Developing Effective Controls for the 21st Century

BOB SCOTT, CPA

Objectives

- Encourage participants to take a fresh look at their organization's control environment
- Discuss how specific trends in state & local governments may have rendered previous controls ineffective and new controls that can be used for:
  - Outsourcing of all types:
    - Software as a service
    - Remote hosting
    - Third Party administrators for self-insured healthcare plans
    - Pension Plan administration
    - Billing and collection of specific revenues
  - Growing use of purchasing cards
  - Electronic invoicing and payment
  - Paperless operations
- Develop strategies for addressing paperless applications including general controls over technology

Are Your Internal Controls Relics of a By Gone Era?

How Many of You (or Your Clients) …

Still have a policy for paying only on the original invoice?

Have not developed effective controls for purchasing cards even though it is a large and growing percentage of your total spend?

Do not consider general controls over IT a finance responsibility?

Require manual signatures for large checks but not for ACH's or wires of the same amount?

Have not obtained SOC reports for all outsourced financial activity?

Do not reconcile chargebacks on credit cards?

Consider prevention of cyber threats an IT function?

Do not consider data mining a integral part of internal controls?

Bad Things Can Happen to Good Governments

Recent headlines:

Eight hundred City Employee's W-2s Exposed in Phishing Scam

E-mails reveal how city and regional mobility authority were scammed out of $3.2 million

School District secretary racks up $100,000 in personal purchases on purchasing card

City's Tax billing firm uses the wrong rate on tax bills

Employee of Not for Profit embezzles $350,000 through credit card refunds

Tax refund scam may have cost County $350,000-On-line transparency blamed.

While the concepts are relatively simple…

1992 COSO Cube

We Often Forget…

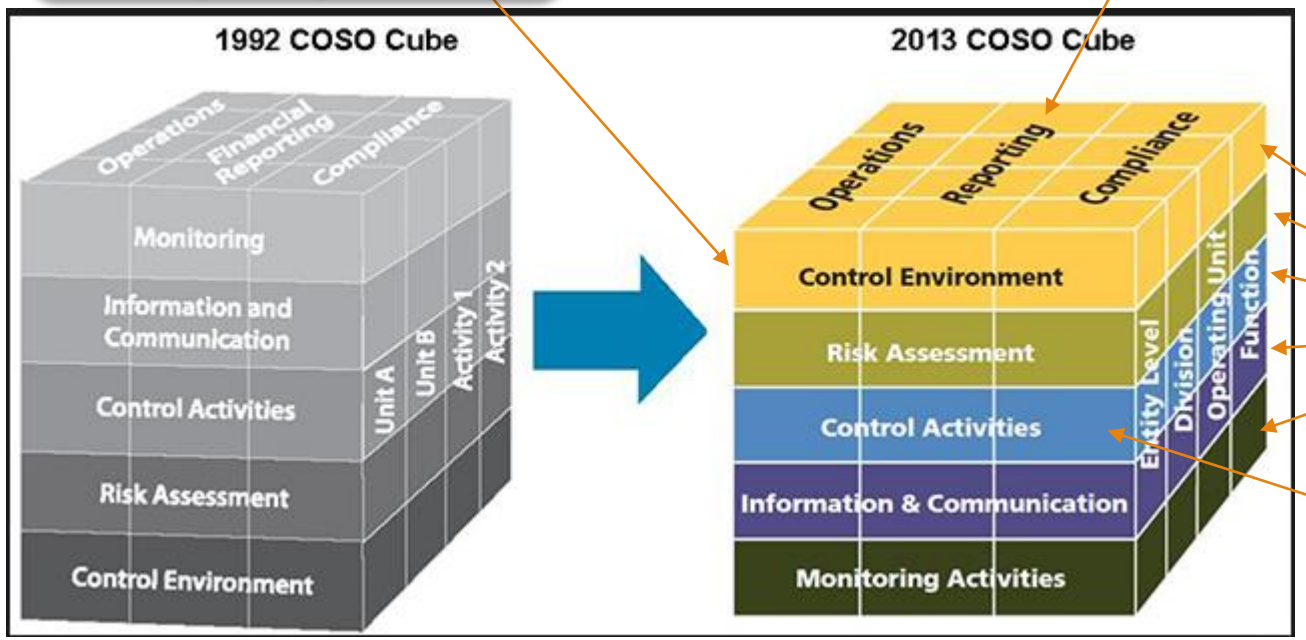
- Systems change
- Technology evolves
- People leave and retire
- People forget
- New hires need to be told
- Threats are world wide
- Criminals adapt

That we are never done!

COSO Changes

Importance of control environment and "tone at top" emphasized

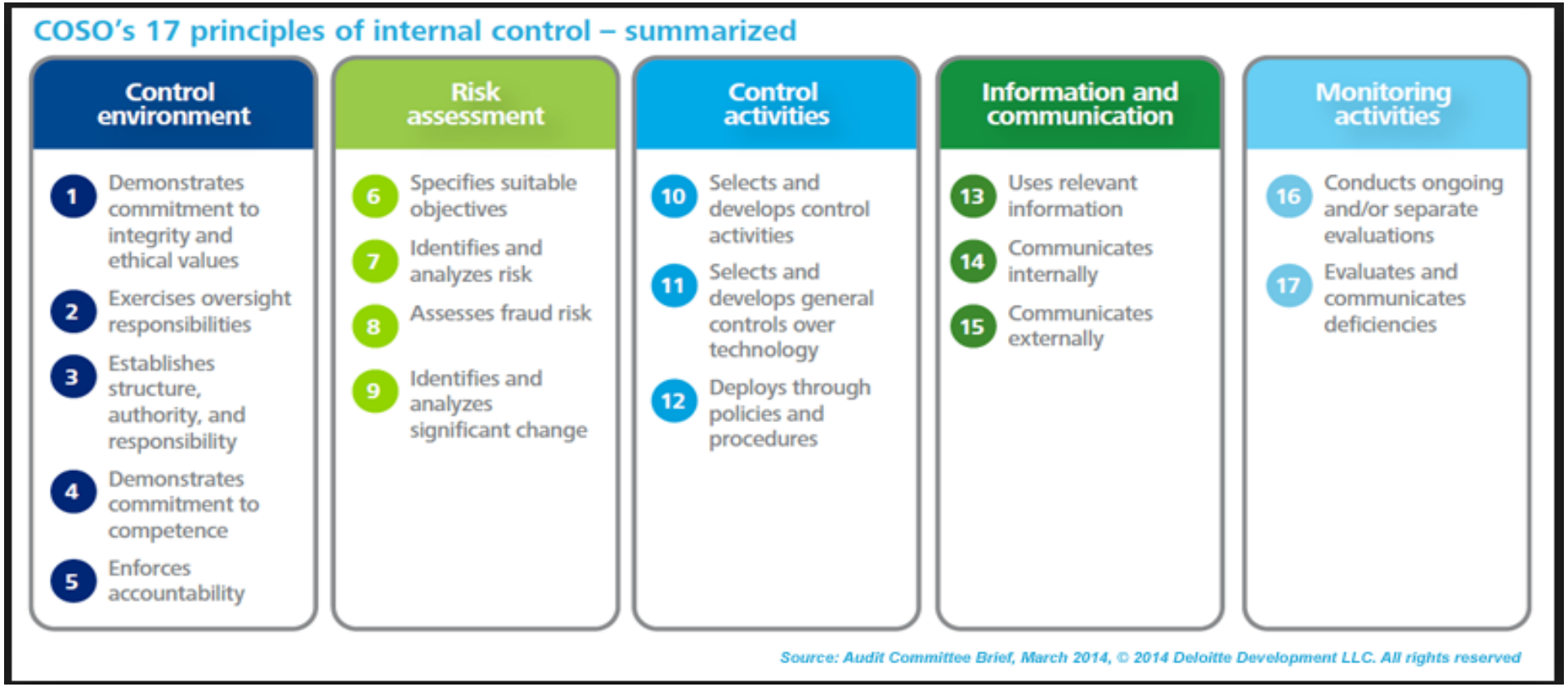
Reporting Broadened



Principles added for each element

Importance of general controls over technology singled out

COSO Principles



Outsourcing

Government Outsourcing

Government outsourcing of finance functions is an accelerating trend:

- Payroll
- Accounts Payable
- Software as a service
- Remote processing/cloud computing
- Pensions
- Third-party administration of self-insured health plans
- Billing and collection of specific revenues

You can outsource the task but not the responsibility and regardless of what has been outsourced the government is ultimately responsible for its financial operations and its financial statements

Internal Control Strategies for Outsourcing

- **Procurement**
  - Specifications
  - Benchmarking
  - Reference Checks
  - SOC 1 Type 2 Reporting
- **Strong Contracts**
  - Compliance Standards
  - Remedies/Enforceability
  - Insurance
- **Monitoring**
  - Performance
  - Financial
  - SOC 1 Type 2 

History of Service Organization Reports

- SAS 55-1988 “Consideration of the Internal Control Structure in a Financial Statement Audit” required auditors to assess internal controls for outsourced operations
- Service organizations were inundated with information requests from their client’s auditors leading to the issuance of SAS 70 Service Organizations in 1992
- Originally used primarily for remote IT processing, applications are expanding rapidly
- SLGEP use of SOC reports to address GASB 68 implementation issues is the latest example
- SOC reports can also be used Investment Managers, Third Party Administrators, Revenue billing and collection and a variety of other outsourced financial services

History of Service Organization Reports

- SSAE 16 (AT 801) became effective in June 2011 utilizing AICPA's attest standards.
- SSAE 16 more closely resembles its international equivalent ISAE 3402
- Unlike SAS 70, SSAE 16 now requires the service organization to provide written assertions regarding the "system" of controls
- SSAE 18 was the AICPA's comprehensive effort to restate all existing SSAEs 10-17 as part of the clarity initiative. Only Chapter 7 of SSAE 10 (Management Discussion & Analysis) and SSAE 15 (Examination of Internal Controls). All affected attest standards will now be referred to as AT-C.
- Service Organization Controls is now referred to as AT-C 801. In addition to use of the clarified language, service organizations must monitor the controls of subservice organizations.
- AT-C 801 is effective for SOC report opinions dated on or after May 1, 2017.

Service Organization Control Reports

Categories of SOC reports will be a 1 or 2 based on the COSO definition of the three objectives of all organizations

- Financial Reporting (1)
- Compliance (2)
- Operations

In addition, SOC reports can be either Type 1 or 2

- **Type I** includes the service auditor's opinion on the fairness of the presentation of the service organization's description of controls that had been placed in operation and the suitability of the design of the controls to achieve the specified control objectives **as of a point in time.**
- **Type II** starts with the information contained in a Type I service auditor's report and adds to it the service auditor's opinion on whether those controls were operating effectively during a specified period of time.

Characteristics of SOC Reports

A SOC 1 Type 2 report will be reporting on a service organizations internal controls over the generation of information included by a third party in its financial statements for a specified period of time (i.e. one year)

- To issue the report, the service auditor will need to have performed testing throughout the time period specified.
- By definition testing cannot be done after the period has ended and as a result SOC 1 Type 2 reports are typically issued shortly after the end of time period (i.e. four to six weeks)
- With complex organizations processing millions of transactions per year, the service auditor will invariably have some findings (often called exceptions) that they will report and management will furnish a response
- Exceptions do not necessarily mean that the system of controls are not working effectively and can occur without the service auditor modifying their report
- Users of SOC reports should note the frequency of exceptions including whether the same exception is noted in multiple years to consider possible impacts on financial information

Purchasing Cards

LOVE THEM OR HATE THEM, YOU MUST LEARN TO DEAL WITH THEM.

Purchasing Cards

ADVANTAGES

Allows field personnel to obtain parts and supplies quickly

Reduces the need for large parts inventories reducing shrinkage and obsolescence

Eliminates the need for petty cash funds

Provides a 1 to 1 accountability to the card holder

Individual cards can have different spending limits and purchasing restrictions

Eliminates return fraud

Often provides for cash back

Can reduce workload of purchasing and accounts payable

Allows for easy on-line monitoring

DISADVANTAGES

Does not allow for approval in advance

Death of the 3-Way match-Invoice to Purchase Order to Receiver

Does not allow for segregation of duties

Can be a temptation to employees to use for personal purchases

Can be used to circumvent normal purchasing controls

Makes it easy for supervisors to not be involved in purchases

Can be embarrassing to explain certain purchases to reporters

Controlling Purchasing Cards

Purchasing Cards merit specific policies and procedures. Start with the Cube:

Tone at the Top, Clear strong policy signed by City Manager

Purchasing Manager given clear authority to administer program, set card limits based on risk and need and monitor activity on-line

Each department responsible for their department's cards and can have cards revoked if abuses persist

Tax ID is on the card, Picture of CH on the card so difficult to use by mistake, expectations for proper use clearly in policy.

An entire month for every department is audited at least once per year with report going to ACM and City Manager

Electronic Invoicing and Payment


So, is the the original, the first time I print off the PDF invoice ?

Payment Controls Must Evolve

OLD

Paying on the original invoice provided assurance as to authenticity and avoided duplicate payments

Mailed checks to physical addresses were difficult to intercept or divert

Positive pay provided a final opportunity to approve payment before it cleared the bank

NEW

With PDF invoices being incredibly easy to generate and look authentic greater emphasis should be placed on:

- Vendor File controls including existence, completeness, ability to modify, address verifications
- Completeness of the invoice including invoice #
- Application controls should check for duplicate invoice #s

Data mining should be a second line of defense searching for duplicate payments, vendor/ employee or vendor/vendor relationships

Disbursement review and approval should be identical or stronger than traditional checks

Paperless Environments & General Controls Over Technology

Application vs. General Controls

Application controls are simply the automated version of what we have always done:

TRADITONAL	AUTOMATED
Locked filing cabinet	User ID and Password
Physical segregation of duties	Password hierarchies that segregate duties through screen access
Illegible initials on paper invoices	Automated workflow approvals
Manual review, paper forms, footing of inputs	Input controls, automatic population of certain fields, edit checks
Using reports to monitor and control budget	System controls that refuse to process transactions if budget authorization is inadequate.

Application vs. General Controls

General controls represents what happens in the IT department to keep:

- computers connected.
- data bases humming.
- applications running and reliable.
- response times fast.
- information trustworthy.
- hackers at bay.

In addition, when bad things happen, general controls ensure rapid recovery and backup.

Importance of General Controls

COSO 2013 Principle 11 states: **Selects and develops general controls over technology.**

To single out general controls over IT from all other control activities signifies their importance to the entire organization. Expressed another way:

"If top management does not know and control what happens in the IT department, then they are deluding themselves regarding the effectiveness of their entire system of internal controls"

IT General Controls

ADMINISTRATIVE CONTROLS

- Alignment with strategic goals
- Policies
- Risk assessment
- Administer Security program
- Hiring and screening
- User access process (new user, terminations, changes)
- Access authorization
- License Management
- Change Log monitoring and reconciliation
- Contingency planning / business continuation/ data backup
- Budgeting for maintenance, upgrade and replacement aka-sustainability

PHYSICAL CONTROLS

- Facility access controls
- Workstation controls
- Device and media controls
- Facility maintenance
- UPS
- Back up facilities

IT General Controls

TECHNICAL CONTROLS

- Authentication controls (password, etc.)
- Access controls (operating system, application)
- Audit controls (monitoring and testing)
- Encryption controls
- Architecture controls (firewalls, VPN, etc.)
- Configuration controls

VENDOR MANAGEMENT CONTROLS

- Contract language (confidentiality, ownership, regulatory and legal compliance)
- Performance monitoring and enforcement
- Controls audit, SOC/AT-C 801
- Vendor access control
- Vendor copies of confidential information

IT General Controls

SECURITY CONTROLS

- Perform an Information Security Risk Assessment
- Security incident response
- Security awareness & training-every employee who has access to a computer should consider themselves a security team member
- Threat monitoring
- Regularly test or monitor effectiveness of controls
- Have outside party perform penetration testing
- Periodically evaluate and adjust the Information Security Program

Making Every Employee an IT Security Officer

- Internet based tutorials for all employees is available at very reasonable costs-often starting at less than $10 per employee per year
- Services can range from simple tutorials, to creating baselines and conducting Phishing campaigns to assess and reduce employee gullibility over time
- Some providers:

www.securitymentor.com

www.knowbe4.com

www.mediapro.com

www.wombatsecurity.com

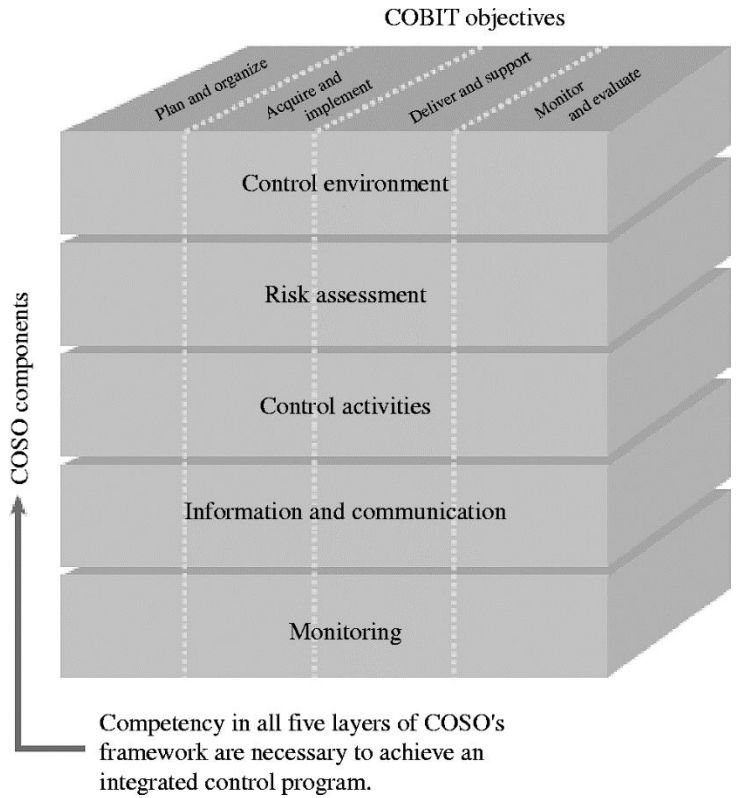
At the Risk of Appearing Geekish meet COSOs Younger Sibling, COBIT

General internal control - COSO

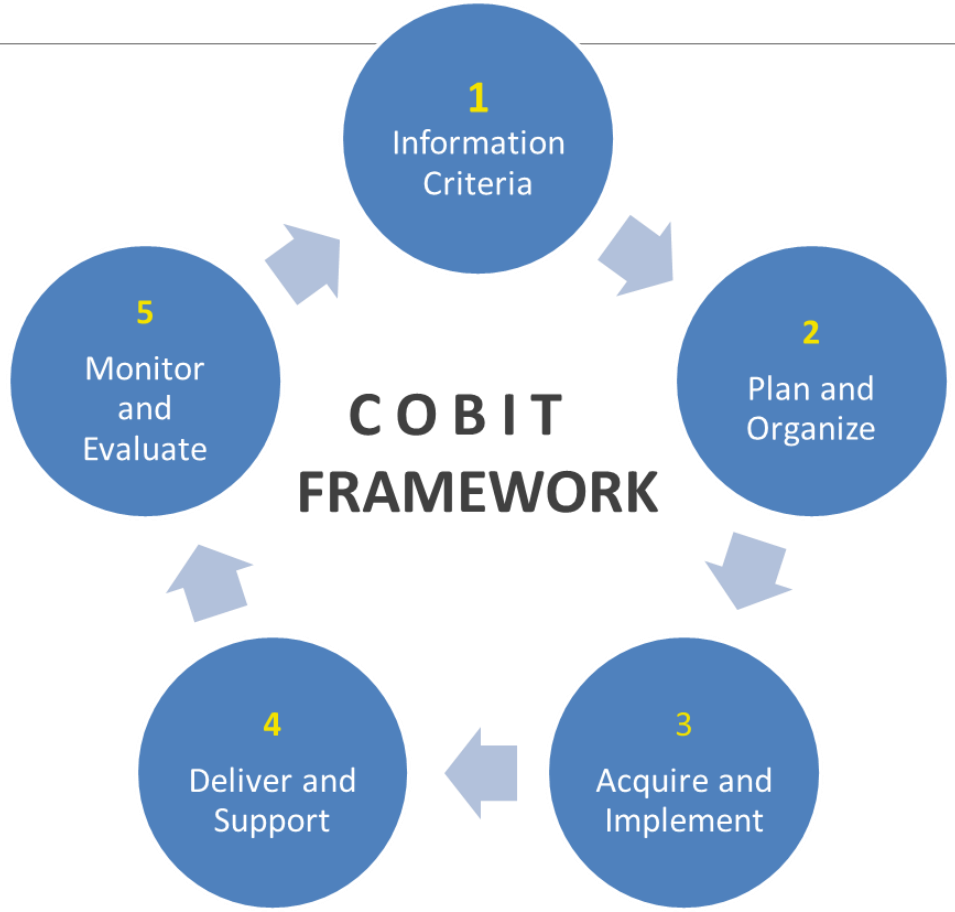
Information technology internal control – COBIT

Control OBjectives for Information & related Technology (COBIT)

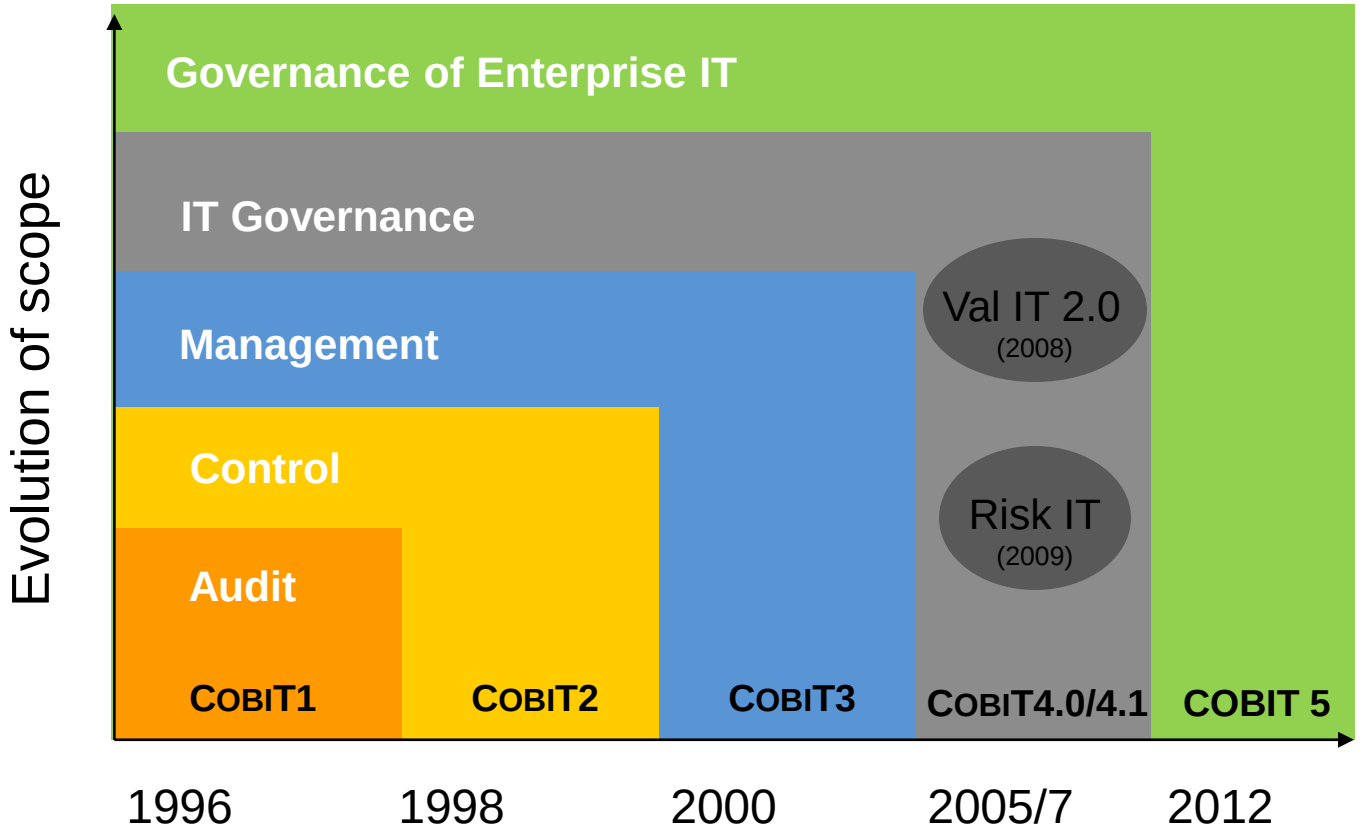
Developed by ISACA - Information Systems Audit & Control Association



COBIT *framework*



COBIT *evolution*



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

This and That

Credit Cards-contrary to popular belief, credit cards can facilitate money leaving the building just as easily as coming in. Reconcile charge-backs and refunds daily and always trace back to the original transactions.

Documentation –with an aging workforce and normal turnover, up to date documentation of system procedures and controls is vital. Unfortunately, most us would rather have a tooth pulled than update our procedures manual.

Consider:

1) Hiring a contract technical writer to interview staff and put the manuals together for you.

2) Have staff put together "You Tube" style how to videos for key processes. They can interject personality and (appropriate) humor and may even find that they enjoy it.

Final Thought

Remember the Hawthorne Effect

Aerial view of the Hawthorne Works, ca. 1925.

So what does a 90 year old management study have to do with 21st century Internal Controls?

Hawthorne Effect

Most things improve when management is involved and observing