completely, accurately and timely.	No exceptions noted.

*Refer to **Section III E** (page 16) for the listing of Complementary User Entity Controls. Customers should maintain effective controls related to the set-up, modification and deletion of user IDs and access levels on the system.*

McCRACKEN
FINANCIAL SOLUTIONS CORP.

8 Suburban Park Drive, Unit #2, Billerica, MA 01821-3903
978.439.9000: Main Number 978.439.9068: Fax Number
www.mccrackenfs.com