

SECURE360 conference

TOM WOJCINSKI AND DAN STEINER
THE VALUE OF SOC 2 COMPLIANCE
BEYOND COMPLIANCE ENGAGEMENTS:
TUESDAY, MAY 14 - 1:00

WELCOME TO SECURE360 2013



- Don't forget to pick up your Certificate of Attendance at the end of each day.
- Please complete the Session Survey front and back, and leave it on your seat.
- Are you tweeting? #Sec360

INTRODUCTIONS

Tom Wojcinski, CISA, CRISC

- Director, Baker Tilly Virchow Krause, LLP
- Phone: 414-777-5536
- Email: Tom.Wojcinski@bakertilly.com

Daniel Steiner, MBA, CPA, CFE, ARM

- Manager, Baker Tilly Virchow Krause, LLP
- Phone: 608-220-5528
- Email: Daniel.Steiner@bakertilly.com



BAKER TILLY VIRCHOW KRAUSE, LLP

With more than 1,400 employees, Baker Tilly provides a wide range of accounting, tax, and advisory services. Ranked as one of the top twenty largest firms in the country*, Baker Tilly serves clients from offices in Chicago, Detroit, Minneapolis, New York, Washington DC, and throughout Wisconsin.

Baker Tilly International is a worldwide network of independent accounting and business advisory firms in 125 countries, with more than 25,000 professionals. The combined worldwide revenue of independent member firms exceeds \$3 billion

**According to the 2012 Accounting Today "Top 100 Firms."*



Candor. Insight. Results.

AGENDA

A brief history and perspective of the new SOC landscape

- SOC reporting defined and clarified

SOC 2

- Trust services overview
- Report structure
- Examination process

Benefits beyond compliance

Alignment with other compliance frameworks



THE SOC LANDSCAPE

AICPA replaced SAS 70

- Effective for audit periods ending after June 15, 2011
- Established the Statement of Control Framework (SOC Framework)

Why

- Confusion in the market – “we are SAS 70 certified”
- Frequently misused to report on controls not relevant to financial reporting – market demand for expanded scope of report
 - Security
 - Availability
 - Processing integrity
 - Confidentiality
 - Privacy

THE SOC LANDSCAPE

Why - continued

- Growth of the service organization landscape
 - New technologies
 - Cloud computing (SAAS, PAAS, IAAS)
 - Convergence of US and international standards
 - Increased leverage on outsourced service offerings from experts
- 

THE SOC LANDSCAPE

SOC 1

(Service organization control 1)

Applicable to services that are likely to be relevant to user entities' internal control over financial reporting

Reports on controls supporting financial statement audits

Restricted to customers during the audit period

Example organizations: payroll processors, transaction processors

SOC 2

(Service organization control 2)

Applicable to services that don't directly impact financial reporting

Reports on controls related to operations

Restricted to those familiar with the subject matter

Example organizations: Direct mailers, call centers

SOC 3

(Service organization control 3)

Applicable to services that don't directly impact financial reporting

Reports on controls related to operations

General use report

Example organizations: Direct mailers, call centers

SOC 1 REPORT

What's in the report?

- **Formal audit letter**
- **Management's assertion**
- **Management's system description, including specified control objectives**
- **Tests of controls and results**

Impacts to service organizations

- **Written assertion about the accuracy and relevance of the system description and the design and operating effectiveness of controls**
- **Specify the criteria used in making the assertion**
- **Management must have a reasonable basis for its assertion**
- **Document and disclose changes in controls during the period**

Impacts to user entities

- **Can be used to support financial statement audit**
- **Need to evaluate exceptions and determine relevance and any additional analysis**
- **Should be evaluated and confirm compliance with user control considerations**

SOC 2 REPORT

What's in the report?

- **Formal audit letter**
- **Management's assertion**
- **Management's system description, including trust Services principles and criteria instead of control objectives**
- **Tests of controls and results**

Impacts to service organizations

- **Additional requirements for system description - much clearer guidance on how to describe the system**
- **Similar requirements as SOC 1 for management's assertion**

Impacts to user entities

- **Focused on control assurance**
- **Not likely useful in a financial statement audit**

SOC 3 REPORT

What's in the report?

- **Audit report with limited opinion**
- **Abbreviated system description**

Impacts to service organizations

- **Enhanced marketing potential**
- **May not be possible in scenarios with subservice organizations or significant reliance on user control considerations**

Impacts to user entities

- **Useful where detailed understanding of controls isn't required**

THE THREAT FROM WITHIN

- **Texas** data breach exposed 3.5 million records: Names, addresses, and social security numbers of state retirees and unemployment beneficiaries were posted, unencrypted, on a public server. (InformationWeek, April 13 2011)
 - Internal staff error
 - **Bank of America** gets hit twice by internal staff: ATMs and data were compromised in separate attacks stemming from an employee theft of bank customer data and a multi-ATM heist perpetrated by a Diebold employee. (Bank Technology News – American Banker, May 2011)
 - Internal staff and vendor staff purposeful breach
- 

THE THREAT FROM WITHIN

- **New York State Electric & Gas (NYSEG) and Rochester Gas and Electric (RG&E)** data breach of Social Security numbers, dates of birth and financial institution account numbers through an independent software development consulting firm employee who allowed unauthorized access to one of the companies' customer information systems.

(http://www.databreaches.net/?p=22960&goback=%2Egde_860307_member_91453823, January 24, 2012)

- Contractor data breach
- **Telstra** (an internet and email service provider) data breach of detailed information outlining the customer's account number, what broadband plan they are on, other Telstra services they were signed up to and notes associated with the accounts, including user names and passwords causing the company to suspend services to almost 1 million users.

(<http://www.smh.com.au/it-pro/it-news/network-outage-as-telstra-probes-privacy-breach-20111210-1oohk.html>, December 10, 2011)

- Unspecified internal staff error

SOC 2 DEFINED

TRUST SERVICES

What are trust services (“TS”)?

- A set of professional attestation and advisory services
 - based on a core set of principles and criteria that addresses the risks and opportunities of IT-enabled systems and privacy programs.
- Consists of five key components organized to achieve a specified objective.

KEY COMPONENTS OF TRUST SERVICES

Infrastructure

- The physical and hardware components of a system (facilities, equipment, and networks)

Software

- The programs and operating software of a system (systems, applications, and utilities)

People

- The personnel involved in the operation and use of a system (e.g. developers, operators, users, and managers)

Procedures

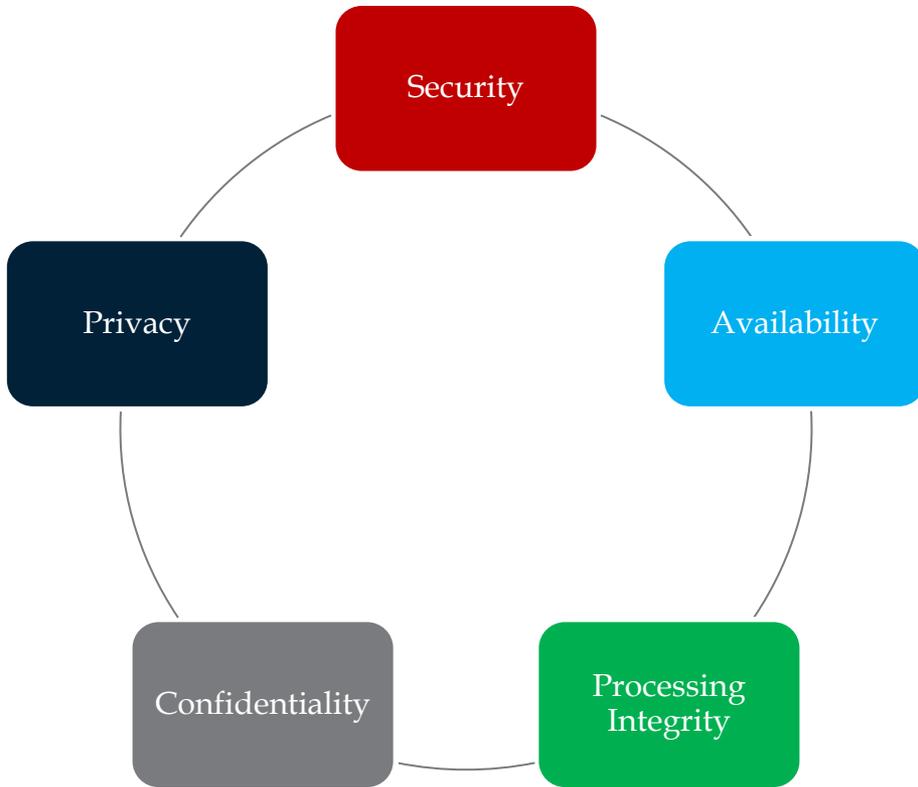
- The programmed and manual procedures involved in the operation of a system (automated or manual)

Data

- The information used and supported by a system (e.g. transaction streams, files, databases, and tables)



TRUST PRINCIPLES



| Principles | Objectives |
|-----------------------------|--|
| Security | The protection of the system from unauthorized access, both logical and physical |
| Availability | The accessibility to the system, products, or services as advertised or committed by contact, service-level, or other agreements |
| Processing integrity | The completeness, accuracy, validity, timeliness, and authorization of system processing |
| Confidentiality | The system's ability to protect the information designated as confidential, as committed or agreed |
| Privacy | Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the privacy notice |

TRUST SERVICES PRINCIPLES AND CRITERIA

Defined criteria in five trust principle areas

- Further subdivided into trust services criteria domains:
 - Policies
 - Communication
 - Procedures
 - Monitoring

A lot of overlap built into the criteria

- 51 unique criteria across security, availability, processing integrity, confidentiality
- Separate criteria specific to privacy

GENERALLY ACCEPTED PRIVACY PRINCIPLES

Privacy principles

- Provides criteria and related material for protecting the privacy of personal information
 - Incorporates concepts from significant domestic and international privacy laws, regulations, and guidelines
 - Used to guide and assist organizations in implementing privacy programs
-
- <http://www.aicpa.org/privacy>

GENERALLY ACCEPTED PRIVACY PRINCIPLES

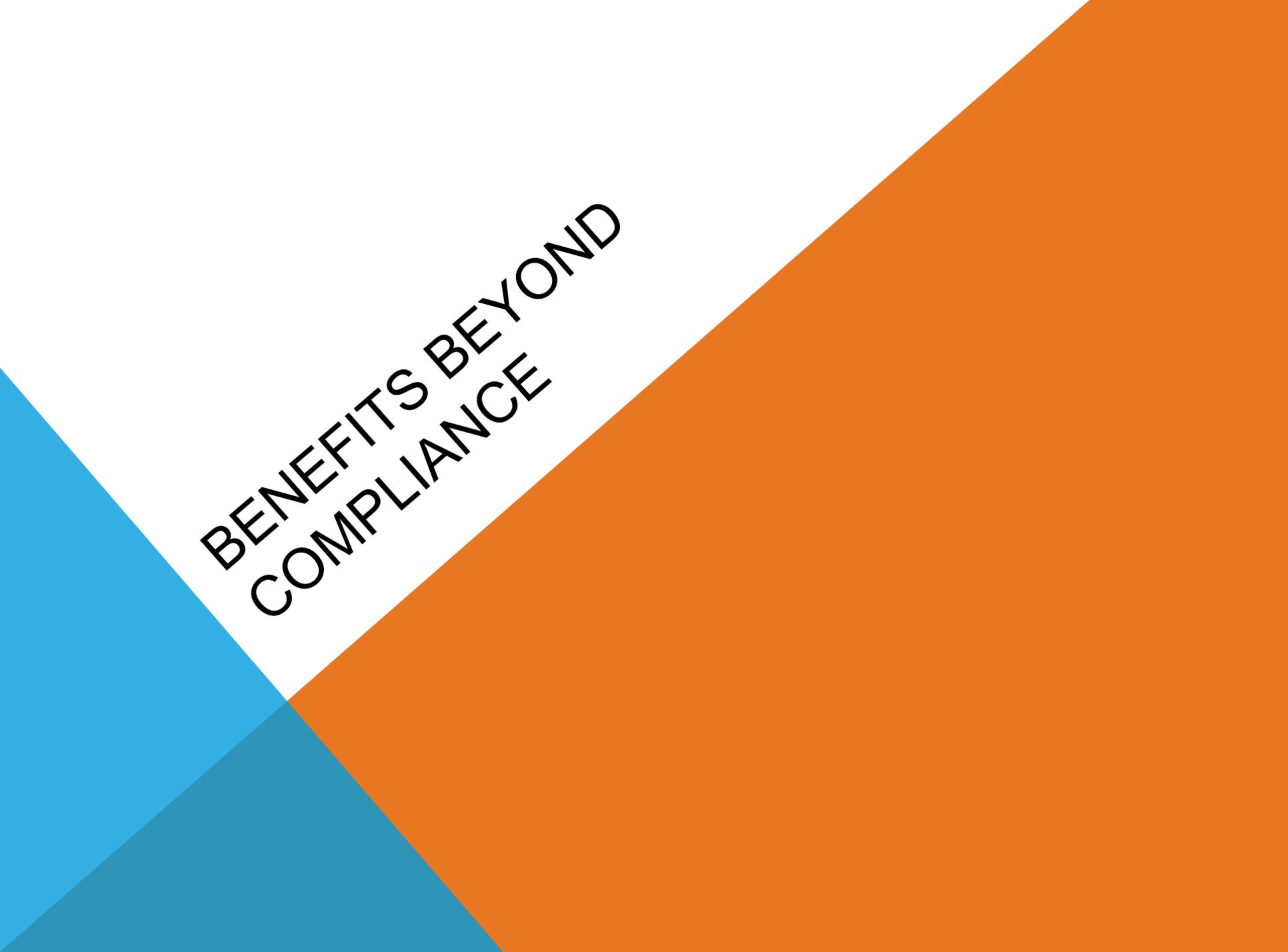
- 1) Management
- 2) Notice
- 3) Choice and consent
- 4) Collection
- 5) Use and retention
- 6) Access
- 7) Disclosure to third parties
- 8) Security for privacy
- 9) Quality
- 10) Monitoring and enforcement

<http://www.aicpa.org/privacy>

REPORT STRUCTURE

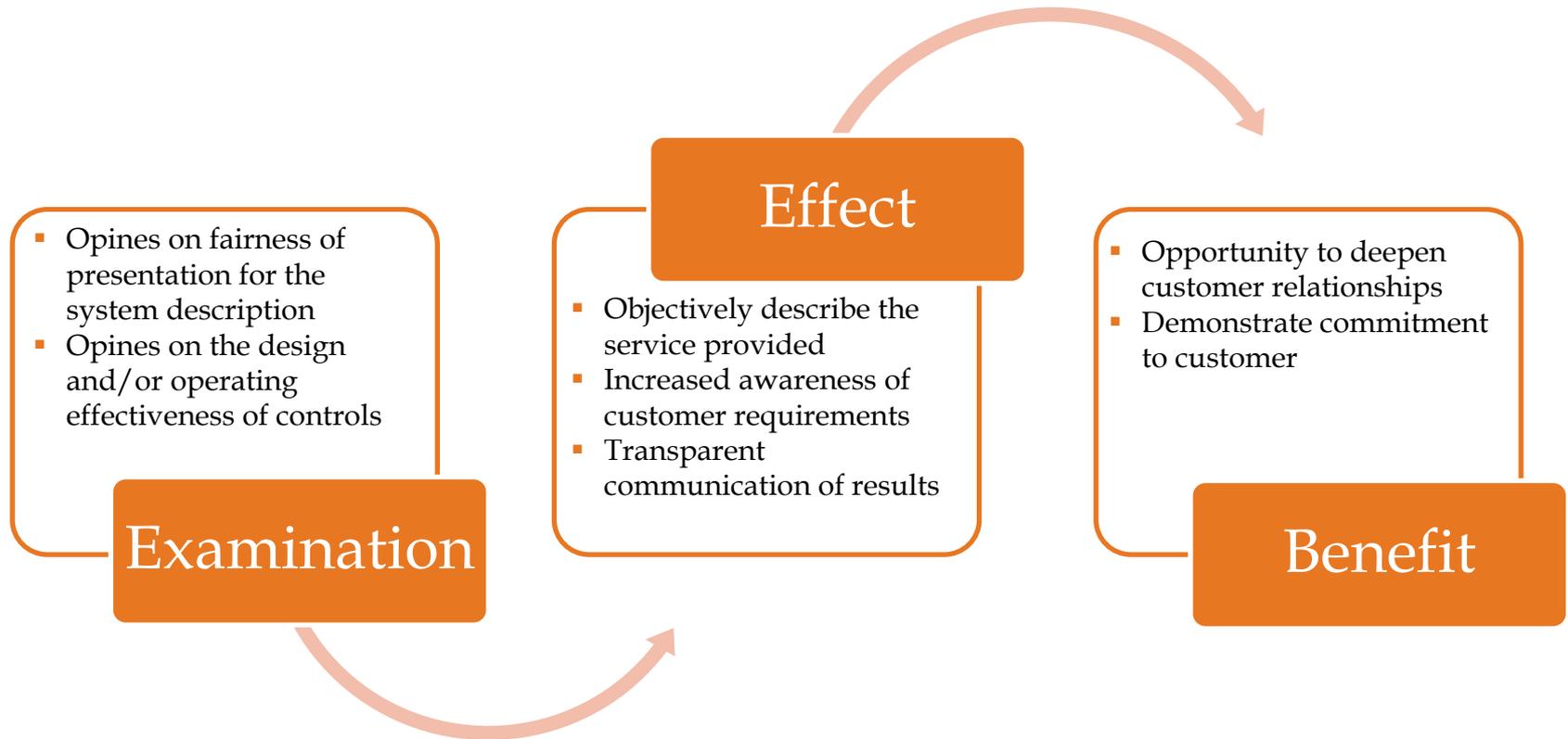
Sections

- 1) Service auditor's report (the opinion)
 - 2) Management's assertion
 - 3) System description
 - 4) Tests of controls and results
 - 5) Additional information provided by the service organization
- 

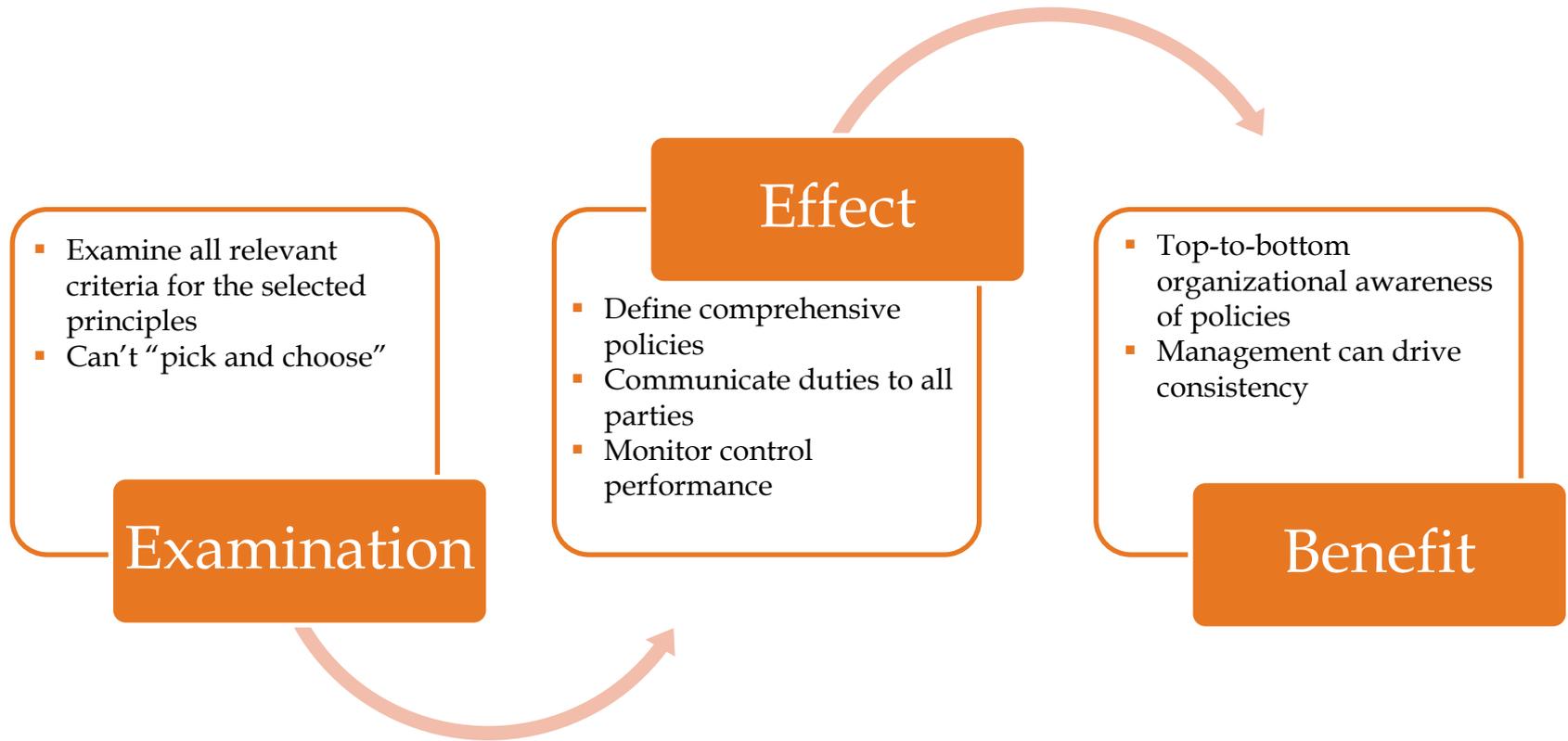
The background features a white central area where the text is located. This white area is bounded by a diagonal line from the top-left to the bottom-right. To the left of this line, there are two overlapping triangles: a larger light blue one and a smaller, darker blue one. To the right of the diagonal line, there is a large, solid orange triangle that fills the right side of the frame.

**BENEFITS BEYOND
COMPLIANCE**

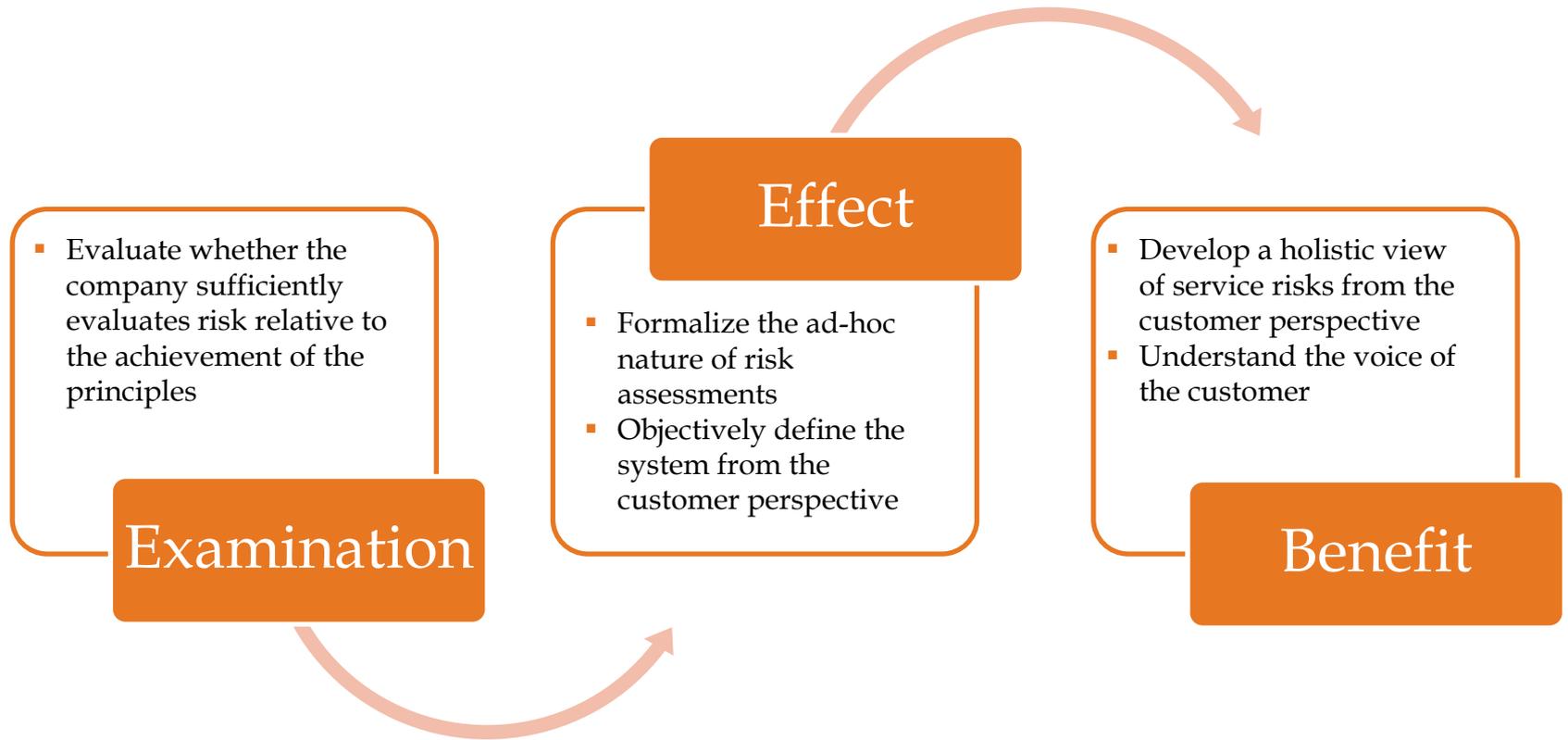
BUILD TRUST AND COMMUNICATION



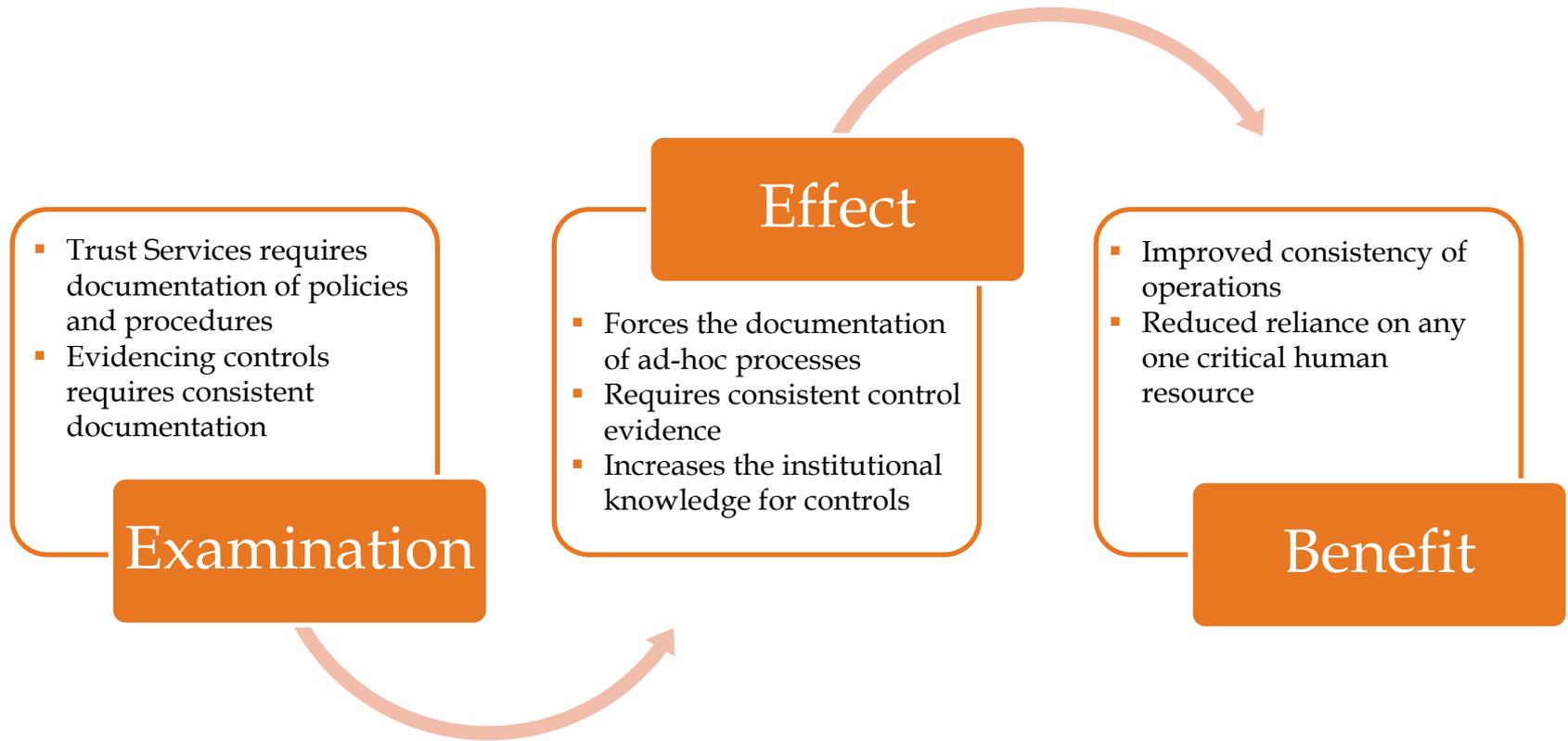
STRENGTHEN ENTITY LEVEL CONTROLS



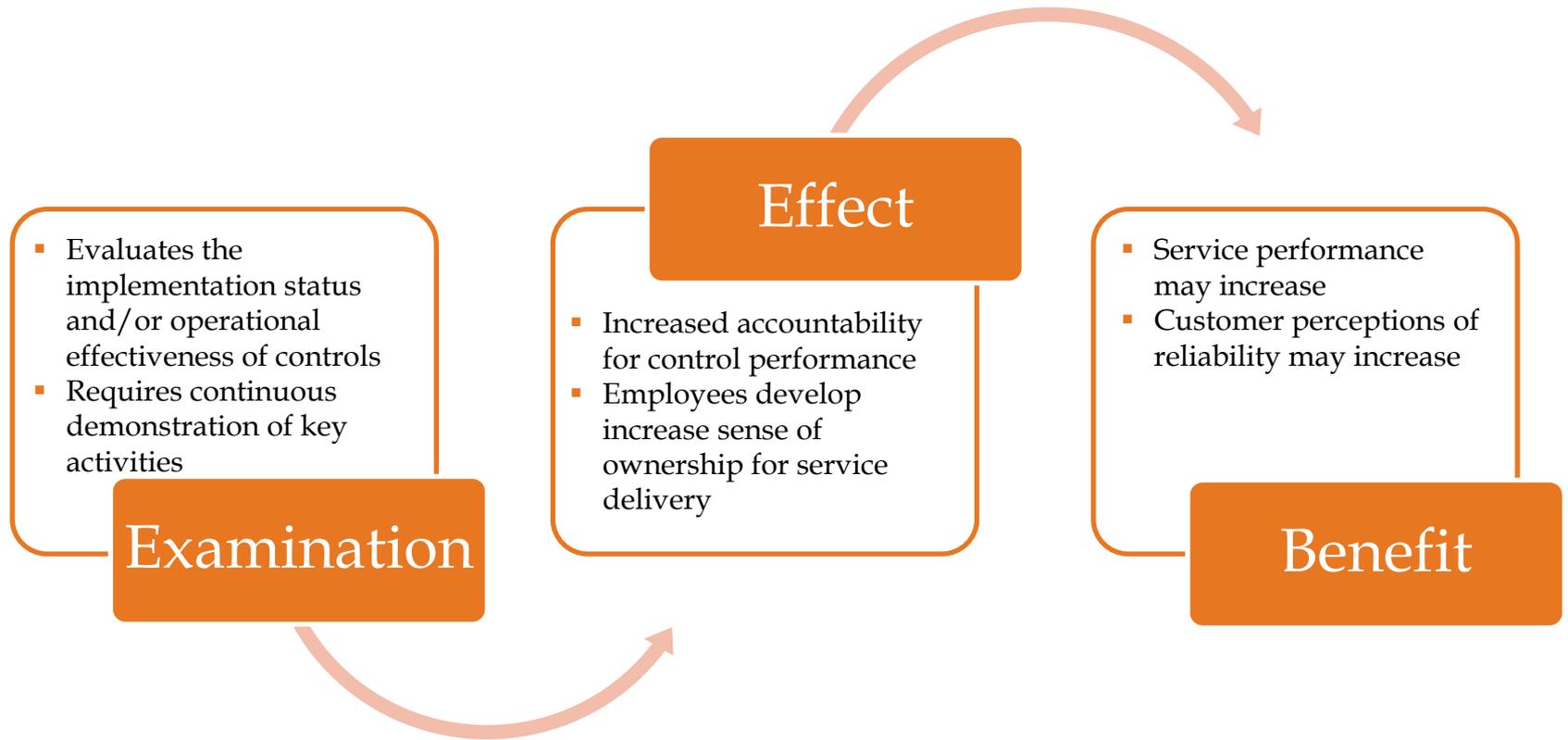
ENHANCED RISK AWARENESS



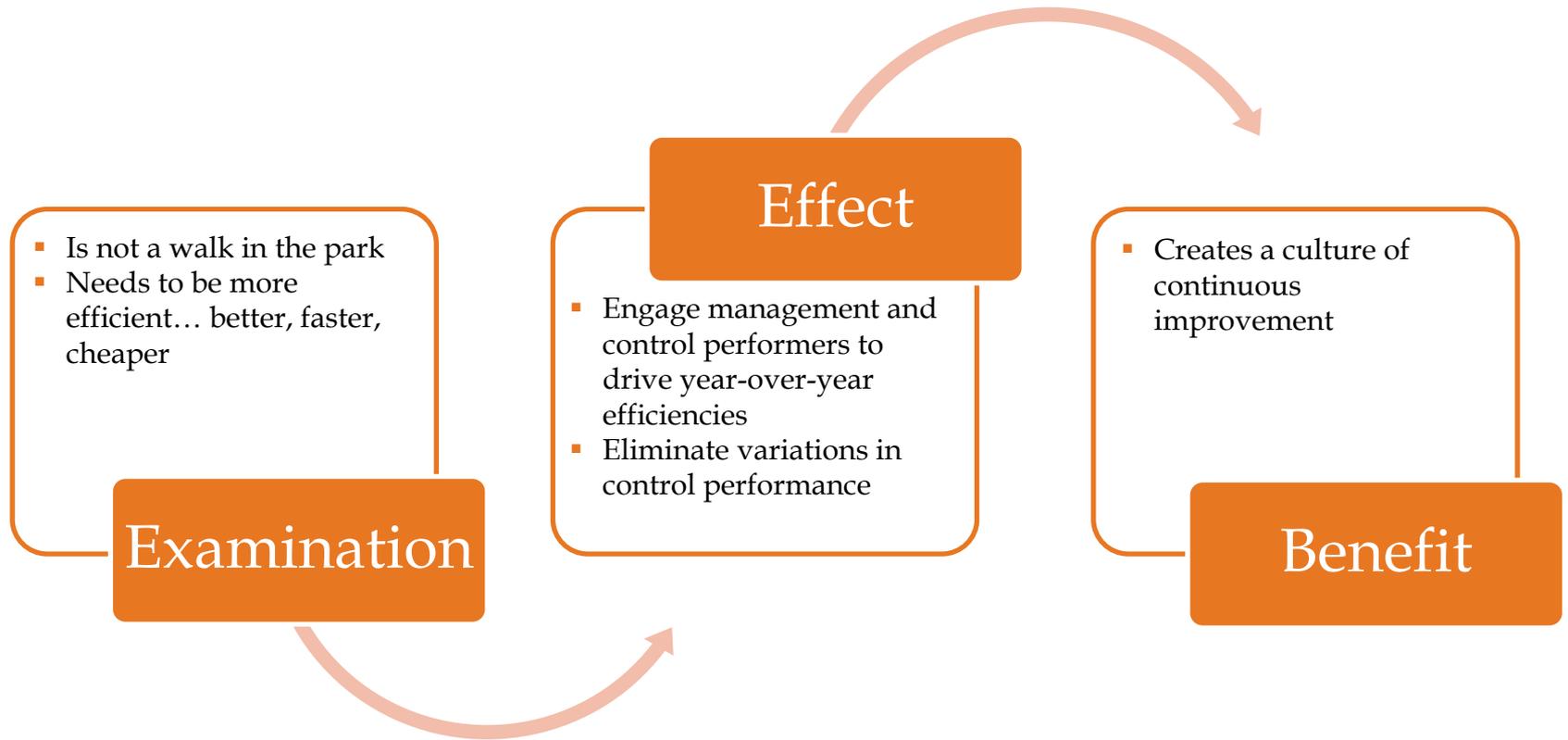
IMPROVED CONSISTENCY



ENHANCED RELIABILITY



CULTURE OF CONTINUOUS IMPROVEMENT



ALIGNMENT WITH OTHER COMPLIANCE FRAMEWORKS

ALIGNMENT WITH OTHER COMPLIANCE FRAMEWORKS

Written at high level, thus often can be mapped to specific regulatory requirements and recognized control frameworks

- HIPAA Security Standards
- ISO
- PCI
- Cloud security

Separate assertion, description, testing, and opinion paragraph

HIPAA standards are written at a more detailed level, and map well with SOC 2 security



ALIGNMENT WITH OTHER COMPLIANCE FRAMEWORKS

Determining what report is best:

- What needs to be communicated?
- Who is requiring/intended audience?
- What are the intended uses of the report?

Avoid overly complex reports



QUESTIONS?



REQUIRED DISCLOSURE AND CIRCULAR 230 PROMINENT DISCLOSURE

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Pursuant to the rules of professional conduct set forth in Circular 230, as promulgated by the United States Department of the Treasury, nothing contained in this communication was intended or written to be used by any taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer by the Internal Revenue Service, and it cannot be used by any taxpayer for such purpose. No one, without our express prior written permission, may use or refer to any tax advice in this communication in promoting, marketing, or recommending a partnership or other entity, investment plan or arrangement to any other party.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2012 Baker Tilly Virchow Krause, LLP.

