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

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

BAKER TILLY

Guest/Customer Panelist

Tom Wojcinski,
CISA, CRISC, CCSK, CCSFP

Principal, Cybersecurity and IT Risk practice lead

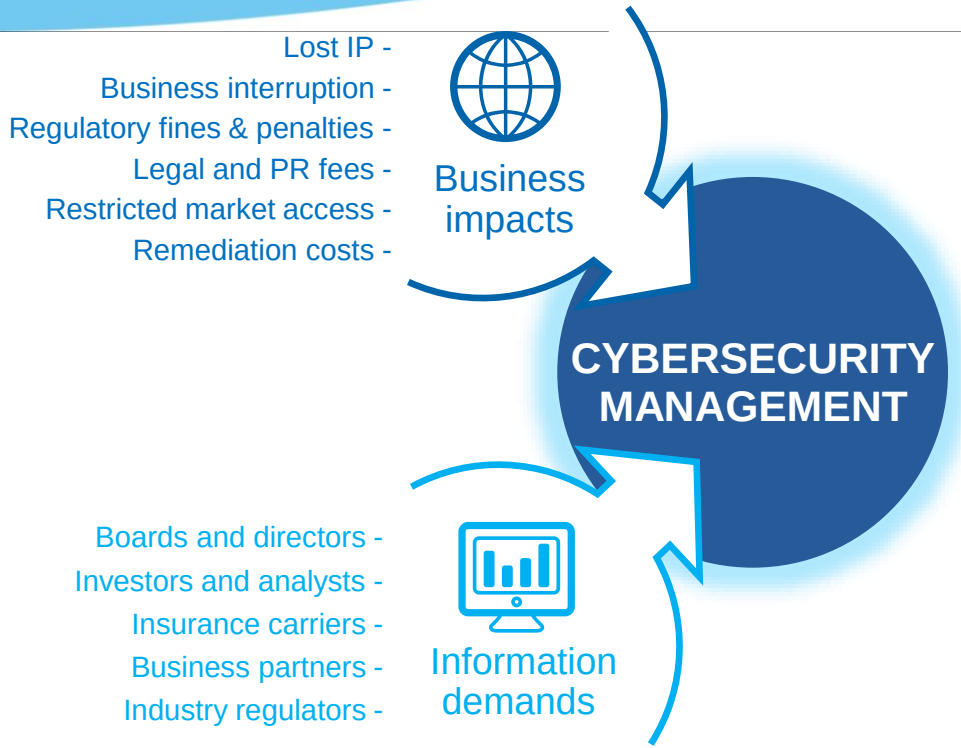
Tom.Wojcinski@bakertilly.com

BAKER TILLY

Cybersecurity assurance reporting

BAKER TILLY

Increasing pressures and demands



SOC for CYBERSECURITY

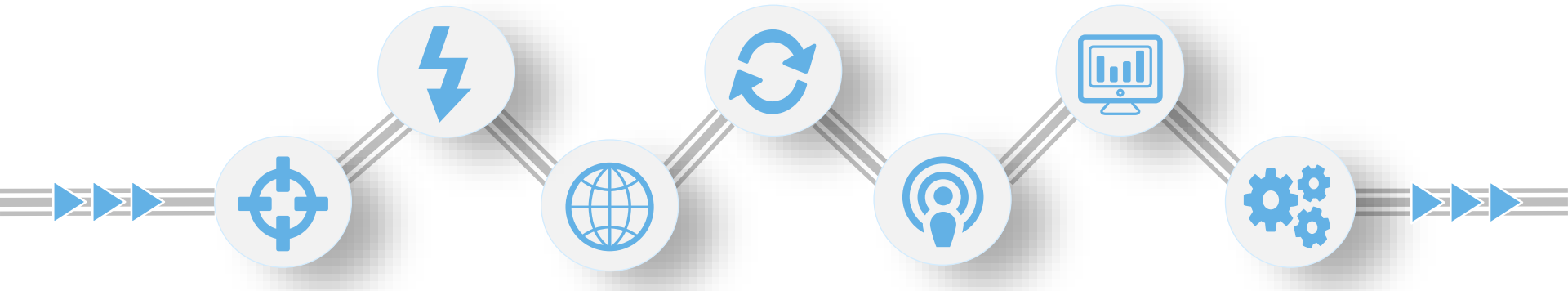
- Provide transparency & assurance
- Assess program effectiveness
- Reduce communication burden
- Established standard for completeness & comparability
- Minimize the risk of creating vulnerabilities
- Permit management flexibility for controls and compliance

BAKER TILLY

Features of a robust cybersecurity management process

BAKER TILLY

Features of a robust cybersecurity management process



OBJECTIVES
Defined cybersecurity risk management program objectives

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

GOVERNANCE
Established cybersecurity risk governance structure

PROCESS
Established cybersecurity risk assessment process

COMMUNICATION
Regular cybersecurity communications

MONITORING
Monitoring of the cybersecurity risk management program

IMPLEMENTATION
Implemented cybersecurity control processes

BAKER TILLY

Cybersecurity risk management program objectives

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

BAKER TILLY

Factors effecting inherent risks

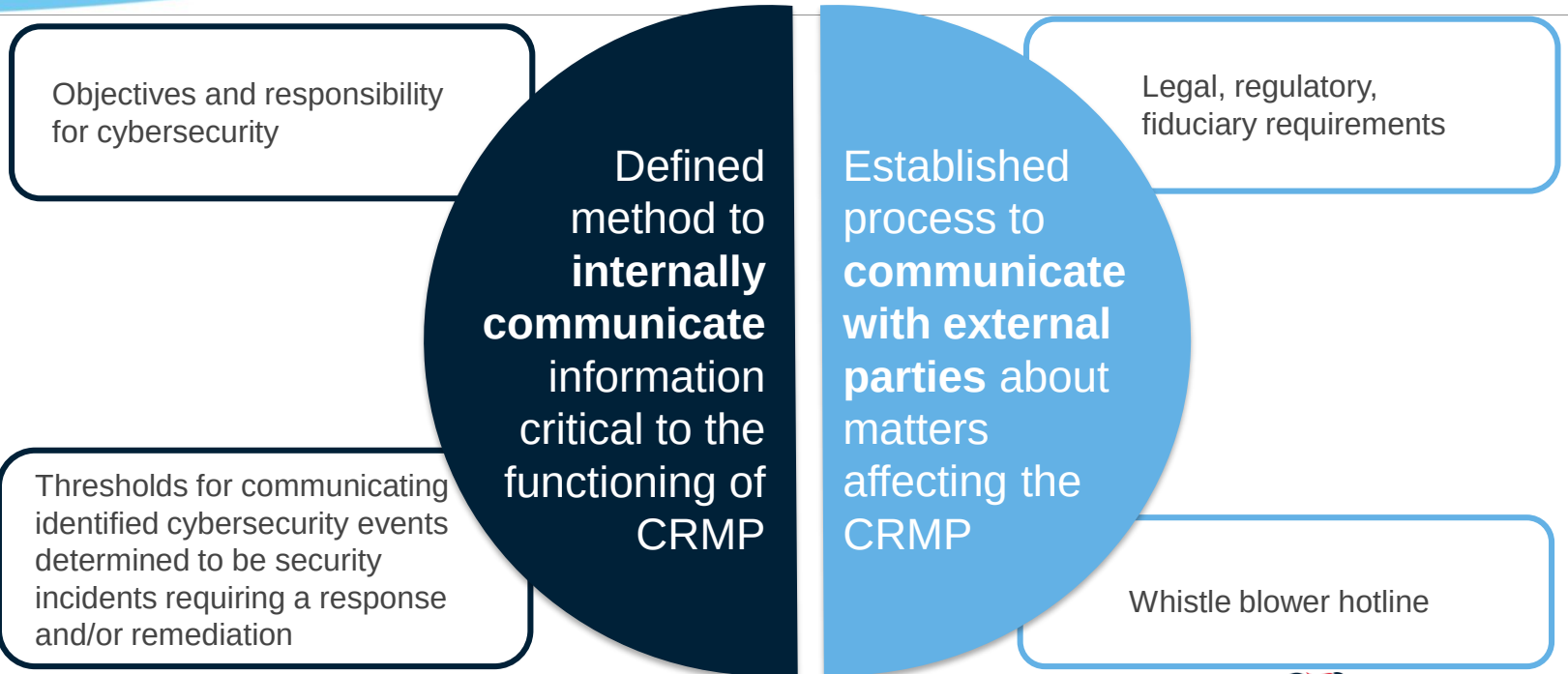
Technology in place	Known security incidents
Characteristics of technology, connection types, delivery channels	What's happened in the past year
Organizational and user characteristics	Impaired achievement of cybersecurity objectives
Environmental, technological and organizational	Required disclosures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

Governance structure

Risk assessment process

BAKER TILLY

Cybersecurity communications



BAKER TILLY

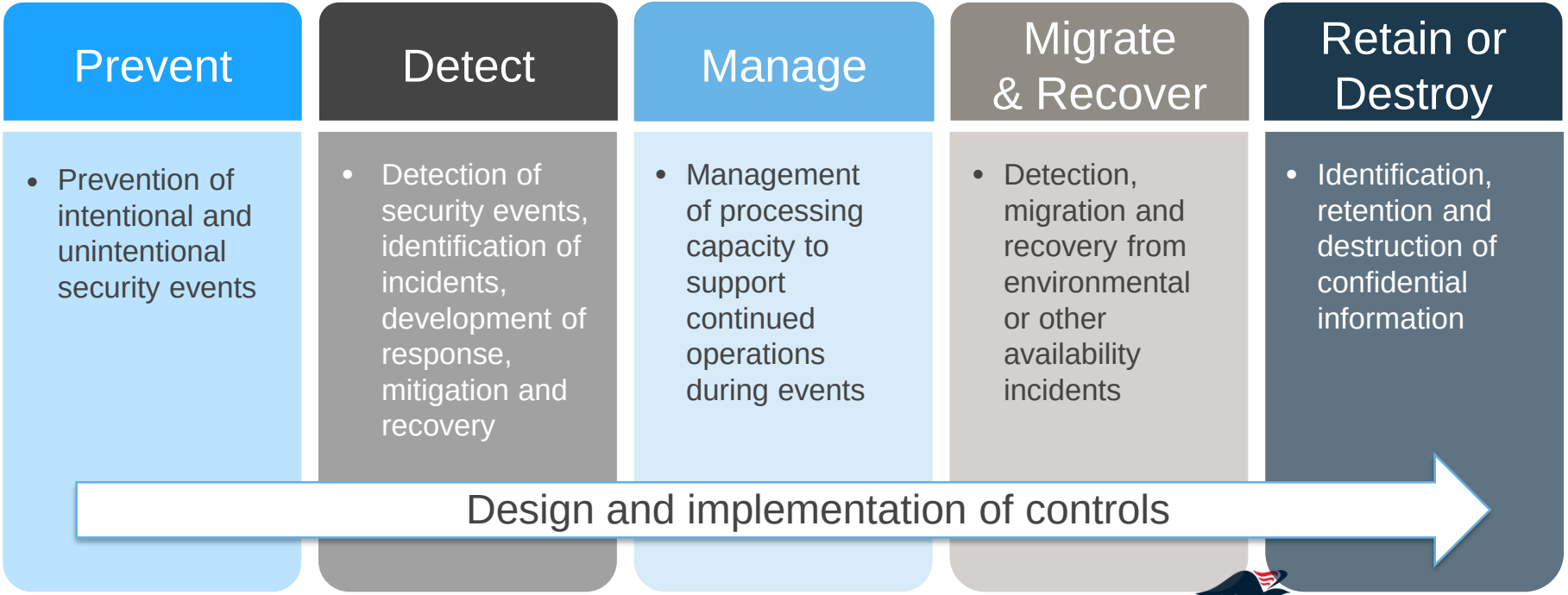
Monitoring the program

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

BAKER TILLY

Cybersecurity control processes



BAKER TILLY

Cybersecurity control criteria

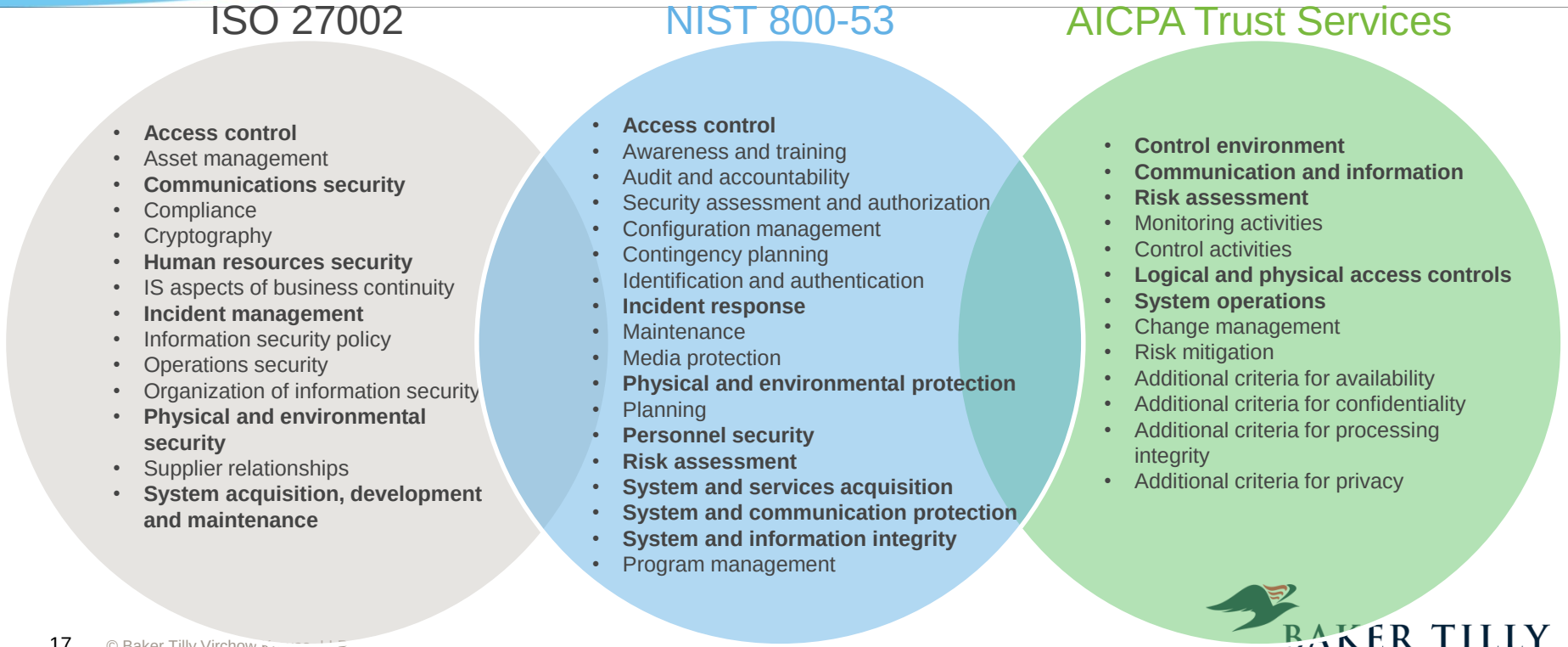
BAKER TILLY

Framework flexibility

AICPA American Institute of CPAs®	Trust services criteria
ISO	ISO 27002
NIST National Institute of Standards and Technology	NIST 800-53

BAKER TILLY

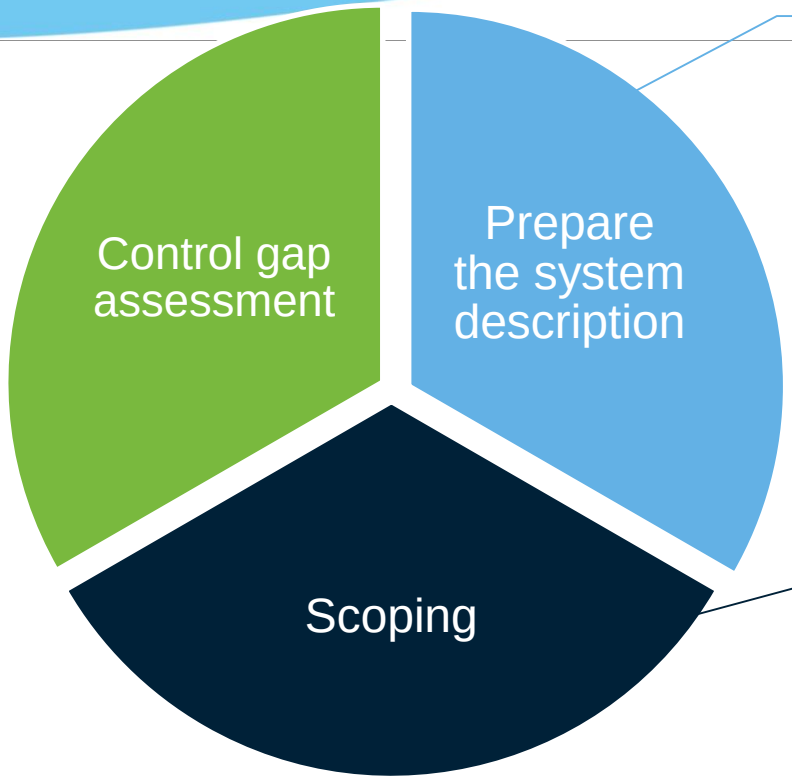
Framework comparison



What to expect in a SOC for Cybersecurity exam

BAKER TILLY

Readiness effort



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

- Identify systems
- Classify and locate data

BAKER TILLY

Examination

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

BAKER TILLY

Differences from SOC 2

BAKER TILLY

Questions?

Tom Wojcinski

Principal, Cybersecurity and IT Risk practice lead

Tom.Wojcinski@bakertilly.com

bakertilly.com/cybersecurity

CISA, CRISC, CCSK, CCSFP

BAKER TILLY

Thank you!