Sarbanes-Oxley:

A Focus on IT Controls

Company Case Study - Viacom Inc.

IT General Controls -
Sustaining Compliance Efforts

Anthony Noble

VP, IT Internal Audit

Today's Agenda

- Introduction
- Viacom Methodology
  - Viacom SOX Background
  - Year 1 Methods
  - Lessons Learned
- Current Approach
  - Methodology
  - Key IT SOX 404 Controls Going Forward
  - Sustainability

ISACA
Serving IT Governance Professionals

Introduction

- What
  - Objective: To share SOX experiences (successes and issues) and to discuss a methodology to enhance the process for your IT General Controls compliance efforts going forward.
- Why
  - Learn from our growth.
  - Make ongoing process more efficient for everyone.
- Caveats
  - Everyone will have a unique solution for SOX or J-SOX. There is no one perfect way.
  - Not all good controls need to be tested for compliance efforts.
  - Is from my personal viewpoint and not that of Viacom Inc.

SOX Big Picture - Risks

- Annual Exposure (Risk)
  - Defined as the potential probability and magnitude of an error in the financial statements.
- Risk is the key driver for control objectives and controls
- Value
  - Annualized Risk to Company - Annual Cost of Control = Value
- How Much Risk?
  - SOX risk of failure to pass in Year 1 perceived as very large.
  - Hence almost unlimited budget to comply as easy to justify value.
- Year 2 + SOX risk tolerance higher

IT Entity/Company Level Controls

- Tone at The Top
  - Policy and procedures that communicate management's aims and directives
    - Security policy and procedures
    - Software Development Life Cycle (SDLC) standards
    - IT Human Resources policy and procedures
    - Record/data retention requirements

Application (Embedded) Controls

- **Integrated with process documentation and must be developed with the business units input**
- **Inherent embedded controls**
  - Integrated balancing/posting
  - Real time online data
  - Log files (transaction, program change and/or configuration history)
- **Configurable controls**
  - Edit checks and tolerances
  - Pre-defined master data
  - Forced reason codes

Application (Embedded) Controls

- **Reporting (Hybrid) controls**
  - Standard reports
  - Audit reports
- **Logical Security controls**
  - User access to programs, transactions, tables, fields
  - Tools for the development and maintenance of user access rights
  - Parameters for general security settings, such as password rules, time out intervals, lock-outs, etc.
  - Tools for detection and prevention of unauthorized access

General Computer Controls

- All application controls are dependent on general controls.
- IT General Controls can fall into six broad categories:
  - IT Strategy
  - Program Development & Implementation
  - Program Change Control
  - Computer Operations
  - Access Controls
  - Security Configuration

Viacom Year 1 Metrics

Locations	❖ 12 decentralized business units across 11 locations in scope
People	❖ 700 people directly involved in SOX 404 ❖ 1,100+ people passed CBT training on internal controls
Significant Processes	❖ 116 business processes in scope ❖ 75 applications in scope
Key Controls	❖ 1,560 Business Process controls – of which 93% were manual ❖ 540 IT General Controls in addition to BP Controls
Financial Statement Coverage	❖ 90% asset coverage ❖ 77% revenue coverage
Tool	❖ SOX Express used to capture SOX documentation and for reporting

ISACA®
Serving IT Governance Professionals

Year 1 - IT General Controls

- **Used as a basis for selecting IT general controls the ITGI Document "IT Controls Objectives for Sarbanes-Oxley" 1st Edition.**
  - **Viacom Internal Audit defined General Control Objectives (COs) over:**
    - Program Development & Implementation
    - Program Change Control
    - Computer Operations
    - Access Controls
  - **Then met with External Audit and IT to agree COs and included them where External Audit insisted due to Catch-22.**
  - **Leveraged financial groups risk assessment in selecting applications for testing.**

ISACA
Serving IT Governance Professionals

Year 1 Approach - Information Technology

- Eventually, Viacom Management, Internal Audit and our External Auditors agreed to a total of 45 key risks/control objectives for Viacom's IT general controls for high priority business areas at the:
  - Company Level
  - Data Center Level
  - Application Level
- IT Internal Audit heavily involved acting on behalf of CIOs with Corporate Finance and External Audit.
- External Audit approached from a "Zero Risk" attitude.
- Developed pilot control procedures at one division and rolled out to other divisions as a template for efficiency once approved by External Audit.

Common Problems to Avoid in Year 1

- Testing
  - Tests were not adequately proving the effectiveness of the control.
  - Testing was not adequately documented .
  - Defined similar risks resulting in similar controls causing duplicated testing.
  - Did not educate both the control owners & testers on their responsibilities.
  - Testers and reviewers needed to document and maintain specific details of their testing so the test could be independently reviewed and re-performed or relied on by External Auditors.
  - Reviewers did not review test results and supporting documentation to confirm the tester correctly assessed the results and root cause of any exceptions.

Common Problems to Avoid Year 1

- Controls
  - Control descriptions not captured and documented clearly.
  - Need accurate identification of control frequency, which directly impacts sample sizes.
- Other
  - Controls themselves not performed adequately; additional training was needed to ensure not just signing off without review.
  - Defined too many levels of review for controls.
  - Need to define repeatable provable testing for embedded controls.
  - Documentation reviews and walkthroughs with External Auditors should take place early in the year.
  - Avoid waiting until year-end to test annual controls (i.e., embedded controls) in case of failures.

Common Problems to Avoid in Year 1

- Defined too many key controls in IT.
- Test performers had various experience, backgrounds and often no formal audit training. As such:
  - Training should have been directly focused on helping the individuals performing testing to understand if a control is not working.
  - Testers needed to have a sufficient knowledge of the area they are evaluating in order to determine whether a control operated effectively.
- Controls were not structured as part of an individual's day-to-day job responsibilities and were additional actions that needed to be undertaken for SOX compliance.
- Controls were not designed in many cases by the staff that had to perform them and so were not understood or adequate.

New Viacom

Key Achievements for New Viacom

- Addressed & cleared IT access control deficiencies:
  - Identified and tested mitigating business controls where security parameters (i.e., expiration, minimum length) could not be systematically enforced in older applications to comply with the Viacom written security policy.
  - Identified and tested mitigating business controls where transaction logging could not be implemented to monitor the actions of DBAs, application or system programmers.
  - Created an automated system to notify system administrators when staff joined or left the company to ensure system access is granted or removed.

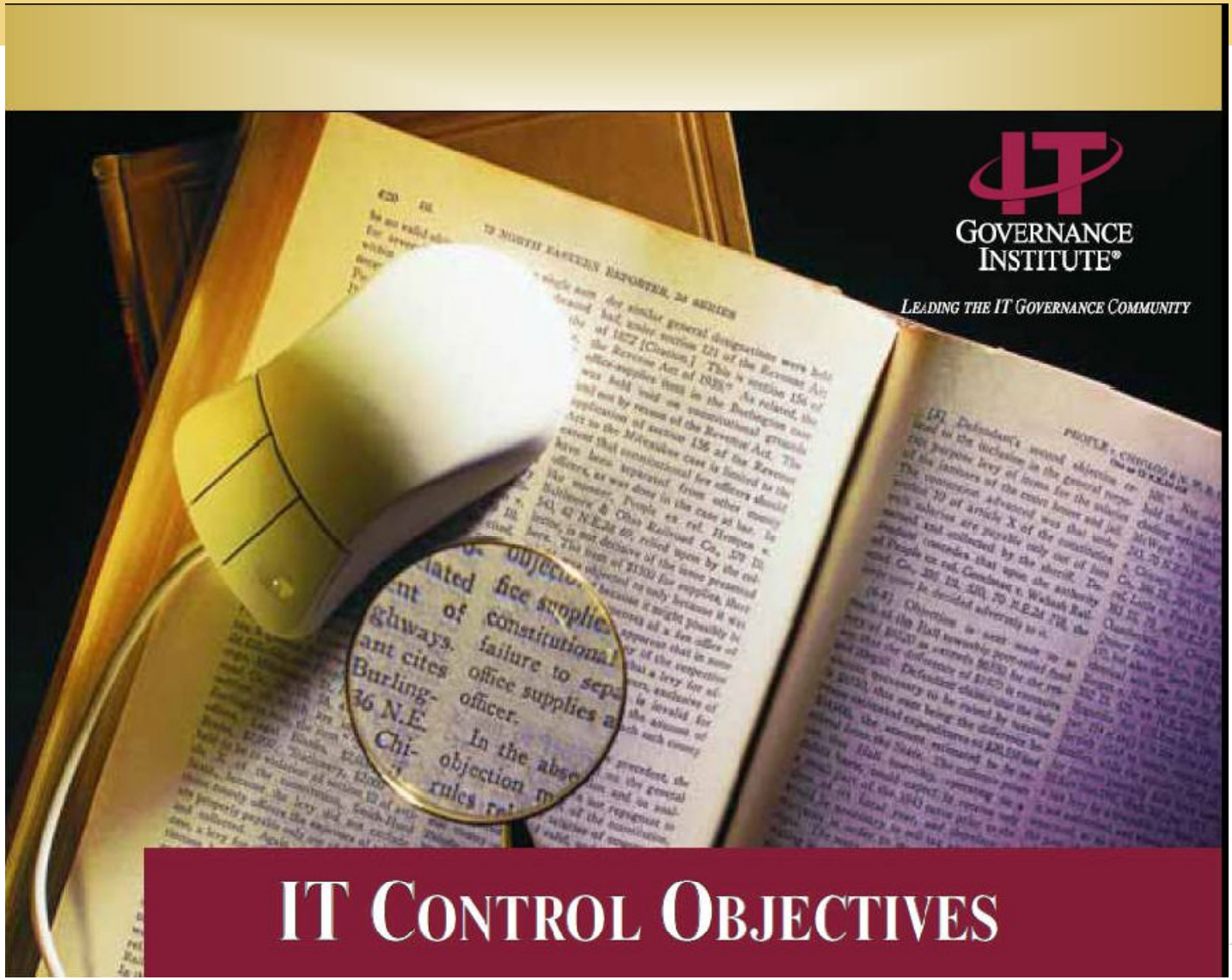
Key Achievements for New Viacom

- Addressed the new SEC guidance by implementing a "Top-Down" risk-based methodology as specified by the SEC.
  - "For purposes of the assessment management only need to test those IT general controls that are necessary for the proper and consistent operation of other controls designed to adequately mitigate financial reporting risks."
  - "Management should consider program development, program changes, computer operations, and access to data and programs."
  - "Specifically it is unnecessary to evaluate controls that primarily relate to the efficiency and effectiveness of a company's operations, but which are not relevant to financial reporting risks."

Source: www.sec.gov

ISACA
Serving IT Governance Professionals

Viacom used ISACA's Booklet



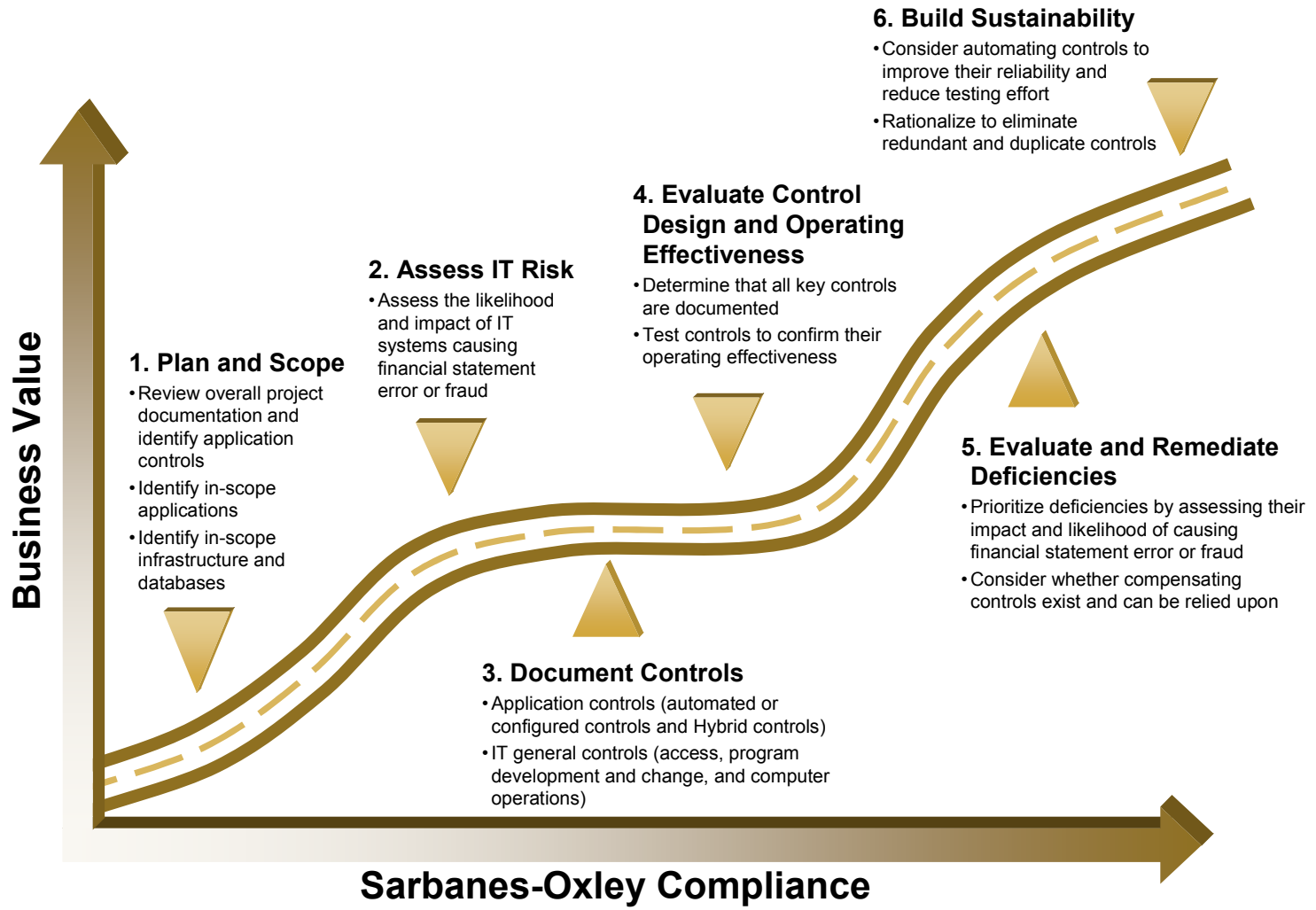
ISACA®
Serving IT Governance Professionals

Key Achievements for New Viacom

- Used as a basis for selecting key IT general controls the ITGI Document "IT Controls Objectives for Sarbanes-Oxley" 2nd Edition.
  - Focused on the controls flagged in the document as "most relevant."
  - Removed controls we considered to be designed for efficiency and effectiveness, for example, IT Job Descriptions, Problem Management and Physical Security.
  - Leveraged financial group's "Top-Down" risk assessment in selecting applications.

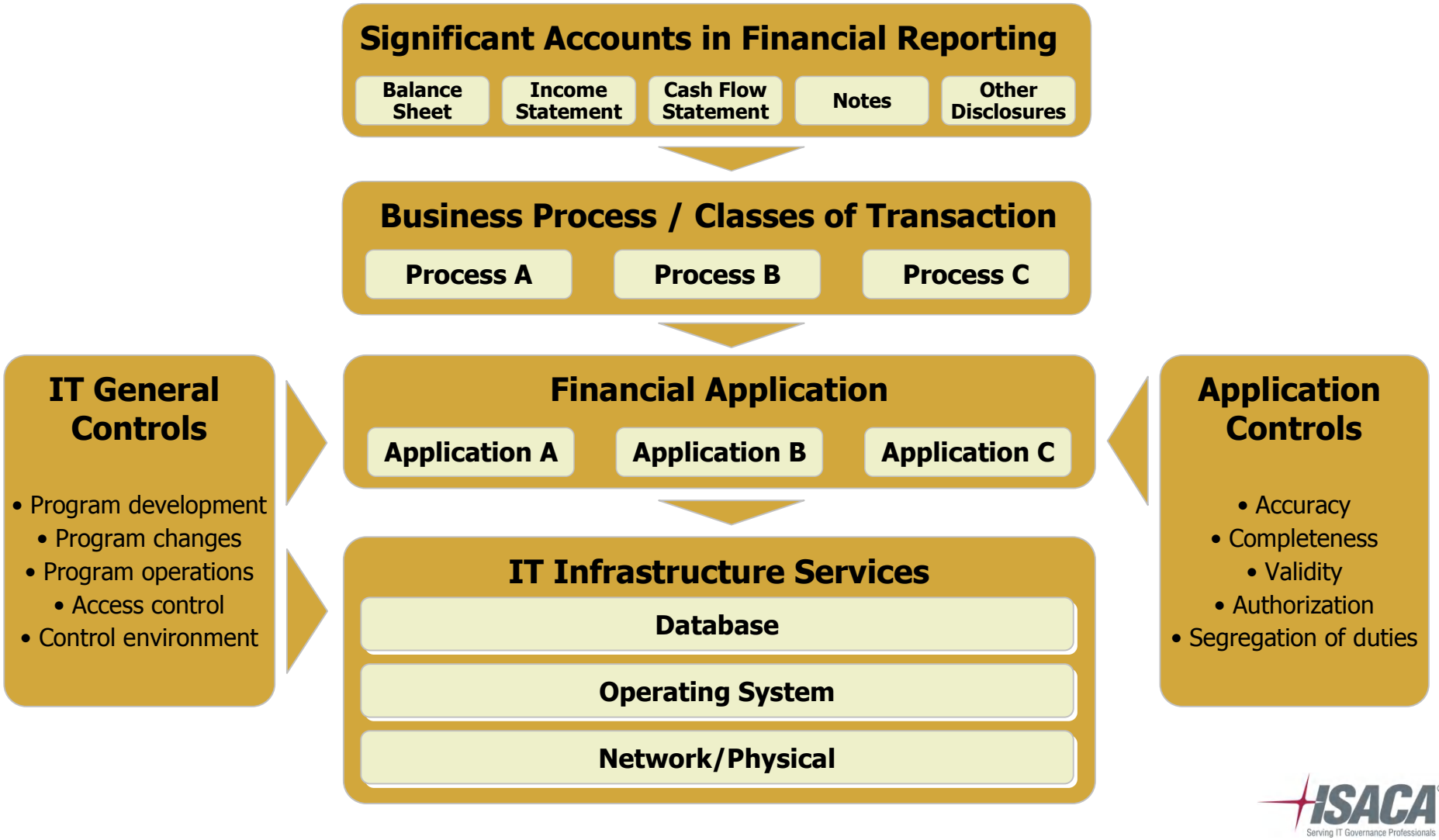
ISACA
Serving IT Governance Professionals

SOX Compliance Methodology



ISACA
Serving IT Governance Professionals

Top Down Scoping



ISACA
Serving IT Governance Professionals

Identified our “in-scope” accounts

- The first step was to assess inherent risks by account to drive scoping
- Qualitative Factors:
  - Degree of judgment / estimation
  - Routine vs. non routine
  - Likelihood and impact of misstatement
  - Fraud considerations
- Quantitative Factors
  - Materiality (5% pre tax operating income)

ISACA
Serving IT Governance Professionals

Next Steps in Process: Control Risk Assessment

- The next step was to link the in-scope accounts to their related business cycles
- Why? Because this enabled us to determine what the control risks were

Financial Example:

For accounts receivable – trade, the pertinent business cycle is the revenue and receivables cycle

Key IT Risks Identified

- Unauthorized or excessive access by users or security administrators
- Security settings are not consistent with policy
- Programmer segregation of duties
- Unauthorized system changes
- Lack of policies and procedures

Control Risk Assessment Guidelines

- **Sub-Process Ranking Criteria**
  1. Ratio of transaction to monitoring controls
  2. Volume of activity
  3. Percentage of manual to automated controls
  4. Complexity of sub-process
  5. Percentage of preventative / detective controls
  6. Core business activity
  7. Overall assessment (common sense, historical insights)

Control Risk Assessment Guidelines

- Each sub process assessment was assigned a value:
  - Each high / yes assessment equals: √√√
  - Each moderate assessment equals: √√
  - Each low / no assessment equals: √
- The total score (number of checks) dictates your overall cycle risk

ISACA
Serving IT Governance Professionals

Walkthrough of IT Operations Cycle

For illustrative purposes, here is an example of how the sub-processes for this cycle were assessed:

	Sub process	Assessment	Score (# Checks)
1	IT Operations	M	√√
2	Change Management	H	√√√
3	Strategy Development	M	√√
4	Access Authentication	H	√√√
5	Security Configuration	H	√√√
6	Program Development and Implementation	H	√√√
		TOTAL	16

ISACA
Serving IT Governance Professionals

Control Risk Assessment Guidelines

# of Cycle Sub-processes	OVERALL CYCLE RISK		
	LOW	MEDIUM	HIGH
3	3-4	5-6	>6
4	4-5	6-8	>8
5	5-7	8-11	>11
6	6-9	10-14	>14
7	7-11	12-16	>16

ISACA®
Serving IT Governance Professionals

What does the Control Risk Assessment Mean?

- The ranking drives how we test
  - High overall risk: test transaction & monitoring controls
  - Moderate overall risk: limited transaction tests; test monitoring controls
  - Low overall risk: test monitoring controls and perform walkthrough of the cycle

Testing Operating Effectiveness

- We vary the nature, timing and extent of the test methods based on:
  - The risk of control failure
  - The risk of material misstatement
- There is significant flexibility in making judgments about what types of evidence to gather based on risk.
- We consider the persuasiveness of the evidence needed (i.e., its qualitative characteristics, not just quantity)
- We use a risk-based approach and consideration for testing information technology general controls and vary the nature, timing and extent of test methods accordingly

Focus on Critical Process Key Controls

- Link process level key controls to residual risks
- Evaluate controls and identify redundancies
- Evaluate impact of critical process level key controls on the consolidated financial statement risk assessment taken as a whole
- Identify IT general controls that may help ensure effectiveness of automated controls
- Challenge the business processes – only test the controls that directly mitigate residual risk

*Identify **only** those critical process level key controls that are necessary to mitigate the residual risk of **material misstatement** after considering CLC's*

ISACA
Serving IT Governance Professionals

New Viacom IT General Controls

- Viacom Management, Internal Audit and our External Auditors agreed to a total of 26 key risks/control objectives for Viacom's IT general controls for high priority business areas within:
  - Acquire and Maintain Application Software (AI2)
  - Enable Operations (PO6, PO8, AI6, DS13)
  - Install and Accredit Solutions and Changes (AI7)
  - Manage Changes (AI6, AI7)
  - Manage Third-Party Services (DS2)
  - Ensure Systems Security (DS5)
  - Manage the Configuration (DS9)
  - Manage Operations (DS13)
  - End-User Computing

Example: Manage Changes (AI6, AI7)

- Risk:
  - Applications supporting critical business processes may not be operating as management intended.
- Control Objective:
  - Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.

ISACA
Serving IT Governance Professionals

Example: Manage Changes (AI6, AI7)

- Controls Selected
  - Requests for program changes, system changes and maintenance (including changes to system software) are standardized, logged, approved, documented and subject to formal change management procedures.
  - Emergency change requests are documented and subject to formal change management procedures.
  - Controls are in place to restrict migration of programs to production by authorized individuals only.

Example: Manage Operations (DS13)

- **Risk:**
  - The lack of sufficient batch processing procedures and logs for review could result in uncorrected processing failures and/or financial misstatement.
- **Control Objective:**
  - Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring.

Example: Manage Operations (DS13)

- Controls Selected
  - Management has established, documented and follows standard procedures for IT operations, including job scheduling and monitoring and responding to security and processing integrity events.

Example: Current Maturity (DS13)

- **Current State: 3 Defined Process**
  - The need for computer operations management is understood and accepted within the organization. Resources have been allocated and some on-the-job training occurs. Repeatable functions are formally defined, standardized, documented and communicated. The events and completed task results are recorded, with limited reporting to management. The use of automated scheduling and other tools is introduced to limit operator intervention. Controls are introduced for the placement of new jobs in operations.
  - Specifically, we identified the following strengths and weaknesses:
    - Although operations procedures have been documented, they have not been updated recently to reflect current practices. In addition, there is no evidence of review of the procedures.
    - Logs are prepared and summarized for management to record operational events, however, review of the logs is not formally evidenced.

ISACA
Serving IT Governance Professionals

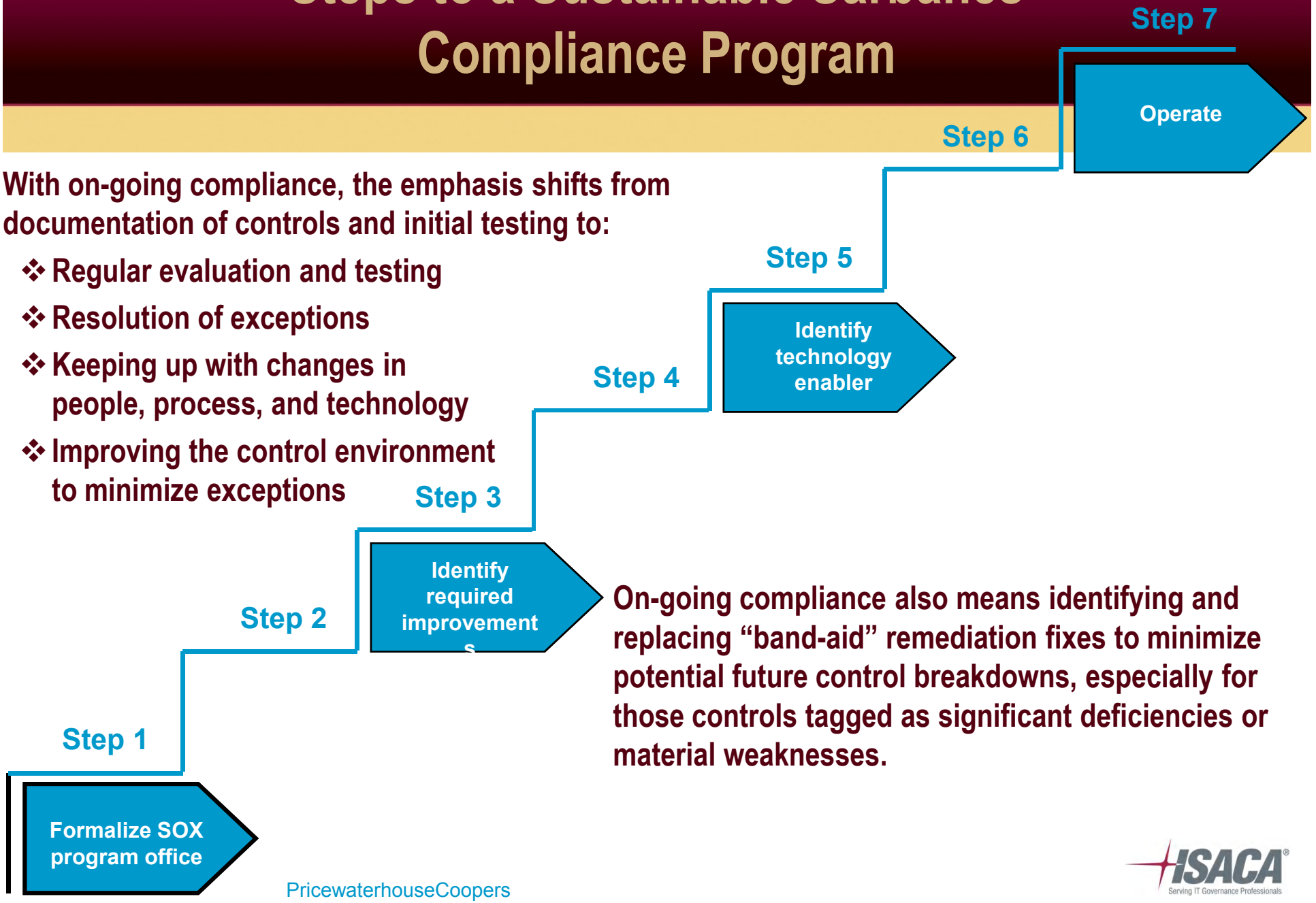
Example: Desired Maturity (DS13)

- **Desired State:** 3.5 Defined Process/Managed and Measurable
  - The need for computer operations is understood and accepted within the organization. The computer operations and support responsibilities are clearly defined and ownership is assigned. Training is formalized and ongoing. Repeatable functions are formally defined, standardized, documented and communicated. Any deviations from established norms are quickly addressed and corrected. Management monitors the use of computing resources and completion of work or assigned tasks. There is full alignment with problem, capacity and availability management processes, supported by an analysis of the causes of errors and failures.

Steps to a Sustainable Sarbanes Compliance Program

With on-going compliance, the emphasis shifts from documentation of controls and initial testing to:

- Regular evaluation and testing
- Resolution of exceptions
- Keeping up with changes in people, process, and technology
- Improving the control environment to minimize exceptions



On-going compliance also means identifying and replacing "band-aid" remediation fixes to minimize potential future control breakdowns, especially for those controls tagged as significant deficiencies or material weaknesses.

PricewaterhouseCoopers

ISACA
Serving IT Governance Professionals

Key On-Going Goals

- Document the risk/control decisions made
- Standardize controls and testing to reduce effort
- Deliver on-going training on risk and control objectives to help IT management determine key exposures facing the company. Train on topics such as segregation of duties and risk assessment.
- Champion the use of a consistent framework to base the IT General Controls around, e.g., COBIT and/or ITIL.

ISACA®
Serving IT Governance Professionals

Summary

- Select a compliance methodology.
  - Firstly document key risks to the accuracy of financial statements.
  - Determine current controls in key process areas.
  - Select key IT controls for testing based upon business risk.
- Continually Evaluate.
  - Review controls selected for testing annually.
  - Use control frameworks.
  - REMEMBER: Not every control performed needs to be tested for your compliance efforts.

For More Information

Anthony Noble

anthony.noble@viacom.com

ISACA®
Serving IT Governance Professionals

Questions?

Thank You!

ISACA
Serving IT Governance Professionals