Managing Security and External Service Providers using SOC Reports

Jorge Rey, CISA, CISM
Kaufman, Rossin & Co.

FELABAN XIII CL@B Miami 2013

Organizado por: FIBA FELABAN

Septiembre 11-13, 2013 | Miami, FL | Hotel InterContinental

During the course

of this presentation….

- ✓ Overview of SOC 2/SOC3 Reporting
- ✓ SOC 2/SOC 3 versus SOC 1 Reports
- ✓ Outsourcing Technology Services and Application of SOC 2/SOC 3 Reporting

Overview of SOC 2/SOC3 Reporting

Internal control over financial reporting	***Operational controls***	
SOC 1	SOC 2	SOC 3
Detailed report for users and their auditors	Detailed report for users, their auditors and specified parties	General-use report – detail not needed
• Scope on financial reporting • Applicable when the provider is responsible for financial transactions processing or supports transaction processing	Scope 1. Security 2. Availability 3. Processing integrity 4. Confidentiality 5. Privacy	

SOC 2/SOC 3 versus SOC 1 Reports

	Internal control over financial reporting	*Operational controls*	
	SOC 1	SOC 2	SOC 3
Scope of system	• Classes of transactions • Procedures for processing and reporting transactions • Accounting records and handling of significant events	• Infrastructure • Software • Procedures • People • Data	
Domains covered	• Transaction processing controls • Supporting IT General Controls	• Security • Availability • Processing integrity • Confidentiality • Privacy	
Controls / Criteria to be tested	• Defined by service organization	• Principles are selected by the service organization • Specific criteria is used instead of control objectives	

SOC 2/SOC 3 Trust Services Principles

Domain	*Trust Services Principle*	*Applicability*
Security	• The system is protected against unauthorized access (both physical and logical).	• Applies to all outsourced environments • Helps with vendor GLBA due-diligence and monitoring activities
Availability	• The system is available for operation and use as committed or agreed.	• Relevant when disaster recovery is provided by the service organization or the Bank relies on the service organization to meet it's recovery time objective
Processing Integrity	• System processing is complete, accurate, timely, and authorized.	• Applies to service organizations that process financial and no-financial data

SOC 2/SOC 3 Trust Services Principles

Domain	*Trust Services Principle*	*Applicability*
Confidentiality	• Information designated as confidential is protected as committed or agreed.	• Helps with vendor GLBA due-diligence and monitoring activities • Provides assurance on the provider's practices to protecting sensitive information
Privacy	• Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.	• Helps with vendor GLBA due-diligence and monitoring activities • Applicable when the service organizations interacts directly with Bank's customers

SOC 2/SOC 3 Security Principle

- ✓ IT Security policy
- ✓ Security awareness and communication
- ✓ Risk assessment
- ✓ Logical access
- ✓ Physical access

- ✓ Security monitoring
- ✓ User authentication
- ✓ Incident management
- ✓ Asset classification, and management
- ✓ Systems development, and maintenance
- ✓ Personnel security
- ✓ Configuration management
- ✓ Change management
- ✓ Monitoring, and compliance

SOC 2/SOC 3 Availability Principle

- ✓ **Availability policy**
- ✓ **Backup, and restoration**
- ✓ **Environmental controls**
- ✓ **Disaster recovery**
- ✓ **Business continuity management**

SOC 2/SOC 3 Confidentiality Principle

- ✓ Confidentiality policy
- ✓ Confidentiality of inputs
- ✓ Confidentiality of data processing
- ✓ Confidentiality of outputs
- ✓ Information disclosures
- ✓ Encryption
- ✓ Confidentiality of information in systems development, management and configuration

SOC 2/SOC 3 Processing Integrity Principle

- ✓ Processing policies
- ✓ System boundaries and communication
- ✓ Completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management
- ✓ Procedures to enable tracing of information inputs from their source to their final disposition and vice versa

SOC 2/SOC 3 Privacy Principle

- ✓ Management
- ✓ Notice
- ✓ Choice, and consent
- ✓ Collection
- ✓ Use, and retention
- ✓ Access
- ✓ Disclosure to third parties
- ✓ Quality
- ✓ Monitoring, and enforcement

Structure of the SOC Reports

SOC 1	SOC 2	SOC 3
Service auditor's opinion	Service auditor's opinion	Service auditor's opinion
Management's assertion	Management's assertion	Management's assertion
Description of systems (including controls)	Description of systems (including controls)	Description of systems (including controls)
Control objectives	Principle(s)/ Criteria	Principle(s)/ Criteria
Description of tests as of a date (Type 1) or throughout a period (Type 2) and results of tests	Description of tests as of a date (Type 1) or throughout a period (Type 2) and results of tests	N/A
Other information (if applicable)	Other information (if applicable)	N/A

Structure of the SOC Reports

SOC 1

Control Objective 1: XXXXXXXXXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX

Control Objective 2: XXXXXXXXXXXXXXX

Description of Controls	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX

Control Objective 3: XXXXXXXXXXXXXXX

Description of Controls	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX

SOC 2

Availability Principle Criteria, Test of Controls and Results of Tests

1.0 Policies: The entity defines and documents its policies for the availability of its system.

Availability Criteria	Description of Controls	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX

2.0 Communications: The entity communicates the defined system availability policies to responsible parties and authorized users.

Availability Criteria	Description of Controls	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX

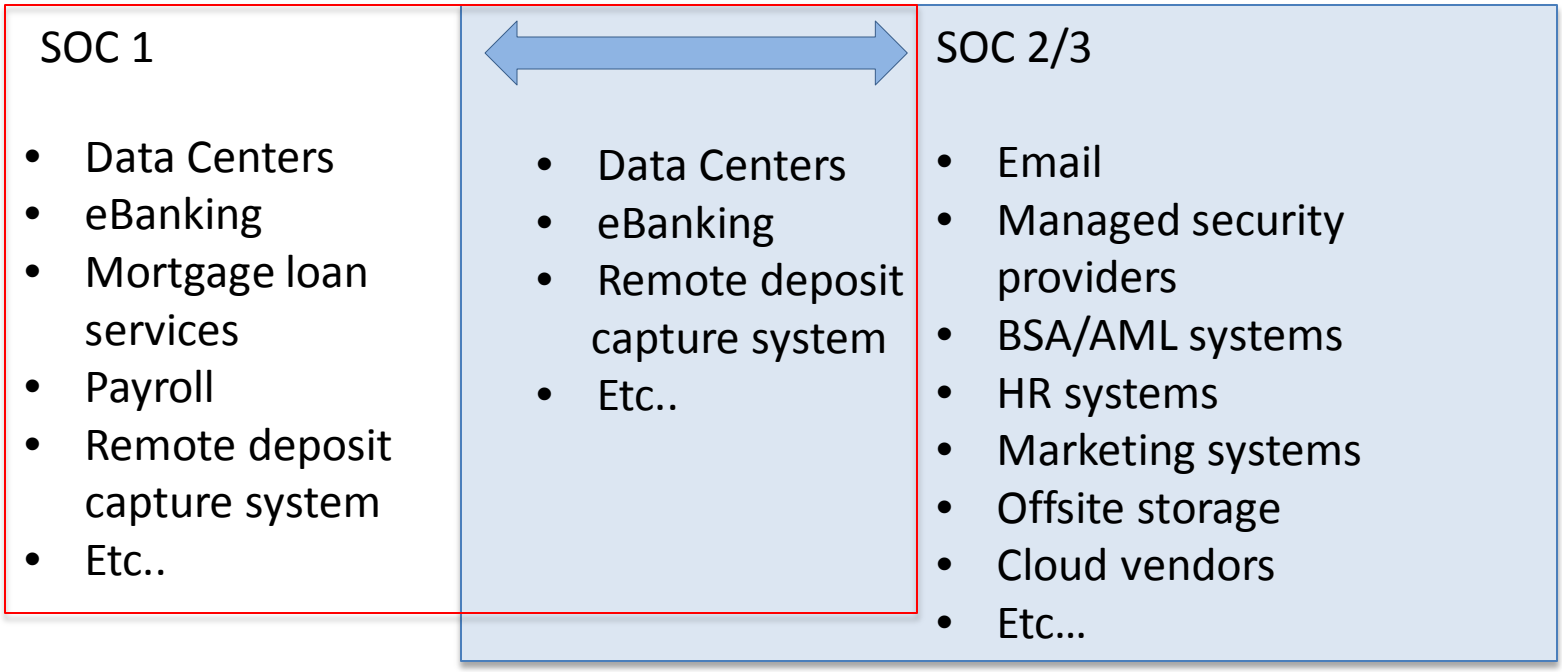
3.0 Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.

Availability Criteria	Description of Controls	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system availability policies.

Availability Criteria	Description of Controls	Test Procedures	Results of Tests
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX
XXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX

SOC Reports In Use



Outsourcing of Technology Services

Financial Intuitions must have a process to determine whether the service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities; have the ability:

- to respond to service disruptions;
- to comply with appropriate federal and state laws. In particular, ensure management has assessed the providers' ability to comply with federal laws

Monitoring the risk presented by the service provider relationship. Monitoring should addresses:

- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports;
- Service provider's disaster recovery program and testing;
- Information security;
- Subcontractor relationships including any changes or control concerns;
- Foreign third party relationships.

Outsourcing and SOC Reports

Activity	Description
Inventory of vendors	• Obtain a list from Accounts Payable and identify all vendors
Assess vendor risk	• Assess risks associated with each vendor (i.e. Security, Confidentiality, Availability, Integrity, etc..) • Identify whether SOC reports have been requested
Identify relevant SOC reports / Vendor Monitoring	• Determine which SOC reports are required for each vendor • Frequency of the reports
Vendor Due diligence	• Consider requesting what SOC reports are available from the vendor during the RFP process

Questions, Now or Later

Jorge Rey CISA, CISM, CGEIT
Director, Information Security
E: jrey@kaufmanrossin.com
P: 305.646.6076

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS