Introduction to COSO & COBIT®

Steve Shofner, Moss Adams IT Consultant

Debra Mallette, Senior Process Consultant/Specialist, Kaiser Permanente

Core Competencies – C31

Learning Objectives

- History of Controls Frameworks
- Overview of Financial Controls & Their Use
- COSO Overview
- COBIT® Overview

HISTORY OF CONTROLS FRAMEWORKS

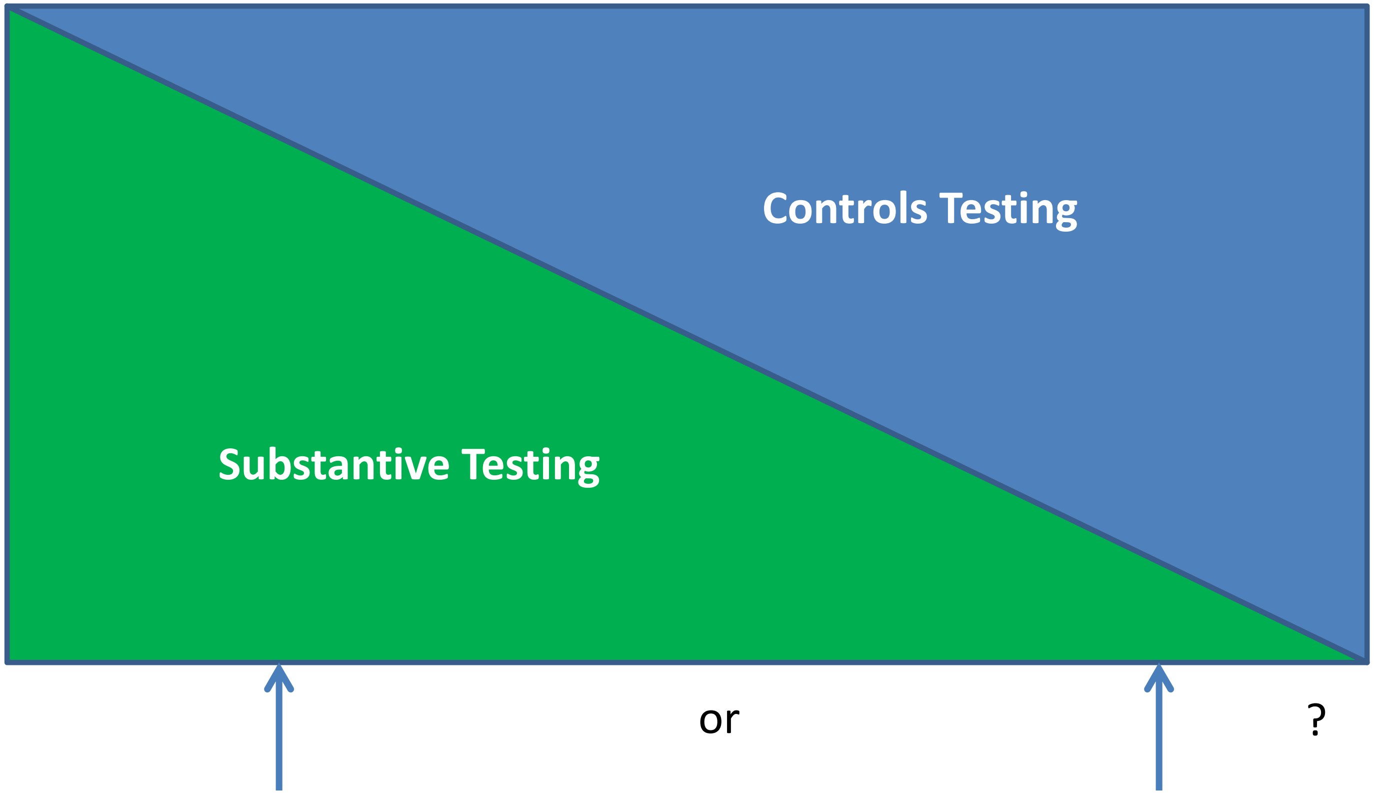
History of Controls Frameworks

- 1929: Wall Street Crash
- 1934: US Security and Exchange Commission (SEC) formed
  - Public Companies *required* to perform annual audits
- 1987: Treadway Commission, in response to corrupt mid-1970s accounting practices, retains Coopers & Lybrand to perform project to create an accounting control framework.

History of Controls Frameworks

- 1992: “Internal Control – Integrated Framework,” a four-volume report, was released by the Committee of Sponsoring Organizations (COSO)
  - Per CFO Magazine, COSO used by 82% of survey respondents

Substantive vs. Control Testing



Controls Testing

Substantive Testing

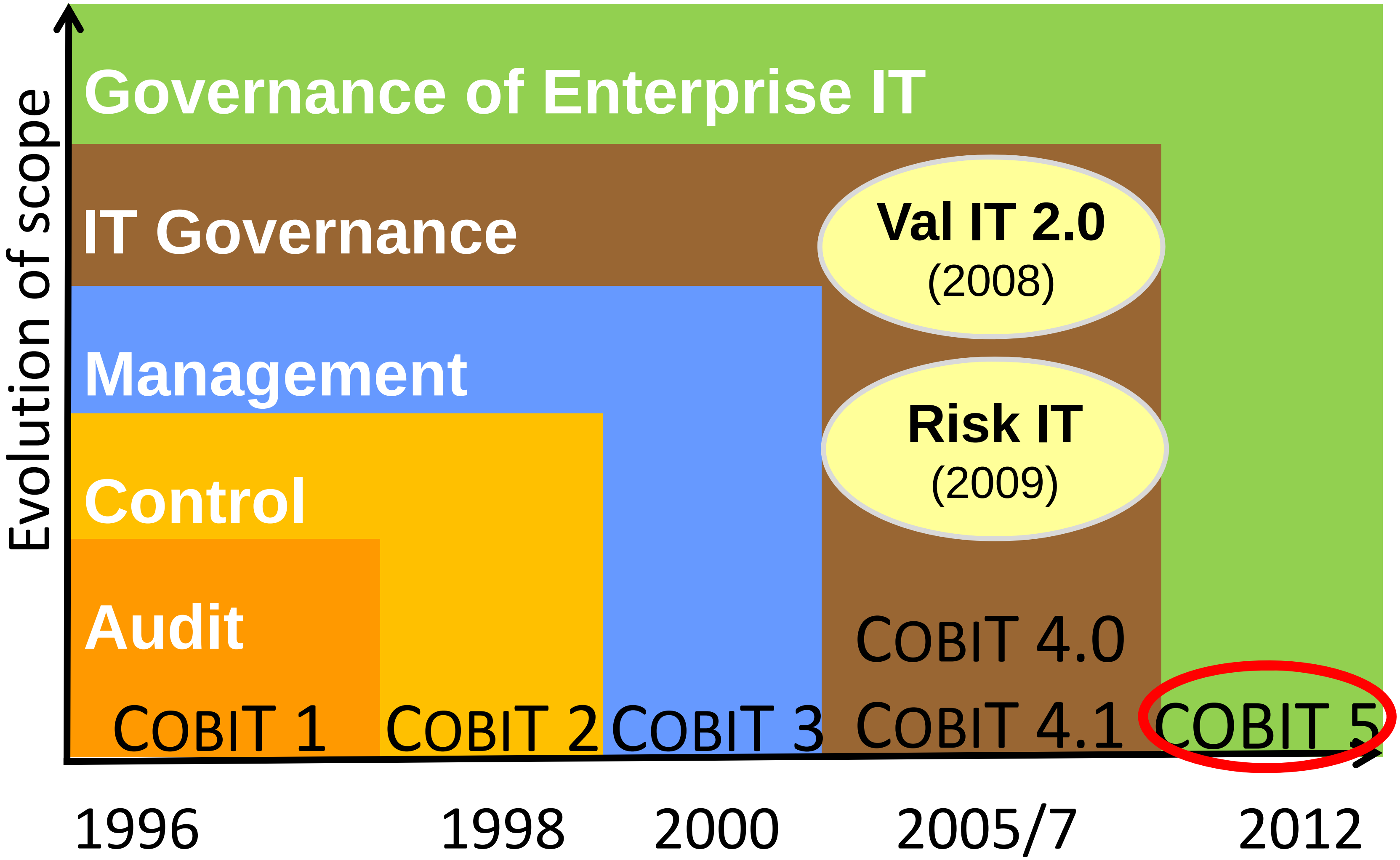
or

?

History of Controls Frameworks

- 1996: Information Technology Governance Institute (ITGI) releases the Control Objectives for Information and Related Technology (COBIT) Framework
- 2002: Sarbanes-Oxley (SOX) Act Passed, requiring companies to adopt and declare a framework used to define and assess internal controls

History of COBIT



A business framework from ISACA, at www.isaca.org/cobit

OVERVIEW OF FINANCIAL CONTROLS & THEIR USE

Controls

- CONTROL: A proactive step taken by "management" to accomplish an objective
  - Management is any employee of the firm
  - The term management is used because they are usually responsible for implementing and maintaining effective controls
- Controls attain OBJECTIVES: The purpose one's efforts or actions are intended to attain or accomplish (to address risks)
- Objectives address RISKS: The potential for loss (financial or operational)

Types Of Objectives

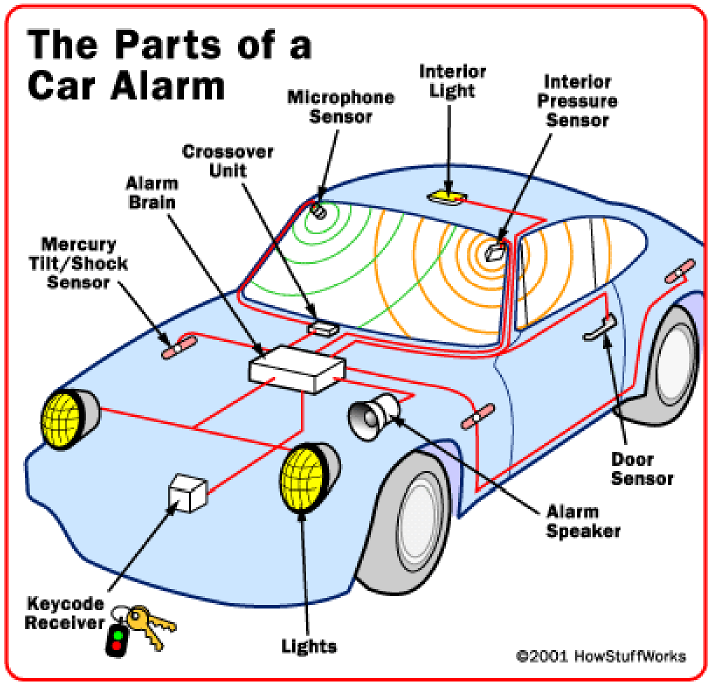
- Financial Objectives
  - Completeness
  - Accuracy
  - Validity
  - Authorization
  - Real
  - Rights & Obligations
  - Presentation & Disclosure
- IT & Operational Objectives
  - Security
  - Availability
  - Confidentiality
  - Integrity
  - Scalability
  - Reliability
  - Effectiveness
  - Efficiency

Types of Controls

- Automated Controls
  - These are programmed financial controls
  - They are *very* strong: The programmed logic will function the same way every time, as long as the logic is not changed
  - Test of one versus a statistical test of many
- Partially-Automated Controls
  - People-enabled controls
  - People rely on information from IT systems (also referred to as Electronic Evidence) for the control to function
- Manual Controls (no IT-Dependence)
  - People enable the control
  - Controls that are 100% independent of IT systems

Other Ways To Categorize Controls

- Prevent Controls
  - The locks on your car doors
- Detect Controls
  - Your car alarm
- Correct Controls
  - Your auto insurance
  - A LoJack system (a device that transmits a signal used by law enforcement to locate your stolen car)



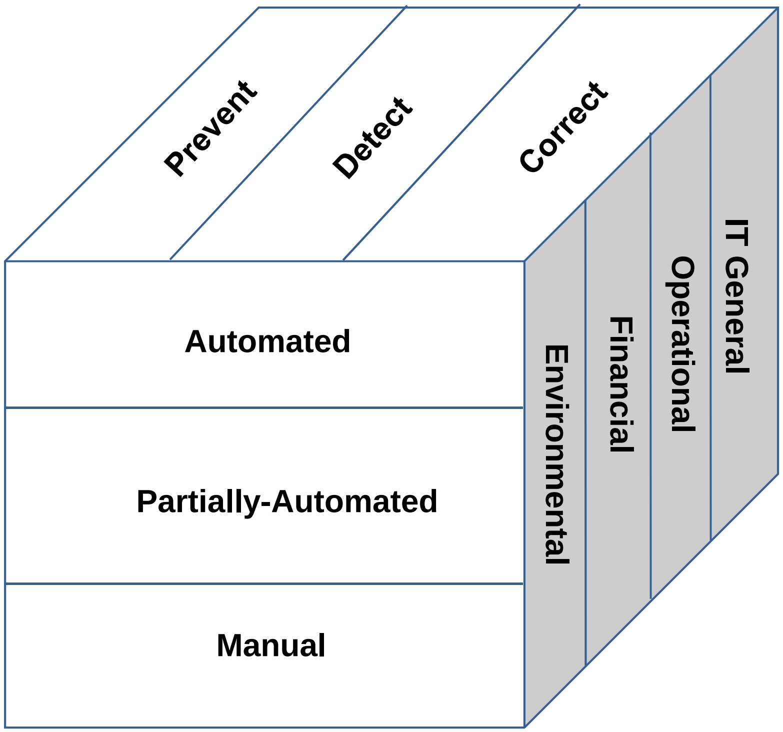
The Parts of a Car Alarm

©2001 HowStuffWorks

Yet More Ways To Categorize Controls

- Environmental Controls
  - (a.k.a. “Governance”)
- Financial Controls
- Operational Controls
- IT General Controls
  - User Administration
  - Change Management
  - IT Operations
  - Physical Environment

Controls: Multidimensional



Classifying Controls

- To ensure that only *authorized* payments are made, all checks issued require a signature.

- Accomplishes the *financial* objective, *authorized.*
- Someone *manually* signs the check
- An unsigned check *prevents* it from being cashed

- All user requests (on MAC forms) must have a supervisor’s signature *authorizing* the user’s access.

- Accomplishes the *IT General Control* objective, *authorized.*
- Someone *manually* signs the MAC form
- Unsigned MAC forms will not be processed, thereby *preventing* unauthorized access

Control Activities (Examples)

Objective	Manual Control	Automated Control
Buyers will only open Purchase Orders upon receipt of an approved Purchase Request	Buyer compares signature on Purchase Request to list of approvers	Application only allows authorized approvers to approve
Goods can only be purchased from vendors who have been pre-approved	Buyer only purchases from hardcopy list of approved vendors	PO system provides limited options in a drop-down menu, populated from a list of approved vendors.
AP Clerk prepares a “voucher package,” including: • Purchase Order • Shipping Slip • Invoice • Check (Payment) AP Clerk ties out all information across three documents to ensure completeness & accuracy	AP Clerk ties out all information across three sources	Application ties out all information across all three sources, and… (see next control)
Receiving Clerk counts all items received, ties them to shipping slip, and will only receive complete shipments	Receiving Clerk manually performs control	<none>

COSO OVERVIEW

COSO Framework

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

“Environmental Controls” or “Entity-Level Controls”

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Control Environment

- Sets the tone of an organization, influencing the control consciousness of its people
- Is the foundation for all other components of internal control
- Provides discipline and structure
- Factors include:
  - The integrity, ethical values and competence of the entity's people;
  - Management's philosophy and operating style;
  - The way management assigns authority and responsibility, and organizes and develops its people;
  - The attention and direction provided by the board of directors.

Risk Assessment

- Evaluates risks from external and internal sources, through the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed
- Economic, industry, regulatory and operating conditions will continue to change

Information and Communication

- Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities.
- “Information systems” (not necessarily technology) produce reports containing operational, financial and compliance-related information that make it possible to run and control the business.
- Information needs to flow up, down, and across the organization

Monitoring

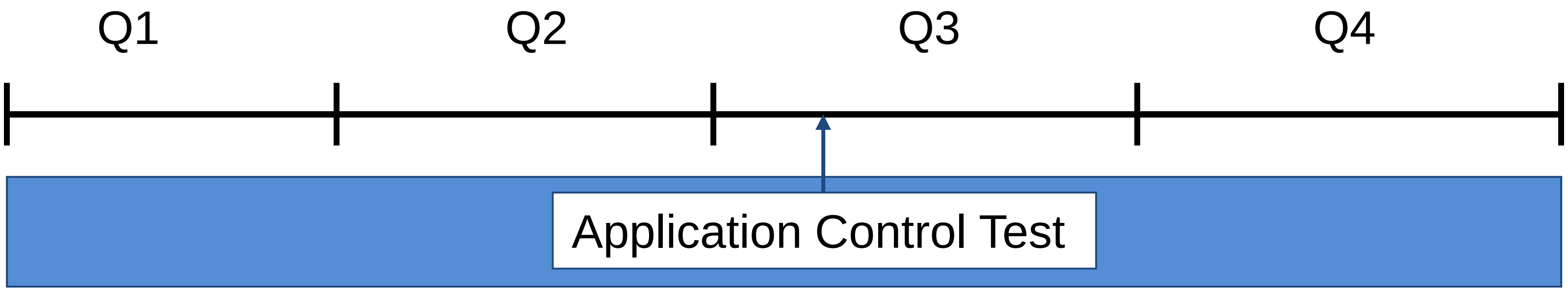
- Monitoring of internal control effectiveness
- Accomplished through ongoing monitoring activities, separate evaluations or a combination of the two

Control Activities

- COSO Financial Assertions
  - Existence
  - Occurrence
  - Completeness
  - Valuation
  - Rights & Obligations
  - Presentation & Disclosure
  - Reasonableness

WHY COSO (ALONE) IS NOT ENOUGH

Expanding Coverage Beyond ‘A Point In Time”


Q1

Q2

Q3

Q4

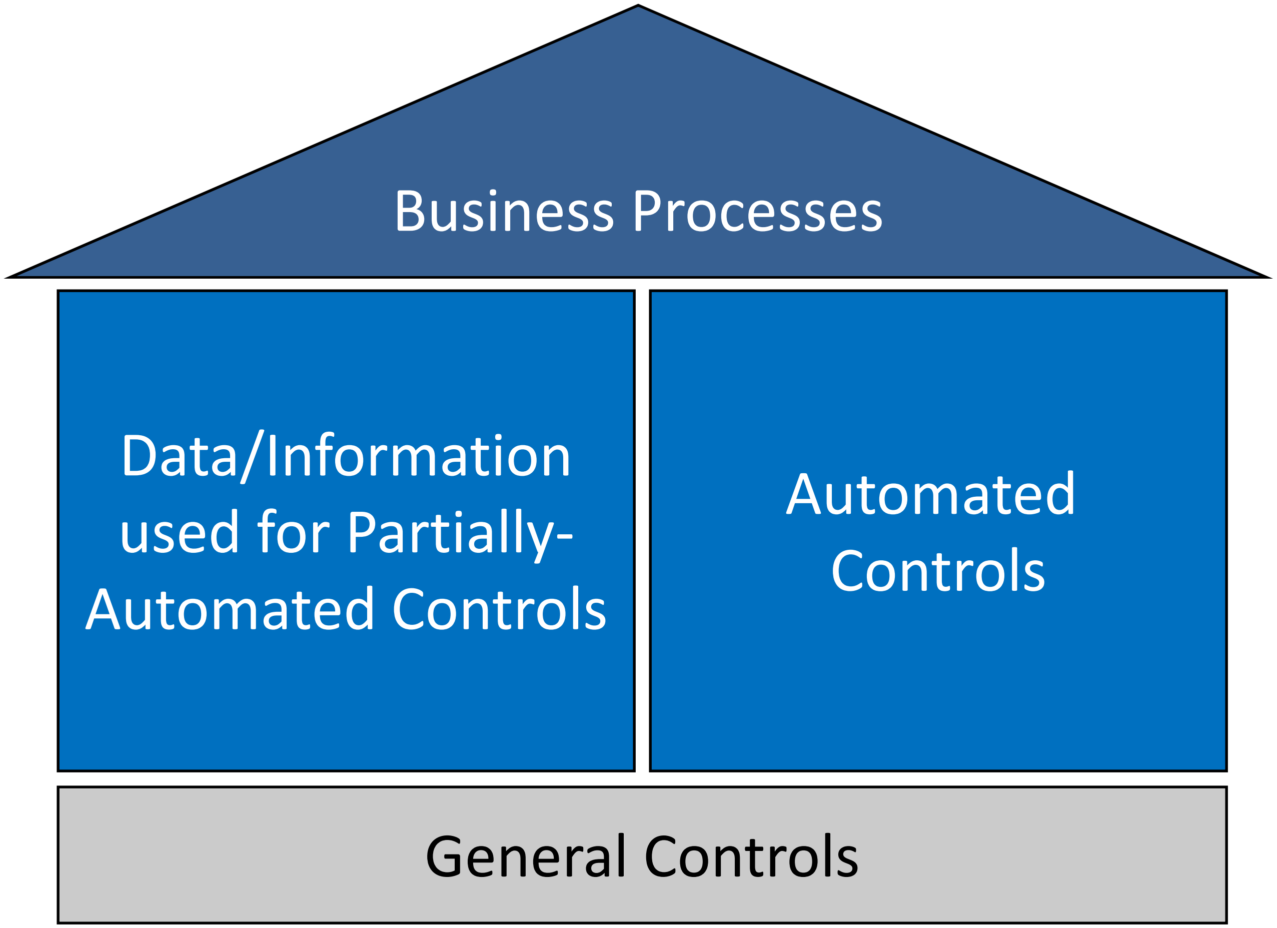
Application Control Test

IT General Controls

IT General Controls

- ★Change Management
- ★User Administration
- IT Operations
- Physical Environment

Effective General Controls



Business Processes

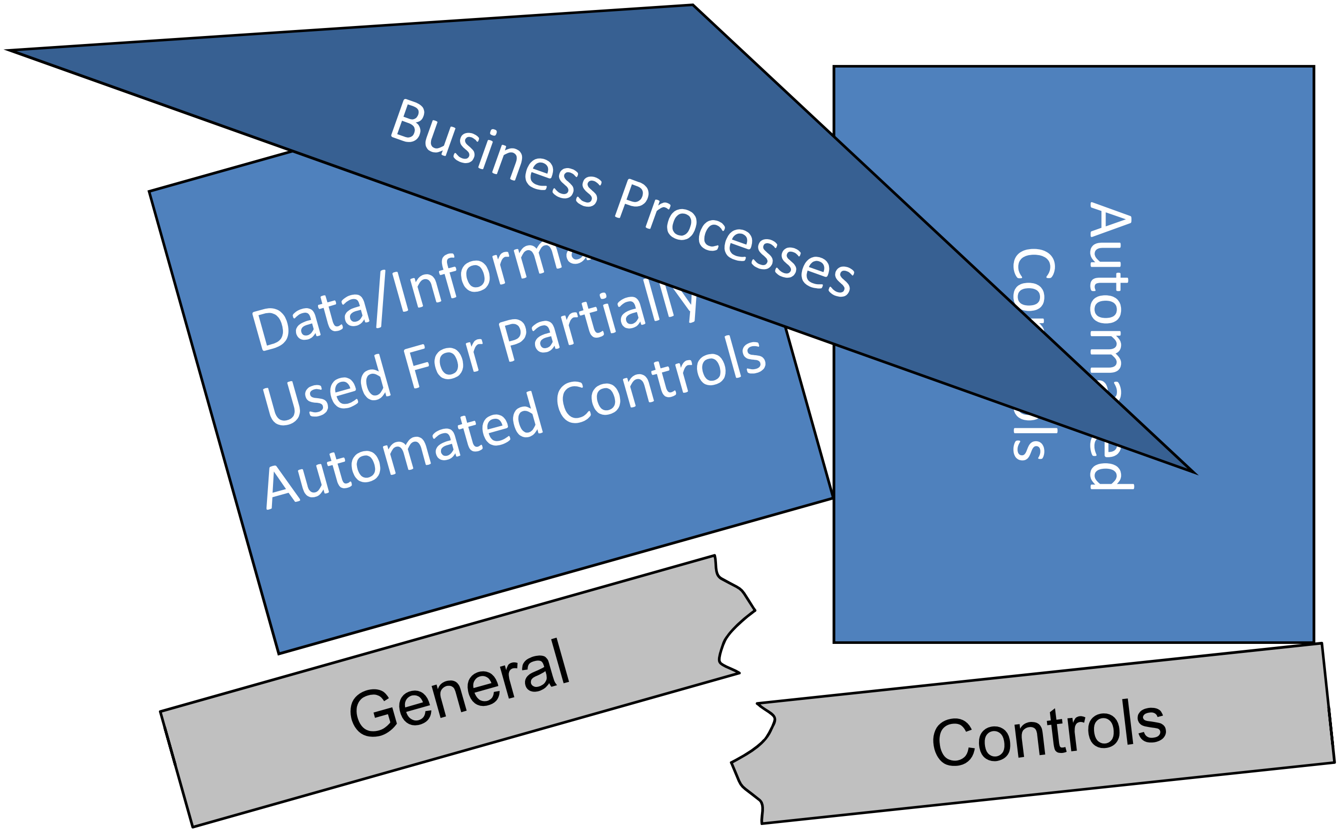
Data/Information used for Partially-Automated Controls

Automated Controls

General Controls

Without Effective General Controls

Potential For Significant Problems Exists



COBIT OVERVIEW

COBIT®

- The Framework formerly known as "Control Objectives for Information Technology"
- Intellectual Property of ISACA® and the IT Governance Institute

ISACA Download links for references:

- COBIT® 5.0 An Introduction
- COBIT® 4.1
- IT Assurance Guide: Using COBIT
- IT Control Objectives For Sarbanes-Oxley The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition ©2006 ITGI