



*A Discussion About
Internal Controls
February 2016*

What we will cover today...

001 Introductions

002 Defining
Internal
Controls

003 COSO Internal
Controls
Integrated
Framework

004 Approach to
Designing
Internal
Controls

005 Testing
Internal
Controls



Introductions

Giselle Read – Risk Assurance Director

Definition of Internal Control

Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

~The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Benefits of Effective Internal Control

Effective internal control **provides reasonable**, not absolute, assurance that objectives are met and risks are controlled, and it:

- Facilitates consistency and efficiency
- Increases credibility with third parties
- Provides for more timely and accurate information for decision makers
- Reduces substantive audit testing
- May help prevent litigation
- May help prevent fines and penalties (e.g., from regulators)
- Increases risk awareness across the organization
- Reinforces achievement of strategic objectives

Concept of Internal Controls

Internal control is a process that “controls” or mitigates risk, for example:

- In accounting, **internal control** is a process to provide reasonable assurance over the accuracy and reliability of financial reporting (internal and external).
- In compliance, **internal control** is a process to provide reasonable assurance over adherence to laws, regulations, internal policies, etc.
- In operations, **internal control** is a process to provide reasonable assurance over consistent and predictable outcomes of transactions and underlying data.
- In information technology, **internal control** is a process to provide reasonable assurance over proper systems development, computer operations, program changes and access.
- In fraud management, **internal control** is a process to provide reasonable assurance over the detection and prevention of fraud, including both internal and external risks.

Who Needs Internal Controls?

Every company needs internal controls.

- New and old
- Small and large
- Public / private / government
- US based and international

The degree of risk a company can accept is variable, which drives the design and testing approach, however; minimum standards for the internal control framework used must be met.

How effective is your system(s) of internal control?

- Do your business goals, initiatives, and priorities, or operating decisions introduce new risks that impact your internal control?
- How do your controls adapt to change? Is your organization prepared to respond to change?
- What breakdowns have you experienced with existing controls? Why didn't you know about those before? How could they have been prevented?
- Are you considering new opportunities for applying internal control to reporting, operations, and compliance objectives?

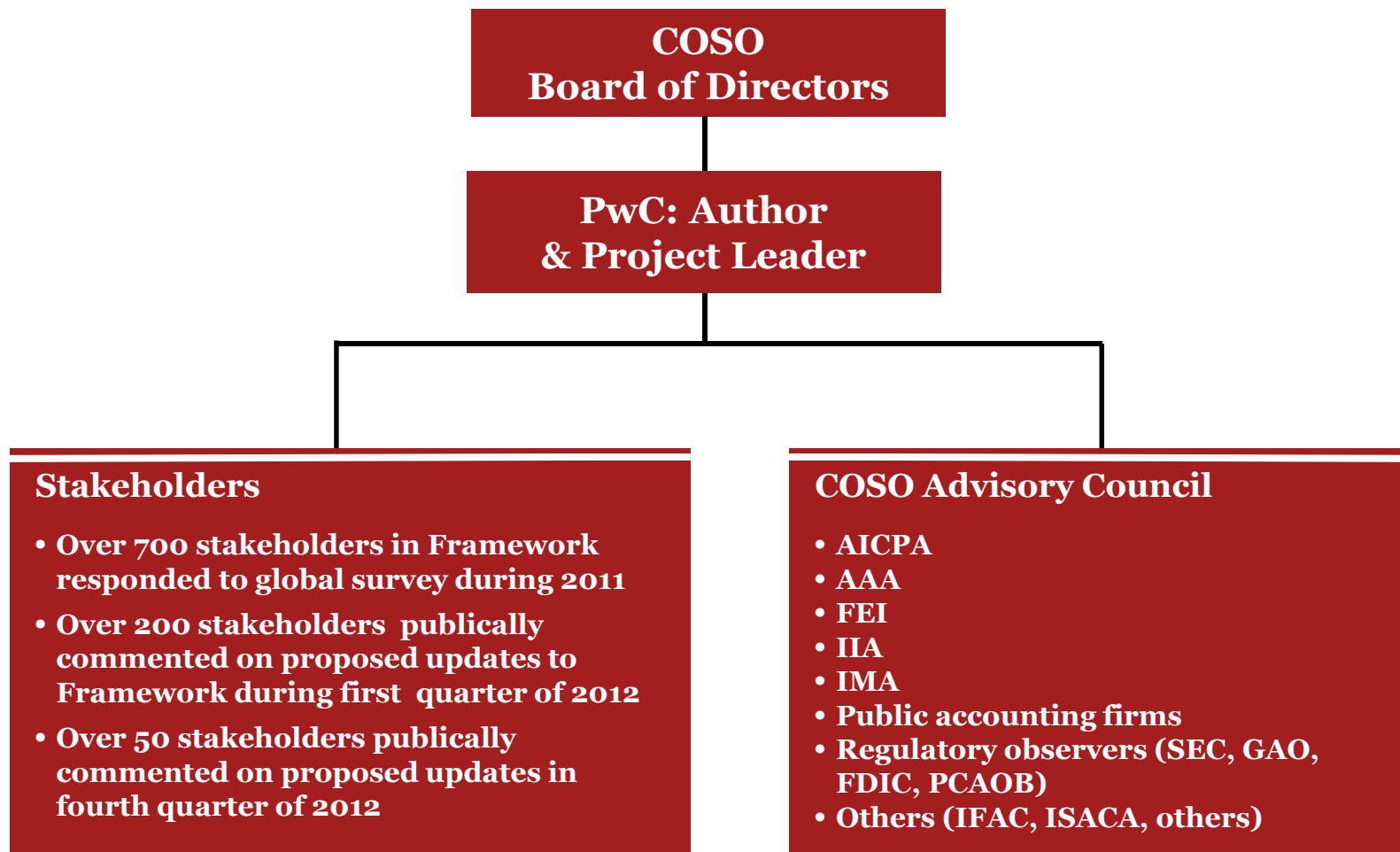
An Overview of the 2013 COSO Framework

The Committee of Sponsoring Organizations (“COSO”) of the Treadway Commission was created in 1985 through the joint sponsorship of the AICPA, American Accounting Association, Financial Executives Institute and the Institute of Management Accountants to identify factors associated with fraudulent financial reporting and to make recommendations to reduce fraudulent reporting.

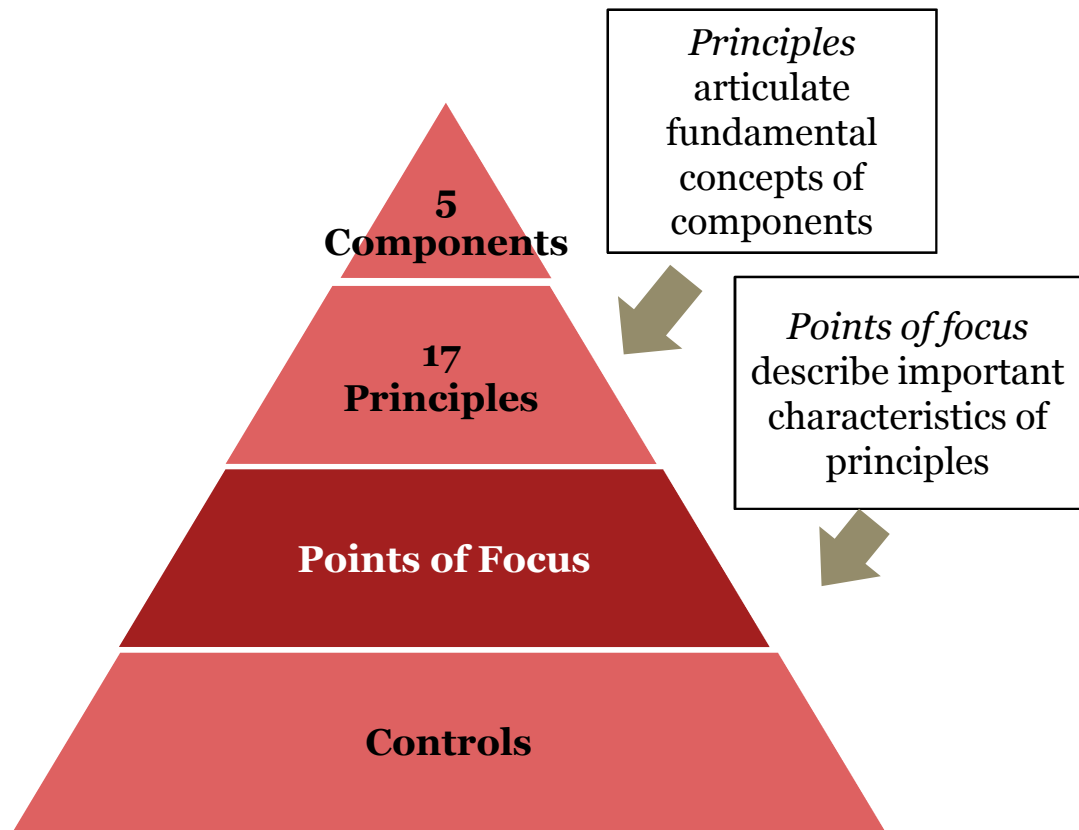
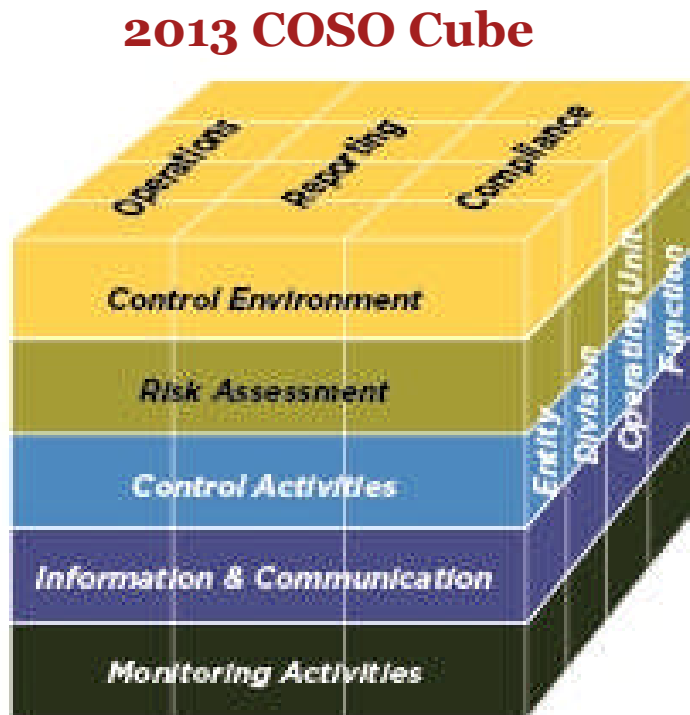
In 1992, COSO developed the *Internal Control – Integrated Framework* (COSO IC-IF, or the “Framework”), a framework which would allow the management of an organization to establish, monitor, evaluate and report on internal controls.

In 2013, they released an updated Internal Control-Integrated Framework, superseding what had been in place since 1992.

An Overview of the 2013 COSO Framework



An Overview of the 2013 COSO Framework



Legend

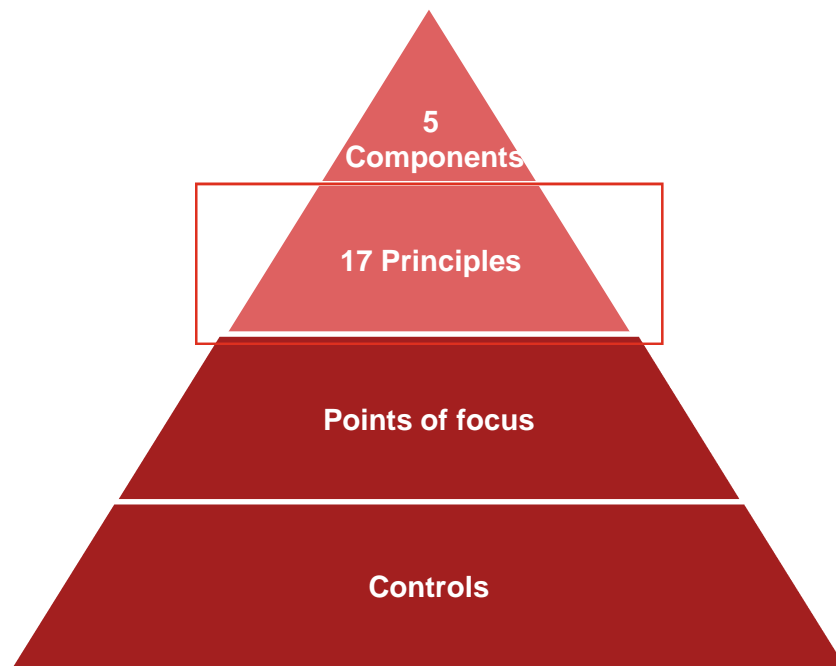
- Components and Principles are requirements for an effective system of internal control
- Points of Focus do not require a separate assessment

COSO's Internal Control Framework

Principles of Effective Internal Control by Component

Control Environment	<ol style="list-style-type: none">1. Demonstrates commitment to integrity and ethical values2. Exercises oversight responsibility3. Establishes structure, authority and responsibility4. Demonstrates commitment to competence5. Enforces accountability.
Risk Assessment	<ol style="list-style-type: none">6. Specifies suitable objectives7. Identifies and analyzes risk8. Assesses fraud risk9. Identifies and analyzes significant change
Control Activities	<ol style="list-style-type: none">10. Selects and develops control activities11. Selects and develops general controls over technology12. Deploys through policies and procedures
Information & Communication	<ol style="list-style-type: none">13. Uses relevant information14. Communicates internally15. Communicates externally
Monitoring Activities	<ol style="list-style-type: none">16. Conducts ongoing and/or separate evaluations17. Evaluates and communicates deficiencies

COSO's Internal Control Framework

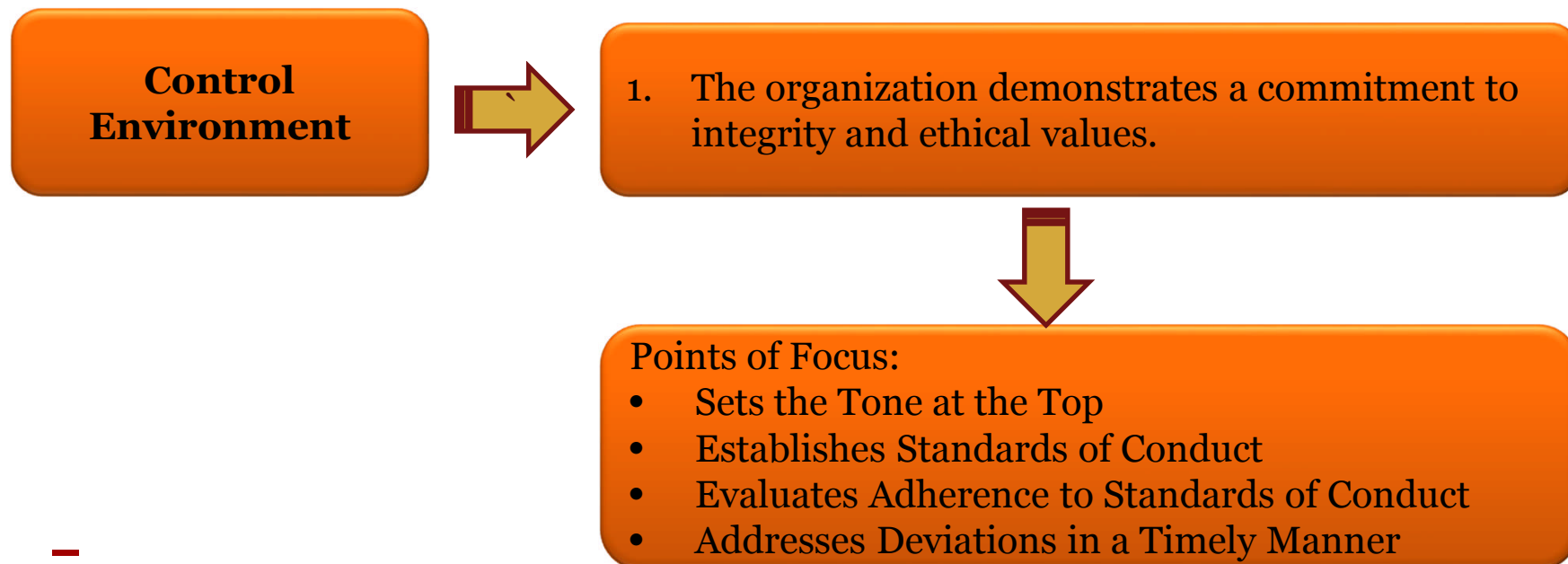


- Principles are suitable and presumed relevant for all entities
- Principles can support achievement of a single, multiple, or overlapping objectives
- When principles are present and functioning, objectives are specified with sufficient clarity to assess risk and deploy controls to mitigate risk to acceptable level
- Applying principles provides a basis for checking what's covered and what's missing across the business—including dispersed and outsourced operations

COSO's Internal Control Framework

Important Characteristics of Principles

- Points of focus may not be suitable or relevant, and others may be identified
- Points of focus may facilitate designing, implementing, and conducting internal control
- There is no requirement to separately assess whether points of focus are in place



COSO's Internal Control Framework

“An effective system of internal control...requires that:

- “Each of the five components of internal control and relevant principles is present and functioning
- The five components are operating together in an integrated manner”

“Management can demonstrate that components operate together when:

- Components are present and functioning
- Internal control deficiencies aggregated across components do not result in the determination that one or more major deficiencies exist”

COSO's Internal Control Framework

Role of Controls to Effect Principles

- The Framework does not prescribe controls to be selected, developed, and deployed for effective internal control
- An organization's selection of controls to effect relevant principles and associated components is a function of management judgment based on factors unique to the entity
- A major deficiency in a component or principle cannot be mitigated to an acceptable level by the presence and functioning of other components and principles
- However, understanding and considering how controls effect multiple principles can provide persuasive evidence supporting management's assessment of whether components and relevant principles are present and functioning

COSO's Internal Control Framework

Role of Various Controls to Effect Principles

Component

Control Environment

Principle

1. The organization demonstrates a commitment to integrity and ethical values.

Controls embedded in other components may effect this principle

Human Resources review employees' confirmations to assess whether standards of conduct are understood and adhered to by staff across the entity

Control Environment

Management obtains and reviews data and information underlying potential deviations captured in whistleblower hot-line to assess quality of information

Information & Communication

Internal Audit separately evaluates Control Environment, considering employee behaviors and whistleblower hotline results and reports thereon

Monitoring Activities

Activity: Addressing COSO Principle

Principle 8: Assess Fraud Risk

The organization considers the potential for fraud in assessing risks to the achievement of objectives

Relevant Points of Focus:

➤ **Considers Various Types of Fraud**

The assessment of fraud considers fraudulent reporting, possible loss of assets and corruption resulting from the various ways fraud or misconduct can occur

➤ **Assesses Incentive and Pressures**

Fraud risk considers incentives and pressure

➤ **Assesses Opportunities**

Assessment considers opportunities for unauthorized acquisition, use, or disposal of assets, altering reporting records or committing other inappropriate acts

➤ **Assesses Attitudes and Rationalizations**

Considers how management or other personnel might engage in or justify inappropriate actions.

Activity: Addressing COSO Principle

One Entity-Level Control surrounds the performance or Enterprise Risk Management Assessment and considers fraud as a component of the exercise

Control includes the following key elements:



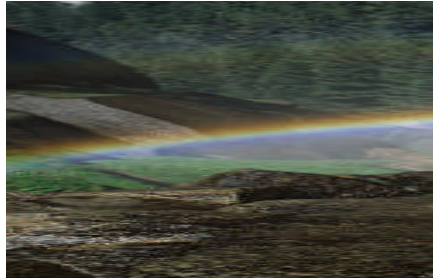
- Considers historical known fraud and related mitigating controls
- Considers emerging industry fraud schemes
- Uses data analytics to understand baseline averages (# of manual j/e's)
- Conducts interviews of key / non-key personnel in all locations
- Consider the risks related to elements of the fraud triangle
 - **Pressure**
 - Considers results of annual comp. committee review of exec. incentives
 - Considers reasonableness of financial targets & trends
 - **Opportunity**
 - Consider the effectiveness of the internal control assessments (IT & BP)
 - **Rationalization**
 - Consider enterprise wages against industry compensation
- Considers personnel awareness of Whistleblower Hotline & reviews reports
- Assessment results socialized with the Board

Concept of Risk

Definition

Risk is the combination of:

- the probability that an event will occur that could affect the implementation of strategy or achievement of objectives, the source of which can be internal or external, and
- the consequences of that event, which can range from positive to negative.

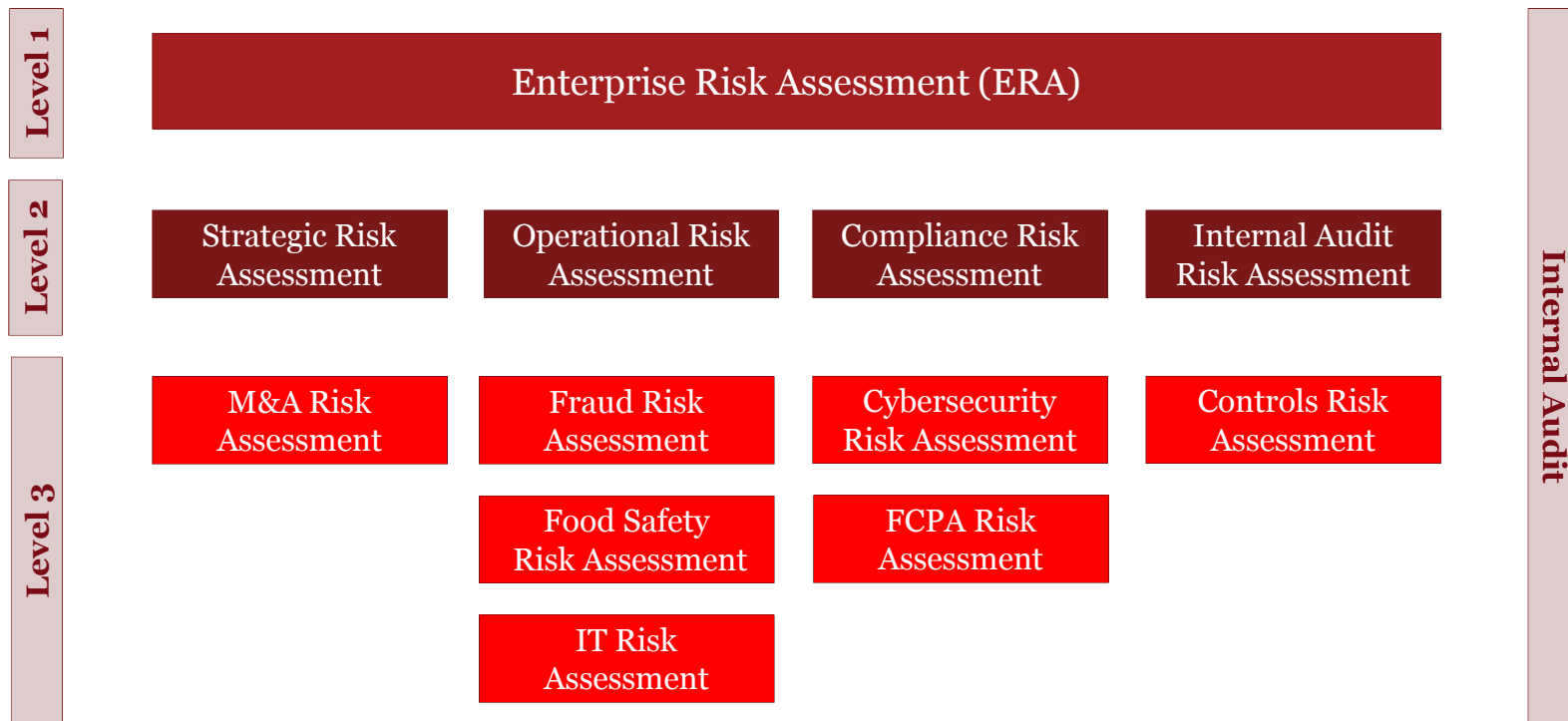
		
<p style="text-align: center;">Hazard</p>	<p style="text-align: center;">Uncertainty</p>	<p style="text-align: center;">Opportunity</p>
<p>Threat of loss - an event may occur and negatively impact the achievement of objectives - Response tends to be reactive.</p>	<p>Risk of variability and possibility that an event will occur causing actual outcome to differ from desired objective - Response tends to be proactive.</p>	<p>Risk that an event will occur and positively impact the achievement of objectives - Response is opportunistic.</p>

Approach to Designing Internal Controls

Risk Assessment

Risk Assessments provide a consistent and integrated approach to consider how potential events might affect the achievement of objectives in terms of probability and impact.

Below are **examples** of Level 2 and Level 3 risk assessments that may be performed.



Approach to Designing Internal Controls Risk Assessment

The risk assessment process should:

- Identify objectives for area under review;
- Consider external and internal factors that could impact achievement of such objectives;
- Consider fraud and technology;
- Analyze the risks (impact and likelihood);
- Serve to prioritize the highest and best use of resources (in terms of auditing identified areas of risk via testing of controls); and
- Result in the identification of controls to meet risks and objectives.

Approach to Designing Internal Controls

Each control should be:

- Mapped to a specific risk and control objective;
- Defined in terms of control design and risk level;
- Detailed (i.e., when, who, what, why, how); and
- Drive the nature, timing and extent of audit procedures based on risk rating.

Approach to Designing Internal Controls

1. There are two categories of **internal controls**:

- Preventative
- Detective

2. There are four types of controls:

- Application Controls
- IT Dependent Manual Controls
- Manual Controls
- IT General Controls

Companies typically have a mix of each category and type listed above.

Approach to Designing Internal Controls

Design Elements of a Control

How often [**when**] is it performed?

Who performs the control?

What inputs are used to perform the control?

Why is the control performed?

How are exceptions reviewed and approved?

How is the control evidenced?

Activity: Find the elements of the control

Example Control Activity:

On a daily basis, the Payroll clerk receives PAF forms from HR and performs a review of the changes made to employee records in the Lawson application. They indicate their review by initialing the PAF forms. The Payroll Supervisor is responsible for and oversees this process. He indicates his review by signing off on each PAF form.

If the Payroll clerk finds any exceptions, the associated PAF form is returned to HR for correction. The Payroll clerk records the PAF forms returned to HR on a manual Exception log and monitors the time taken to make the correction. Once corrected, the Payroll clerk and Payroll Supervisor sign-off on the Exception log.

Activity: Find the elements of the control

Example Control Activity:

On a daily basis, the Payroll clerk receives Personnel Action Form (PAF) from HR and performs a review of the changes made to employee records in the Lawson application. They indicate their review by initialing the PAF. The Payroll Supervisor is responsible for and oversees this process. He indicates his review by signing off on each PAF.

If the Payroll clerk finds any exceptions, the associated PAF is returned to HR for correction. The Payroll clerk records the PAF returned to HR on a manual Exception log and monitors the time taken to make the correction. Once corrected, the Payroll clerk and Payroll Supervisor sign-off on the Exception log.

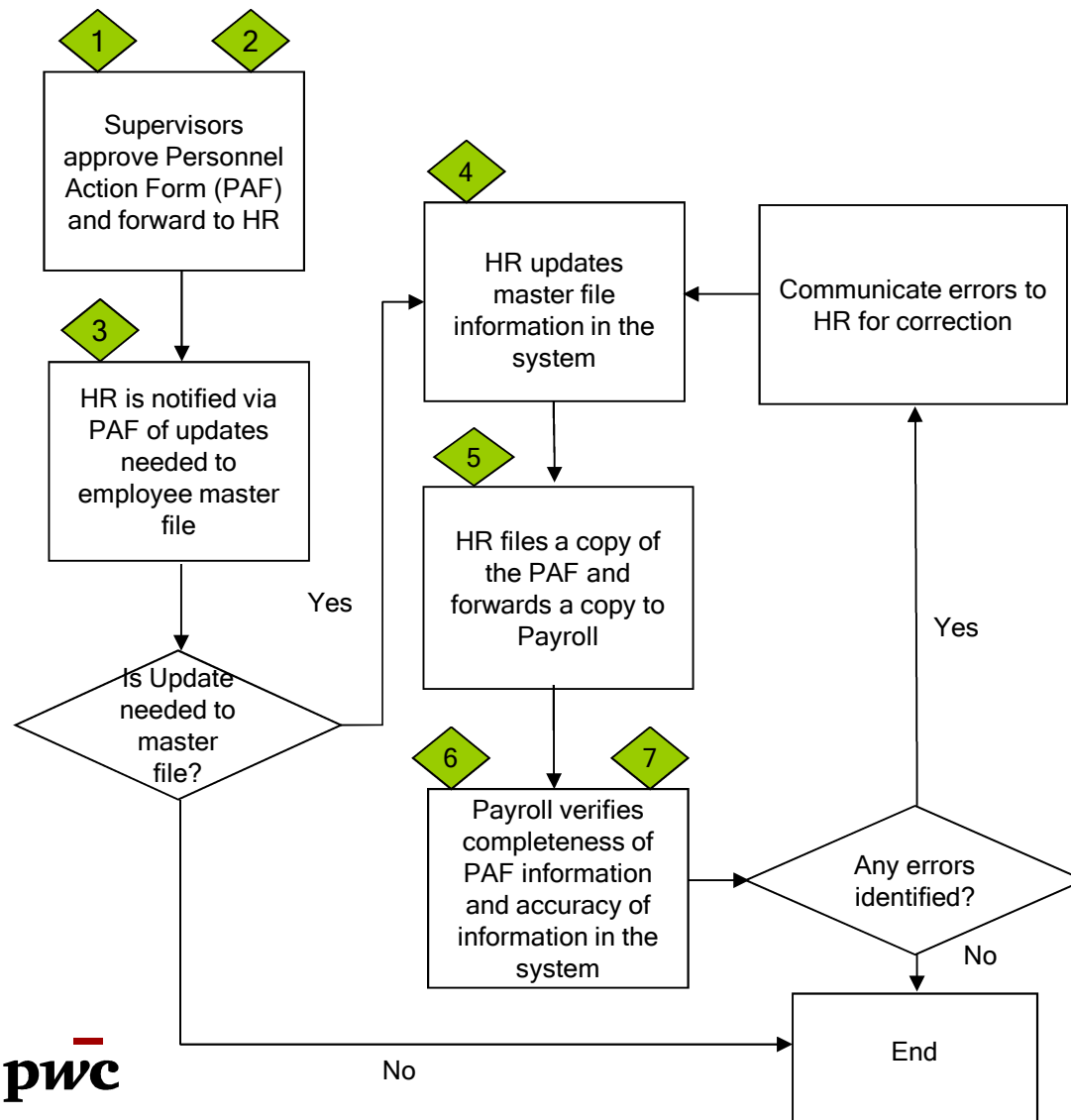
Approach to Designing Internal Controls

What are **Key Controls**?

According to the Public Company Accounting Oversight Board (PCAOB), factors to consider in determining key controls include:

- The likelihood that failure of the control could result in a misstatement.
- The degree to which other controls, if effective, achieve the same control objectives.

Activity: Identifying Key Controls



1. Supervisors approve PAFs and forward to HR. (Completeness, Accuracy)

2. Personnel Action Forms are standardized forms. (Completeness)

3. Approval of PAFs by HR (Validity)

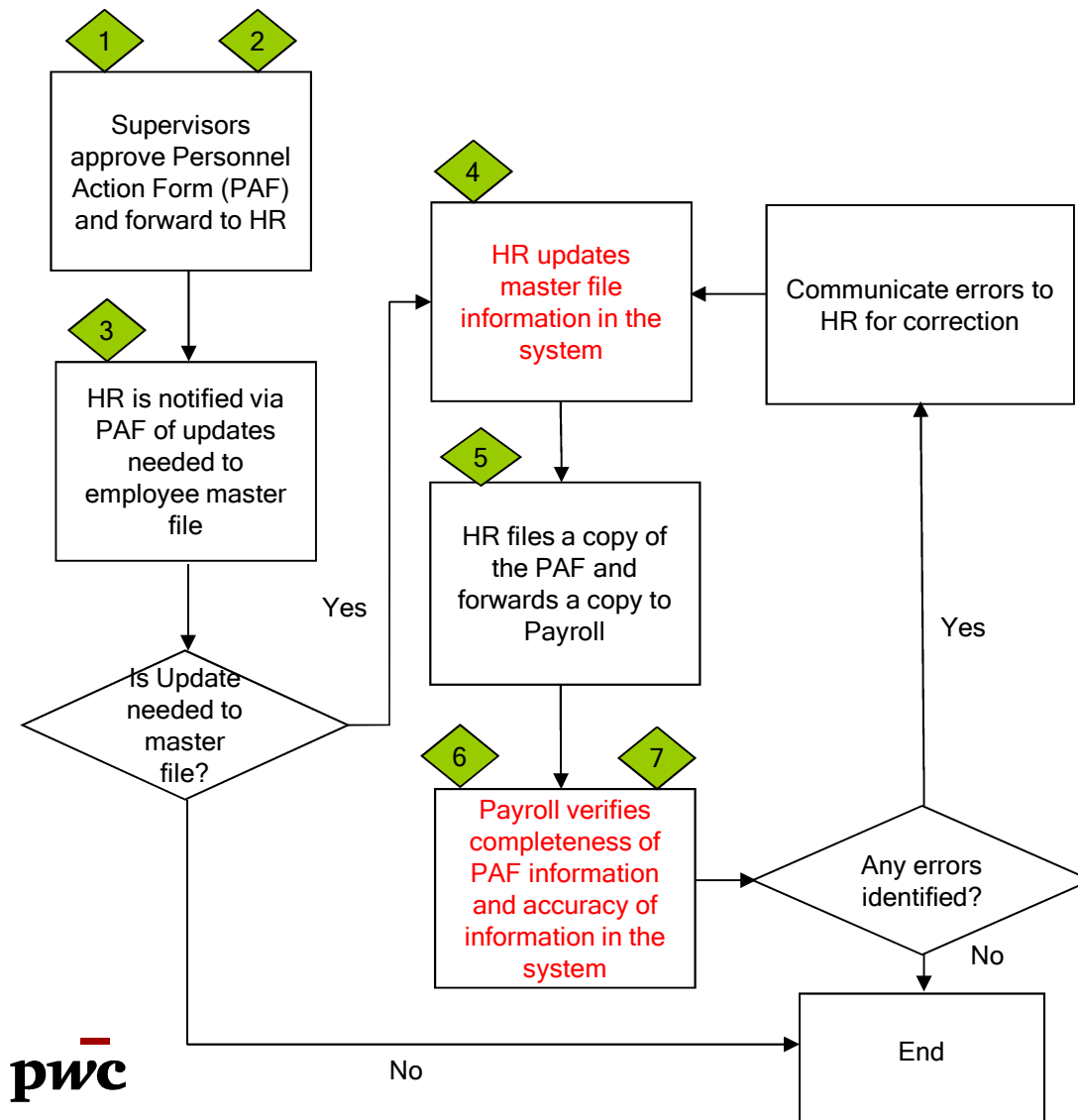
4. Employee set up and updates are restricted to HR. (Restricted Access)

5. Forms are maintained by appropriate Payroll/HR personnel in locked cabinets. (Restricted Access)

6. Independent review of PAF forms / Integrity of data input. (Accuracy, Validity)

7. System edit checks on certain fields. (Accuracy)

Activity: Identifying Key Controls



1. Supervisors approve PAFs and forward to HR. (Completeness, Accuracy)

2. Personnel Action Forms are standardized forms. (Completeness)

3. Approval of PAFs by HR (Validity)

4. Employee set up and updates are restricted to HR. (Restricted Access)

5. Forms are maintained by appropriate Payroll/HR personnel in locked cabinets. (Restricted Access)

6. Independent review of PAF forms / Integrity of data input. (Accuracy, Validity)

7. System edit checks on certain fields. (Accuracy)

Testing Internal Controls

Nature, Timing & Extent of Fieldwork

Once the Controls Risk Assessment has been completed, and controls have been mapped, defined and categorized, testing procedures are defined in alignment with the categorization of risk(s) mapped to each control.



Testing Internal Controls

Nature, Timing & Extent of Fieldwork

The control risk, as well as other elements defined in the Risks and Controls Matrix, assist in determining the nature, timing and extent of audit procedures.

[Example Approach to Determine Nature of Audit Procedures]

Control Risk Level	Example of Nature of Audit Procedures
High	Inspection/Examination and/or Re-performance
Medium	Observation, Inspection/Examination and/or Re-performance
Low	Inquiry, Observation and/or Inspection/Examination

Methodologies should be in place to be used as reference for determining the nature, timing and extent of audit procedures.

Testing Internal Controls

Example of Sampling Methodology

The table below portrays an example of a sampling methodology used to identify the related number of selections to test for operating effectiveness:

Frequency of Control	Assumed Population of Control Occurrences	Number of Items to Test		
		Low	Med	High
Annual	1	1		
Quarterly	4	2		
Monthly	12	2 to 5		
Weekly	52	5	10	15
Daily	250	20	30	40
Multiple times per day	Over 250	25	45	60

Questions?

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.