Systems and Organization Controls for Cybersecurity

THE AICPA'S CYBERSECURITY RISK MANAGEMENT REPORTING FRAMEWORK

BY
ROBIN PENNINGTON
ASSOCIATE PROFESSOR

1

Topical Overview

- The rise in cybersecurity incidents
- Cybersecurity Risk Management Programs in organizations
- Cybersecurity control frameworks
- Communications to stakeholders
- The basics of the new cybersecurity reporting framework developed by the AICPA
- The description criteria for management's report

2

Cybersecurity breaches on the rise

National Governors Association:

"States are attractive targets because they collect and store massive amounts of personal and financial data. They also own, control and regulate critical infrastructure. Yet all states struggle to defend agencies against cybersecurity threats. Some of the most sophisticated cyber hacking tools—once the sole purview of militaries and intelligence agencies—are now widely available to anyone with an Internet connection. States are on the front lines of cybersecurity, and adversaries will continue to target them."

Cybersecurity breaches on the rise

Notorious Financial Data/Credit Card/Personal Data Examples:

- 2018 Marriott, British Airways, Macy's, Bloomingdales, Facebook
- 2017 Equifax
- 2014 JP Morgan
- 2014 Home Depot
- 2013 Target

Cybersecurity breaches on the rise

Notorious Government Examples:

- 2019 City of Tallahassee
- 2018 Medicare and Medicaid
- 2016 Democratic National Committee
- 2014 US Office of Personnel Management
- 2014 German Parliament
- 2013 Singapore cyberattacks

Cybersecurity breaches on the rise

University Examples:

- 2019 Georgia Tech
- 2018 Yale (from a decade ago)
- 2017 Washington State University
- 2016 NC State University
- 2014 Duke University and Duke Medicine

Cybersecurity Risk Management Programs

An entity's policies and procedures (i.e., internal controls) put in place to secure and protect information and systems from cybersecurity events and to detect, respond and recover from events that are not prevented from occurring.

Cybersecurity Control Frameworks

- National Institute of Standards and Technology (NIST)
  - Adopted by the state of North Carolina
- ISO 27001/27002
- HITRUST
- Trust Services Framework
- COBIT

Communication to Stakeholders

How informed are stakeholders?

- How do stakeholders learn about an entity's cybersecurity risk management initiatives?
- How important is communication to stakeholders?
- What about communication of cybersecurity breaches?
  - Current guidelines
  - Press Releases

Polling Question #1

What cybersecurity risk management framework does the State of NC use?

- ❑ National Institute of Standards and Technology (NIST)
- ❑ ISO 27001/27002
- ❑ HITRUST
- ❑ Trust Services Framework
- ❑ COBIT

SOC for Cybersecurity

SOC for Cybersecurity - History

- SAS 70
- Service Organization Controls:
  - SOC 1
  - SOC 2
  - SOC 3
- SSAE 16
- Systems and Organization Controls
- SSAE 18
- SOC Suite of Services

SOC for Cybersecurity - History

Why SOC for Cybersecurity?

- Numerous risk management frameworks
- No common criteria for disclosures about the entity's cybersecurity risk management program
- No widely accepted approach or professional standards for providing security assessments

SOC for Cybersecurity

Cybersecurity Risk Management Reporting Framework – a few objectives:

- Common description criteria
  - Helps to reduce communication and compliance burden
  - Useful information for stakeholders
  - Comparability among organizations
- Common criteria for assessment

SOC for Cybersecurity

Flexibility built in:

- Voluntary disclosure
- Framework choice
- Best practices
- Scalable and flexible
- Evolving

SOC for Cybersecurity

3 Reporting Levels:

- Entity
- Service Provider
- Supply Chain

SOC for Cybersecurity

Entity Level Reporting

1. Management's Description
2. Management's Assertion
3. Practitioner's Opinion

SOC for Cybersecurity

Entity Level Reporting – two sets of criteria:

1. Description Criteria
2. Control Criteria

SOC for Cybersecurity

Criteria flexibility:

AICPA has developed criteria based on the Trust Services Framework, however, management may select other criteria (control frameworks) for the description criteria and control criteria

Polling Question #2

SOC for Cybersecurity provides which of the following criteria:

- Description Criteria
- Control Criteria
- Both Description and Control Criteria

SOC for Cybersecurity

Entity Level Reporting:
Management's Description

SOC for Cybersecurity

Description Criteria include the following categories:

a. Nature of Business and Operations
b. Nature of Information at Risk
c. Cybersecurity Risk Management Program Objectives

SOC for Cybersecurity

Description Criteria include the following categories:

d. Factors that have a Significant Effect on Inherent Cybersecurity Risks
e. Cybersecurity Risk Governance Structure
f. Cybersecurity Risk Assessment Process

SOC for Cybersecurity

Description Criteria include the following categories:

g. Cybersecurity Communications and the Quality of Cybersecurity Information
h. Monitoring of the Cybersecurity Risk Management Program
i. Cybersecurity Control Processes

Polling Question #3

The description criteria elements recommended in SOC for Cybersecurity reporting framework are intended for voluntary disclosure.

- True
- False

SOC for Cybersecurity

Entity Level Reporting:
Management's Assertion

SOC for Cybersecurity

Management's Assertion:

Management provides an assertion regarding whether the description is presented in accordance with the stated criteria and whether the controls in place were effective to achieve the entity's cybersecurity objectives based on the control criteria.

SOC for Cybersecurity – Management's Assertion Example

Section 1—Assertion of the Management of XYZ Manufacturing

Introduction

We have prepared the attached XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in the AICPA *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established XYZ Manufacturing's cybersecurity objectives, which are presented on page XX of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

SOC for Cybersecurity – Management's Assertion Example

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

SOC for Cybersecurity – Management's Assertion Example

Assertion

We assert that the description throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls included within the cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, using the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

SOC for Cybersecurity

Entity Level Reporting:
Practitioner's Opinion

SOC for Cybersecurity

Practitioner's Opinion:

CPA's opinion on the description and the effectiveness of the controls based on the criteria.

Polling Question #4

Does a third party validate your entity's cybersecurity risk management program?

- Yes
- No
- Not Sure

Key Takeaways – SOC for Cybersecurity

- Cybersecurity incidents are on the rise
- Organizations need robust cybersecurity risk management programs to control risks
- Many cybersecurity control frameworks exist
- Communications to stakeholders is important
- The AICPA developed the SOC cybersecurity reporting framework to address the market need for a common language and common criteria regarding cybersecurity initiatives

Thank You!

References

AICPA (2017) Description criteria for management's description of the entity's cybersecurity risk management program. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/description-criteria.pdf

AICPA (2018) Illustrative cybersecurity risk management report. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/illustrative-cybersercurity-risk-management-report.pdf

AICPA (2018) SOC for cybersecurity: a backgrounder. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-backgrounder.pdf

National Governors Association (2019). Meet the Threat: A compact to improve state cybersecurity. https://files.nc.gov/ncdit/documents/files/NGA-Cybersecurity-Compact-2017-07-14.pdf