Sarbanes-Oxley:

A Focus on IT Controls

Company Case Study - Viacom Inc.

IT Governance -

Establishing Sound Internal Controls

Anthony Noble

VP, IT Internal Audit

Today’s Agenda

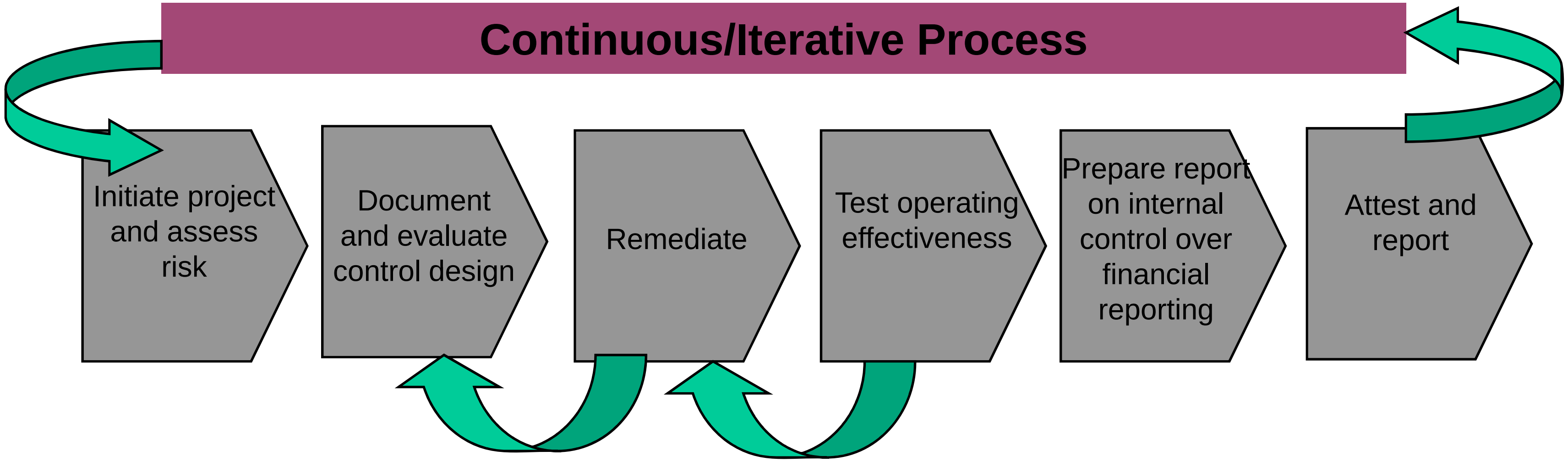
- ❑Introduction to SOX
- ❑Historical Overview of SOX Effort at Viacom
  - ❖Viacom Background
  - ❖Year 1 Methods
  - ❖Common Problems to be Aware of
- ❑Current Approach
  - ❖Key IT SOX 404 Controls Going Forward
  - ❖Value Gained

Introduction

- ❑ What
  - ❖ Objective: To share SOX experiences (successes and issues) and to discuss a series of topics to enhance the process for your implementation and going forward.
- ❑ Why
  - ❖ Learn from our growth.
  - ❖ Make ongoing process more efficient for everyone.
- ❑ Outcome
  - ❖ Suggestions for improving the approach of others.
- ❑ Caveats
  - ❖ Everyone will have a unique solution for SOX or J-SOX. There is no one perfect way.
  - ❖ Is from my personal viewpoint and not that of Viacom Inc.

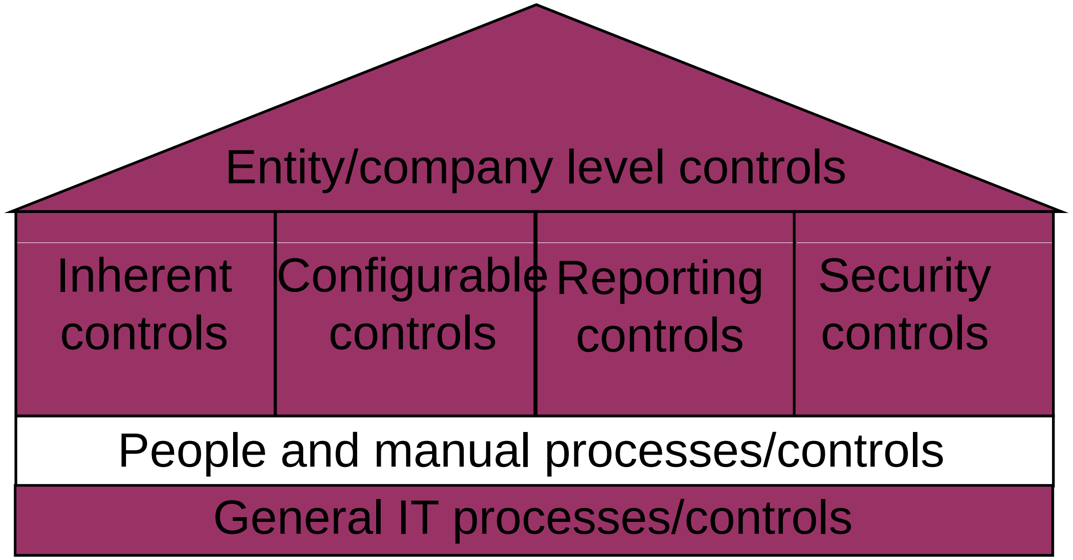
What is SOX 404?

Review of Controls over Reporting of Financial Statements Only


Continuous/Iterative Process
Initiate project and assess risk
Document and evaluate control design
Remediate
Test operating effectiveness
Prepare report on internal control over financial reporting
Attest and report

Importance of Information Technology Internal Controls

- The House of Internal Controls
  - IT related controls 🟪


Entity/company level controls
Inherent controls
Configurable controls
Reporting controls
Security controls
People and manual processes/controls
General IT processes/controls

Entity/Company Level Controls

- ❑Tone at The Top
  - ❖Policy and procedures that communicate management’s aims and directives
    - o Security policy and procedures
    - o Software Development Life Cycle (SDLC) standards
    - o IT Human Resources policy and procedures
    - o 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.
- ❑ General controls tend to fall into four broad categories:
  - ❖ Program Development & Implementation
  - ❖ Program Change Control
  - ❖ Computer Operations
  - ❖ Access Controls

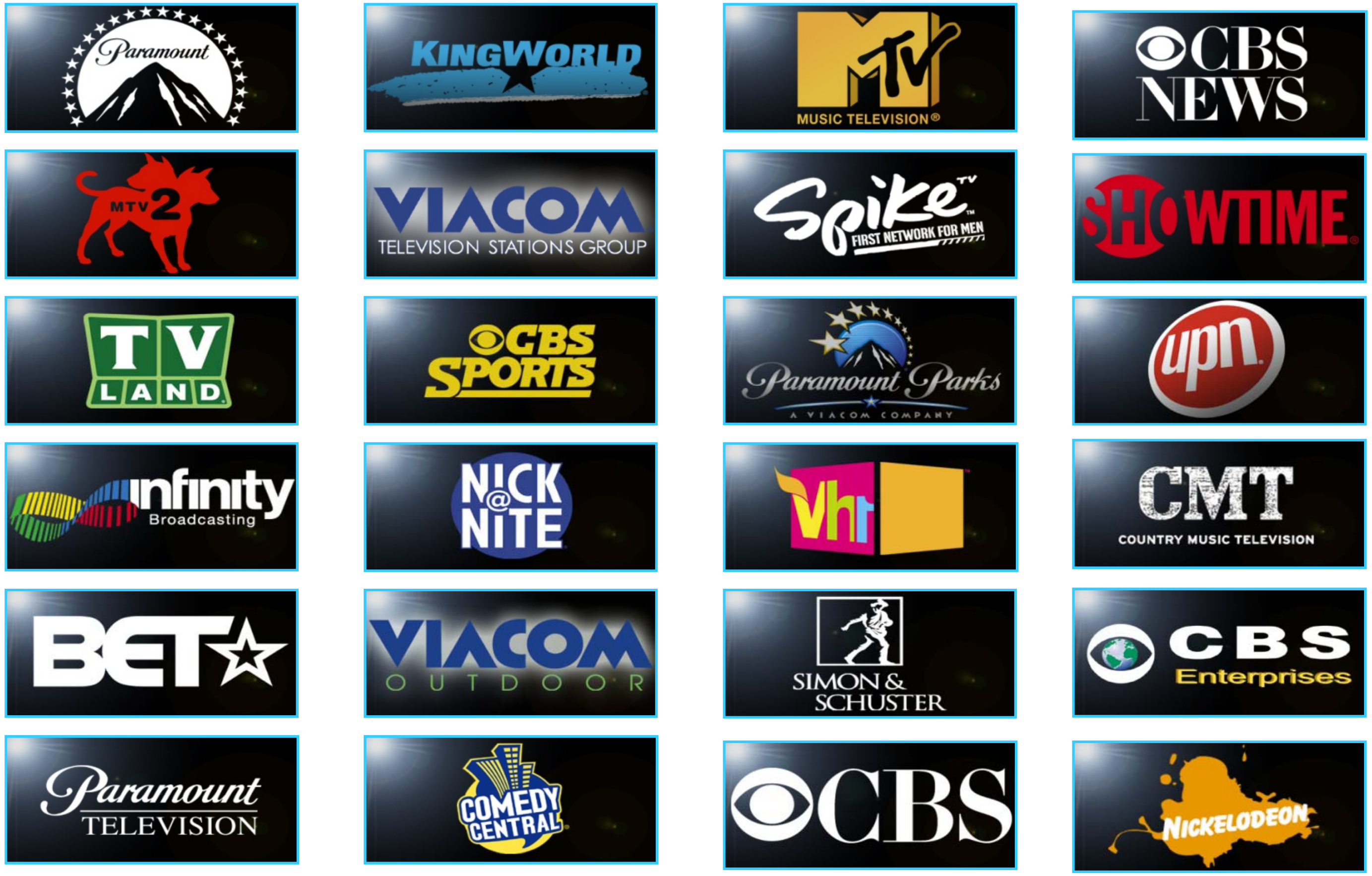
SOX Big Picture

- 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.

Introduction

- ❑ SOX principles
  - ❖ Useful to view and sell to IT as a mandatory Quality Improvement Process (QIP) that will create value over time.
  - ❖ Need to institute “Plan, Do, Check (Test), Act” process for each control.
- ❑ COBIT Framework
  - ❖ Useful to help evaluate current maturity level of key processes selected.
  - ❖ Gives common language from which to discuss controls.
  - ❖ Allows easier justification of controls implemented.
  - ❖ Each process under SOX needed to be at a minimum maturity level of 3 (meaning there are documented procedures over the process and a method for detecting exceptions to the process, but that an exception would likely not be detected).
- ❑ ITIL
  - ❖ Useful to select best practice procedures for areas selected to emulate. Saves time and effort.
  - ❖ Helpful for defining metrics.

Viacom Year 1



Viacom Year 1

- ❑ Many decentralized global locations spanning a wide variety of media & entertainment outlets
  - ❖ Cable (200 channels - MTVN, Nickelodeon, Comedy Central across the globe)
  - ❖ Film (Paramount Movies and DVDs – distributed across the globe)
  - ❖ Music Publishing (Famous Music – mainly movie scores and Eminem)
  - ❖ Radio (Infinity - comprised of 185 individual stations across the US)
  - ❖ Television (Network (CBS), Programs & stations across the US)
  - ❖ Publishing (Simon & Schuster – entertainment titles)
  - ❖ Amusement Parks (Paramount Parks - six parks across US & Canada)
  - ❖ Outdoor Advertising (Billboards in North America and Europe)
  - ❖ Blockbuster Video Stores (8,000 stores across the globe)
- ❑ Autonomous Divisions with own management and computer systems

Viacom Year 1

- Variety of businesses from Old Money to New Media.
- Paramount and CBS
  - Old Money – Finance in Black Suit, White Shirt and Red Ties
  - Traditional controls performed by Finance not Business
- MTVN
  - New Media – T-Shirts and Jeans
  - Few if any controls or controls understanding in Finance or Business
- Informality of controls common in industry. Creative process not to be affected. SOX resulted in a change in culture, requiring enormous effort to be compliant.
- Little if any Segregation of Duties for key financial staff.
- 30% Annual Revenue Growth so no one cared.

Getting Started with Buy-In

- ❑ Tone at the Top
  - ❖ Good tone from CFO, less so from senior business management .
- ❑ Intimidation/Fear of Failure
  - ❖ Threat of job loss required for some controls to be performed effectively and division year end bonus is now based partly on success in SOX testing.
- ❑ Training
  - ❖ MTVN performs controls training for Ad Sales staff on a regular basis to get over the point SOX is not just for finance.
  - ❖ Internal Audit gave Internal Controls training to IT staff.
- ❑ Persistence
  - ❖ Frequent meetings with some business control owners required to keep them performing controls.

Getting Started: Buy-In

- ❑Tone at the Top
  - ❖CFO stated would not be next to be led away.

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:
  - o Program Development & Implementation
  - o Program Change Control
  - o Computer Operations
  - o 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.

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.

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.

ISACA®
Serving IT Governance Professionals

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:
  - o 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.
  - o Logs are prepared and summarized for management to record operational events, however, review of the logs is not formally evidenced.

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.

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.

Year 1 Approach - Financial

- ❑ Developed standardized risks for each common business process with External Auditors.
- ❑ Piloted and rolled out a template-based approach to documenting business controls and tests.
- ❑ IT IA met with business to identify automated (embedded) controls for in-scope processes and design tests.
- ❑ Determined that most controls were manual and involved the reconciliation of reports from two interfaced systems or the review for a physical signature of approval on data input.
- ❑ Developed a consistent approach to spreadsheet controls as Viacom relies heavily on spreadsheets to calculate accruals.
- ❑ Implemented a Computer-Based Training (CBT) course on Internal Controls that all staff involved in SOX were required to pass.

Year 1 Approach – Outsourced Providers

- Identified third party providers of services for business processes in scope for SoX.
- Determined if a SAS 70 Type II report existed.
- If no SAS 70 Type II report existed, we performed alternate procedures:
  - Business conducted site visits to outsourced provider to identify, document and test key control activities and apply the SAS 70 standard.
  - For one of our business providers, Viacom IT IA covered the 11 key risks identified for limited scope business units.
    - Visited facilities where controls performed that related to key risks.
    - Identified, documented and tested controls.
    - Issued report to one our divisions using format of a SAS 70 Type II, which they relied upon for SoX.

Our Success Stories from Year 1

❑ Completed a huge documentation effort.

❑ Successfully remediated many control gaps.

❑ Completed testing using a very aggressive timeline.

❑ Identified testing synergies in IT across divisions.

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

Common Problems to Avoid in Year 1

- Defined too many key controls in some processes including 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.

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.

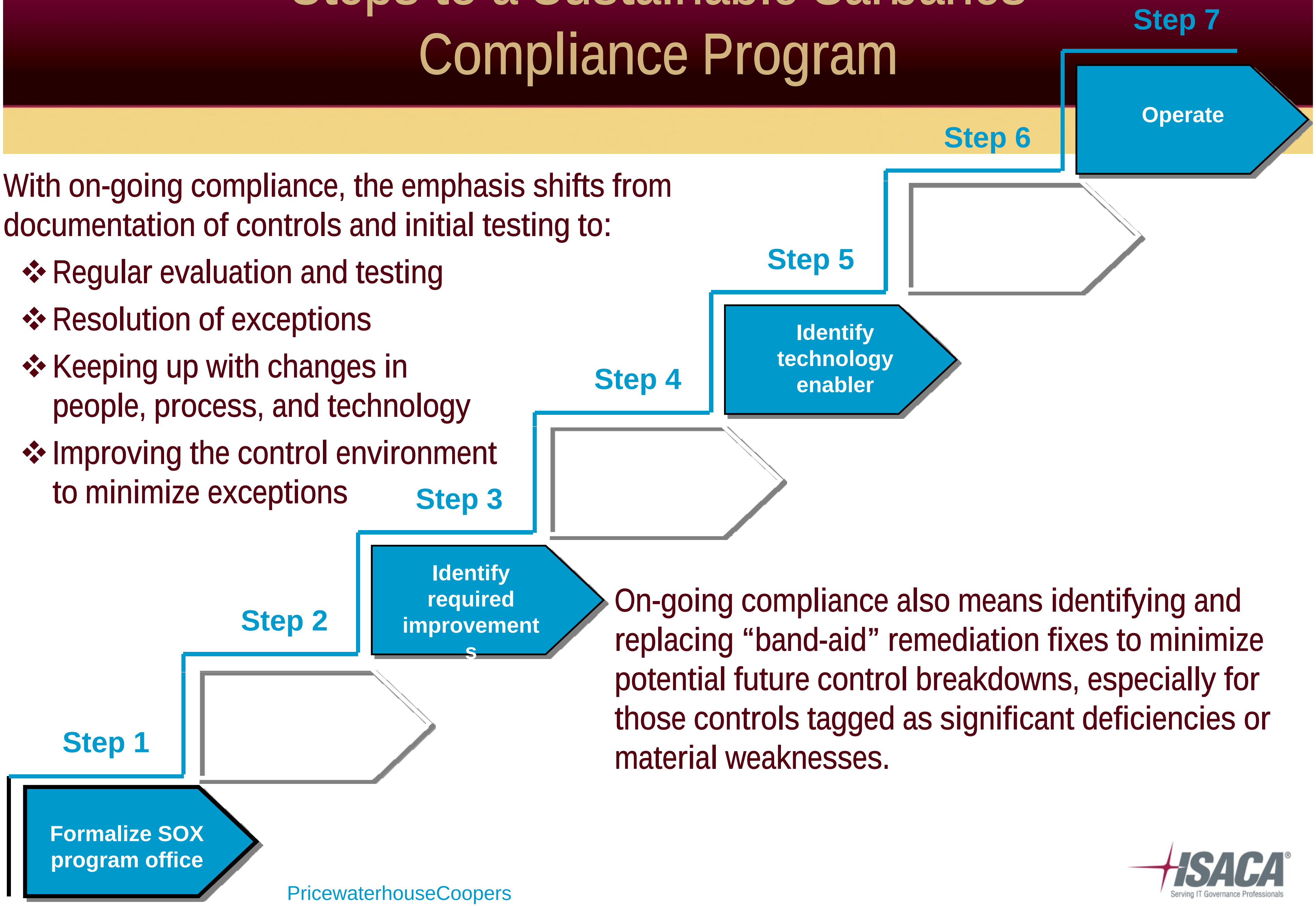
Common Problems to Avoid Year 1

- ❑ 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.

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


Step 1
Formalize SOX program office
Step 2
Step 3
Identify required improvements
Step 4
Step 5
Identify technology enabler
Step 6
Step 7
Operate

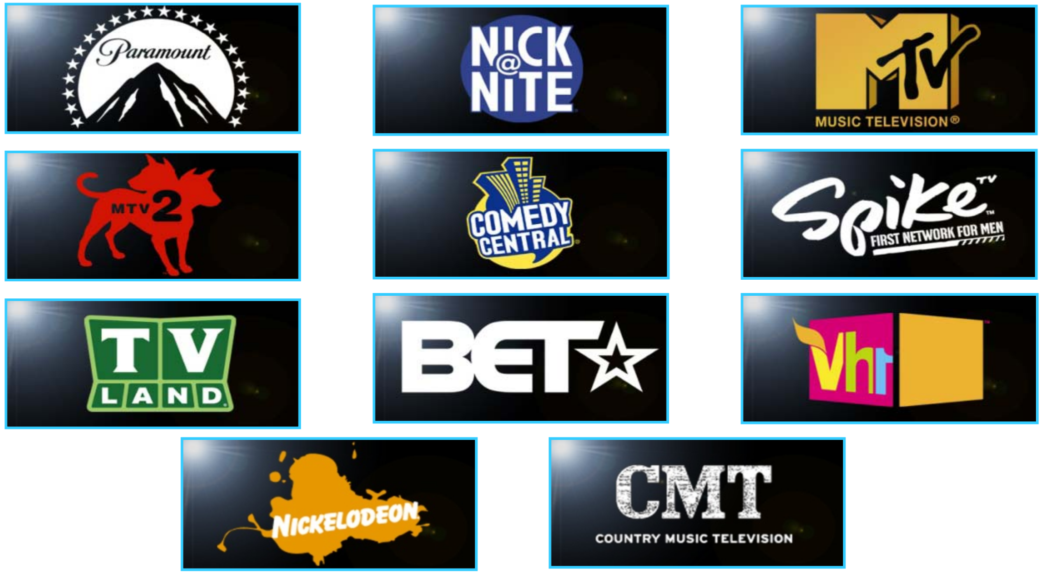
On-going compliance also means identifying and replacing “band-aid” remediation fixes to minimize potential future control breakdowns, especially for those controls tagged as significant deficiencies or material weaknesses.

PricewaterhouseCoopers

Key On-Going Goals

- ❑ Avoid a knee jerk reaction to what are considered onerous controls and tests by just not performing the controls.
- ❑ Address the “when is this going away” question with IT and Business.
- ❑ 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.

New Viacom


Paramount
NICK @ NITE
MTV MUSIC TELEVISION®
MTV2
COMEDY CENTRAL
Spike TV FIRST NETWORK FOR MEN
TV LAND
BET
Vh1
NICKELODEON
CMT COUNTRY MUSIC TELEVISION

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

- ❑Rolled-out pre-implementation checklist.
  - ❖Mandatory for new and significantly changed systems in scope for SOX 404.
  - ❖Tool helps management ensure they document and preserve evidence necessary to support a controlled system implementation.
  - ❖Ensures IT project team and management the design control system from ground up to be SOX 404 ready and identify and test key controls prior to implementation.

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

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, Problem Management and Physical Security.
  - ❖Leveraged financial group’s “Top-Down” risk assessment in selecting applications.

Key Achievements for New Viacom

- For Year 4, 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

2004 Approach - Spreadsheet Controls

- ❑ Approach to spreadsheet testing developed based on white paper titled, “The Use of Spreadsheets” issued by PricewaterhouseCoopers
- ❑ Each business unit was required to compile an inventory of spreadsheets used to directly determine financial statement transaction amounts or balances that are populated into the general ledger and/or financial statements
  - ❖ The inventory identifies spreadsheets that are in scope for SOX.
  - ❖ Spreadsheets are classified as simple or complex. A set of controls was defined for both types of spreadsheets.
  - ❖ The inventory is updated and reviewed quarterly to assess in-scope spreadsheets that require controls.

2004 Approach - Spreadsheet Controls

- Simple Spreadsheet Controls
  - Management review and approval, including verification that formula calculations within the spreadsheet were checked to ensure their accuracy (manual footing & cross-footing).
- Complex Spreadsheet Controls
  - Reconciliation Control: Management review and approval in writing.
  - Security and Access Controls:
    - Spreadsheets are backed up following backup and recovery standards;
    - Complex spreadsheets are logically secured and formula cells are locked. Access to the spreadsheets is reviewed quarterly.
  - Change Control: The logic in critical spreadsheets is tested annually by someone other than the user of the spreadsheet. Changes are tested and approved prior to moved to production. Prior versions are maintained in a secure directory.

Summary – Additional Value Gained

- ❑ Initial IT reaction was controls added no value just extra work.
- ❑ System access used to be granted with different form for each system.
  - ❖ Now HR system automates the provisioning and de-provisioning of users for all in-scope SOX systems.
- ❑ Users allowed IT to perform all testing of system changes.
  - ❖ User now more involved in testing and less issues in production systems.
- ❑ Business users used to give their system requirements verbally for IT to document.
  - ❖ Now have to document requirements and approve before coding. Unrealistic requirements are flushed out before coding starts.

Summary

- ❑ Train staff and control owners on controls and integrate controls into workflow.
- ❑ Train testers on how to test and document the testing.
- ❑ Select a control framework.
  - ❖ Evaluate key risks to accuracy of financial statements.
  - ❖ Determine current maturity level in key process areas.
  - ❖ Get into "Plan, Do, Check, Act" mode to raise maturity level.
- ❑ Continually Evaluate.
  - ❖ Review controls selected annually.
  - ❖ Sell the use of control frameworks.
  - ❖ Train where needed.

For More Information

Anthony Noble

anthony.noble@viacom.com

Questions?

Thank You!