

## Item 3.1: Committee Education on Cybersecurity Risk Management: Leading Practices and the New SOC for Cybersecurity Report

Tom Wojcinski, CISA, CRISC, CCSK, CCSFP Principal, Cybersecurity and IT Risk practice lead Baker Tilly

Finance & Audit Committee Meeting

ERCOT Public October 16, 2017

# **Cybersecurity Risk Management**

Leading practices and the new SOC for Cybersecurity report



### Key Takeaways

- Understand key features of a cybersecurity risk management program
- Understand how the new SOC for Cybersecurity report addresses control assurance requirements
- Identify differences between a SOC 2 and SOC for Cybersecurity
- Develop awareness of required cybersecurity control criteria

### Guest/Customer Panelist



Tom Wojcinski, CISA, CRISC, CCSK, CCSFP Principal, Cybersecurity and IT Risk practice lead Tom.Wojcinski@bakertilly.com



# Cybersecurity assurance reporting



### Increasing pressures and demands



**Business interruption -**

Regulatory fines & penalties -

Legal and PR fees -

Restricted market access -

Remediation costs -



Business impacts

CYBERSECURITY

MANAGEMENT

1

SOC for CYBERSECURITY

- Provide transparency & assurance
- Assess program effectiveness
- Reduce communication burden
- Established standard for completeness & comparability
- Minimize the risk of creating vulnerabilities
- Permit management flexibility for controls and compliance

Boards and directors -

Investors and analysts -

Insurance carriers -

Business partners -

Industry regulators -



Information demands



# Features of a robust cybersecurity management process



### Features of a robust cybersecurity management process

#### **RISK FACTORS**

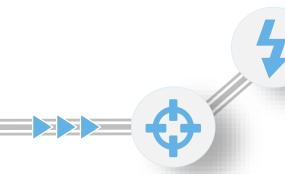
Understanding of factors that have a significant effect on inherent cybersecurity risks

#### **PROCESS**

Established cybersecurity risk assessment process

#### **MONITORING**

Monitoring of the cybersecurity risk management program



#### **OBJECTIVES**

Defined cybersecurity risk management program objectives

#### **GOVERNANCE**

Established cybersecurity risk governance structure

#### COMMUNICATION

Regular cybersecurity communications



Implemented cybersecurity control processes



### Cybersecurity risk management program objectives

to establish cybersecurity objectives and gain BoD or executive management approval of objectives





### Factors effecting inherent risks

Technology in place	Known security incidents
Characteristics of technology, connection types, delivery channels	What's happened in the past year
Organizational and user characteristics	Impaired achievement of cybersecurity objectives
Environmental, technological and organizational	Required disclosures of nature, timing and extent of incident



### Governance structure

ACCOUNTABILITY AND REPORTING LINES

PROCESS TO HIRE AND DEVELOP COMPETENT INDIVIDUALS

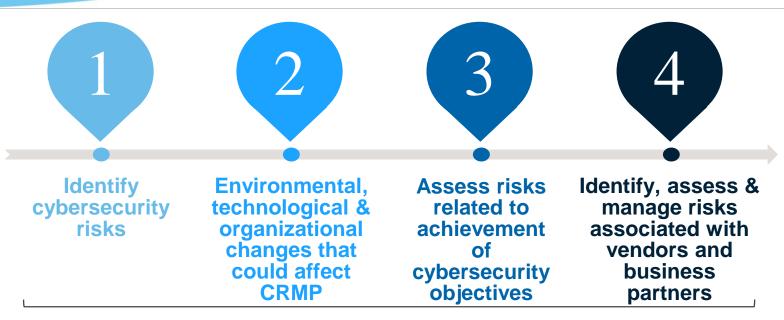
PROCESS FOR BOARD OVERSIGHT OF CRMP

✓ Board's level of expertise and committee oversight

DEFINED PROCESS TO ESTABLISH,
MAINTAIN AND COMMUNICATE
INTEGRITY

- ✓ Tone at the top; Standards for conduct including vendors and contractors
- ✓ Process to identify and remediate unmet standards

### Risk assessment process



**Establish processes** 



### Cybersecurity communications

Objectives and responsibility for cybersecurity

Thresholds for communicating identified cybersecurity events determined to be security incidents requiring a response and/or remediation

Defined method to internally communicate information critical to the functioning of CRMP

Legal, regulatory, fiduciary requirements

Established process to communicate with external parties about matters affecting the CRMP

Whistle blower hotline



### Monitoring the program



Established process to periodically evaluate operating effectiveness of key control activities related to cybersecurity



Established process for timely evaluation and communication of threats, vulnerabilities, and control deficiencies



### Cybersecurity control processes

#### Prevent

 Prevention of intentional and unintentional security events

#### Detect

Detection of security events, identification of incidents, development of response, mitigation and recovery

#### Manage

 Management of processing capacity to support continued operations during events

### Migrate & Recover

 Detection, migration and recovery from environmental or other availability incidents

### Retain or Destroy

 Identification, retention and destruction of confidential information

Design and implementation of controls

# Cybersecurity control criteria



### Framework flexibility



Trust services criteria



ISO 27002



NIST 800-53



### Framework comparison

ISO 27002

#### NIST 800-53

#### **AICPA Trust Services**

- Access control
- Asset management
- · Communications security
- Compliance
- Cryptography
- · Human resources security
- · IS aspects of business continuity
- · Incident management
- Information security policy
- Operations security
- · Organization of information security
- Physical and environmental security
- · Supplier relationships
- System acquisition, development and maintenance

- · Access control
- Awareness and training
- Audit and accountability
- Security assessment and authorization
- · Configuration management
- Contingency planning
  - Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Planning
- Personnel security
- · Risk assessment
- System and services acquisition
- System and communication protection
- System and information integrity
- Program management

- Control environment
- Communication and information
- Risk assessment
- Monitoring activities
- Control activities
- Logical and physical access controls
- System operations
- Change management
- Risk mitigation
- · Additional criteria for availability
- Additional criteria for confidentiality
- Additional criteria for processing integrity
- Additional criteria for privacy



## What to expect in a SOC for Cybersecurity exam



### Readiness effort Prepare Control gap the system assessment description Scoping

- Nature of business and operations
- Nature of information at risk
- Cybersecurity risk management process

- Identify systems
- Classify and locate data

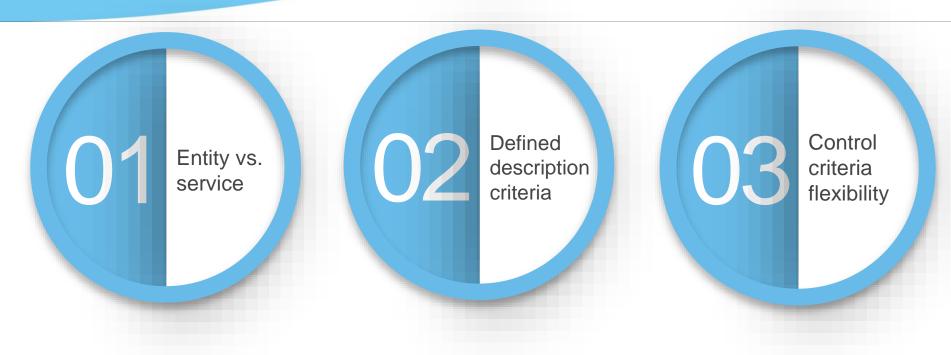


#### Examination

- > Parallels to SOX audit
  - Identifying populations
  - Selections and samples
  - IPE
  - Control testing
- > Treating exceptions
  - Response
  - Qualification



### Differences from SOC 2





#### Questions?



**Tom Wojcinski** 

Principal, Cybersecurity and IT Risk practice lead Tom.Wojcinski@bakertilly.com

bakertilly.com/cybersecurity

CISA, CRISC, CCSK, CCSFP



### Thank you!

