Internal Controls and Fraud Detection

Florida School Finance Officers Association
November 10, 2015

Presented by
Jennifer Christensen, Partner
Cheri Swain, Manager

CRI CARR RIGGS & INGRAM
CPAs and Advisors

TODAY'S PRESENTATION

- Types of fraud
- Preventing fraud
- Understanding IT risks

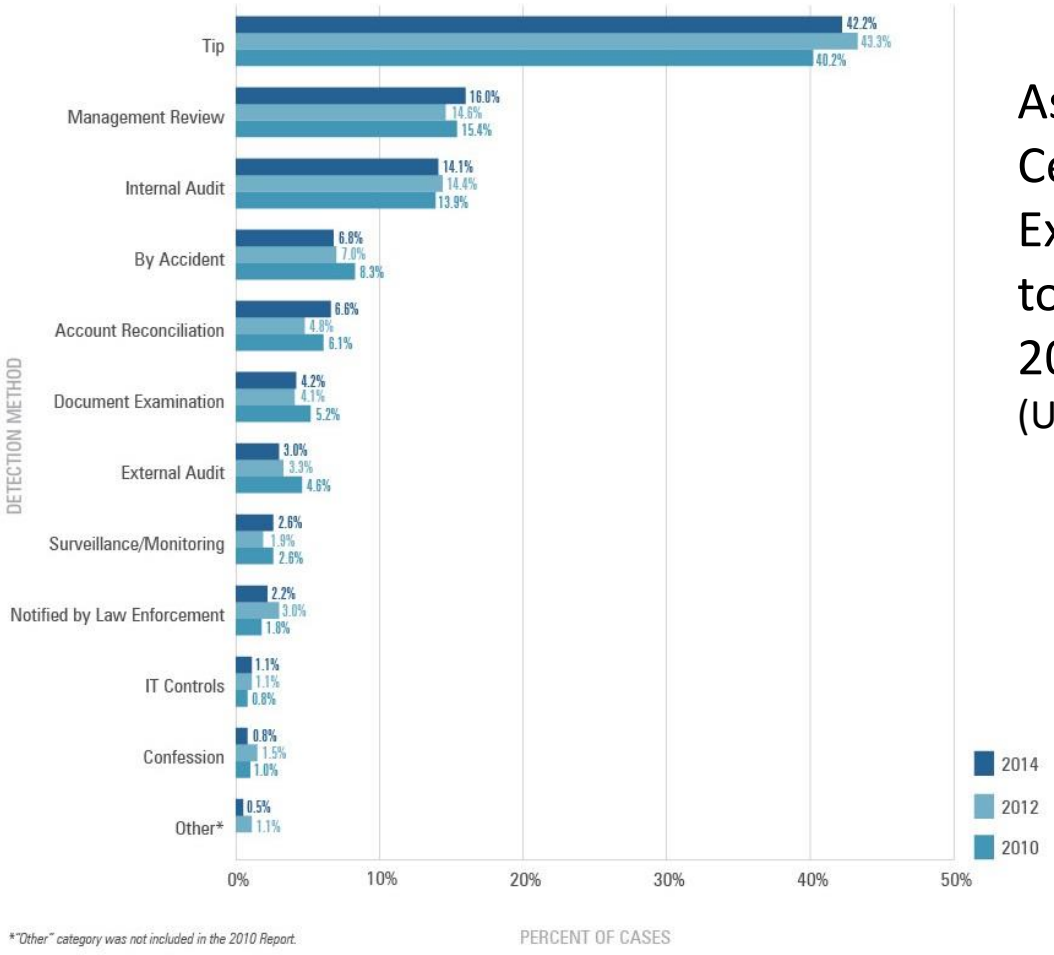
TYPES OF GOVERNMENT FRAUD

Fraud: Misappropriation of Assets and Misstating Financial Information

- **Skimming**
  - Funds are diverted before they are ever recorded in the books.
- **Purchase Card Abuse**
  - Use of organization-issued cards for personal use or misuse of credit card and identity information.
- **Fictitious Vendors**
  - Perpetrators set up a company and submit fake/altered invoices for payments.
- **Conflicts of Interest**
  - School Board or principals have financial interest from or with vendors.
- **Payroll**
  - Fictitious employees, continued payment of terminated employees, fraudulent timekeeping.
- **Theft of Assets**
  - Theft of school district property.

DETECTING FRAUD

Figure 11: Initial Detection of Occupational Frauds

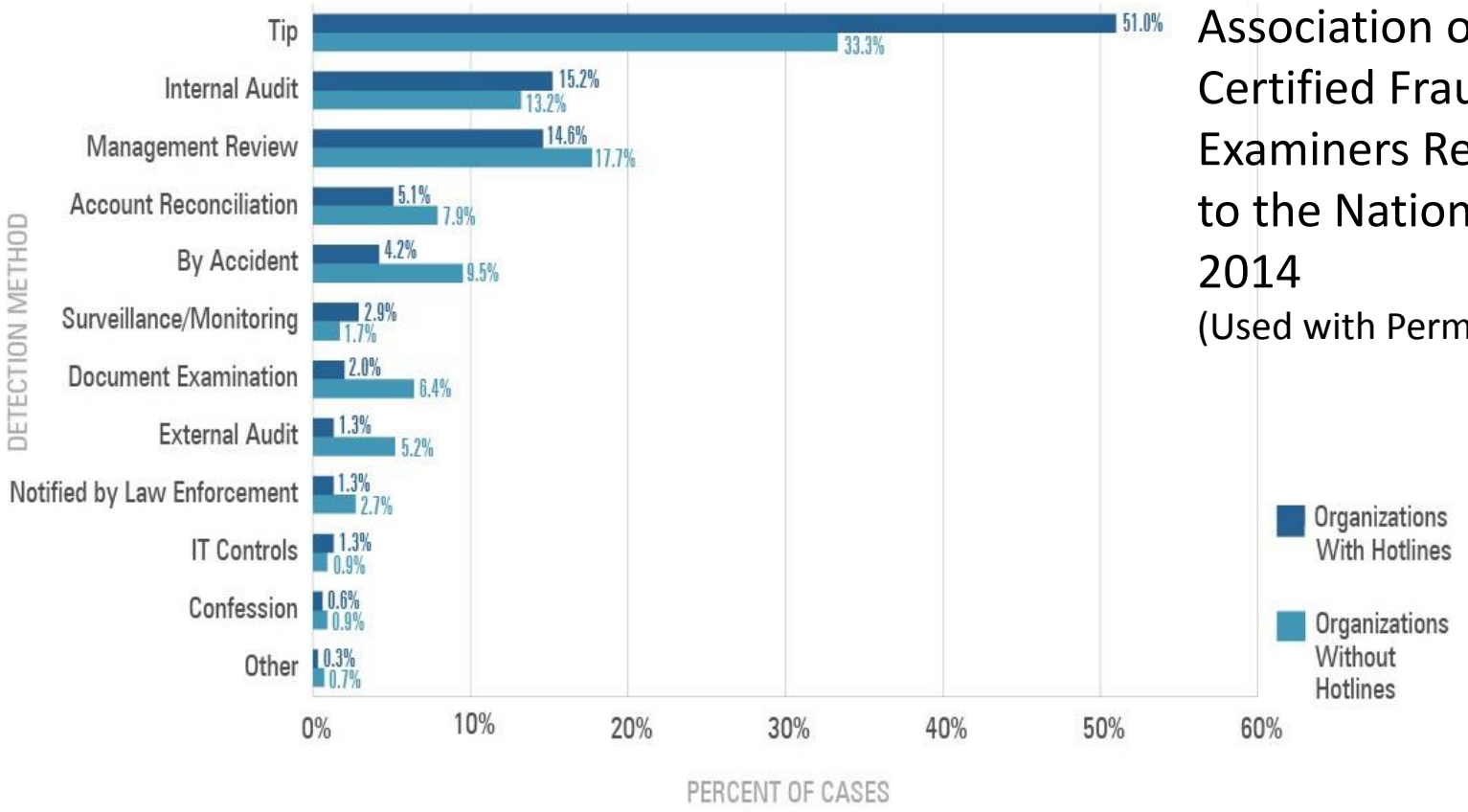


Association of Certified Fraud Examiners Report to the Nation – 2014
(Used with Permission)

CARR, RIGGS & INGRAM, LLC

DETECTING FRAUD

Figure 14: Impact of Hotlines

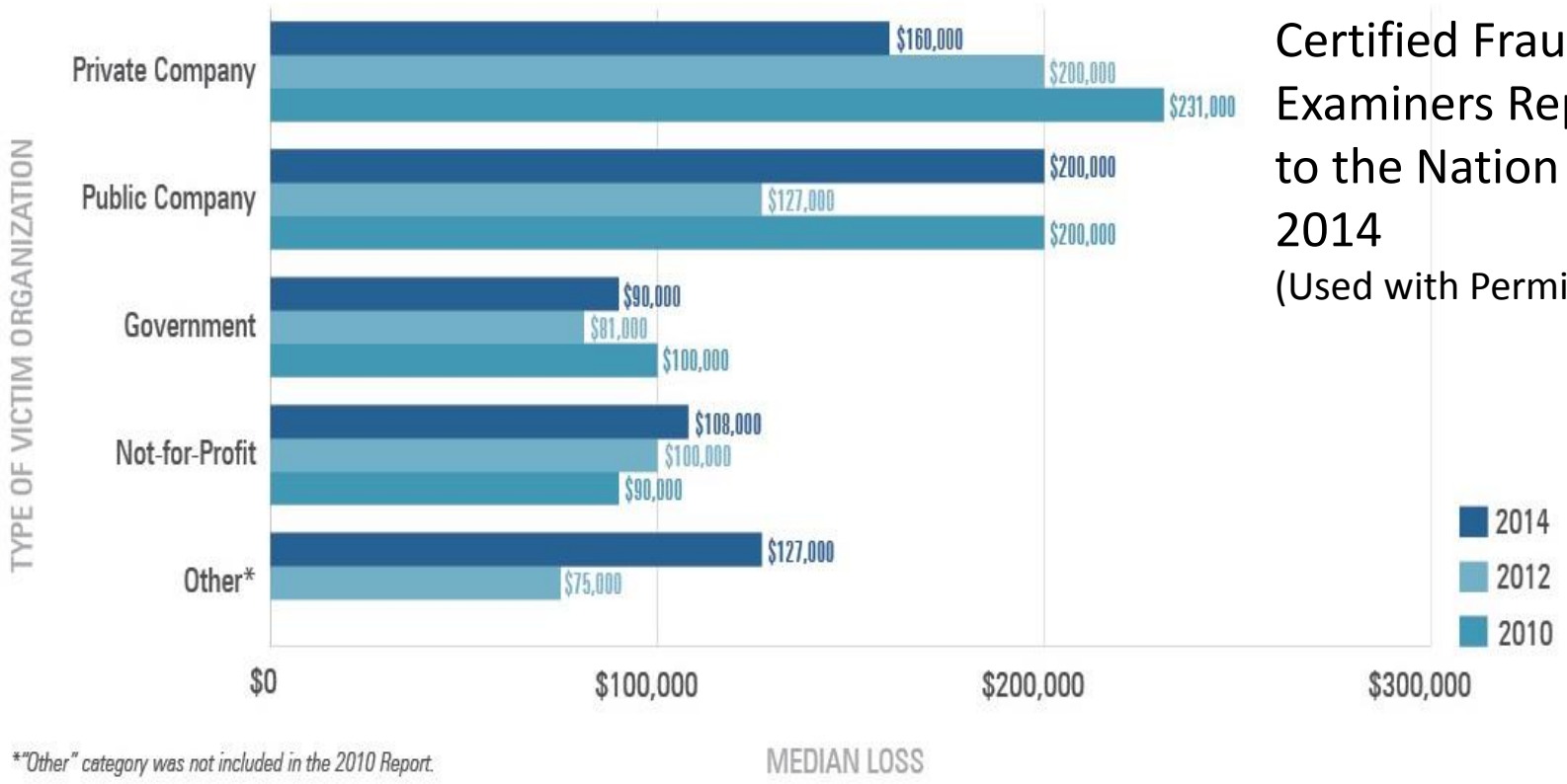


Association of Certified Fraud Examiners Report to the Nation – 2014
(Used with Permission)

CARR, RIGGS & INGRAM, LLC

DETECTING FRAUD

Figure 18: Type of Victim Organization — Median Loss



*"Other" category was not included in the 2010 Report.

Association of Certified Fraud Examiners Report to the Nation – 2014
(Used with Permission)

CARR, RIGGS & INGRAM, LLC

ACFE STATISTICS

- Approximately **40%** of fraud cases are due to a simple lack of internal controls.
- Following a fraud, approximately **80%** of organizations modify internal controls.
- People **36 - 50** account for more than **60%** of fraud perpetrators.
- Approximately **90%** of perpetrators have been on the job at least one year. **50%** have been for six or more years.
- More than **85%** have never been charged/convicted of fraud.
- More than **82%** have never been punished or terminated during their employment.

PREVENTING FRAUD

- **Set clear standards of what is expected**
  - Need to set tone at the top (i.e. School Board, Administrators, Principals)
  - Code of conduct
- **Establish an anti-fraud program**
  - Whistle-blower policy
  - Tip hotline (phone, email, text) and advertise it to employees, vendors, and the public
  - Respond appropriately to any discovered fraud
  - Educate all employees on program (increases perception of being caught)
  - Ask questions

PREVENTING FRAUD

- **Educate Administrators and Management**
  - Basic fraud training
    - What is fraud?
    - How can fraud be detected and prevented and what is your responsibility to do this?
    - How to read and understand financial reports?
  - How to identify risks and what to look for
    - Know your employees
    - Observe sudden and unusual lifestyle changes

PREVENTING FRAUD

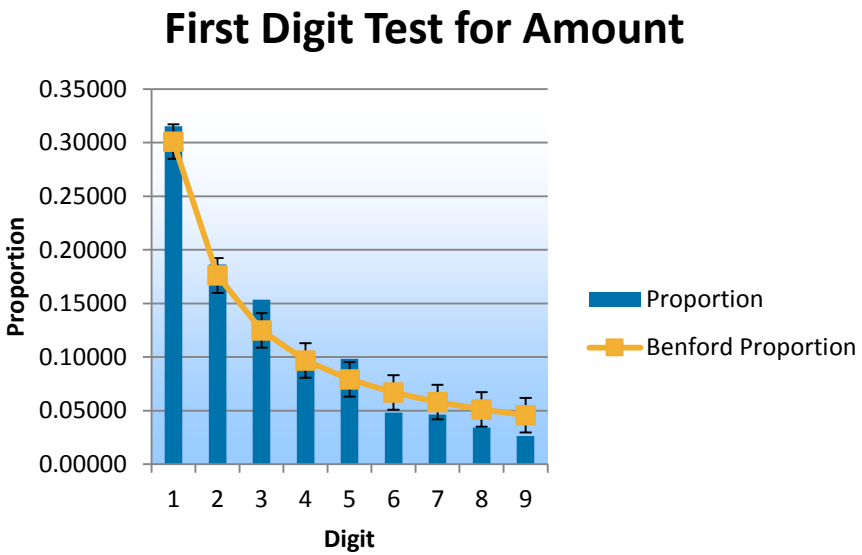
- **Create an audit committee**
  - Should have finance and audit background
  - Assesses high risk areas
  - Provides independent look at processes
- **Create formal purchasing (and purchasing card) policies**
  - Include reviews of transactions - who is reviewing the administrators' charges?
  - Require School Board approval for purchases over a certain threshold
  - Restrict purchasing cards with spending limits and merchant accounting codes
  - Require receipts as evidence of items purchased and amount of purchase
  - Require shipping documents (proof of delivery) for all transactions and review document to see what location goods were delivered to

PREVENTING FRAUD

- **Rotation of duties for departments such as payroll, accounts payable, account receivable, purchasing**
  - Do all of your employees use vacation time?
  - Are staffing levels sufficient?
- **Online collections/payments**
  - Reduces fraud and risk of human error
  - Provides efficiency with bookkeeping
  - Need to have proper access controls in place
  - Theft of cash likely small amount, but can add up when multiple people do it over a long length of time
- **Use of internal/external auditors**
  - How many internal auditors do you have on staff?
  - Perform surprise audits
  - Monitoring plans – use of data extraction tools

TESTS FOR INTERNAL/EXTERNAL AUDITORS

- **Data extraction tests**
  - Matching vendor addresses with employee addresses
  - Reviewing direct deposit information for multiple deposits into same bank account
  - Review of night and weekend journal entries
  - Benford's analysis



FRAUD: NOT JUST A FINANCIAL CONCERN

- **Education Theft**
  - Residency fraud
- **Fraudulent reporting of educational statistics**
  - Test scores
  - Learning gains
  - Enrollment numbers
- **Information Technology**
  - Theft of personal information – social security numbers, health information, credit card numbers

INFORMATION TECHNOLOGY

- **Why its important to understand information technology general controls**
  - User access controls
  - Availability
  - Security
- **Factors to consider when analyzing complexity/risks:**
  - Number of users
  - Number of interfaces with other applications
  - Length of time in service
  - Physical location of programs and data
  - Necessary to include in disaster plan
- **Understanding service organizations**

SERVICE ORGANIZATIONS

- **SOC reports**
  - **SOC 1** report provides information on an organization's processes and controls.
  - **SOC 2** provides a description of the organization's processes and controls and measures that description against the AICPA's Trust Service Principals: **Security, Availability, Processing Integrity, Confidentiality, Privacy**.
  - **Type 2** verifies that the controls functioned as described during a specified period.
  - **SOC 3** provides a limited view of the organization's system and controls related to information technology and data security and, therefore, is suitable to be used in the service organization's marketing and sales efforts

READING A SOC REPORT

- **3 Parts**
  - Auditor's report & management's assertion
  - Description of the organization's processes and controls
  - Auditor testing
- **Subservice organizations**
- **User control considerations**

SOC REPORT EXAMPLE

TABLE OF CONTENTS

I. *Independent Service Auditors' Report* 3

Independent Service Auditors' Report 4

II. *Information Provided by ABC Company, Inc.* 6

Management Assertions Letter 7

Description of ABC Company's IT and Collection Management Systems 9

Company Overview 9

ABC Company's Products and Services Overview 9

Relevant Aspects of the Control Environment, Risk Assessment, Informaiton and Communication, Control Activities, and Monitoring 11

Control Environment 11

Risk Assessment 13

Information and Communications 13

Control Activities 17

Monitoring 18

Subservice Organizations 18

User Control Considerations 19

III. *Information Provided by Auditor* 20

Control Objectives, Related Controls, and Tests of Operating Effectiveness 21

1.0 – Organization and Administration 21

2.0 – Access 24

3.0 – Network Infrastructure 26

4.0 – Backup and Recovery 27

5.0 – Client Setup and Collections Processing 28

6.0 – Payment Processing 30

7.0 –Trust Account Reconciliation 31

SOC REPORT EXAMPLE

Independent Service Auditors' Report

To the Management of ABC Company, Inc.

Scope

We have examined ABC Company, Inc.'s ("ABC", or "the Company") description of its information technology (IT) and collection management systems for processing user entities' transactions throughout the period January 1, 2014 to December 31, 2014 ("description") and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

ABC uses a subservice organization for data center services. The description of the system in Section II of this report includes only the control objectives and related controls of ABC and excludes the control objectives and related controls of the subservice organization. Our examination did not extend to controls of the subservice organization.

ABC's Responsibilities

In Section II of this report, the Company provided an assertion about the fair presentation of the description and the suitability of design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and 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.

Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the 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 from January 1, 2014 through December 31, 2014.

An examination of a description of a service organization's systems 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 presentation of the description of the systems and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion in Section II of this report. 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 Company's assertion in Section II of this report,

a. The description fairly presents the IT and collection management systems that were designed and implemented throughout the period January 1, 2014 to December 31, 2014.

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, 2014 to December 31, 2014.

c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period January 1, 2014 to December 31, 2014 .

Description of Tests of Controls

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

Restricted Use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of the Company, user entities of the Company's IT and collection management systems during some or all of the period January 1, 2014 to December 31, 2014 , and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities 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.

Auditor

SOC REPORT EXAMPLE

User Control Considerations

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether or not the following controls are implemented at user organizations:

- Controls to inform ABC of any regulatory issues that may affect the service provided by ABC.
- Controls to timely notify ABC of any actual or suspected information security breaches, including compromised user accounts.
- Controls to provide reasonable assurance that only authorized personnel are granted access to ABC information assets.
- Controls to notify ABC of changes in the authorized contact lists.
- Controls to provide reasonable assurance that procedures are in place to reconcile placements of collections sent to ABC with inventory listing received from ABC.
- Controls to govern the use of encryption.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of transactions for customers by ABC covers only a portion of the overall internal control structure of each customer. ABC's products and services were not designed to be the only control component in the internal control environment. Additional control procedures require implementation at the customer level. It is not feasible for all control objectives relating to the processing of transactions to be fully achieved by ABC. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SOC 1 TYPE 2 REPORT EXAMPLE

2.0 – Access

CO2 – Controls provide reasonable assurance that access to assets, resources, and applications is restricted to authorized personnel.

	Controls Specified by ACT	Testing Performed by Audior	Results of Tests
C2.1	Access to programs, data, and computer resources are restricted to appropriate, authorized personnel.	Inspected a sample of new hires' access to determine that access to programs, data, and computer resources were authorized and restricted to appropriate personnel during the examination period.	No exceptions noted.
C2.2	User access right reviews are performed no less than annually to provide that unauthorized access to programs, data, and computer resources is restricted to appropriate, authorized personnel.	Inspected the user access rights review performed during the examination period to determine that a user access rights review was performed to provide that unauthorized access to programs, data, and computer resources is restricted to appropriate, authorized personnel.	No exceptions noted.
C2.3	Authorization and creation of user accounts are performed by separate individuals.	Inspected a sample of new hire accounts created during the examination period and verified the authorization and creation of user accounts were performed by separate individuals.	No exceptions noted.
C2.4	Terminated employees' access to programs, data, and computer resources are removed timely upon their termination.	Inspected the status of a sample of employees terminated during the examination period to determine that terminated employees' access to programs, data, and computer resources were removed timely upon their termination.	No exceptions noted.
C2.5	Passwords conform to the following minimum requirements as enforced by the network operating system: • Password history • Maximum age • Minimum length • Complexity requirements	Inspected the network operating system configuration to determine that network passwords were required to conform to the following requirements: • Password history • Maximum age • Minimum length • Complexity requirements	***Exceptions noted:*** Company policy requires minimum password age of 10 days, however the system was configured with no minimum password.

SOC 2 TYPE 2 REPORT EXAMPLE

SECURITY PRINCIPLE

1.0 – Policies

ABC defines and documents its policies for the security of its system.

	Trust Services Criteria for the Security Principle	Description of MSI's Controls	Test of Controls Performed	Testing Results
1.1	The Company's security policies are established and periodically reviewed and approved by a designated individual or group.	ABC's Information Security Policy addresses both physical and logical security and is reviewed and approved at least once each calendar year by the SIT Department.	Inspected the Information Security Policy revision history to determine that the policy was reviewed and revised at least semi-annually.	No exceptions noted.
1.2	The Company's security policies include, but may not be limited to, the following matters:			
	a. Identifying and documenting the security requirements of authorized users.	ABC's Information Security Policy addresses security requirements of authorized users.	Inspected the Information Security Policy to determine that it included documentation on Identifying and documenting the security requirements of authorized users.	No exceptions noted.
	b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.	ABC's Information Security Policy addresses security requirements of classifying data.	Inspected the Information Security Policy to determine that the policy addressed data classification.	No exceptions noted.

TODAY'S PRESENTERS

Jennifer Christensen, Partner
CRI Orlando
407-644-7455
JChristensen@cricpa.com

Cheri Swain, Manager
CRI Orlando
407-644-7455
CSwain@cricpa.com