Flying in the Clouds

How to Gain Visibility of Outsourced Information Services

Wednesday, January 29, 2020 | 2:00 p.m. – 3:15 p.m.

PRESENTED BY

Michele McDonald, IT / Cyber Security Manager, MGO
Jasmine Costa, IT Audit Manager, MGO
Brian Kelleher, Chief Financial Officer, CCTA

MGO
TYPE ATYPICAL

Bios - Our Panelists

Michele McDonald
IT / Cyber Security Manager, MGO Technology Group

Michele is an IT / Cyber Security Manager with 20 years of experience in IT infrastructure, cyber and business risk management.
Her area of expertise includes Threat and Vulnerability Evaluation and Management, Incident Response, Network Operations Security, Data Classification, Physical Asset and Facilities Security, Identity Access Management, Third Party Risk Management, General IT and Application Controls and Compliance. She also managed the Security Operations Center at a major mortgage company.
Michele has worked in a variety of industries including government, technology, home-building, mortgage and marketing.

CSMFO

SPEAKER PRESENTATION

YESTERDAY, TOMORROW AND FINANCE
2020 CSMFO ANNUAL CONFERENCE
JANUARY 28-31, 2020
DISNEYLAND CA

Jasmine Costa, CISA
IT Audit Manager, MGO Technology Group

Jasmine is an IT Audit Manager and has over 12 years of experience in IT audit and compliance, risk management, and information security, with a major emphasis on IT SOX 404 and operational audits.

Her areas of expertise include developing and executing comprehensive IT general controls and application controls test plans, development of controls where necessary, documentation, testing, and remediation, and overall project management. She has also managed first year audits and IT compliance initiatives, including SSAE16 SOC reviews, mapping of service provider controls to company's internal control framework, and working with third-party vendors to ensure compliance with company's policies and standards. She has worked in a variety of industries from healthcare and for-profit higher education to financial services.

Brian Kelleher

Chief Financial Officer, Contra Costa Transportation Authority

As the Chief Financial Officer of Contra Costa Transportation Authority, Brian develops and implements divisional goals, objectives, policies, procedures and work standards to align with the Authority's vision and strategic goals of operational excellence and financial sustainability.

He is responsible for long-range strategic financial planning, budgeting, financial audits, procurement activities, debt issuance, and debt administration of the agency, in addition to directing and supervising the day-to-day operations of the Finance Division.

Agenda

Today we will cover:

- Security Triad
- What is “The Cloud?”
- Risks vs. Rewards
- 2019 Data Breaches
- Prevent Misconfigurations
- Service Organization Control (SOC) Reports
- Outsourced Services Risk Management
- Experiences from a CFO

SECURITY TRIAD

What is "The Cloud?"

Traditional On-Premises IT	Co-location	Hosting	IaaS	PaaS	SaaS
Data	Data	Data	Data	Data	Data
Application	Application	Application	Application	Application	Application
Databases	Databases	Databases	Databases	Databases	Databases
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Physical Servers	Physical Servers	Physical Servers	Physical Servers	Physical Servers	Physical Servers
Network & Storage	Network & Storage	Network & Storage	Network & Storage	Network & Storage	Network & Storage
Data Center	Data Center	Data Center	Data Center	Data Center	Data Center

Self-Managed Provider-Supplied

Risks vs. Rewards

Pros	Cons
Switch from CAPEX to OPEX	Potential downtime of services
Quickly launch new apps and business processes that are available from anywhere	Potential performance issues
Improved disaster recovery	Could be more prone to attacks
Environmentally friendly	Once you go to the cloud it can be difficult to go back
Staff can focus on new projects	Cost increases and billing complexity
	Staff need to learn new technologies

2019 Data Breaches

- BenefitMall
- Rubrik
- Microsoft Email Services
- Federal Emergency Management Agency (FEMA)
- Evernote
- Foxit
- Adobe
- Network Solutions

Prevent Misconfigurations

- Lack of Logging
- **Lack of access control** and access managing – leaving access wide open
- Unsecure AWS S3 buckets – left open to find on Internet, open to download from, or even write
- Unmanaged or mismanaged permissions controls
- Not selecting or turning on controls provided by cloud vendor that protects you
- Lack of audit and governing controls
- **Lack of understanding the shared responsibility model**
- Lack of knowledge, skills, or experience in utilizing and deploying cloud solutions
- Unsecure data storage elements
- **Default credentials**
- Default configuration settings
- **Unpatched systems**
- Unrestricted access to ports
- Unrestricted access to services
- Absence of change control – change control in cloud environment is inherently different than an on premises environment

Service Organization Control (SOC) Reports

SOC 1

- Your financial statements and audits
- You and your CPAs
- Evaluate the effect of service organization's controls on your financial statements

SOC 2

- Your confidential and private data and information.
- You and your stakeholders
- Provides information and assurance about service organization's controls relevant to security, availability, and processing integrity of their systems
  - ✓ Oversight of the organization
  - ✓ Vendor management programs
  - ✓ Internal corporate governance and risk management processes
  - ✓ Regulatory oversight

SOC 3

- General use report – for free distribution purposes

Definitions

Service Organization (outsourced service vendor): an organization that provides services to user entities, which are likely to be relevant to those user entities' internal control over financial reporting

Sub-service Organizations: organizations that provide outsourced services to the service organization (third-party vendor, a vendor's vendor)

Inclusive Method: when a description of a sub-service organization's services, control objectives, and related controls is included in the *Service Organization's SOC report*

Carve-out Method: only describes the sub-service organization's services

Definitions

SOC I Reports: AICPA attestation reports

Type 1: SOC report (opinion) on a service organization's system that was designed and implemented as of a **specified date** (suitability of the design of controls)

Type 2: SOC report (opinion) on a service organization's system that was designed and implemented throughout the **specified period** (suitability of the design and operating effectiveness of controls)

User Entity: An entity that uses a outsourced services vendor for services that are likely to be relevant to that entity's internal control over financial reporting

Complementary User Entity Controls (CUEC): Controls the service organization assumes will be implemented by user entities and are necessary to achieve the service organization's (outsourced service vendor) control objectives

Outsourced Services Risk Management

1. Risk Assessment of Outsourced Vendor Services
2. Obtain SOC Reports
3. Determine the Type of SOC Report
4. Verify Scope of Report Covers the Services Received
5. Determine the Time Period
6. Verify the SOC Report Auditor's Credentials
7. Review the SOC Opinion and Management Assertions
8. Repeat #2 – #7 for Carve-out Sub-Service Organizations
9. Review Exceptions and Management Response Plan
10. Map Complementary User Entity Controls to Your Controls
11. Identify Control Gaps
12. Manage the Control Gap Risks

Outsourced Services Risk Management

Risk Assessment of Outsourced Vendor Services

- **Identify**
  - ✓ Financial Statement, Critical Operations Systems, Management Information
    - Third Party Administrators (Insurance)
    - Investment Services
    - Accounting Information System
    - Data Centers
- **Prioritize**
  - ✓ Information Security Class
  - ✓ Operational Continuity
    - Systems Outage (how long can we be without systems, applications, and information?)
    - Damages: Reputation and Monetary
    - Regulatory Impact
    - Dollars
    - Volume

Outsourced Services Risk Management

SOC Reports

- **Obtain**
  - ✓ All identified outsourced services (and third-party vendors)
  - ✓ Prioritize
- **Determine Type**
  - ✓ SOC 1, SOC 2
  - ✓ Type 1, Type 2
- **Verify Scope**
  - ✓ Section III
- **Determine Time Period**
  - ✓ Financial statement period
  - ✓ 6 or more months

Outsourced Services Risk Management

Verify the SOC Report Auditor's Credentials

- **Name Recognition**

- **Internet Survey**
  - ✓ CPA firm
  - ✓ SOC services
  - ✓ Key employee certifications and experience
  - ✓ News (litigation, settlements, regulatory actions)

- **State Board of Accountancy**

- **Peer Review**

Outsourced Services Risk Management

SOC Opinion and Management Assertions

- **Auditor's Opinion**
  - ✓ Section 1
  - ✓ Opinion types

- **Service Organization's Management Assertions**
  - ✓ Section 2

Outsourced Services Risk Management

Carve-Out Sub-Service Organizations

- BestBuy, Sears, Kmart, Delta
- Exposed records: unknown
- Reported April & May 2018
- Electronics, home goods, mom jeans, and air travel – these companies don't have much in common – except for a big weak link. **[24]7.ai, a chat and customer services vendor** for many brand names, was hacked via malware, compromising credit card information, addresses, CVV numbers, card expiration dates, and other personal data across multiple customer groups.

Outsourced Services Risk Management

Review Exceptions and Management Response Plan

- **Section I, Auditor's Report**
  - ✓ Exceptions will be described in the Auditor's report
    - Determine whether it is a threat to your systems, applications, or information

- **Section IV, Control Testing**
  - ✓ Gain an understanding of the control objective, control, and failure

- **Section V, Other Information**
  - ✓ Management response is generally located in this section

Outsourced Services Risk Management

Map Complementary User Entity Controls to Your Controls

- **Where? Section III, System & Controls Description**
  - ✓ Section III, system & controls description
  - ✓ Typically last section
- **What Are They?**
  - ✓ Contractor controls that only work if the user has certain controls effectively implemented in the user organization
- **Example – Access (logical)**
  - ✓ Systems, applications, and data housed and provided by out-sourced service provider
  - ✓ ERP and financial data are in vendor cloud via Internet
  - ✓ User organization does not remove or disable separated employees network and/or applications until 30 days after separation
  - ✓ Former employee uses a VPN token or ID badge to access the system, change application configurations, create accounting entries, and delete key transactions, then invokes back-up routine

Outsourced Services Risk Management

Control Gaps

- **Identify the Gaps**
  - ✓ Exceptions will be described in the Auditor's report.

- **Manage the Gaps**
  - ✓ Assess
  - ✓ Rank
  - ✓ Respond

Experiences from a CFO

Who We Are

- CCTA is a public agency formed by voters in 1988 to manage the county's transportation sales tax program and to lead transportation planning efforts.
- We are responsible for maintaining and improving the county's transportation system by delivering critical transportation infrastructure projects to safely and efficiently get people where they need to go.
- Managing entity of autonomous vehicle (AV) testing site: GoMentum Station.

Experiences from a CFO

CONTRA COSTA transportation authority

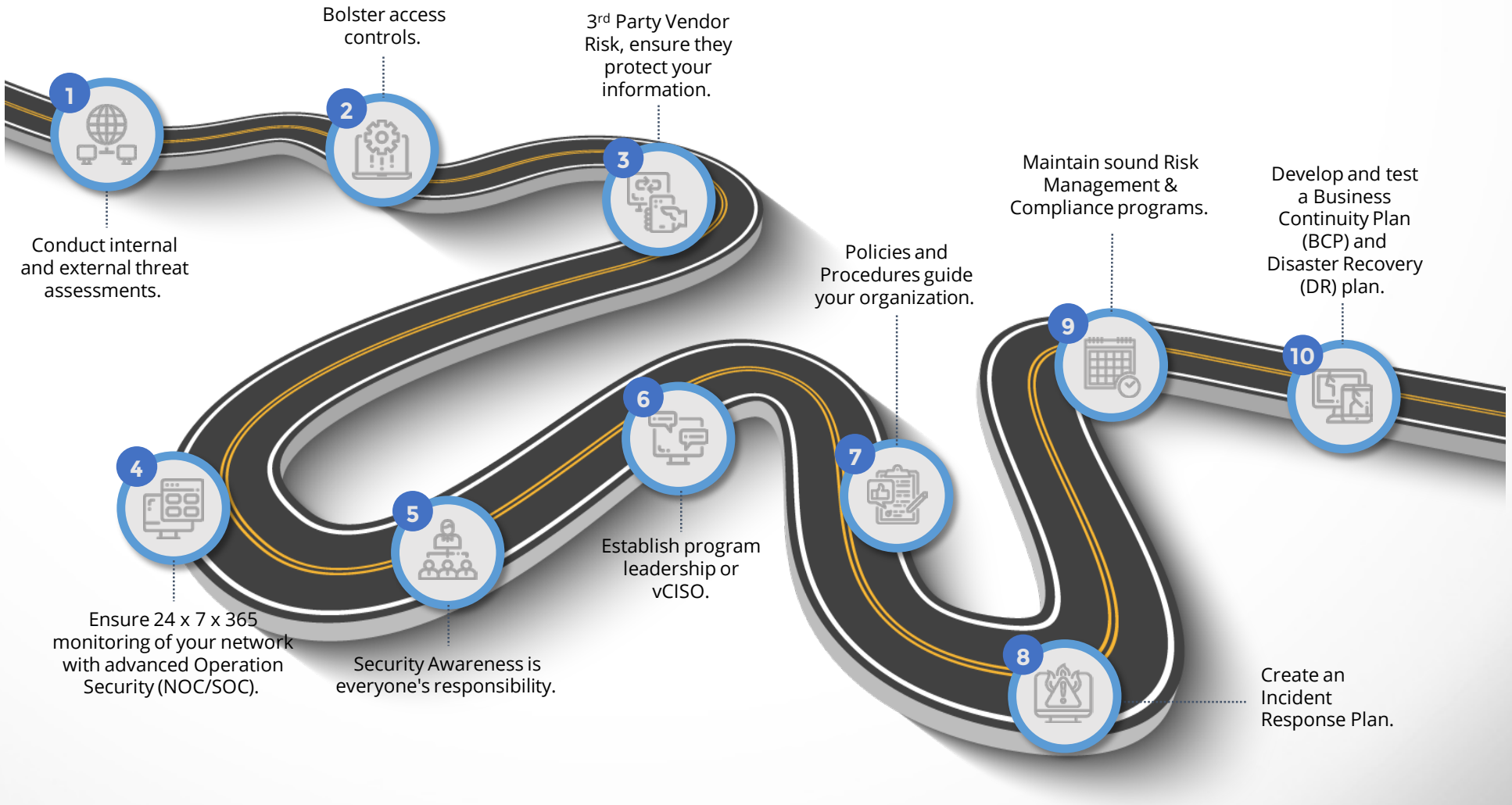
Conduct internal and external assessment

- **How CCTA and MGOTG performed an internal technology audit**
  - ✓ The plan was to ensure CCTA's current infrastructure systems and applications would stand up to a self-test or identify any vulnerabilities
  - ✓ MGOTG delivered a Cyber Security Assessment report on Vulnerability and Penetration Testing
- **Implementation of plan**
  - ✓ CCTA utilized the report to address any concerns and implement a plan
    - ✓ Lifecycle replacement of computers and server – Microsoft Windows 7 support ending January 4, 2020
    - ✓ Migration to the Cloud via Office 365 and SharePoint
    - ✓ CCTA worked with our current IT vendor to implement these plans and receive quotes for executing he upgrades, security enhancements and staff training
    - ✓ Future re-tests will be preformed to ensure the IT infrastructure systems and applications remain safe

Cyber & Information Security Roadmap

MGO TYPE ATYPICAL — A new breed of professional services firm

Addressing Business Risks and Providing Peace of Mind



Questions?
Let's Talk.

MGO
TYPE ATYPICAL