

 **The North Carolina
Office of the State Controller**

**Topics Pertaining to
Fraud and Third-Party
Service Organization
Controls**

November 19, 2012 **David McCoy
State Controller**

Introduction 

Enhancing
Accountability in
Government through
Leadership and
Education



Introduction 

Administrative Items

- Presentation materials have been provided in advance.
- Qualifies for up to 2 hours of CPE.
- Please be sure to sign-in before leaving today.
- Following the webinar, all registered attendees will receive web links to request CPE credit and to provide feedback on today's webinar.
- Phone lines have been muted. Please use the chat box to ask questions.





Introduction - Agenda

Estimated Time	Topic
9:30 - 9:35	Welcome and Introduction - Ben McLawhorn
9:35 - 10:10	Overview of NCFACTS - Kay Meyer and Carol Burroughs
10:10- 10:30	Opportunity for Fraud - Jennifer Trivette
10:30 - 11:00	Overview of Internal Controls - Jennifer Trivette and Wynona Cash
11:00 - 11:30	Reliance on Third Party Service Organization Controls - Wynona Cash

4



North Carolina Financial Accountability and Compliance Technology System (NC FACTS)

Kay Meyer, Program Director
Carol Burroughs, Project Director

5



Data Integration

Purpose:
Merge and reconcile dispersed data for analytical purposes using standardized tools to support quick, agile, event-driven analysis for business. The Data Integration Program objective is to establish a framework to promote the use of data as an asset to support strategic business decisions.

Responsibilities:

- Establish a North Carolina Business Intelligence Competency Center (NC BICC)
- Manage the development, implementation and support of the statewide criminal justice data integration program CJLEADS
- Manage the development and implementation of the enterprise fraud, waste and improper payments detection program NC FACTS
- Support agency data integration projects

6



CJLEADS

The **Criminal Justice Law Enforcement Automated Data Services (CJLEADS)** program integrates data found in the state's various criminal justice applications to provide up-to-date criminal information in a centralized location via a secure connection for use by state and local government criminal justice professionals.

Objectives

- To provide a comprehensive view of an offender's statewide criminal information through a single web portal, allowing for identification with a photographic image
- To provide an "Offender Watch" capability to monitor offender status

Status

- Statewide deployment began in January, 2011 and will complete in June, 2012
- Over 20,000 courts, corrections and law enforcement using the system statewide
- Design and development for additional data sources and user functionality is on-going

Challenges

- Governance and inhibitors to data sharing
- Individuating and matching of information

7



NC FACTS

The **North Carolina Financial Accountability and Compliance Technology System (NC FACTS)** program will strive to develop an enterprise process to detect fraud, waste, and improper payments across State agencies. The OSC has contracted with SAS to design, develop and host NC FACTS, leveraging the SAS Fraud Framework technology.

Objectives

- To coordinate with State agencies to identify on-going fraud activities, data, and interest in participating in the enterprise fraud, waste, and improper payment initiative
- To set priorities for developing and implementing potential applications
- To identify a pilot application area
- To coordinate with State agencies to recommend program resources necessary to address incidents of fraud, waste, or improper payments identified by the system

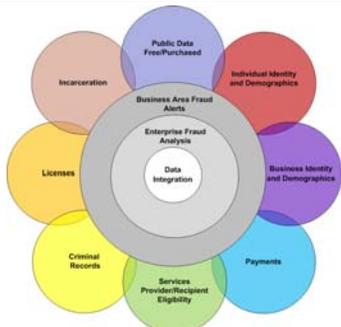
Approach

- Identify regulatory and statutory inhibitors to data sharing
- Identify initial data sources and pilot area of focus
- Establish the technical environment at SAS data center
- Develop retrospective fraud analysis
- Implement appropriate controls based on identified fraud

8



NC FACTS



9



NC FACTS

Pilot Areas of Focus:

- Secretary of State Corporate Information
- Department of Commerce, Division of Employment Security
- State Health Plan of North Carolina
- Department of State Treasurer Retirement Systems
- Department of Health and Human Services Eligibility

Additional Sources of Data:

- SSA Master Death Index
- CJLEADS Information
- Public sources of information

10



GBICC

The purpose of the GBICC is to support coordinated, effective and efficient development of North Carolina BI capability to generate greater efficiencies in, and improved services by State agencies.

Objectives

- Research current BI efforts and identify BI needs
- Manage data governance to resolve inhibitors to and facilitate interagency data sharing
- Recommend an enterprise BI strategy to ensure BI projects support enterprise efforts
- Facilitate the implementation of BI solutions to meet business needs
- Establish data standards and tools to foster interagency sharing and data consistency
- Foster continuing research on BI solutions for better decision making

Status

- Statewide inventory of current data analysis processes, data needs, tools and challenges
- Report of key areas identified in the inventory results for further research

Challenges

- Definition of BI
- Governance and inhibitors to data sharing
- Business stakeholder buy-in and adoption

11



Contact Information

Kay Meyer, Program Director
Office of the State Controller
kay.meyer@osc.nc.gov
919-707-0656

Carol Burroughs, Project Manager
Office of the State Controller
carol.burroughs@osc.nc.gov
919-707-0765

12



Opportunity for Fraud

13



Opportunity for Fraud

What is Fraud?

A collection of irregularities and illegal acts characterized by intentional deception, committed by individuals inside or outside of the organization for their personal benefit or to benefit the organization.

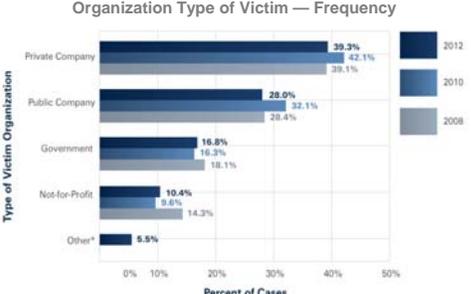


14



Opportunity for Fraud

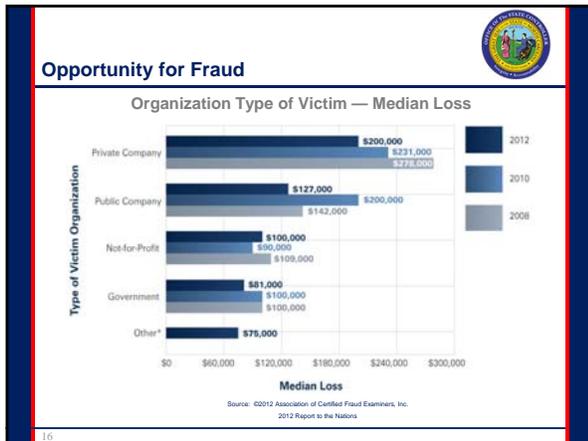
Organization Type of Victim — Frequency



Organization Type	2012 (%)	2010 (%)	2008 (%)
Private Company	39.3%	42.1%	38.1%
Public Company	28.0%	32.1%	28.4%
Government	16.8%	18.3%	18.1%
Not-for-Profit	10.4%	9.6%	14.3%
Other*	5.5%		

Source: ©2012 Association of Certified Fraud Examiners, Inc.
2012 Report to the Nations

15





Opportunity for Fraud

What is Occupational Fraud?

The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

Opportunity for Fraud

Fraud Triangle

- Opportunity: Fraud Conducted by Employees, Fraud Conducted by Individuals on Behalf of the Agency
- Rationalization: Personal Characteristics
- Pressure: Situational

19

Opportunity for Fraud

Opportunity

- Familiarity with operations
- Turnover of key employees
- Absence of explicit and uniform personnel policies
- Weak internal controls

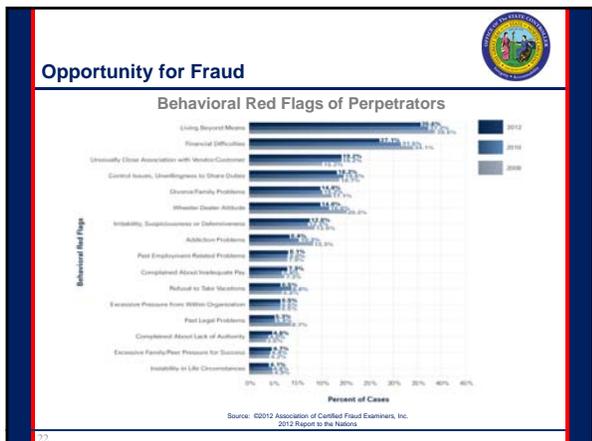
20

Opportunity for Fraud

Rationalization

Behavioral	Personal Characteristics
<ul style="list-style-type: none">• "I need it more than the other person."• "I'm borrowing and will pay it back later."• "Everybody does it."• "I'm not paid enough."	<ul style="list-style-type: none">• Lack of strong code of personal ethics• A wheeler-dealer personality• A strong desire to beat the system• A criminal or questionable background

21



- ### Opportunity for Fraud
- #### Pressure
- High personal debts or financial losses
 - Inadequate income for lifestyle
 - Excessive gambling
 - Emotional trauma in home life or work life
 - Peer group pressures
-

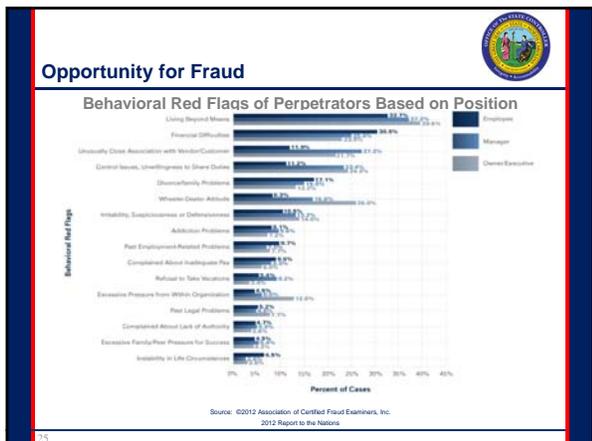
Opportunity for Fraud

Accountability and Control Red Flags

In 81% of cases, the fraudster displayed one or more behavioral red flags that are often associated with fraudulent conduct.

- Living beyond means (36% of cases),
- Financial difficulties (27%)
- Unusually close association with vendors or customers (19%)
- Excessive control issues (18%) were the most commonly observed behavioral warning signs

Source: ©2012 Association of Certified Fraud Examiners, Inc. 2012 Report to the Nations.



Opportunity for Fraud

Types of Red Flags

Red flags that are common to most types of fraudulent activity can be categorized as employee and management red flags.

- ### Opportunity for Fraud
- #### Types of Employee Red Flags
- Employee lifestyle changes
 - Significant personal debt and credit problems
 - Behavioral changes
 - High employee turnover
 - Refusal to take vacation or sick leave
 - Lack of segregation of duties



Opportunity for Fraud

Types of Management Red Flags

- Reluctance to provide information to auditors
- Management decisions are dominated by an individual or small group
- Weak internal control environment
- Excessive number of checking accounts
- Excessive number of year end transactions
- Service contracts result in no product

28



Opportunity for Fraud

Victim Organizations

Government and Public Administration
141 Cases

Scheme	Number of Cases	Percent of Cases
Corruption	50	35.5%
Billing	33	23.4%
Non-Cash	27	19.1%
Skimming	25	17.7%
Expense Reimbursements	19	13.5%
Payroll	18	12.8%
Check Tampering	15	10.6%
Cash on Hand	12	8.5%
Cash Larceny	10	7.1%
Financial Statement Fraud	9	6.4%
Register Disbursements	4	2.8%

Source: ©2012 Association of Certified Fraud Examiners, Inc. 2012 Report to the Nations

29



Opportunity for Fraud

Duration of Fraud Based on Scheme Type

Scheme Type	2012	2010	2008
Payroll	28	27	26
Check Tampering	22	22	20
Financial Statement Fraud	24	23	20
Expense Reimbursements	24	24	25
Billing	24	24	24
Skimming	12	12	24
Cash on Hand	19	17	18
Cash Larceny	18	18	20
Corruption	18	18	24
Non-Cash	12	18	21
Register Disbursements	12	12	22

Source: ©2012 Association of Certified Fraud Examiners, Inc. 2012 Report to the Nations

30

Opportunity for Fraud 

Red Flags in Cash/Accounts Receivable

- Consistent shortages in cash on hand
- Excessive number of voided transactions on a regular basis without proper explanation
- Not balancing cash to accounts receivable subledger
- No segregation of duties between the following:
 - Receiving cash
 - Posting to customer accounts
 - Issuing receipts
 - Deposit preparation

31

Opportunity for Fraud 

Cash Disbursement Process Red Flags

- High volume of manually prepared disbursement checks
- Paid invoices not properly canceled
- Unrestricted access to blank checks, signature plates, and check-signing equipment
- Frequent volume of voided or missing checks

32

Opportunity for Fraud 

Payroll Process Red Flags

- Adding fictitious (ghost) employees to the payroll.
- Submitting dubious overtime claims.
- Making unauthorized changes to employee records, earnings, rates, etc.

33



Opportunity for Fraud

Purchasing/Inventory Process Red Flags

- Unusual or unauthorized vendors
- Unusual increase in vendor spending
- Unusual/large/round-dollar amounts paid
- Copies of supporting documentation in lieu of originals
- Duplicate Payments
- Vendors without physical addresses

34



Opportunity for Fraud

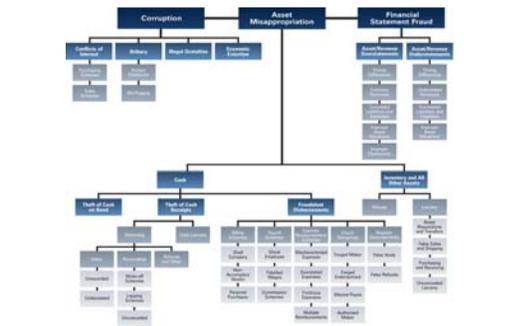
Purchasing/Inventory Process Red Flags

- Tips and complaints
- Sequential invoices paid
- Payments just under authorization level
- Employee-vendor address match
- Multiple invoices paid on same date
- Slight variation of vendor names

35



Occupational Fraud and Abuse Classification System



Source: ©2012 Association of Certified Fraud Examiners, Inc. - 2012 Report to the Nations

36



Overview of Internal Controls

37



Overview of Internal Controls

A control is any action taken to mitigate or manage risk and increase the probability that the organization's process will achieve its goal or objectives.



38



Overview of Internal Controls

What is the difference between a procedure and a control?

- A procedure is a series of steps taken to accomplish an end; they detail the established/prescribed methods to be followed. They describe "how it should be done".
- A control is a series of checks and balances that help managers detect and prevent errors.



39

Overview of Internal Controls 

What do we mean by "internal control"?

Internal control is an integral process, effected by an entity's governing body, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Effectiveness and efficiency of operations

40

Overview of Internal Controls 

Types of Internal Control Activities:

- Adequate segregation of duties
- Proper authorization of transactions and activities
- Adequate documentation and records
- Security of assets and records
- Review and reconciliations

41

Overview of Internal Controls 

Adequate segregation of duties

Requires that different individuals be assigned responsibility for different elements of related activities, particularly those involving authorization, custody, or recording.



42

Overview of Internal Controls

Proper authorization of transactions and activities

- Requires the review of transactions by an appropriate person to ensure that all activities adhere to established guidelines, it may be general or specific.
- For example:
Giving a department permission to expend funds from an approved budget-**general authorization**.
Review and approval of an individual transaction-**specific authorization**.

43

Overview of Internal Controls

Adequate documents and records

- Provide evidence that financial statements are accurate. The source documents ensure adequate recordkeeping.
- For example, pre-numbered checks, original invoices stamped paid, etc.



44

Overview of Internal Controls

Security of assets and records

The most important measure for safeguarding assets and records is the use of physical precautions – limit access to assets/records

- Physical Controls – fireproof file cabinets, safe, security cameras
- Access Controls – passwords, ID cards
- Backup and recovery procedures – Disaster Recovery Plan



45

Overview of Internal Controls 

Review and reconciliations

The need for independent checks arises because internal controls tend to change over time unless there is a mechanism for frequent review.



46

Overview of Internal Controls 

Management uses a mix of **Preventative Controls** and **Detective Controls**;

and a combination of **Manual Controls** and **Automated Controls**

47

Overview of Internal Controls 

Preventative Controls
Controls used by management to prevent errors from occurring, i.e. stop something from going wrong.

- Segregation of duties
- Authorization of payments prior to processing
- Restricting user access to IT systems

48

Overview of Internal Controls 

Detective Controls
Control activities that are designed to detect and correct in a timely manner an error or irregularity that would materially affect the achievement of the organization's objectives.

- General ledger reconciliations
- Review of exception reports
- Quarterly review of system access

49

Overview of Internal Controls 

**Nature of Controls
Manual vs. Automated**

50

Overview of Internal Controls 

Manual Controls
Control activities that requires an action by the control owner to prevent or detect an error or fraud.

- Independent review of general ledger reconciliations
- Authorization of employee expense reports
- Review and approval of journal entries

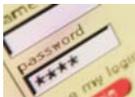


51

Overview of Internal Controls

Automated Controls
Control activities within a system that do not require action by the control owner to prevent or detect an error or fraud.

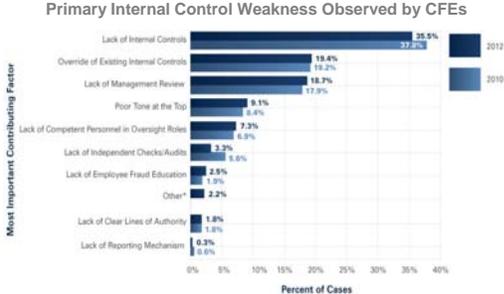
- Automated three-way match
- Data input validation checks
- Restricted user access



52

Overview of Internal Controls

Primary Internal Control Weakness Observed by CFEs



Most Important Contributing Factor	2012 (%)	2010 (%)
Lack of Internal Controls	33.2%	28.5%
Override of Existing Internal Controls	19.2%	19.8%
Lack of Management Review	18.7%	17.9%
Poor Tone at the Top	9.1%	6.4%
Lack of Competent Personnel in Oversight Roles	7.3%	6.9%
Lack of Independent Checks/Audits	5.2%	1.6%
Lack of Employee Fraud Education	2.9%	1.9%
Other*	3.2%	
Lack of Clear Lines of Authority	1.8%	1.8%
Lack of Reporting Mechanism	0.3%	0.6%

Source: ©2012 Association of Certified Fraud Examiners, Inc. 2012 Report to the Nations

53

Overview of Internal Controls

Median Loss Based on Presence of Anti-Fraud Controls

Control	Percent of Cases Implemented	Control In Place	Control Not in Place	Percent Reduction
Management Review	60.2%	\$100,000	\$165,000	42.9%
Employee Support Programs	57.0%	\$100,000	\$190,000	44.4%
Hotline	54.0%	\$100,000	\$190,000	44.4%
Fraud Training for Managers/Executives	47.4%	\$100,000	\$158,000	36.7%
External Audit of ICDFR	47.5%	\$120,000	\$187,000	36.6%
Fraud Training for Employees	46.8%	\$100,000	\$158,000	36.5%
Anti-Fraud Policy	46.6%	\$100,000	\$160,000	33.3%
Formal Fraud Risk Assessments	35.5%	\$100,000	\$150,000	33.3%
Internal Audit/FE Department	68.4%	\$120,000	\$180,000	33.3%
Job Rotation/Mandatory Vacation	16.7%	\$100,000	\$150,000	33.3%
Surprise Audits	32.2%	\$100,000	\$150,000	33.3%
Rewards for Whistleblowers	3.4%	\$100,000	\$145,000	31.0%
Code of Conduct	79.0%	\$120,000	\$184,000	26.6%
Independent Audit Committee	59.8%	\$125,000	\$160,000	16.7%
Management Certification of FIS	68.5%	\$138,000	\$164,000	15.9%
External Audit of FIS	80.1%	\$140,000	\$145,000	3.4%

Source: ©2012 Association of Certified Fraud Examiners, Inc. 2012 Report to the Nations

54

Overview of Internal Controls 

Best Practices of Internal Controls

- *Cash/Accounts Receivable*
- *Payroll*
- *Purchasing/Inventory*

55

Overview of Internal Controls 

Cash/Accounts Receivable

Segregation of duties

Different people:

- Receive and deposit cash
- Record cash payments to receivable records
- Reconcile cash receipts to deposits and the general ledger
- Bill for goods and services
- Distribute checks

56

Overview of Internal Controls 

Cash/Accounts Receivable

Accountability, authorization and approval

- Record cash receipts when received
- Keep funds secured
- Document transfers
- Give receipts to customers
- Give each cashier a separate cash drawer
- Supervisor verify bank deposits
- Supervisor approve all voided refunds

57


Overview of Internal Controls

Cash/Accounts Receivable

Security of assets and records

- Conduct proper background checks on prospective cash handlers.
- Restrict access of cash to as few people as possible
- Lock cash in a secure location like a safe
- Provide combinations, passwords only to authorized personnel.
- Change combinations, passwords periodically, or when someone leaves
- Count cash in a non-public area not easily visible to others.

58


Overview of Internal Controls

Cash/Accounts Receivable

Review and reconciliation

- Record cash receipts when received
- Count and balance cash receipts daily
- Compare receipts to deposit records
- Perform monthly reconciliations of the bank statements and Accounts Receivable ledgers

59


Overview of Internal Controls

Payroll

Segregation of duties

Different people:

- Prepare and update online payroll and personnel data
- Approve online payroll actions
- Review monthly payroll expense reports
- Review and reconcile payroll records monthly
- Distribute the payroll

60


Overview of Internal Controls

Payroll

Accountability, authorization, and approval

- Periodically review and update signature authorizations
- Review and authorize all timesheets
- Monthly reconcile payroll ledgers for accuracy of recorded transactions

61


Overview of Internal Controls

Payroll

Security of assets and records

- Keep confidential or sensitive information secured
- Limit access to the payroll and personnel records
- If a payroll check is created, request proof of identify prior to distribution

Review and reconciliation

- Review monthly payroll cost reports
- Compare actual payroll costs to budgeted
- Perform monthly reconciliations of payroll ledgers to ensure accuracy and timeliness of expenses

62


Overview of Internal Controls

Purchasing/Inventory

Segregation of duties

Different people:

- Approve purchases
- Receive ordered materials
- Approve invoices for payment
- Review and reconcile financial records
- Perform inventory counts

63

Overview of Internal Controls 

Purchasing/Inventory

Accountability, authorization, and approval

- Comply with ethical buying practices and policies
- Review and update authorizations periodically
- Obtain pre-approval if required
- Monitor to ensure that invoices are paid in a timely manner

64

Overview of Internal Controls 

Purchasing/Inventory

Security of assets and records

- Secure goods received in a restricted area
- Restrict inventory access to appropriate staff
- Compare inventory records with annual physical inventory count

Review and reconciliation

- Review suppliers invoices for accuracy by comparing charges to purchase orders
- Verify that the goods and services purchased have been received
- Perform monthly reconciliations of the ledgers to ensure accuracy and timeliness of expenses

65

Overview of Internal Controls 

How Can You Minimize Exposure to Fraud?

- Develop internal controls to protect your agency and the employee
- Don't let an individual have complete control of a financial process
- Authorize and approve transactions
- Restrict access to computer facilities and data
- Review and reconcile monthly statements

66



Reliance on Third-Party Service Organization Controls

67



Reliance on Third-Party SOC

Who is a service provider?
An agency/organization that performs services on behalf of another organization.

Service providers can be either a **Central Management Service Agency** or **Third-Party Service Organization**.

68



Reliance on Third-Party SOC

Central Management Service Agency – Colleges :
North Carolina Community College System
Department of the State Treasurer

Central Management Service Agency – Universities :
UNC General Administration
Department of the State Treasurer

69

Reliance on Third-Party SOC 

Central Management Service Agencies:

- Department of the State Treasurer
- Office of Information Technology Services
- Office of the State Controller
- Office of State Budget and Management
- Department of Administration

70

Reliance on Third-Party SOC 

Third-Party Service Organizations are external providers that perform a specific task or replace entire business unit or function of an entity.

They may:

- Execute transactions and/or maintain accountability for entity, or
- Record transactions and process related data for entity.



71

Reliance on Third-Party SOC 

Which report is right for your entity?

SAS 70 standard was retired on June 15, 2011.
AICPA defined Service Organization Control (SOC) Reports as the replacement.

- **SOC 1** Internal Control Over Financial Reporting
- **SOC 2** Operational Controls (detailed)
- **SOC 3** Operational Controls (short form)

Type I: Tests of design effectiveness or
Type II: Tests of design and operating effectiveness

72

Reliance on Third-Party SOC 

SOC 1 Report (SSAE16)

- Focused on financial reporting risks and controls specified by the service provider.
- Most applicable when the service provider performs financial transaction processing or supports transactions processing systems.
- Detailed report for users and auditors

Type I: Point in Time Report (over design)
or
Type II: Period of Time Report (generally, annual or semi-annual issued over operating effectiveness)

73

Reliance on Third-Party SOC 

SOC 2 Report

- Focused on Trust Services Principles:
 - Security
 - Availability
 - Confidentially
 - Processing integrity
 - Privacy
- Applicable to a broad variety of systems
- Detailed report for user organizations, auditors and specified parties

Type I: Point in Time Report (over design)
or
Type II: Period of Time Report (generally, annual or semi-annual issued over operating effectiveness)

74

Reliance on Third-Party SOC 

SOC 3 Report

- Short report that is distributed with the option of displaying a web site seal.
- Focused on Trust Services Principles:
 - Security
 - Availability
 - Confidentially
 - Processing integrity and or
 - Privacy
- Applicable to a broad variety of systems.
- Short report for general public.

Type I: Point in Time Report (over design)

75

Reliance on Third-Party SOC 

Trust Service Principles
Security

- Security policies
- Security awareness and communication
- Risk assessment
- Threat identification
- Information classification
- Logical access
- Physical access
- Security monitoring
- Incident management
- Encryption
- Personnel
- Systems development and maintenance
- Configuration management
- Change management
- Monitoring/compliance

76

Reliance on Third-Party SOC 

Trust Service Principles
Availability **Confidentiality**

- Availability policy
- Backup and restoration
- Environmental controls
- Disaster recovery
- Confidentiality policy
- Confidentiality of inputs, data processing, and outputs
- Information disclosures
- Confidentiality of information in systems development

77

Reliance on Third-Party SOC 

Trust Service Principle
Processing Integrity **Privacy**

- System processing integrity policies
- Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs
- Information tracing from source to disposition
- Management
- Notice
- Choice and consent
- Collection
- Use and retention
- Access
- Disclosure to third-parties
- Monitoring and enforcement

78

Reliance on Third-Party SOC 

- What is the nature of the service organization, what are its intended services?
- What types of attestation reporting is currently being performed at the service organization?
- What is the scope of work being performed and does that cover the relevant risks that are of primary concern to the entity?
- What time frame does the report cover?
- Have there been any recent incidents or concerns around data security or privacy?

79

Reliance on Third-Party SOC 

- How are service organizations addressing regulatory concerns?
- Does the service organization have a contractual responsibility to provide you with transparency over operations, controls, and results?
- Does the service provider use any other service providers or third-party vendors, and how do you derive comfort over these parties?

80

Reliance on Third-Party SOC 

For questions or additional information, you may contact Risk Mitigation Services at:

OSC.EagleSupport@lists.osc.nc.gov

81
