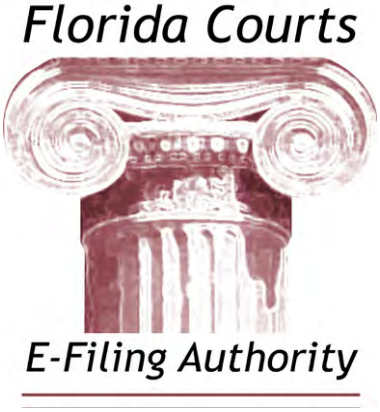
REPORT ON CONTROLS PLACED IN OPERATION
AND TESTS OF OPERATING EFFECTIVENESS
(SSAE No. 16)
FOR

FLORIDA COURTS E-FILING PORTAL



For the period January 1, 2011 through June 30, 2011

LANIGAN & ASSOCIATES, PC
CERTIFIED PUBLIC ACCOUNTANTS
THOMASVILLE, GA
TALLAHASSEE, FL
ATLANTA, GA

TABLE OF CONTENTS

SECTION I.
INDEPENDENT SERVICE AUDITORS' REPORT

LANIGAN & ASSOCIATES, P.C.
CERTIFIED PUBLIC ACCOUNTANTS
BUSINESS ADVISORS
www.lanigancpa.com

Please reply to:
Tallahassee

INDEPENDENT SERVICE AUDITORS' REPORT

Board of Directors
Florida Courts E-Filing Authority

Scope

We have examined the Florida Courts E-Filing Authority's (the "Authority") description of its portal for processing user entities' transactions throughout the period January 1, 2011 to June 30, 2011 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

Service organization's responsibilities

On pages 6-7 of the description, the Authority 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. The Authority is responsible for preparing the description for the 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, and designing, implementing, and documenting 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 January 1, 2011 to June 30, 2011.

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, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion on pages 6-7. 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 the Authority's assertion on pages 6-7;

a. the description fairly presents the system that was designed and implemented throughout the period January 1, 2011 to June 30, 2011.

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 January 1, 2011 to June 30, 2011.

c. the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period January 1, 2011 to June 30, 2011.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed on pages 22-44.

Independent Service Auditors' Report
October 27, 2011

Restricted use

This report, including the description of tests of controls and results thereof on pages 22-44, is intended solely for the information and use of the Authority, user entities of the portal system during some or all of the period January 1, 2011 to June 30, 2011, and the independent auditors of such user entities, who have sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements or user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Lanigan + Associates, P.C.

Lanigna and Associates, P.C.
October 27, 2011

SECTION II.
GENERAL DESCRIPTION OF THE E-FILING PORTAL CONTROL STRUCTURE AND OPERATIONS

FLORIDA COURTS E-FILING AUTHORITY'S ASSERTION

We have prepared the description of the Florida Courts E-Filing Portal for user entities of the portal during some or all of the period January 1, 2011 to June 30, 2011, 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 portal 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 E-Filing Portal made available to user entities during the period January 1, 2011 to June 30, 2011, for processing their transactions. The criteria we used in making this assertion were that the description:

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

- the types of services provided including, as appropriate, the classes of transactions processed.

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

- the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

- how the system captures significant events and conditions, other than transactions.

- the process used to prepare reports and other information for user entities.

- the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

- other aspects of our control environment, risk assessment process, information and communication systems (including 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 E-Filing portal, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the systems and their financial statement auditors, and may not, therefore, include every aspect of the portal that each individual user entity of the portal and its auditor may consider important in its own particular environment.

3. includes relevant details of the changes to the servicing agent system during the period covered by the description.

B. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 2011 to June 30, 2011, to achieve those control objectives. 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 management;

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; and

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

OVERVIEW OF THE E-FILING PORTAL

The Clerks of the Circuit Court are the official custodians of court records within their respective jurisdictions. The Clerk of the Florida Supreme Court is the official custodian of records for the Florida Supreme Court. In 2009, the Florida Legislature and Florida Supreme Court recognized the need for the development and implementation of a statewide electronic court filing system. As a result Chapter 28.22205, Florida Statutes, was passed into law.

> 28.22205 Electronic filing process –Each clerk of court shall implement an electronic filing process. The purpose of the electronic filing process is to reduce judicial costs in the office of the clerk and the judiciary, increase timeliness in the processing of cases, and provide the judiciary with case-related information to allow for improved judicial case management. The Legislature requests that, no later than July 1, 2009, the Supreme Court set statewide standards for electronic filing to be used by the clerks of court to implement electronic filing. The standards should specify the required information for the duties of the clerks of court and the judiciary for case management. The clerks of court shall begin implementation no later than October 1, 2009. The Florida Clerks of Court Operations Corporation shall report to the President of the Senate and the Speaker of the House of Representatives by March 1, 2010, on the status of implementing electronic filing. The report shall include the detailed status of each clerk office's implementation of an electronic filing process, and for those clerks who have not fully implemented electronic filing by March 1, 2010, a description of the additional steps needed and a projected timeline for full implementation. Revenues provided to counties and the clerk of court under s. 28.24(12)(e) for information technology may also be used to implement electronic filing processes.

The Florida Association of Court Clerks (FACC), in conjunction with the Florida Supreme Court, responded to this mandate by creating the Florida Courts E-Filing Authority. This was accomplished by an Interlocal Agreement creating a public agency pursuant to Chapter 163, Florida Statutes, comprised of Clerks of the Circuit Court who join the Authority and the Clerk of the Supreme Court.

The Florida Courts E-Filing Authority contracted with the FACC to design, develop, implement, operate, upgrade, support and maintain a uniform statewide electronic portal for the filing of court records. The portal will provide attorneys and pro se litigants with a common entry point for filing and transmitting court records electronically. In addition, the portal will provide these same persons and other authorized persons the ability to view court records electronically. The features of the portal include the following:

- A single statewide log-in
- A single internet access to court records by authorized users
- Transmission to and from the appropriate courts
- The ability to provide electronic service of notification receipt of an electronic filing and confirmation of filing in the appropriate court file
- Open standards-based integration ability with existing statewide information systems and county e-filing applications.

- Compliance with electronic court filing standard 4.0, the global justice extensible markup language and oasis legal markup language.

The portal was launched in January 2011, as required by the Interlocal Agreement. As of June 2011, sixteen counties were filing court records through the statewide portal. The remaining counties are actively working to connect to the portal.

An electronic filing may be submitted to the portal 24 hours a day and seven days a week. Electronic time/date stamps are attached to the documents as filed. However, the filing is not official information of record until it has been stored on the Clerk's case management system. All dates and times, including when the filing is received at the portal and accepted by the Clerk, are stored in the portal database.

GENERAL DESCRIPTION OF THE E-FILING PORTAL CONTROL STRUCTURE

Control Environment:

The Authority's control environment reflects the overall attitude, awareness, and actions of the board of directors/committees, management, and others concerning the importance of controls and their emphasis within the organization. The effectiveness of specific controls is established, enhanced or mitigated by various factors, including:

- Management's philosophy and operating style
- Organizational structure
- Board of Directors/Committees
- Assignment of authority and responsibility
- Commitment to competence
- Written policies and practices
- Various external influences that affect an entity's operations and practices, such as audits/reviews from external entities

Structure of Organization:

The organizational structure defines how authority and responsibility are delegated and monitored. It provides a framework for planning, executing, controlling, and monitoring operations.

The Authority's Board of Directors has ultimate responsibility for overseeing Authority operations. The Board is comprised of 9-members consisting of the following:

- Board Chairman – the chair of the FACC Technology Committee, as selected by the FACC President each year.
- Seven Clerks of the Circuit Court – in addition to the chair, each of the seven FACC districts nominate a Clerk from the district to serve on this board.
- Clerk of Supreme Court – the Clerk of the Supreme Court serves as the Chief Justice's designee on behalf of the state courts.

The Florida Courts E-Filing Authority contracted with the FACC to develop and maintain a uniform statewide electronic portal for the filing of court records. As a result, the remainder of this section of the report is discussed with respect to the structure and operations of the FACC.

The FACC Technology Committee has more hands on management of the technical aspects of the portal. The function of the Technology Committee is to provide program and policy direction relating to the application of technology within the Clerks' offices. In addition, the Committee provides development and management oversight for FACC sponsored applications (including the E-Filing Portal system, operations, controls, etc.). The Technology Committee is comprised of six Clerks presiding in the State of Florida. This committee meets several times throughout the year.

The FACC is headed by the Executive Director who reports directly to the Executive Committee. Overseeing the day to day operations of the E-Filing Portal is the Information Technology (IT) Director. The FACC Technology Division is comprised of approximately 52 staff.

The Technical Division performs the following functions:

- Systems Engineering and Operations
- Application Development
- Service Center
- Technical Projects

Supporting the FACC Technology Division is the accounting function which is responsible for recording and reconciling the daily activity processed through the internet portal.

Integrity and Ethical Values:

The FACC believes that maintaining an environment of integrity and ethical values is critical to the establishment and maintenance of its internal control structure. The effectiveness of internal controls is a function of the integrity and ethical values of the individuals who create, administer, and monitor the controls.

Commitment to Competence:

Competence is the knowledge and skills necessary to accomplish the tasks that define an individual's job. The FACC specifies the competence level for a particular job and translates it into the required level of knowledge and skills. As noted below, the FACC has job descriptions for each job associated with the portal.

The FACC believes that it has good Human Resource practices that help attract and retain competent and trustworthy employees. This is evidenced by the fact that the FACC has very little employee turnover.

Personnel Policies and Procedures:

The FACC effectively assigns authority and responsibilities throughout the organization. There are several documented controls the FACC has in place to support this. First, the FACC has a well specified organizational chart for the Technical Division which indicates the lines of authority and responsibility. Second, the FACC maintains current employee job descriptions that are reviewed periodically to ensure that employee duties are commensurate with management's expectations. Management ensures that all employees have the required skills to manage the portal and responsibility delegated to them.

The FACC has formal hiring practices designed to ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses

their qualifications related to the expected responsibility level of the individual. In addition, background checks and criminal history checks are conducted on all external candidates.

The FACC's policy requires that all employees receive an annual written performance evaluation and salary review. These reviews are based on goals, responsibilities, and performance factors that are prepared and rated by the employee's supervisor and reviewed with the employee. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

The FACC's progressive discipline system provides a framework for letting employees know when there are problems, giving the employees an opportunity to correct the problems, and permitting some type of review process for the final decision to terminate the employee.

Risk Assessment:

The FACC has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for clients. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address these risks. The risk management systems implemented by the FACC consist of internal controls derived from its policies, processes, personnel, and systems. Specifically, the primary control activities in place to mitigate these risks are described in the column entitled “Description of Controls” in Section III of this report.

Monitoring:

Management monitors operations, performance, quality and internal controls as a normal part of their activities. Management and staff, engaged in the technical and operational responsibilities, meet on a routine basis to discuss various issues pertaining to the portal. The type of issues discussed include, but are not limited to; problem resolution, system modification and enhancements, processing, transaction volume, and banking issues. The FACC has implemented various key reports (i.e. Budget, Transaction Volume and Financial Activity Reports) that measure the results of the portal.

As mentioned previously, the FACC has established and maintains a comprehensive internal control system. The FACC engages the following external audits/reviews:

1. Independent Financial Statement Audit (Annual):

   External CPA firm performs an annual audit in accordance with professional standards. The purpose of the audit is to express an opinion on the FACC’s financial statements.

2. Security Review (Annual):

   An outside consulting company, under contract with the FACC, performs an annual stringent review of security for systems within which the portal operates. This consultant conducts an annual exit conference, issues an executive summary report, issues a detailed technical report and provides to FACC Senior Management recommendations for improvement.

3. Internet Security Review (Quarterly):

   The FACC is required by Visa/Mastercard, who provides credit card services for the portal, to undergo quarterly security reviews. The quarterly reviews focus on internet security and are performed by an outside consulting firm. Upon completion, the FACC is provided a certification for processing transactions

4. SSAE No.16 (Annual):

   The FACC, as part of their risk assessment process, requested a Statement on Standards for Attestation Engagements (SSAE) No. 16 engagement. A SSAE No. 16 audit is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. The FACC plans to have a SSAE No. 16 engagement performed annually.

Information and Communication:

Management has established an organizational structure and has set a tone to help facilitate the communication of important business information. The FACC has implemented various methods of communication to ensure that all employees understand their roles and responsibilities and to ensure that significant events are communicated in a timely manner. As mentioned previously, the FACC has an organizational chart for the Technical Division that clearly depicts the lines of authority. The FACC maintains written job descriptions for all staff. Each description includes the responsibility to communicate significant issues and pertinent information in a timely manner. The FACC has formal meetings on a routine basis to discuss on-going projects associated with the portal. In addition, there are numerous ad-hoc meetings among management and staff for various reasons that may arise.

The FACC has implemented an Information Technology Service Management (ITSM) framework and Information Technology Infrastructure Library (ITIL) best practices for all FACC I.T. projects, including the portal. ITSM/ITIL is an internationally recognized best practice approach for managing I.T. projects. Selected staff have been trained and earned the ITSM/ITIL Foundation Certification.

The FACC has implemented various methods of communication to ensure that user organizations (Clerks) understand the FACC's role and responsibilities in processing transactions. These communication channels also ensure that the users understand how to use and navigate the various systems administered by the FACC. For example, the FACC makes available to those users participating in the portal detailed training/procedures manuals. In addition, the FACC conducts training classes for new Clerk staff. User organizations are encouraged to communicate questions and problems to the FACC liaisons.

The portal website contains clear and concise directions that allow the user to navigate through the system and perform inquiries and complete transactions. FACC staff in the Service Center Function provides ongoing communication with customers. This function maintains records of problems reported by customers and incidents noted during processing. The Service Center Function also communicates information regarding training, changes in processing schedules, system enhancements, and other related information to the user organizations.

Description of Information Systems:

FACC management has established processing procedures for the information system control environment. The systems and processes are defined as follows:

The FACC IT environment currently consists of an operating environment that is located in the Organization's office in Tallahassee, Florida. The office has an onsite server room that supports the company's ethernet-based local area network (LAN) that is used by company employees and consists mainly of Microsoft Windows based servers (equipped with Intel processors) that are used for network authentication, file/print services, internet access, email service and database servers for the company applications. Workstations and laptop computers throughout the Organization have network connectivity or are stand-alone.

The FACC IT environment is located inside a network consisting of various layers of industry standard firewalls to ensure that only authorized individuals are permitted access to the IT FACC Network and other IT Systems. FACC has high-speed leased communication lines to connect out to the Internet.

System Data Backup Procedures

The ability to restore system data after the interruption of services, corruption of data, or failure of computer services is vital to the ability to continue to provide services to users. To ensure that mission, production data is available for restoration in the event of normal production system failure or disaster. The following schedule of backups and controls are currently being performed

- Daily
- Monthly
- Annual

Data is backed-up on premise to a Legato backup server. The database and network documents are backed up to Ultrium LTO4 tapes. The tapes are sent offsite Monday through Friday with a secured vendor. The Systems Engineering staff is responsible for verifying that all backup jobs have been completed successfully. In addition, these individuals are responsible for updating all backup information including schedules, rotations, tape inventory, and tape location. The Systems Engineering Staff is also responsible for ensuring the tape media is rotated off-site, for purchasing additional media when necessary and maintenance of the backup procedures.

Inventory of backup tapes are available via the vendor's secured online inventory system, as well as, the Legato backup server. Both of which are accessible by the Systems Engineering staff.

Physical and Environmental Protection

The FACC facility is located at 3544 Maclay Blvd, Tallahassee, Florida. Controls are in place to provide for intrusion, fire detection and environmental protection.

Security and fire systems are utilized to protect against intrusion and fire. The Security System Vendor monitors the system for both fire and intrusion. In addition, the Vendor periodically inspects and maintains the system. The vendor has the ability to provide records of who activates and deactivates the intrusion system.

Access to the facility is limited with only one public entrance which is located at the front of the building. Access is controlled and monitored by the company's receptionist. Clients and visitors must sign-in at the receptionist's desk and are provided with a visitor's badge that must be worn at all times. Clients and visitors must be escorted by an FACC staff member in order to gain access to the second floor. The server room is located on the second floor. The room is secured and access is restricted to a limited list of key employees. Anyone accessing the server room must be accompanied by one of the authorized individuals, log their time, and record their reason for access. The server room features dedicated air conditioning units to protect the room from heat and humidity.

Fire extinguishers are located throughout the building and server room and are maintained on a regular basis by the vendor. An FM-200 Fire Extinguishing System equipped with smoke and heat detectors is installed in the FACC server room.

Uninterrupted power supply units (UPS), with a constant load, are installed to protect the file servers and telecommunications equipment from power surges and loss of data from sudden power outages. The UPS systems are tested and inspected on a periodic basis.

A diesel generator is located on the company grounds to provide an uninterrupted power solution in the event of a longer term power outage. The generator runs weekly self-tests which are monitored by FACC personnel. The generator is also inspected and maintained on a regular basis.

Network Security

FACC maintains network diagrams illustrating the physical and logical connections between interconnecting equipment. The communications equipment and servers are labeled to facilitate cross-reference to these diagrams.

To protect FACC data and information, a Cisco security appliance is utilized. The security appliance combines dynamic network address translation and packet filtration. Security groups and departments are separated using Virtual Local Area Networks (VLANs) in order to provide an additional layer of security.

Antivirus protection has been implemented at FACC on the server, email gateway and workstation levels to protect company data from infection by malicious code or viruses. The antivirus software is actively monitoring data and traffic with virus signature definitions that are updated on an active basis.

Logical Security

Logical access controls are utilized to restrict access to the FACC network, systems, applications and remote access. The IT Department has administrative access rights to the network and has responsibility for assigning and maintaining access rights to the network and applications.

The addition and deletion of user accounts is performed based on requests for new hires and terminations. FACC management has the authority to add new employees or modify existing employees' access rights. Requests are initiated by the HR department and communicated to the IT Department for processing.

Management provides notification of terminated employees to the IT Support team. The terminated employee’s access credentials are disabled immediately.

Access to the FACC network requires a user to authenticate by entering in their network user ID and a confidential password. User ID composition is based on a combination of the user parameters including their first and last names. Security parameters for the network password include:

- Minimum password length - 8 alphanumeric characters
- Must contain at least one number or special character
- Must contain a capital letter,
- Password expiration – 90 days,
- Password history is maintained for 5 passwords

Virtual Private Network (VPN) access to the FACC network is available using a Secured Socket Layer (SSL) VPN solution. Users must install a Cisco client on their device to authenticate and gain encrypted VPN access to the FACC network. Secondary user credentials are also required to create the VPN connection.

As an additional layer, VPN access is restricted in a Windows Active Directory (AD) and security parameters for remote access password management are controlled by the FACC Domain Security Policy.

Internet Data Authenticity

Since on-line security remains a primary concern of many customers, FACC has taken certain steps to ensure that any data transmitted to the application servers is done so in a secure manner. The E-Filing Portal web site that is hosted at FACC is: https://www.myflcourtaccess.com.

To ensure that sensitive data transmitted to the above web site is protected against disclosure to third parties, the website uses Hypertext Transfer Protocol with Privacy, which connects with RSA 256 bit secure socket layer (SSL) encryption. FACC uses a trusted authority (Secure Server Certificate Authority) as the certificate authority to re-assure on-line customers that the website they are visiting is an authentic site. Website customers are authenticated against the application server upon logging into their respective application.

Website customers are required to use a user ID and password to gain access to their accounts. To provide additional customer protection, the web application includes a session idle timeout feature that will automatically end an online session if the session remains idle for a specified time period.

Description of Functional Services and Processing:

Account Setup (Filer):

Prior to utilizing the portal, filers must establish an account. This can be accomplished by accessing the e-portal log-in page at www.myflcourtaccess.com. Filers are prompted to complete all available fields on the screen. For security purposes, the user is required to create a user name and password. In addition, a security question must be selected from the drop down menu.

Filers receive two separate email notifications associated with the account setup process. The first email notification provides the filer with confirmation that the registration process was successful and provides the filer with profile information entered during the registration process. The second email notification provides the filer with an activation link which the filer must click on to complete the registration process. Prior to activation the filer must select the same security question selected during the registration process and the correct answer.

Account Management:

The filer has access to various links to make changes to profile information and to manage their accounts. For example, the “my filings” link allows the filer to view a list of filings entered using the portal. This page shows the status filings for a specified date range.

Case Filings:

The filer can select an existing case from a list of filings and append additional documents. The filer is required to perform a series of steps and complete all required fields. Prior to submission the filer is given the opportunity to review and edit the information and documents.

Users can file new cases through the portal. The first step in the process is to enter the new case information. Filing fees are automatically calculated based on selections made by the filer. At this point, documents can be added to the case. The filer is able to browse and attach the document.

The portal accepts documents in Word, WordPerfect or PDF. All documents are converted to PDF formats by the portal. By default, the portal will provide the PDF format to the local record system. Each county will also have the option to receive the original Word document if available.

An electronic filing may be submitted to the portal 24 hours a day and seven days a week. Electronic time/date stamps are attached to the documents as filed. However, the filing is not official information of record until it has been stored on the Clerk's case management system. All dates and times, including when the filing is received at the portal and accepted by the Clerk, are stored in the portal database.

Payments:

After a case is added, the filer is then directed to the payment screen. A list of filing fees is presented in the "fee information" portion of the screen. The screen also provides an explanation (in red) of how the convenience fee is calculated.

There are three payment options available: credit card, e-check or fee waiver. The user is required to enter payment information. The system prompts the user if required information is missing. The filing cannot be submitted with missing data. Once the filer selects the submit button, the credit card and e-check routing information is verified with the appropriate institution. This authorization process automatically rejects payments made using an invalid credit card number. The following mechanisms are utilized when authorizing transactions:

- Credit Card Verification Value (CVV): This is a 3 to 4 digit security code found on the back of the credit card. The filer must enter this information.
- Address Verification System (AVS): is used to verify the identity of the person claiming to own the credit card. The system will check the billing address of the credit card provided by the user with the address on file at the credit card company.

Filers receive a confirmation upon successful filing.

Confirmation of Filing:

The filer receives three confirmations during the filing process:

1. Screen Confirmation: Immediately upon submitting the filing, the filer will receive a confirmation notice on the portal screen. A filing reference number is provided. This number is needed for communication with the county prior to a case number being assigned.
2. Email Confirmation: The filer receives an email that verifies the case was successfully submitted.
3. Email Confirmation – Clerk Review: Subsequent to the Clerk's review of the filing, the user receives another email verifying that the filing was processed successfully.

In addition to the confirmations above, the document now appears in the "my filings" on the portal website with the completion date populated.

Accounting and Reconciliation of Portal Transactions:

All transaction data is captured by the portal database ("payment engine"). This includes the order number, order date, time stamp, transaction history, status, description of service, price and quantity.

Transactions that flow through the portal are sequentially numbered. Orders are given a unique identifier at the point that users initiate transactions.

The FACC utilizes an interface called the "IPAS reconciliation system" (Access Database) between the portal and the general ledger accounting system. This process provides for an efficient and effective reconciliation of deposits (receipts) and disbursement transactions. This system produces activity summary reports that are used for reconciliation purposes. Written procedures are in place that outlines the processes for successful reconciliation.

The FACC Accounting function performs monthly bank reconciliations of the portal bank account. The payment engine provides the financial data and reports for the "book side" of the bank reconciliation. Accordingly, the bank reconciliations provide control over both safeguarding assets and data integrity for the processing of financial data through the portal. Once completed, the bank reconciliations are reviewed by FACC Senior Management.

The Authority Banking Function performs a daily confirmation/verification process on E-Filing Portal ACH Files. The purpose of this process is to verify that the transfer amount according to the bank agrees to the E-Filing Portal Payment Engine/Database. This verification process is documented on the "ACH File Transfer Log". This document includes, but is not limited to, the following items by service: 1) confirmation number 2) date of the file 2) dollar amount of the file 3) staff initials performing the process.

Control Objectives and Related Controls:

The Florida Courts E-Filing Portal's control objectives and related controls are included in Section III of this report, *Control Objectives, Related Controls, and Service Auditor's Testing of Controls.* This is to eliminate the redundancy that would result from listing them in this section and repeating them in Section III. Although the control objectives and related controls are included in Section III, they are nevertheless, an integral part of the Authority's description of controls.

Types of Tests Performed

The types of tests performed on the controls specified in Section III are described below:

1. **Inspection**

   Inspected documents and reports indicating performance of the control. This includes, among other things:

   - Examined documents or records for evidence of performance such as the existence of initials or signatures.
   - Examined output control procedures and resulting documents relative to specific transactions to ensure accurate and timely updates of records were achieved.
   - Inspected reconciliations and management reports that age and quantify reconciling items to assess whether balances and reconciling items are properly monitored, controlled and resolved on a timely basis.
   - Examined management exception reports to assess whether exception items are properly monitored, controlled and resolved on a timely basis.
   - Examined source documentation and authorizations to verify propriety of transactions processed.
   - Inspected system documentation, such as operation manuals, flow charts and job descriptions.

2. **Reperformance**

   Re-performed the processing of the control to ensure the accuracy of its operation.

3. **Observation**

   Observed application of specific controls as performed by the Authority personnel as represented.

4. **Inquiry**

   Inquiries seeking relevant information or representation from personnel were performed to obtain, among other things; knowledge and additional information regarding the control.

SECTION III.
DESCRIPTION OF CONTROLS, CONTROL OBJECTIVES, RELATED CONTROL PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

SECTION III.
ORGANIZATIONAL AND ADMINSTRATIVE CONTROLS

CONTROL OBJECTIVE 1: The organization maintains a strong control environment that sets the tone of the organization with respect to the control consciousness of its well-being.

Description of Controls	Test of Controls	Test Results
The FACC maintains a high level of control consciousness and oversight of various systems. Specifically, the FACC has the following audits/reviews: A. Annual financial statement audits B. Annual technical security review C. Quarterly technical security with respect to internet security D. Annual SSAE No. 16 Type II Engagement.	1. Inspected reports and correspondence from each audit/review. 2. Interviewed FACC management about their policies for maintaining appropriate control consciousness.	No relevant exceptions noted.
Routine meetings are held to discuss special processing requests, operational performance and the development and maintenance of projects.	1. Interviewed FACC management about routine meetings that occur related to the portal. 2. Inspected documents from meetings (correspondence, agendas, minutes, etc).	No relevant exceptions noted.
FACC management provides oversight for system security.	1. Inquired to management about system security. 2. Inspected most recent Security Consulting Report.	No relevant exceptions noted.
Written position descriptions are maintained by the FACC. These are periodically updated.	1. Inspected job descriptions for all employees involved with the portal activities. 2. Interviewed employees to verify accuracy of documents.	No relevant exceptions noted.

SECTION III.
ORGANIZATIONAL AND ADMINSTRATIVE CONTROLS

CONTROL OBJECTIVE 1: The organization maintains a strong control environment that sets the tone of the organization with respect to the control consciousness of its well-being.

Description of Controls	Test of Controls	Test Results
Written performance evaluations are administered on an annual basis. These evaluations include stated goals and objectives. Performance evaluations are reviewed by Senior Management and become part of the employees' personnel file.	1. Inquired to management and discussed the evaluation process. Verified that evaluations take place on an annual basis. 2. Reviewed a sample of annual performance evaluations for those employees involved with the E-Filing Portal system. Verified the following: • Annual performance evaluations were present in the file • Each evaluation was signed by the employee and member of management • Evaluation included the employees' goals and objectives • Evaluation contained feedback and constructive criticism	No relevant exceptions noted.
The Clerks of Court and the Clerk of the Supreme Court entered into an Interlocal Agreement establishing an internet portal for the electronic filing of court documents. The E-Filing Authority requires a signed Joinder to the Interlocal Agreement (on file) from all Clerks prior to executing transactions.	1. Inquired to management that signed contracts are on file for each Clerk participating in E-Filing Portal services. 2. Inspected the E-Filing Authority Interlocal Agreement. 3. Inspected a sample of E-Filing Portal contracts to verify that the contract is complete and signed by the respective Clerks.	No relevant exceptions noted.

SECTION III.
ORGANIZATIONAL AND ADMINSTRATIVE CONTROLS

CONTROL OBJECTIVE 1: The organization maintains a strong control environment that sets the tone of the organization with respect to the control consciousness of its well-being.

Description of Controls	Test of Controls	Test Results
FACC staff involved in the E-Filing Portal functions are competent and possess the necessary professional experience.	1. Interviewed FACC management on policy for hiring practices. 2. Reviewed background and technical experience information in employee's personnel file (i.e. work experience, education, certifications, etc). 3. Interviewed staff to verify their background and technical experience.	No relevant exceptions noted.

SECTION III.
TRANSACTION PROCESSING AND RECONCILIATION

CONTROL OBJECTIVE 2: Transactions that are processed through the E-Filing Portal system are authorized, processed, recorded completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
The FACC is organized into separate functional areas to provide adequate segregation of duties.	1. See page 39 for the testing performed on segregation of duties.	No relevant exceptions noted.
The FACC Accounting function performs monthly bank reconciliations of the portal bank account. The portal payment engine provides the financial data and reports for the "book side" of the bank reconciliation. Accordingly, the bank reconciliations provide control over both safeguarding assets and data integrity for the processing of financial data through portal. The bank reconciliations are reviewed by FACC Senior Management.	1. Inquired to Management that portal bank reconciliations are performed in a timely manner. 2. Verified that reconciling items were properly documented and that the FACC provided reasonable explanations as to the nature of the reconciling items. 3. Verified that source documents existed and were available for all amounts on the bank reconciliations. 4. Verified the mathematical accuracy of the bank reconciliations selected. 5. Requested the most recent bank reconciliation to verify that it was completed timely (within 30 days of month end). 6. Inspected a sample of bank reconciliations to verify the required review and approvals were performed and documented.	No relevant exceptions noted.

SECTION III.
TRANSACTION PROCESSING AND RECONCILIATION

CONTROL OBJECTIVE 2: Transactions that are processed through the E-Filing Portal system are authorized, processed, recorded completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
Transactions that flow through the portal are sequentially numbered. Orders are given a unique identifier at the point that users initiate transactions.	1. Interviewed management on the methodology in place to uniquely identify portal transactions. Verified that transactions are sequentially numbered. 2. Inquired to management to verify that order numbers are established at the point a user attempts a transaction. 3. Requested the first and last order numbers processed through the portal. Inspected a sample of transactions to verify that orders were accounted for and within the fiscal year.	No relevant exceptions noted.
The user organizations (Clerks) have online 24/7 access to E-Filing Portal financial data and reports.	1. Interviewed FACC Management and staff to verify that Clerks have 24/7 access to E-Filing Portal systems for relevant financial information. 2. Reviewed FACC training guide/procedure manuals to verify that guidance is available to clerks. 3. Requested FACC IT Management demonstrate the online 24/7 access. Confirmed that the Clerks have access to the system for relevant financial reports and information.	No relevant exceptions noted.

SECTION III.
TRANSACTION PROCESSING AND RECONCILIATION

CONTROL OBJECTIVE 2: Transactions that are processed through the E-Filing Portal system are authorized, processed, recorded completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
The FACC utilizes an interface called the "IPAS reconciliation system" (Access database) between the portal and the accounting system. This process provides for an efficient and effective reconciliation of deposit (receipts) and disbursement transactions. This system produces activity summary reports that are used for reconciliation purposes. Written procedures are in place for using the IPAS reconciliation system.	1. Interviewed the FACC Management to verify that this is performed. 2. Inspected reports generated from the system. Verified the accuracy and completeness of the reports. 3. Traced selected receipt/disbursement transactions from the portal database through to the accounting system and bank statements. 4. Reviewed reconciliation procedures. Verified the consistency with actual procedures observed.	No relevant exceptions noted.
The FACC Banking function scans physical paper checks for certain transactions received in the mail daily. The scanning process electronically sends a deposit to the portal bank accounts. All other payments made on-line via credit card or e-check in the portal are automatically sent as a deposit to the portal bank accounts through the portal payment engine. • All Checks are logged by the mail clerk. • Once checks are scanned and deposited, a report is produced that acts as a deposit slip. This is reconciled with the bank.	1. Inquired to FACC Banking Administrator to gain understanding and verify this process occurs on a daily basis. 2. Reviewed procedures for scanning of the checks. 3. Inspected sample mail logs and deposit documentation.	No relevant exceptions noted.

SECTION III.
TRANSACTION PROCESSING AND RECONCILIATION

CONTROL OBJECTIVE 2: Transactions that are processed through the E-Filing Portal system are authorized, processed, recorded completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
The Authority Banking Function performs a daily confirmation/verification process on portal ACH Files. The purpose of this process is to verify that the transfer amount according to the bank agrees to the portal Payment Engine/Database. This verification process is documented on the "ACH File Transfer Log". This document includes, but is not limited to, the following items by service: 1) confirmation number 2) date of the file 2) dollar amount of the file 3) staff initials performing the process.	1. Interviewed the Banking Administrator to gain understanding of this process. Verified that this process occurs on a daily basis. 2. Observed the Banking Administrator perform the daily ACH file confirmation process for selected dates. 3. Inspected daily logs for a selected month to verify the process had been performed and documented. 4. Requested detailed portal payment engine reports and portal bank statements. Verified that detailed disbursement reports agreed to the transfer amounts listed on the bank statements.	No relevant exceptions noted.
The portal includes banking controls for credit card transactions. This authorization process automatically rejects payments made using an invalid credit card number. The following mechanisms are utilized when authorizing transactions: • Credit Card Verification Value (CVV) • Address Verification System	1. Inquired to FACC Management and staff on the Cybersource authorization process. 2. Observed FACC staff attempting to make several credit card payments on portal using invalid credit card numbers.	No relevant exceptions noted.

SECTION III.
PHYSICAL SECURITY

CONTROL OBJECTIVE 3: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
Electronic badge devices control access to all entrances to the building. The main entrance remains unlocked during business hours (8:00am-5:00pm) for visitors.	1. Observed that all entrances (with exception of main entrance) remained locked at all times. 2. Observed the presence of electronic key devices at the entrances to the FACC building.	No relevant exceptions noted.
Electronic badge devices control the access to the FACC server room. Only specified technical staff have access to this secured location.	1. Verified the server room is locked. 2. Observed the presence of an electronic key device at the entrance of the server room.	No relevant exceptions noted.
Access to the server room is restricted to only members of the FACC Information Technology Department who are responsible for administration and support of the internal network and the technical environment.	1. Inspected a listing of individuals with access to the server room. Verified that only current employees have access. 2. Observed non-authorized staff unsuccessfully attempting access.	No relevant exceptions noted.
Automated electronic reports are periodically generated for monitoring of traffic in and out of the FACC building and server room.	1. Inspected report generated from the system that lists all traffic in and out of the building and server room.	No relevant exceptions noted.
All visitors must use the main entrance of the FACC facility. FACC visitors are required to sign a visitor's log upon entering the facility. In addition, all visitors are provided visitor badges.	1. Verified the front entrance is the only un-locked entrance during normal office hours. 2. Observed visitors entering and exiting the building. 5. Observed receptionist providing visitor badges.	No relevant exceptions noted.

SECTION III.
PHYSICAL SECURITY

CONTROL OBJECTIVE 3: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
An escort (FACC staff) is called to greet their visitors in the lobby.	1. Verified through observation that guests are accompanied by a FACC staff employee at all times.	No relevant exceptions noted.
The FACC conducts employment background checks and criminal history checks on external candidates selected to fill vacant positions.	1. Inspected Human Resource procedures to verify that background checks are required for all new employees. 2. Inspected background/criminal history check log for all employees hired in the audit period. 3. For selected employees, inspected background/ criminal history check documentation.	No relevant exceptions noted.
A security consulting company, under contract with the FACC, performs an annual stringent review of the FACC system's security within which the portal operates. The consulting company conducts an exit conference, issues an executive summary report, issues a detailed technical report and provides recommendations for improvement to FACC Senior Management.	1. Inquired to FACC Management about the Security Consulting engagement and method of addressing recommendations. 2. Inspected the most recent security consulting report.	No relevant exceptions noted.
FACC has an alarm system in place to monitor and notify the company of any unauthorized access. The alarm system is serviced annually by the vendor to ensure that the system is operating correctly.	1. Inspected contract with vendor to verify the existence of alarm system. 2. Performed a walkthrough of the building to verify the existence of an alarm system.	No relevant exceptions noted.

SECTION III. PHYSICAL SECURITY		
CONTROL OBJECTIVE 3: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.		
Description of Controls	**Test of Controls**	**Test Results**
The Authority is required by the credit card companies, who provide credit card services for the portal, to undergo quarterly systems security reviews. The quarterly reviews focus on internet security issues.	1. Inquired to FACC Management about the work performed by this company. 2. Inspected reports to ensure that the FACC passed the security review. 3. Verified that the FACC has posted certification, of successful completion, on the website.	No relevant exceptions noted.

SECTION III.
ENVIRONMENTAL CONTROLS

CONTROL OBJECTIVE 4: Controls provide reasonable assurance that the physical environmental devices are installed to adequately protect the servers, network equipment, and storage media.

Description of Controls	Test of Controls	Test Results
Multiple air-conditioning units are present in order to regulate the temperature in the FACC server room. Periodic inspections and preventative maintenance procedures are performed on the equipment.	1. Observed the FACC server room and verified that air conditioning systems are present in the server room. 2. Verified that a maintenance agreement exists on the air conditioning systems.	No relevant exceptions noted.
An FM-200 Fire Extinguishing System, equipped with smoke and heat detectors, is installed in the FACC server room. FM-200 equipment is under service agreement for semi-annual inspections and receives preventative maintenance as required.	1. Observed the FACC server room and noted the FM-200 release heads were present throughout the server room. 2. Inspected maintenance agreements.	No relevant exceptions noted.
An uninterruptible power supply system (UPS) has been installed to protect against loss of data during a power failure and is subjected to periodic testing and maintenance.	1. Toured facility and verified the presence and location of UPS. 2. Inspected UPS maintenance and test records.	No relevant exceptions noted.
A diesel generator is installed at the FACC facility to provide backup power in the event of a power failure. Diesel generators are configured to self-exercise periodically and are under maintenance agreement to receive preventative maintenance.	1. Observed the diesel generator at the FACC facility and verified that a diesel generator was in place to provide backup power to the facility. 2. Inspected the maintenance agreement and verified that the generator is inspected on an annual basis.	No relevant exceptions noted.

SECTION III.
NETWORK SECURITY AND INTERNET ACCESS

CONTROL OBJECTIVE 5: Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
A network diagram illustrates the physical and logical connections of FACC information systems.	1. Inspected the FACC System/Network Diagram.	No relevant exceptions noted.
Communication equipment and servers are labeled to facilitate cross-reference of these diagrams.	1. Inquired to management about the FACC systems/networks. 2. Observed the server room and compared physical equipment (labeled) to the network diagram.	No relevant exceptions noted.
Firewalls are embedded in the system to prevent unauthorized access. Further, various FACC functions are separated into VLANs that provide access restrictions. The system is capable of generating firewall logs of activity.	1. Verified inclusion of firewalls on system diagram. 2. Observed the FACC produce firewall logs for a specific time frame. 3. Verified that this log reflects all attempted access to the systems.	No relevant exceptions noted.
Antivirus protection has been implemented at FACC server, email gateway, and workstation levels to protect company data from infection by malicious code or viruses.	1. Verified antivirus software exists on servers and a selection of workstations. 2. Reviewed written antivirus policies contained in the Security Policies and Procedures Manual. 3. Obtained log of periodic virus scans on servers and workstations.	No relevant exceptions noted.

SECTION III.
NETWORK SECURITY AND INTERNET ACCESS

CONTROL OBJECTIVE 5: Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
The Florida Courts E-Filing Portal contains a Digital Certificate (SSL - Web Certificate). Certificates have been issued by a known certificate authority and are accessible on the website.	1. Inspected certificate documentation provided from vendor. Verified that the current certificate was current and had not expired. 2. Observed website to verify that the digital certificate is displayed.	No relevant exceptions noted.
Windows and Network password management controls include the following: -Minimum password length. -Character components. -Password expiration/change frequency -Invalid password attempts -Password storage.	1. Obtained the domain security policy and confirmed the parameters match control details and Security Policies & Procedures document. 2. Observed employee unable to log into system with invalid passwords. 3. Viewed history of password expiration.	No relevant exceptions noted.
Change requests (moving, adding, changing, etc) are initiated by the Human Resource Function and communicated to the IT Department.	1. Confirmed through corroborative inquiry with Management of IT that the control activity is in place.	No relevant exceptions noted.
The Human Resource Function notifies the IT Department of all new employees and terminations.	1. Confirmed through corroborative inquiry with Management of IT that the control activity stated is in place. 2. Obtained a list of terminated employees during audit period. Inspected the Windows Active Directory (AD) to verify that all terminated employees were disabled or eliminated.	No relevant exceptions noted.

SECTION III.
NETWORK SECURITY AND INTERNET ACCESS

CONTROL OBJECTIVE 5: Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
FACC has comprehensive data security procedures in place. An annual meeting is held to educate staff members on the policies and procedures.	1. Inspected Security Policies and Procedures document. 2. Obtained documentation on the annual staff meetings regarding the Security Policies and Procedures.	No relevant exceptions noted.
FACC engages an outside consulting company to perform an annual stringent review of security for FACC systems. This company conducts an annual exit conference, issues an executive summary report, and issues a detailed technical report that includes recommendations to management.	1. Inspected most recent annual security report. 2. Verified that the report did not identify major problems or weaknesses in the system. 3. Verified that recommendations were provided to management for improvement.	No relevant exceptions noted.
The FACC is required by the credit card companies to undergo quarterly security reviews. The quarterly reviews focus on internet security and are provided by an outside vendor.	1. Read quarterly review reports to ensure the FACC passed security review. 2. Verified that the FACC has posted certification of successful completion on the website.	No relevant exceptions noted.
FACC uses Microsoft Window Server Update Services (WSUS) to manage and install Microsoft critical and security patches.	1. Observed FACC gain access to the WSUS software. 2. Inspected reports of managed FACC servers and workstations.	No relevant exceptions noted.

SECTION III.
NETWORK SECURITY AND INTERNET ACCESS

CONTROL OBJECTIVE 5: Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
FACC uses third party software to monitor the websites and portals to confirm sites are operating and that connections can be made.	1. Confirmed through corroborative inquiry with IT Management that the control activity stated is in place. 2. Observed access to the monitoring software and confirmed it was active. 3. Inspected periodic email reports sent to FACC IT that reflects monitoring results and any potential issues with the FACC websites.	No relevant exceptions noted.
FACC uses managed software to enforce security on Personal Digital Assistant (PDA) devices.	1. Reviewed written PDA policy contained in the Security Policies and Procedures document. 2. Verified managed software is present with PIN enforcement settings.	No relevant exceptions noted.
A Uniform Resource Locator (URL) filter is in place to detect and block potentially malicious links from being accessed.	1. Verified with management the existence of the URL filtering device. 2. Inspected sample logs of blocked potentially malicious URLs.	No relevant exceptions noted.
FACC has established security roles within the portal website in order to restrict users based on their authorized permissions.	1. Obtained a list of the portal security roles with detailed descriptions showing associated permissions. 2. Obtained screenshot subsequent to logging into the portal to verify security rules had been properly implemented and assigned.	No relevant exceptions noted.

SECTION III.
INFORMATION AND COMMUNICATION

CONTROL OBJECTIVE 6: Controls provide reasonable assurance that the information and communication component includes the procedures and records established by the FACC to initiate, process, and report the user organizations' (Clerks) transactions and maintain accountability for the transactions.

Description of Controls	Test of Controls	Test Results
FACC has established and maintains written policies and procedures for various tasks and activities associated with the portal.	1. Inspected written policies and procedures that pertain to portal. 2. Observed certain processes to verify consistency with written procedures.	No relevant exceptions noted.
The FACC maintains an organizational chart for the Organization and the Technical Division that clearly depicts lines of authority.	1. Inspected FACC organizational chart as it relates to portal. Obtained explanations from the FACC on the various functions presented. 2. During the course of the audit, observed various positions to verify work performed was consistent with organizational chart and job descriptions.	No relevant exceptions noted.
The FACC has routine meetings to discuss special processing requests, operations, and the development and maintenance of projects.	1. Inquired to management about the existence of routine technical meetings. 2. Inspected documentation from meetings (correspondence, agendas, minutes, etc).	No relevant exceptions noted.
The FACC has implemented an Information Technology Service Management (ITSM) framework and Information Technology Infrastructure Library (ITIL) best practices for FACC technical projects. Selected staff have been trained and earned the ITSM/ITIL Foundation certification.	1. Inquired to management about the existence of ITSM/ITIL framework and best practices. 2. Inspected ITSM/ITIL related documents. 3. Inspected employee certifications in ITSM/ITIL.	No relevant exceptions noted.

SECTION III.
INFORMATION AND COMMUNICATION

CONTROL OBJECTIVE 6: Controls provide reasonable assurance that the information and communication component includes the procedures and records established by the FACC to initiate, process, and report the user organizations' (Clerks) transactions and maintain accountability for the transactions.

Description of Controls	Test of Controls	Test Results
The FACC produces several reports that assist management in the monitoring objective of the portal. These are distributed to key management and staff and are discussed at routine meetings.	1. Confirmed through corroborative inquiry that the control activity stated is in place. 2. Inspected samples of each report and documented its nature and purpose.	No relevant exceptions noted.
The FACC has a Service Center function that provides on-going support for the existing FACC applications.	1. Inquired to management as to the nature of the FACC Service Center. 2. During the course of the audit, observed the Service Center staff performing their tasks. 3. Inspected tracking logs or other documentation from the database that tracks issues arising from customers.	No relevant exceptions noted.
The FACC provides necessary training to Clerks engaged in services offered by E-Filing Portal. This is to ensure that the Clerks understand how to use and navigate the various systems administered by the FACC (including E-Filing Portal).	1. Inquired to management as to the type of training/operational procedures in place. 2. Inspected manuals/procedures made available to Clerks for the various components of portal.	No relevant exceptions noted.
Procedure Guides have been developed for the users of the E-Filing Portal. This is to ensure that the users understand how to navigate the system.	1. Inquired to management as to the type of training/operational procedures in place. 2. Inspected procedure manuals made available to users of the E-Filing Portal.	No relevant exceptions noted.

SECTION III. SEGREGATION OF FUNCTIONS (INTERNAL)		
CONTROL OBJECTIVE 7: Controls provide reasonable assurance that FACC activities are organized to provide internal segregation of functions.		
Description of Controls	**Test of Controls**	**Test Results**
The FACC is organized into separate functional areas to provide adequate separation of duties.	1. Reviewed job descriptions and organizational chart noting the degree of separation within the FACC. 2. Interviewed management and staff to determine adherence to the organizational charts and policies. For example, the accounting department should be separate from system programming and operations. 3. Observed various duties/ functions being performed by the FACC staff.	No relevant exceptions noted.
The FACC maintains an organizational chart for the Technical Division that clearly depicts lines of authority.	1. Inspected FACC organizational chart as it relates to the portal. Obtained explanations from the FACC on the various functions presented. 2. During the course of the audit, observed various positions to verify work is performed consistent with organizational chart and job descriptions.	No relevant exceptions noted.
FACC operations personnel do not perform programming functions. Programming personnel do not perform operations duties.	1. Reviewed the IT (Information Technology) organization chart noting the degree to which operations and programming functions are segregated. 2. Interviewed computer operations management to determine adherence to policy.	No relevant exceptions noted.

SECTION III.
SEGREGATION OF FUNCTIONS (INTERNAL)

CONTROL OBJECTIVE 7: Controls provide reasonable assurance that FACC activities are organized to provide internal segregation of functions.

Description of Controls	Test of Controls	Test Results
Programming personnel do not initiate or authorize transactions.	1. Reviewed the policies and procedures of FACC.	No relevant exceptions noted.
Written job descriptions have been prepared for FACC personnel and are periodically updated.	1. Reviewed employee job descriptions for those employees involved with the portal. 2. Interviewed management and employees to verify accuracy of these documents.	No relevant exceptions noted.

SECTION III. SEGREGATION OF FUNCTIONS (EXTERNAL)		
CONTROL OBJECTIVE 8: The FACC and User Organizations (Clerks) are segregated.		
Description of Controls	**Test of Controls**	**Test Results**
FACC is physically separate from the user organizations (Clerks) for which it performs processing.	1. Reviewed policies of the organization and contractual obligations that exist between FACC and user organizations.	No relevant exceptions noted.
The relationship between the FACC and user organizations is contractual in nature.	2. Reviewed policies of FACC and contractual obligations that exist between FACC and user organizations.	No relevant exceptions noted.

SECTION III. SERVICE FEE SCHEDULE		
CONTROL OBJECTIVE 9: Controls provide reasonable assurance that service fees are properly charged and are in accordance with contracts, laws and regulations.		
Description of Controls	**Test of Controls**	**Test Results**
E-Filing Portal has an approved service fee schedule governing on-line transactions.	1. Inspected the uniform E-Filing Portal fee schedule. 2. Verified approval of the service fees by the Board.	No relevant exceptions noted.
The portal has system parameters (source code) for specific transactions in accordance with the service fee schedule.	1. Randomly select transactions occurring during the audit period. 2. Inspected order detail report generated directly from the portal system. 3. Recalculated the service fee(s) for each order to verify that the portal charged the customer correctly.	No relevant exceptions noted.
Users are informed prior to submitting on-line payment of the service fee charged. In addition, the customer is requested to confirm order (payment information).	1. Inspected website as user attempts to make a payment. Verified that the service fee is presented prior to submitting order. Verified that customer is requested to confirm order.	No relevant exceptions noted.

SECTION III.
DATA BACKUP AND RECOVERY

CONTROL OBJECTIVE 10: Controls provide reasonable assurance that Backup and Recovery procedures are available to preserve the integrity of programs and data files.

Description of Controls	Test of Controls	Test Results
The following schedule of backups and controls are being performed: • Daily • Monthly • Annual Backups are performed utilizing a custom script that has been implemented on the server.	1. Inspected automated script utilized by FACC staff in performing the backup. 2. Inquired to management about the system and the backup schedule. 3. Inspected the FACC system diagram/flowchart to understand the various components, servers, databases and etc. 4. Observed a selection of backup logs for various servers identified on the network diagram. 5. Inspected vendor documents that substantiated that selected days were picked up and taken to storage. 6. Performed a backup of randomly sampled files to tape.	No relevant exceptions noted.
The backup process is performed in accordance with detailed written procedures.	1. Inquired to management about the backup procedures and associated processes. 2. Reviewed the backup schedule in place for the FACC server and data files. 3. Inspected a selection of backup logs to verify compliance with procedures.	No relevant exceptions noted.
Tapes are taken off-site by a contracted vendor daily. This process is conducted in accordance with FACC written procedures. The vendor stores the tapes in a safe and secured environment.	1. Interviewed management about procedures for taking tapes off-site to a safe and secured location.	No relevant exceptions noted.

SECTION III.
DATA BACKUP AND RECOVERY

CONTROL OBJECTIVE 10: Controls provide reasonable assurance that Backup and Recovery procedures are available to preserve the integrity of programs and data files.

Description of Controls	Test of Controls	Test Results
Inventory of backup tapes are available via the Vendor's inventory system that is accessible by the company administrative personnel.	1. Inquired to management about the vendor inventory process. 2. Inspected inventory of backup tapes.	No relevant exceptions noted.
Recoveries are performed on a periodic basis.	1. Inquired to management about the recovery process procedures. 2. Performed a recovery of randomly sampled files from tape.	No relevant exceptions noted.