Have You Reviewed Your Internal Controls Lately?

Tom Hazelwood and Tamara Vineyard / November 2, 2023

Meet the Presenters

Tom Hazelwood

Assurance Partner

Nonprofit, Education, & Public Sector

Tamara Vineyard

Assurance Partner

Regional Industry Leader Nonprofit, Education, & Public Sector

FORV/S

Agenda

3:30 PM	Introductions
3:40 PM	Why are Internal Controls important?
3:50 PM	Types of Internal Controls
4:00 PM	Processes vs. Controls
4:10 PM	Elements of Strong Internal Control Environment
4:20 PM	Closing

“We must accept human error as inevitable – and design around that fact.”

– DONALD BERWICK

FORVIS

Participation Trophy

Name an internal control you encountered as an employee.

Has that control changed over time?

This Photo by Unknown Author is licensed under CC BY-SA

How did COVID-19 impact your internal controls?

What Are Internal Controls?

- Internal control is a process — affected by management and other personnel, and those charged with governance, and designed to provide reasonable assurance regarding the achievement of objectives in the reliability of financial reporting.
- Your organization’s policies, procedures, organizational design and physical security are all part of the internal control process.

Why Internal Controls Are Important

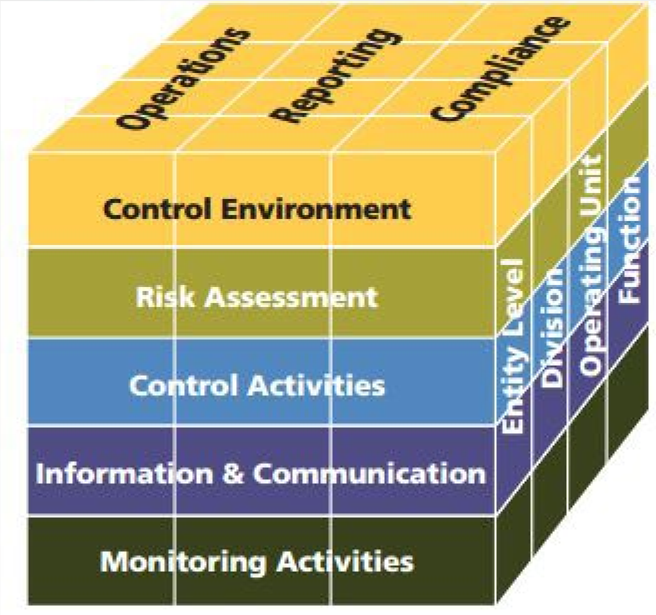
- Effective internal controls:
  - Safeguard assets
  - Protect employees
  - Provide more accurate financial statements
  - Compliance with laws and regulations

This Photo by Unknown Author is licensed under CC BY-SA

FORVIS

The Basis for Internal Controls

Internal Control Framework released by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2013.



This Photo by Unknown Author is licensed under CC BY

FORVIS

What Are Examples of Control Activities?

- **Control activities occur at all levels & functions, in all organizations, & may include**
  - Segregation of duties
  - Authorization
  - Reconciliation
  - Review & approval
  - Education & training
  - Performance planning & evaluation

FORVIS

COSO Components

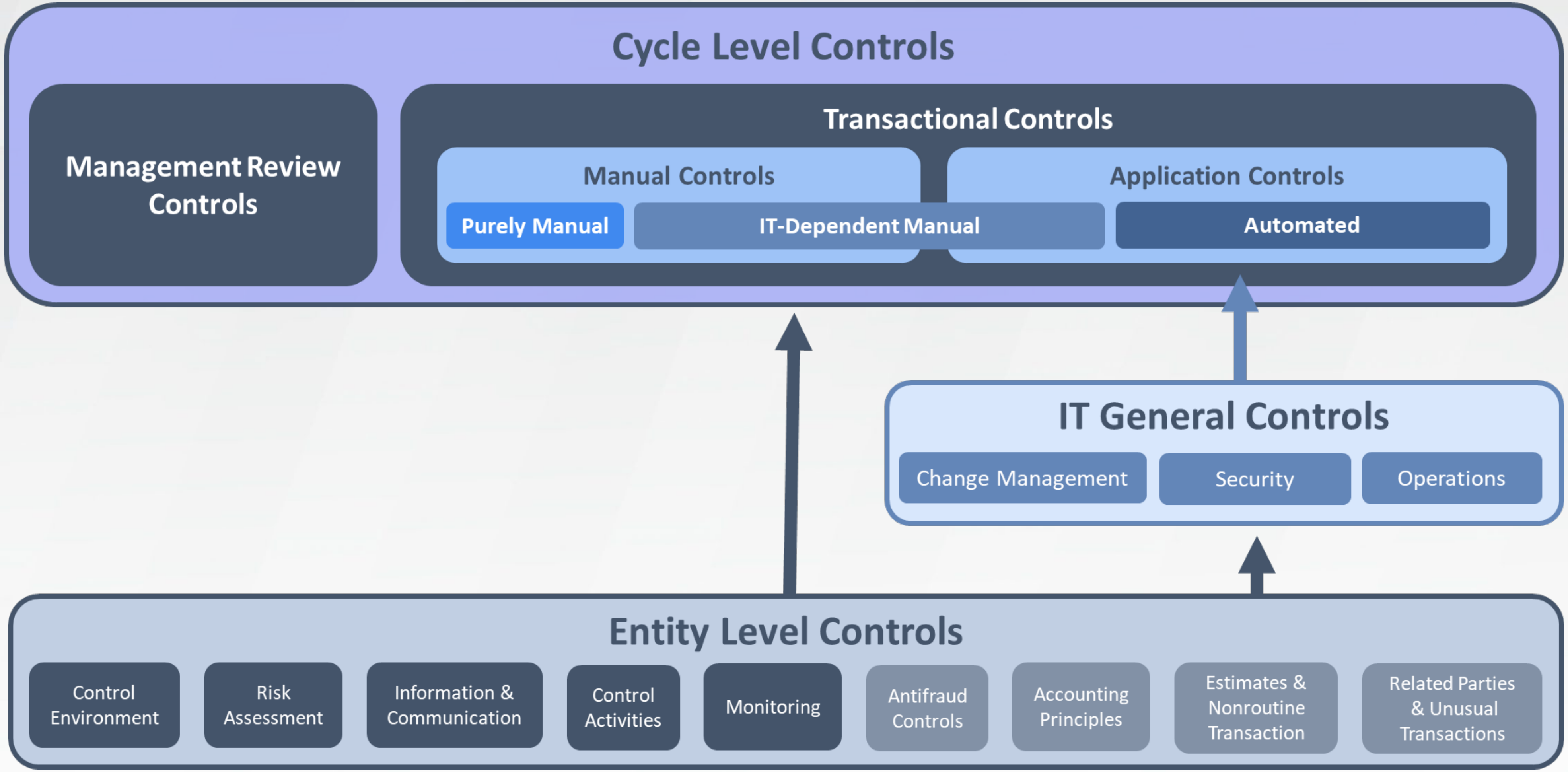
COSO

- The COSO framework consists of 17 principles that support five components

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Demonstrates commitment to integrity & ethical values Exercises oversight responsibility Establishes structure, authority, & responsibility Demonstrates commitment to competent talent Enforces accountability	Specifies clear objectives Identifies & analyzes risk Assesses fraud risk Identifies & assesses significant changes	Selects & develops control activities Selects & develops general controls over technology Deploys control activities through policies & procedures	Uses quality information Communicates internally Communicates externally	Conducts ongoing &/or separate evaluations Evaluates & communicates deficiencies timely

Source: COSO

Types of Controls



FORVIS

Types of Controls

- **Entity-Level Controls** - address financial statement risks related to the entire entity.
  - Foundational to the effective operation of *cycle-level* controls, but not typically designed to detect material misstatements, *i.e.*, these are the policies and procedures that ensure the controls that catch the misstatements work.
  - Some entity-level controls might operate at a level of precision sufficient to detect material misstatements, such as with some management review controls. For example, a control related to hiring competent accounting personnel would not directly relate to the detection of a material misstatement, but a control related to a detailed review of monthly financial statements by business line might detect a material misstatement.

Entity-Level Controls

Entity-level controls consist of the following categories:

- Control environment: The attitude of management and those charged with governance toward accurate financial reporting, *i.e.*, the *tone at the top*
- Risk assessment: Management’s response to financial reporting risks from changes to the accounting or business environment
- Information and communication: Management’s process to ensure information necessary for financial reporting is accurately communicated to those who need it, including IT systems and the financial reporting process
- Control activities: Management’s process to ensure adequate design and implementation of controls at the cycle level
- Monitoring: Management’s process to ensure internal controls continue to operate effectively

Examples of Entity-Level Controls

- Board of Directors meets quarterly; minutes are documented
- Employees sign off on The Code of Ethics during new-hire orientation & annually thereafter
- Employees undergo background checks before hiring into “sensitive” positions
- Management annually reviews policies & procedures to ensure they represent current business practices

Examples of Entity-Level Controls (cont.)

- The Continuity of Operations Plan (COOP) is tested annually
- Annual user access reviews are performed by management to confirm that the principle of least privilege & segregation of duties controls are maintained
- Security awareness training is taken by all employees annually

Types of Controls

- **IT General Controls (ITGC)** – companywide policies and procedures that ensure the proper function and control of information technology (sort of the “entity-level controls” for IT).
  - Not usually designed to prevent or detect misstatements (as opposed to *IT application* controls).
  - Are essential to the effective functioning of *IT application* controls.

ITGC

- Relate to one of the following "domains":
  - System development and change management: making sure people can't inappropriately change the way the system works, the information in the system, or the parameters of key reports.
  - Logical and physical security: making sure people can't access the system and do things they shouldn't do.
  - Operations: making sure the system doesn't work incorrectly, *e.g.*, accessing the wrong database in extending prices.

Types of Controls

- **Cycle-Level Controls** - Sometimes referred to as transaction-level, process-level, activity-level, or assertion-level controls.
  - Control activities at the account balance and class of transaction, *i.e.*, cycle
  - Designed to prevent or detect and correct material misstatements.

Cycle-Level Controls

- The controls associated with process walk-throughs, such as:
  - Cash inflows (including revenue, cash receipts and accounts receivable)
  - Cash outflows (including purchases, payables, and payments)
  - Payroll cycle
  - Inventory cycle
  - Investing and financing cycle
  - Various industry-specific cycles

Types of Controls

- **Transactional Controls** – cycle-level controls applied to each transaction or item (or each transaction or item in a range)
  - May be manual, automated, or IT-dependent manual controls

Transactional Control Examples

- Procurements over $X are approved by the Purchasing Director, Finance Director, & the Division Director requesting the purchase
- Review and approval of new employee setup
- Review of monthly bank reconciliations
- Matching invoices to shipping documents
- System edit check that prevents alphabetic characters from being entered into a numeric field
- Travel & expense vouchers are approved by employees’ supervisors before being processed for payment

Types of Controls

- **Management Review Controls** – typically involve management review of summarized information (such as monthly financial information) and differ from *transactional* controls in that they are not applied to each individual transaction.

Management Review Controls

- *Analytical procedures* performed by management focused on estimates and other kinds of financial information for *reasonableness*. As such, the evaluation of management review controls includes consideration of the precision of, and quality of information used in, the control (similar to how an auditor would assess a substantive analytical procedure). For example, a CFO may review monthly financial statements by comparing tuition revenue to the number of students and average rates to determine that revenue is reasonable.
- *Top-level reviews* performed by someone other than the process owner. For example, in an IT environment, a transactional control might be the approval of access rights for each new employee. The related management review control might be a periodic access review (monthly, quarterly, or annually) by the manager of the person performing the initial approval to determine that access appears reasonable.

Management Review Controls

- Management review controls (like transactional controls) may be found in each control category, including entity-level controls, IT general controls, and cycle-level controls. The key distinction between management review controls classified as entity-level controls and those classified as cycle-level controls is the level of precision.
- Management review controls that are not precise enough to detect material misstatements but are still effective as monitoring or information and communication controls are entity-level controls. Management review controls that operate with sufficient precision to detect material misstatements are also cycle-level controls.

Types of Controls

- **IT Application Controls** – system settings that determine how transactions and data are input to, processed by, and output from the computer system.
  - Effectiveness of application controls depends on ITGCs such as access and change management controls, *i.e.*, if anyone can change the data or override the output, then it doesn't matter what the system is designed to do.
  - Includes automated and IT-dependent manual controls.

IT Application Controls

- Understanding application controls usually involves understanding:
  - The application logic (code) configured and “locked down” by the entity. For example, the way the application calculates interest income for past due student receivables.
  - The user-selected parameters of ***system-generated reports***, *e.g.*, the date range and customer type selected in a report of overdue student accounts receivable.

IT Application Controls

- Common IT application controls include the following:
  - Calculation: Mathematically determine complex or large volume transactions based upon a predefined formula
  - Validation checks: Ensure data accuracy and completeness
  - Workflow: Procedures or processes created to ensure the proper routing of a transaction
  - Approval: Procedures to ensure data and transactions meet required criteria, including prompting manual intervention
  - Security: Determines what a user can do in the system; restricted access, roles and responsibilities, segregation of duties

Types of Controls

- **Automated Controls** – IT application controls are fully automated

Automated Controls

- Examples of automated controls include:
  - Customer orders only processed if there is a valid customer number
  - Segregation of duties: Access to system limited to functions needed to perform job
  - Calculation of tuition
  - Depreciation of assets over a fixed period depending on asset class
  - Three-way match in the cash outflows cycle performed by the system, *i.e.*, purchase order, receiving report, and invoice
  - Correct account numbers setup to ensure correct posting to general ledger. For example, system updates revenue and accounts receivable when a student registers
  - Calculation of interest income and interest expense
  - Automated routing for approval

Automated Controls

*An automated <u>process</u> becomes an automated <u>control</u> when the inherent consistency in its application eliminates a risk that would exist if the process were performed manually. For example, if the calculation of interest income were performed manually an error could occur in the calculation, *i.e.*, a person might make a math error, or in the input, *i.e.*, a person might erroneously type in the wrong amount. Furthermore, a person might perform the calculation correctly many times and still make an error another time. The same process performed automatically eliminates the calculation and input errors (assuming the IT logic is correct) and ensures consistent application of the result.

Types of Controls

- **IT-Dependent Manual Controls** – controls that depend on effective human and IT system interaction to function properly.
  - For example, if an automated three-way match (automated control) identifies unmatched documents, the system generates an exception report, and the transaction cannot be processed until the exception is cleared by a human. The match, generation of the exception report, and restriction on further processing are automated controls. Resolving, correcting, and approving the exceptions are IT-dependent manual controls because they depend on the automated control to function properly.

IT-Dependent Manual

- IT-dependent manual controls usually fall into one of the following categories:
  - Manual controls that depend on information in a ***system-generated report***. For example, a review of a monthly aging report.
  - Automated controls that trigger human intervention. For example, the manual follow-up on an exception report.
  - Automated controls that require human intervention. For example, manual approval of a transaction exceeding certain parameters before the transaction can be processed in the system.

IT-Dependent Manual

- Often depend on the completeness and accuracy of ***system-generated reports***
  - Source data likely governed by ITGCs
  - User-selected parameters of the report are not

Types of Controls

- **Purely Manual Controls** – controls performed by people without any ***system-generated reports*** or other assistance of applications or technology systems.
  - Subject to inherent risk of human error.

Purely Manual Controls

- Examples of purely manual controls include:
  - Authorization of employee expense reports
  - Written authorizations, such as signature on check
  - Signing a policy acknowledgment, *i.e.*, code of conduct

Types of Controls

- **Preventative** – designed to prevent a misstatement from being processed.
- **Detective** – designed to detect and correct misstatements after they have already been processed.

Process vs. Control

Process	Control
Captures originates, changes data & potentially introduces possible errors	Does not change data

FORVIS

Process vs. Control

Process	Control
Potentially can introduce possible errors	Cannot generate errors

Process vs. Control

Process	Control
Needed to get information from point A to point B; necessary for bookkeeping	Prevents or detects a misstatement; not necessary for bookkeeping

Process vs. Control

Process	Control
What do they do?	What do they do about what could go wrong?

FORVIS

Process vs. Control

- Exercise

FORVIS

Strong Control Environment

- General characteristics of satisfactory internal control over financial reporting:
    - Policies and procedures that provide for appropriate segregation of duties to reduce the likelihood that deliberate fraud can occur
    - Personnel qualified to perform their assigned responsibilities
    - Sound practices to be followed by personnel in performing their duties and functions
    - A system that ensures proper authorization and recordation procedures for financial transactions

Components of Internal Control

- Control environment
- Risk assessment
- **Control activities**
- Information and communication
- Monitoring

FORVIS

Control Activities

- What controls are in place for your institution:
  - Cash receipts
  - Cash disbursements
  - Payroll
  - Financial close and reporting
  - State compliance
  - Grant compliance

Benefits of Implementing a Strong Internal Control Program

Weak Internal Controls

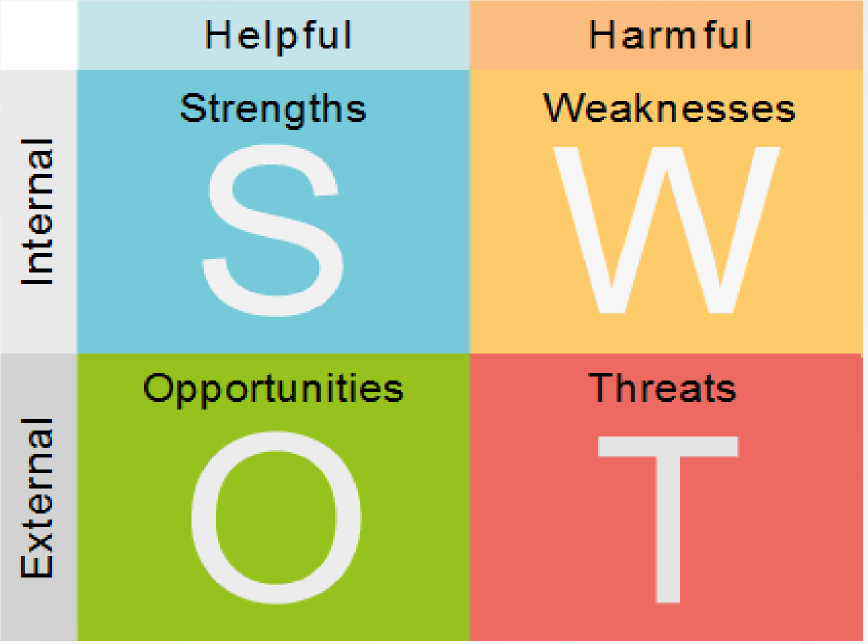
- Insufficient documentation to support a complete entity-level evaluation
- An entity-wide risk assessment is not performed
- Insufficient documentation of risk assessments for each significant fiscal process
- Insufficient documentation of testing controls for each significant fiscal process

Strong Internal Control Program

- **Implemented**
  - Entity-wide risk assessment
- **Identified, documented, & tested**
  - Entity-level controls
  - Transaction-level controls
  - IT controls
- **Benefits**
  - Effective/efficient operations
  - Reliable financial reporting
  - Compliant with laws/regulations
  - Safeguard assets

Best Practice – Complete Entity-Wide Risk Assessment Using SWOT

- Assess entity-wide risks using questionnaires &/or meetings
- Use SWOT analysis; leverage management surveys/meetings to develop common themes
- Do not treat as a task; take action to better your institution



	Helpful	Harmful
Internal	Strengths S	Weaknesses W
External	Opportunities O	Threats T

Questions

Tom Hazelwood, CPA

Assurance Partner

Phone: 336-714-8136

Tom.hazelwood@forvis.com

Tamara Vineyard, CPA

Assurance Partner

Phone: 703-970-0482

Tamara.vineyard@forvis.com

Thank you!

forvis.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by FORVIS or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities.
FORVIS has been registered in the U.S. Patent and Trademark Office, which registration is pending.

FORVIS

Assurance / Tax / Consulting

Check Out Code

22AT5