XXVII Congreso de Seguridad Bancaria

CELAES 2012

Security and External Service Providers

How to ensure regulatory compliance and manage risks with Service Organization Control (SOC) Reports

Jorge Rey, CISA, CISM, CGEIT
Director, Information Security & Compliance
Kaufman, Rossin & Co.

“Cómo Convertir los Riesgos en Oportunidades de Negocio””

FIBA

Organizado por:

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

During the course

of this presentation….

- ✓ Evolution of SAS 70 Reports and Why the Change
- ✓ Service Organization Control (SOC) Reports 101
- ✓ Outsourcing Technology Services and SOC reports

Definitions

Service organization. An organization or segment of an organization that provides services to a Bank (aka service provider).

User entity. An entity that uses a service organization (aka Bank of a service organization).

Service auditor. A practitioner (CPA firm) who reports on controls.

SOC 1,2,3 reports. Report(s) on a service organization's controls.

SSAE 16 . New SAS 70 or SOC 1 report.

SysTrust. SOC 3 report .

SAS 70 has been around since 1992

C-90
Rp. 6.000,-

Z-6373

SIDE A :
- I'LL BE THERE — Mariah Carey & Trey Lorenz
- 'TIL I LOVED YOU — Restless Heart
- IF WE HOLD ON TOGETHER — Diana Ross
- OVER YOU — Timmy T.
- SAVE THE BEST FOR LAST — Vanessa Williams
- DO IT TO ME — Lionel Richie
- BEAUTY AND THE BEAST — Celine Dion & Peabo Bryson
- TO BE WITH YOU — Mr. Big
- TEARS IN HEAVEN — Eric Clapton
- BACK TO YOU — Bobby Caldwell & Marilyn Scott
- BOHEMIAN RHAPSODY — Queen

SIDE B :
- MOM — Tomoe Sawa
- I FALL ALL OVER AGAIN — Dan Hill
- WHY — Annie Lennox
- LOST IN YOUR LOVE — Tony Hadley
- YOU — Ten Sharp
- JUST FOR TONIGHT — Vanessa Williams
- WHAT BECOMES OF A BROKEN HEARTED — Paul Young
- YOU WON'T SEE ME CRY — Wilson Phillips
- SEPARATE TABLES — Chris Deburgh
- IF YOU ASKED ME TO — Celine Dion
- MASTERPIECE — Atlantic Starr

LOVE SONGS OF THE YEAR 1992

1	I'LL BE THERE	MARIAH CAREY & TREY LORENZ
2	'TIL I LOVED YOU	RETLESS HEART
3	IF WE HOLD ON TOGETHER	DIANA ROSS
4	OVER YOU	TIMMY T.
5	SAVE THE BEST FOR LAST	VANESSA WILLIAMS
6	DO IT TO ME	LIONEL RICHIE
7	BEAUTY AND THE BEAST	CELINE DION & PEABO BRYSON
8	TO BE WITH YOU	MR. BIG
9	TEARS IN HEAVEN	ERIC CLAPTON
10	BACK TO YOU	BOBBY CALDWELL & MARILYN SCOTT
11	BOHEMIAN RHAPSODY	QUEEN
12	MOM	TOMOE SAWA
13	I FALL ALL OVER AGAIN	DAN HILL
14	WHY	ANNIE LENNOX
15	LOST IN YOUR LOVE	TONY HADLEY
16	YOU	TEN SHARP
17	JUST FOR TONIGHT	VANESSA WILLIAMS
18	WHAT BECOMES OF A BROKENHEARTED	PAUL YOUNG
19	YOU WON'T SEE ME CRY	WILSON PHILLIPS
20	SEPARATE TABLES	CHRIS DE BURGH
21	IF YOU ASKED ME TO	CELINE DION
22	MASTERPIECE	ATLANTIC STARR

In 1992, compact discs surpassed cassette tapes as the preferred medium for recorded music!

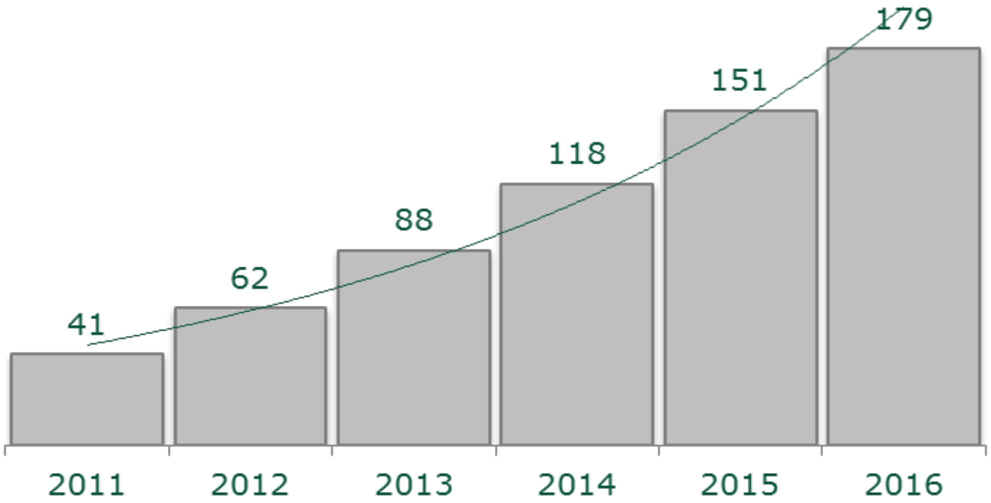
SAS 70, the Swiss Army of Reports

- adequately addresses risks and reporting needs of customers of a service organization
- can be used to report on controls related to compliance and operational matters, such as confidentiality, privacy, processing integrity, etc.
- demonstrates best practices
- is a "Certification" or demonstrates "Compliance"
- is designed to help with sales/marketing.

Why the Change?

Confidentiality • Availability • Integrity • Compliance
SAS
70
Type II

Public, Virtual, And Private Cloud Market Growth (In Billions US$)



Source: Forrester Research, Inc.

Service Organization Controls (SOC) Reports

Report	On	Why
SOC 1^{SM}	Financial Controls Restricted use (Type 1 or 2 Report)	Audit of financial statements
SOC 2^{SM}	Trust Services Principles Restricted use (Type 1 or 2 Report)	User's oversight controls
SOC 3^{SM}	Trust Services Principles General-use report (Public seal)	Marketing purposes – detail not needed

SOC Reports

Report	Types of Service Providers
SOC 1^{SM}	Payroll, Data Centers, Bill payments, eBanking, Imaging Processors, etc..
SOC 2^{SM}	Data centers, IT outsourcing, business outsourcing, Cloud providers, Managed Security Service Providers
SOC 3^{SM}	Data centers, IT outsourcing, business outsourcing, Cloud providers, Managed Security Service Providers

Two Types of SOC 1 and SOC 2 Reports

Content	Type I	Type II
Service Auditor's Opinion	X	X
Management's Assertion	X	X
Description of Systems	X	X
Controls Designed and Implemented as of a Date	X	X
Description of Tests throughout a specified period and the Results of Tests	-	X

Trust Services Principles

Security

- The system is protected against unauthorized access (both physical and logical).

Availability

- The system is available for operation and use as committed or agreed.

Processing Integrity

- System processing is complete, accurate, timely, and authorized.

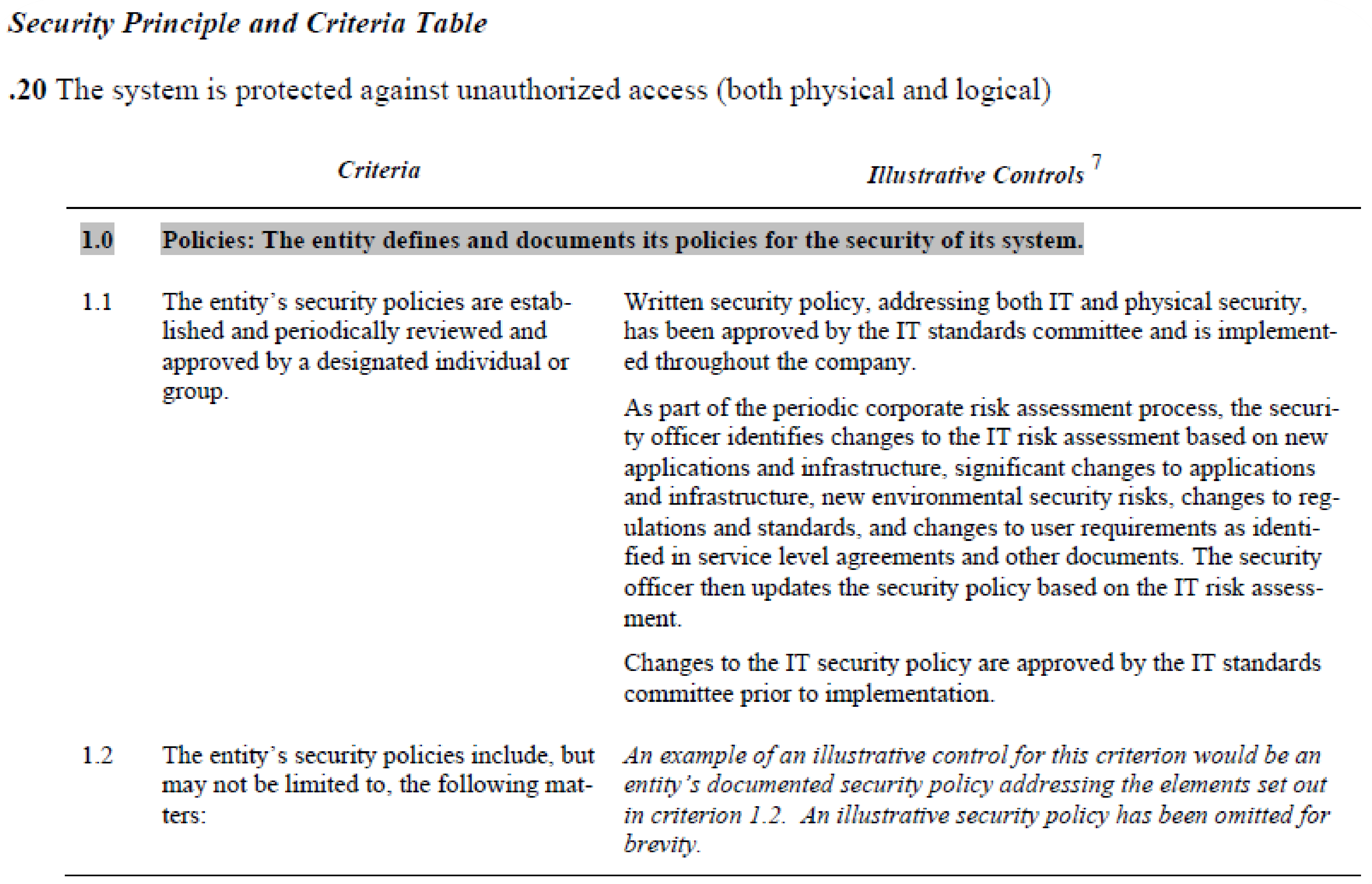
Confidentiality

- Information designated as confidential is protecte committed or agreed.

Privacy

- Generally Accepted Privacy Principles (GAPP)

Trust Services Principles and Criteria Sample



Security Principle and Criteria Table

.20 The system is protected against unauthorized access (both physical and logical)

	Criteria	*Illustrative Controls* [7]
1.0	**Policies: The entity defines and documents its policies for the security of its system.**	
1.1	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	Written security policy, addressing both IT and physical security, has been approved by the IT standards committee and is implemented throughout the company. As part of the periodic corporate risk assessment process, the security officer identifies changes to the IT risk assessment based on new applications and infrastructure, significant changes to applications and infrastructure, new environmental security risks, changes to regulations and standards, and changes to user requirements as identified in service level agreements and other documents. The security officer then updates the security policy based on the IT risk assessment. Changes to the IT security policy are approved by the IT standards committee prior to implementation.
1.2	The entity's security policies include, but may not be limited to, the following matters:	*An example of an illustrative control for this criterion would be an entity's documented security policy addressing the elements set out in criterion 1.2. An illustrative security policy has been omitted for brevity.*

SOC 2 vs. SOC 3

- **SOC 2 Report Components**
  - Service Auditor’s Opinion
  - Management’s Assertion
  - Description of System
  - Controls Designed and Implemented as of a Date (Type 1)
  - Description of Tests and the Results of Tests (Type 2)

- **SOC 3 Report Components**
  - Service Auditor’s Opinion
  - Management’s Assertion
  - Description of System (Not as detailed as SOC 2)

SOC 2 vs. SOC 3

- **SOC 2 Report Distribution**
  - Restricted Use
  - AICPA SOC Logo

- **SOC 3 Report Distribution**
  - Publicly Available
  - SysTrust/WebTrust Seal Issuance Optional

SOC 1^{SM} Reports On The Service Provider's Financial Controls

- Like SAS 70 – reports on controls over financial reporting

What is New?

- Attestation standard, no longer Auditing Standard. Uses the Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
  - Auditor evaluation based on suitable criteria relative to written management assertions – that are included in the report.
- Materiality, use of internal audit and opinion format

SOC 2^{SM} Reports On The Service Provider's Security , Availability, Processing Integrity, Confidentiality or Privacy Controls

Everything is New !

- It is not like SAS 70, it looks like a SAS 70
- Reports can be issued on **one** or **multiple** Trust Services principles (security, availability, processing integrity, confidentiality and privacy)
- Uses the AT Section 101, *Attest Engagements*, of SSAEs (AICPA, *Professional Standards*, vol. 1)
  - CPA's opinion on fairness of description, suitability of design and operating effectiveness of controls. Description of tests of controls and results.
- Report is restricted to existing user entities (not potential customers)

SOC 3^{SM} Trust Services Report for Service Organizations

Everything is New !

- Uses the AICPA's Trust Service Principles and AT Section 101, *Attest Engagements*, of SSAEs (AICPA, *Professional Standards*, vol. 1)

- CPA's opinion on whether the entity maintained effective controls over its system. No description.

- General use reports, they can be freely distributed or posted on a website

SOC 3$^{\text{SM}}$ Trust Services Report for Service Organizations - SysTrust® and WebTrust® Seals

Type of Engagement	IT Systems	e-commerce Systems
Security	SysTrust	WebTrust
Privacy	—	WebTrust
Processing Integrity	SysTrust	WebTrust
Availability	SysTrust	WebTrust
Confidentiality	SysTrust	WebTrust
Consumer Protection	—	WebTrust
System Reliability	SysTrust	—
Other Engagement Combinations	SysTrust	WebTrust

FFIEC IT Examination Handbook Infobase

Applicable changes as of July 10, 2012

Date	Description	Booklets Changed	Comments
07/10/12	Added the FFIEC Cloud Computing Statement	N/A – Reference Material Section	Maps risks to FFIEC IT Booklets
05/07/12	Revised multiple booklets to address the transition from SAS-70 to the SSAE-16 attestation review process and other third-party review processes.	Audit, BCP, E-Banking, Information Security, Operations, Outsourcing, and Retail Payments	Generally, the term SAS-70 was changed to embrace a broader set of review processes.

FFIEC IT Examination Handbook Infobase

Applicable changes as of July 10, 2012

Date	Description	Booklets Changed	Comments
04/27/12	Added the FFIEC Supplement to Authentication in an Internet Environment to Appendix C (resource).	Information Security	Issued June 29, 2011
04/09/12	Added Appendix D to address the risks associated with outsourcing IT Security.	Outsourcing	Includes Examination Procedures and Request Letter criteria
04/02/12	Modified Appendix A to address the risks associated with Cloud Computing.	Outsourcing	

Outsourcing of Technology Services

Appendix D – Managed Security Service Providers - MSSP Engagement Criteria

Criteria	SOC 1 Type II	SOC 2 Type II	SOC 3
Service Availability	N/A	Yes, only if availability is tested.	No
Incident Response and Notification	N/A	Yes, only if security and privacy is tested.	No
State/Federal Compliance	N/A	Yes, depends on the compliance requirements.	No
Third-Parties and Subcontractors	N/A	Yes	No
Handling Sensitive Data	N/A	Yes, only if security, confidentiality and privacy is tested.	No
Disaster Recovery	N/A	Yes, only if availability is tested.	No
Customer Support	N/A	Yes, only if processing integrity is tested.	No
Hardware Replacement	N/A	Yes, only if availability is tested.	No
Technology	N/A	Yes	No
Staffing, Service Scalability, Training/Education	No	No	No

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.

Supervision of Technology Service Providers

Underlying Risks	**SOC 1 Type II**	**SOC 2 Type II**	**SOC 3**
Management of Technology	N/A	N/A	N/A
Integrity of Data	Yes	Yes, only if **Processing Integrity** is tested.	No
Confidentiality of Information	No	Yes, only if **Security** and **Confidentiality** is tested.	No
Availability of Services	No	Yes, only if **Availability** is tested.	No
Financial Stability	N/A	N/A	N/A

Changes – What To Expect?

- Slow adoption at first for SOC 2 and SOC 3
- Service providers will be providing a combination of reports (i.e. SOC 1 & SOC 3)
- Institutions are starting to request SOC 1 & SOC 2 in RFPs
  - Make sure that the SOC 2 reports have the trust principles relevant to your organization
- Vendor management procedures to address cloud computing, MSSPs and SOC reports

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