Risk assessment

Building a better
working world

Agenda

- Introduction to the risk management process
- Risk assessment lifecycle
- Risk assessment and audit planning model
- Internal audit's role in risk management
- Keys to success
- Hot topics and emerging risk considerations

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk management process

- **Risk** is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of **impact** and **likelihood**.
  - Risk management is "a process to identify, assess, manage and control potential events or situations to provide **reasonable assurance** regarding the achievement of the organization's objectives."

Performance Standard 2120
Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk management process (cont'd..)

- **Responsibility for Aspects of Organizational Risk Management**
  - Risk management is a key responsibility of senior management and the board.
    - Boards have an oversight function. They determine that risk management processes are in place, adequate, and effective.
    - Management ensures that sound risk management processes are functioning.
  - Senior management and the board determine the internal audit (IA) activity's role in risk management based on factors such as (1) organizational culture, (2) abilities of the IA activity staff, and (3) local conditions and customs.
    - That role may range from no role; to auditing the process as part of the audit plan; to active, continuous support and involvement in the process; to managing and coordinating the process.
  - The CAE must understand management's and the board's expectations of the IA activity in risk management. The understanding is codified in the charters of the IA activity and the board.
    - If there is no formal risk management processes, the CAE has formal discussions with management and the board about IA duty for understanding, managing and monitoring risks.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk management process (cont'd..)

- **Risk Management Process** includes:
  1. Identification of context;
  2. Risk identification;
  3. **Risk assessment and prioritization**;
  4. Risk response; and
  5. Risk monitoring.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk management process (cont'd..)

- **Risk Management Process …**
  - **Step 3 - Risk Assessment and Prioritization….**
    - Risk modeling is a method of risk assessment and prioritization.
      - This simple model and the resulting risk assessment process can be depicted as follows

EXAMPLE

A chief audit executive is reviewing the following enterprise-wide **risk map**:

IMPACT		LIKELIHOOD		
		Remote	**Possible**	**Likely**
	Critical	Risk A	Risk B	
	Major			Risk D
	Minor		Risk C	

      - Open channels of communication with senior management and the board are necessary to ensure the audit plan is based on the appropriate risk assessments and audit priorities. The audit plan should be reevaluated as needed.
      - Risk modeling in a consulting service is done by ranking the engagement's potential to (1) improve management of risks, (2) add value, and (3) improve the organization's operations.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment lifecycle

The Risk Assessment lifecycle can be classified into six key steps

1

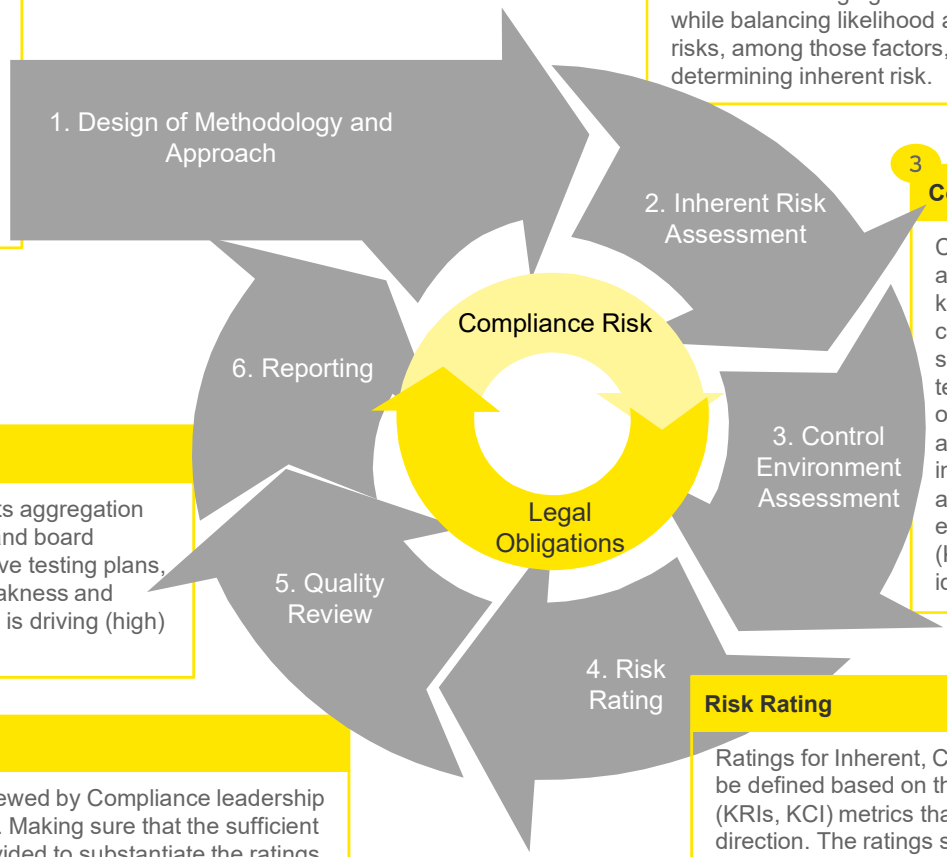
Design of Methodology & Approach

- Determine structure, frequency, and scope of risk assessment necessary to assess the Compliance Risk across products, businesses and geographies including:
  - Legal entities
  - Products and services over the lifecycle
  - Change Management
  - Linkage with Conduct risks through the use of taxonomy

2

Inherent Risk Assessment

Factors that drive risks posed by the laws rules and regulations that organization is obligated towards. Leveraging metrics (KRIs and KPIs) while balancing likelihood and impact of the risks, among those factors, is critical when determining inherent risk.



3

Control Environment Assessment

Compliance officers conduct their assessment based on their knowledge of the business and controls using different inputs (e.g., self-identified issues (RSCA), testing results, findings and observations from external parties, and management of issues and incidents) to enable a fact-based assessment of the control environment. Key Control Indicators (KCIs) should also be levered to identify control weakness.

6

Reporting and Outputs

Determine appropriate levels of results aggregation and roll-ups for senior management and board reporting. The outputs are used to drive testing plans, enhancement to identified control weakness and review of the risk-taking activities that is driving (high) risk.

5

Quality Review

The initial responses are reviewed by Compliance leadership for consistency and accuracy. Making sure that the sufficient documentation has been provided to substantiate the ratings.

4

Risk Rating

Ratings for Inherent, Control and Residual risks should be defined based on the qualitative and quantitative (KRIs, KCI) metrics that objectively inform the risk direction. The ratings scale should enable consistency and comparability across the organization.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model

Several factors to consider when performing the risk assessment process as it ultimately drives internal audit's audit plan.

- "Bottoms-up" risk assessment demonstrates an appropriate understanding of the audit universe and an assessment of key risks which are prioritized.
- "Top-down" risk assessment helps gain an understanding of overall enterprise priorities and associated risks.

Top down risk assessment

- Economic factors
- Regulatory environment
- Technology and other change
- Changes in risk management
- Changes in risk appetite
- Focus on risks that matter
- Comprehensiveness of risk assessments
- Recognition of impact to value drivers
- Coverage of emerging risks

Auditable unit risk assessments | Mandated audits | Audits driven by coverage | Themes and significant risks | Additional coverage for opinion | Legal entity risk assessments

Bottoms-up risk assessment

- Audit universe
- Impact and likelihood of occurrence
- Process change factors
- Control effectiveness
- Residual risk
- Recent operational events
- Risk appetite
- Materiality factors
- Risk control self assessments

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

Information gathering

- Review prior year's internal audit results, industry trends, recent regulatory rulings, and business/technology environment changes
- Identify and interview key stakeholders to obtain an understanding of current goals, critical success factors, strategies, and risks
- Obtain Management's perspective on potential internal audit focus areas and define the audit universe

Risk assessment

- Identify, assess, and document inherent, control, and residual risks for each auditable unit
- Determine the overall residual risk rating per auditable unit and identify target short-term reviews to include within the annual internal audit plan.
- Prepare an internal audit risk assessment summary and design a proposed three or four year rotational internal audit plan based on residual risk

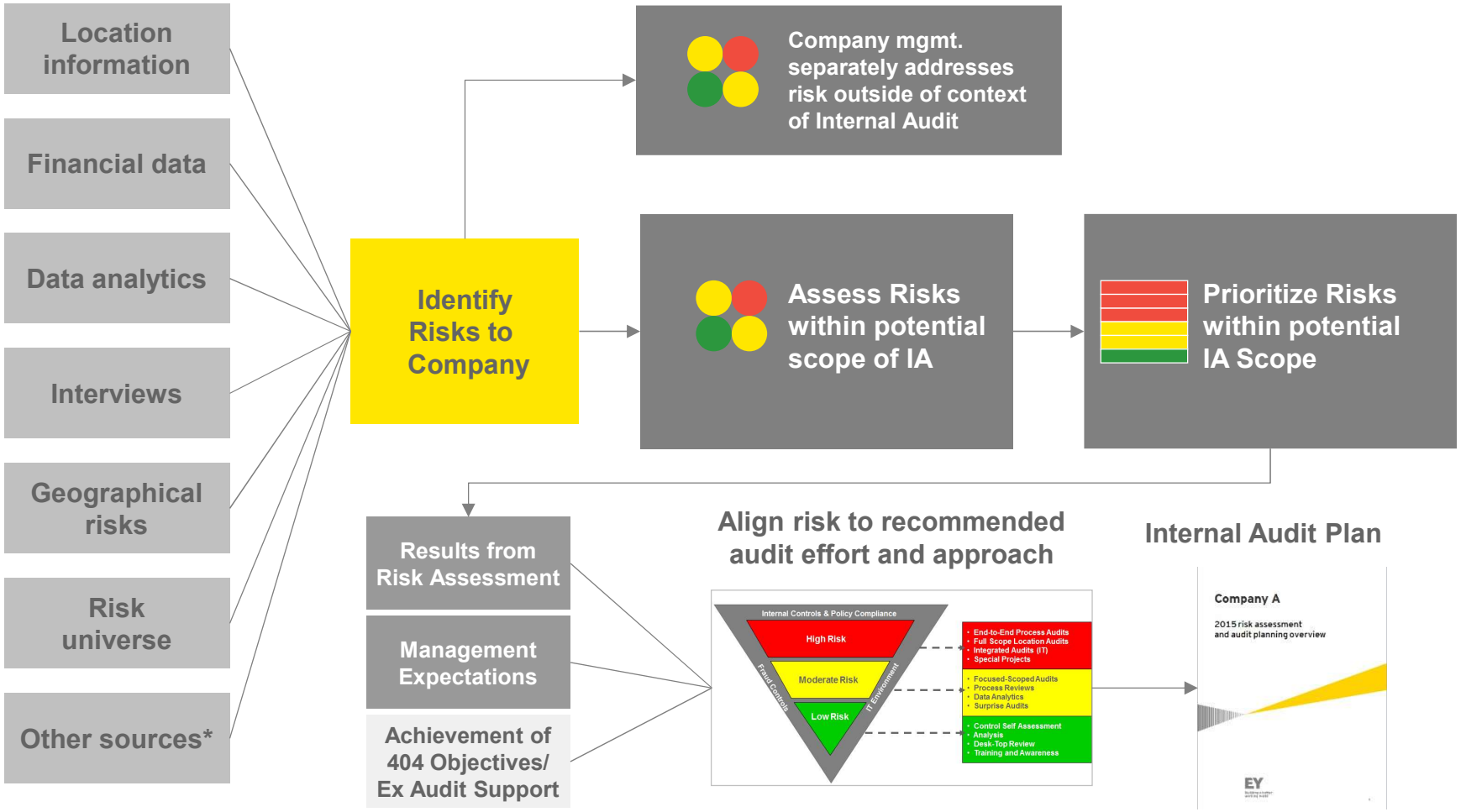
Prepare internal audit plan

- Develop an internal audit plan that aligns with the risk profile of the organization
- Review the internal audit plan with Management to agree on coverage
- Present internal audit risk assessment results and the internal audit plan to the Audit Committee

- Focus audit resources to the areas of highest risk and value
- Gain insight from key stakeholders to uncover and identify risks
- Gain insight from sources outside of the organization to understand risks that may impact your organization.
- Establishment of a risk criteria matrix that defines what would constitute a high, moderately high, moderate or low risk

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)



** Third party service providers, mega trends, market analysis, etc.*

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

- **Location information**
  - Traditional rotational analysis
    - Remains in place as one of several guidelines/factors used to determine the internal audit scope each year.
    - While the rotation analysis has a significant impact on the overall audit plan development, judgment is used when considering the overall spectrum of other risk assessment inputs – accordingly, departures from the rotation analysis may sometimes occur to accommodate other priorities.

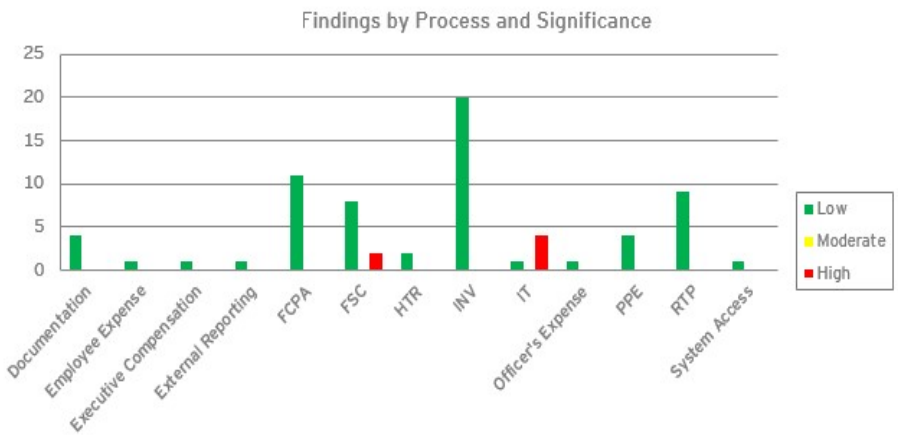
Location/BU	Division	2017 Sales	Internal audit frequency	2012	2013	2014	2015	2017 Plan	2018 plan needed to achieve frequency
North America	All		Annual	●	●	●	●	✓	✓
Asia	All		Annual	●	●	●	●	✓	✓
EMEA	All		Annual	●	●	●	●	✓	✓
Korea	CDT		Annual	n/a	n/a	n/a	HC	✓	✓
Tainan & Taichung	CDT		Annual	●	●	●	●	✓	✓
China	CSM		Annual	●	●		●		✓
China	CDT		2 Years		●	●		✓	
OFC	COC		2 Years	●		●		✓	

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

- **Location information (cont'd..)**
  - Key changes
    - Information technology risks and changes
    - Employee turnover analysis
  - Prior year results
    - Internal audit results and control gap trend analysis
    - Aggregated results
  - Corporate process risk analysis
    - The complexity of each proces combined with materiality and emerging risk considerations were reviewed and analyzed

Location - Key Employee Turnover Analysis					
Location Name	New External Hire Plant Controller or Plant Manager	Small Location (under $100m in sales)	Integrated into SSC	Date of last audit	Inclusion in 2018 Plan
Reynosa, MX	PM & PC	No	Yes	2014	Yes
Poland	PM	Yes	Yes	2011	No
Middlton	PC	Yes	Yes	2014	No
Toronto	PC	No	Yes	2012	No
Brazil	PC	Yes	No	2014	Yes



© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

- **Financial data**
  - Significant location
  - Materiality coverage analysis
    - Account level materiality
  - Trial balance analysis

COMPANY				
Materiality Assessment				
**** Based on FYXX Financial Information as of 2/22/XX**				
MATERIALITY CALCULATION				
	TOTAL			
Pretax Income	$ 23,508,000			
Interest	$ 9,992,000			
Depr & Amort	$ 5,000,000			
EBITDA	$ 40,000,000			
Gross Profit	$ 100,000,000			
Materiality	2%	2.5%	3%	3
Pretax Income	$ 23,508,000	$ 23,508,000	$ 23,508,000	$ 2
Planning Materiality Level	$ 470,160	$ 587,700	$ 705,240	$
Tolerable Error @ 50%	$ 235,080	$ 293,850	$ 352,620	$
Tolerable Error @ 75%	$ 352,620	$ 440,775	$ 528,930	$
SAD/P&L De Minimus Posting Level (5% of planning materiality)	$ 23,508	$ 29,385	$ 35,262	$
Balance Sheet Reclassification De Minimus Posting Level (set at Tolerable Error @ 75%)	$ 352,620	$ 440,775	$ 528,930	$

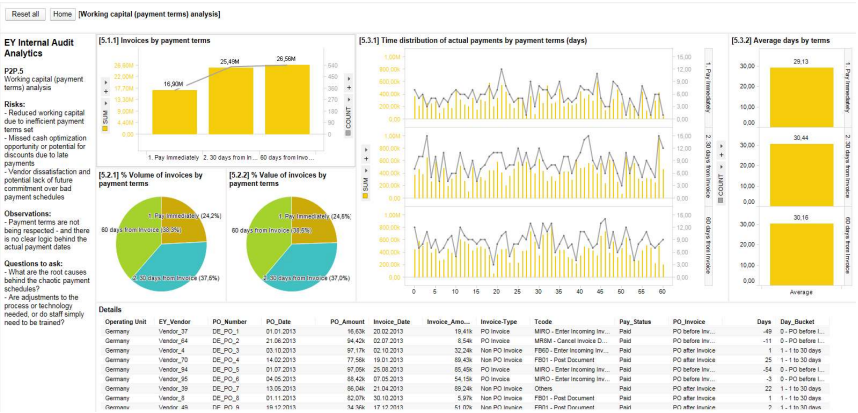
Locations with sales representing over 5% of total incorporated sales

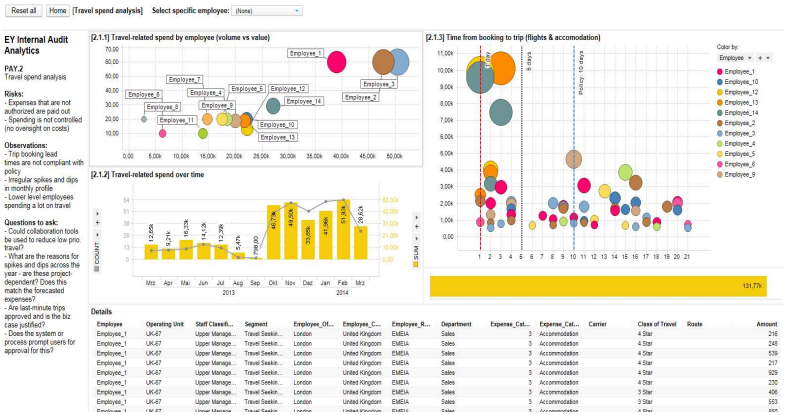
Location	Net sales amount	% of Total sales ($40b)	Location included in 2018 Plan
Korea	$5b	12.5%	✓
Taiwan	$3b	7.5%	✓
Illinois	$1b	2.5%	
Mexico	$600m	1.5%	
Canada	$500m	1.25%	

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

- **Data analytics**
  - Risk Assessment Dashboards
    - Metric-driven real-time reporting based on key risk indicators that are forward-looking
    - Identify risk assessment priorities
    - Determine scope of audit plan activities





© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

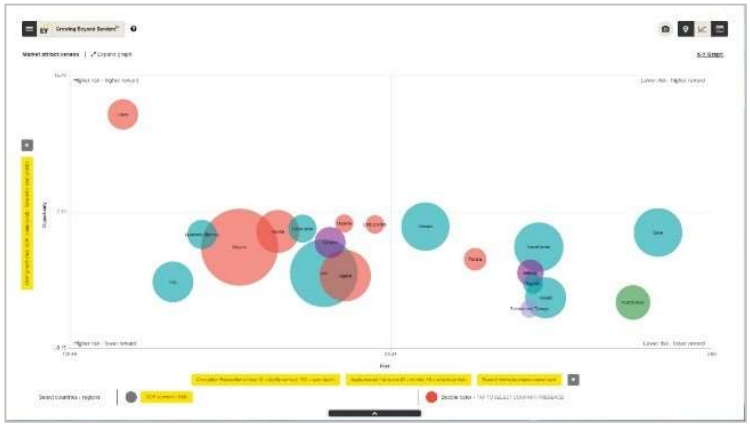
► Interviews:

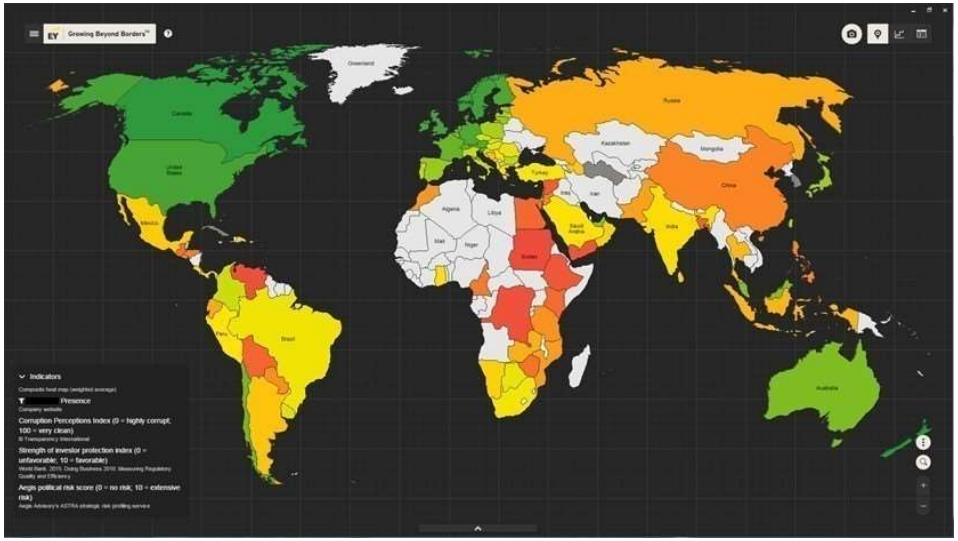
	Focused interviews: Top down	Virtual interviews: Bottom up	Risk assessment: Merge results
Activities	► Individual interviews with key executives ► Understand key strategic initiatives ► Understand Executive perspectives on risk	► Real-time virtual sessions by business units to allow for expanded participation ► Select risks from the company's predefined risk universe ► Identify additional risks ► Gain participants' insights on impact, likelihood and management capabilities	► Qualitative analysis of the information obtained ► Management perspectives on organizational risks ► Risk ranking based on likelihood and impact to the organization and relevant business unit
Enablers	► Risk Universe	► Questionnaire	► Risk heat maps
Outputs	► Top risks ► Risk priorities ► Upcoming initiatives	► Top risks ► Detailed listing of all risks identified and corresponding ranking	► Prioritized audit plan ► Audit committee reporting (themes, risks, results)

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

- **Geographical risks**
  - Fraud risks as part of the risk assessment
    - An analysis to determine that appropriate internal audit "coverage" is achieved in geographies with a high rate of fraud and corruption
  - Market data
  - Geopolitical issues





© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Risk assessment and audit planning process model (cont'd..)

- **Risk universe**
  - Industry and company risk universe
    - Level of input varies based on the established Enterprise Risk Management function
    - Refreshed based on stakeholder inputs and changes in the market impacting the organization

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

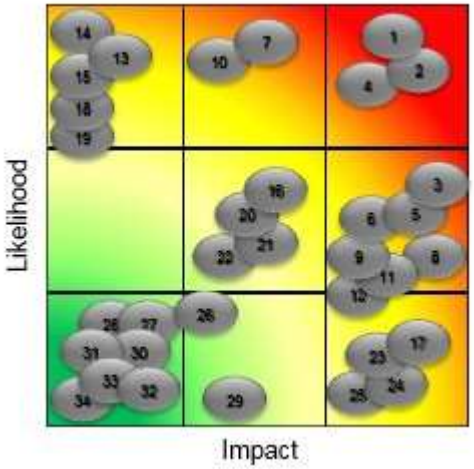
Risk assessment and audit planning process model (cont'd..)

- **Internal audits role**
  - Assess Risks within potential scope of IA
  - Prioritize Risks within potential IA Scope
    - Identify and rank risks
    - Consider management's risk appetite
    - Industry/regulatory requirements

Dashboards and reports

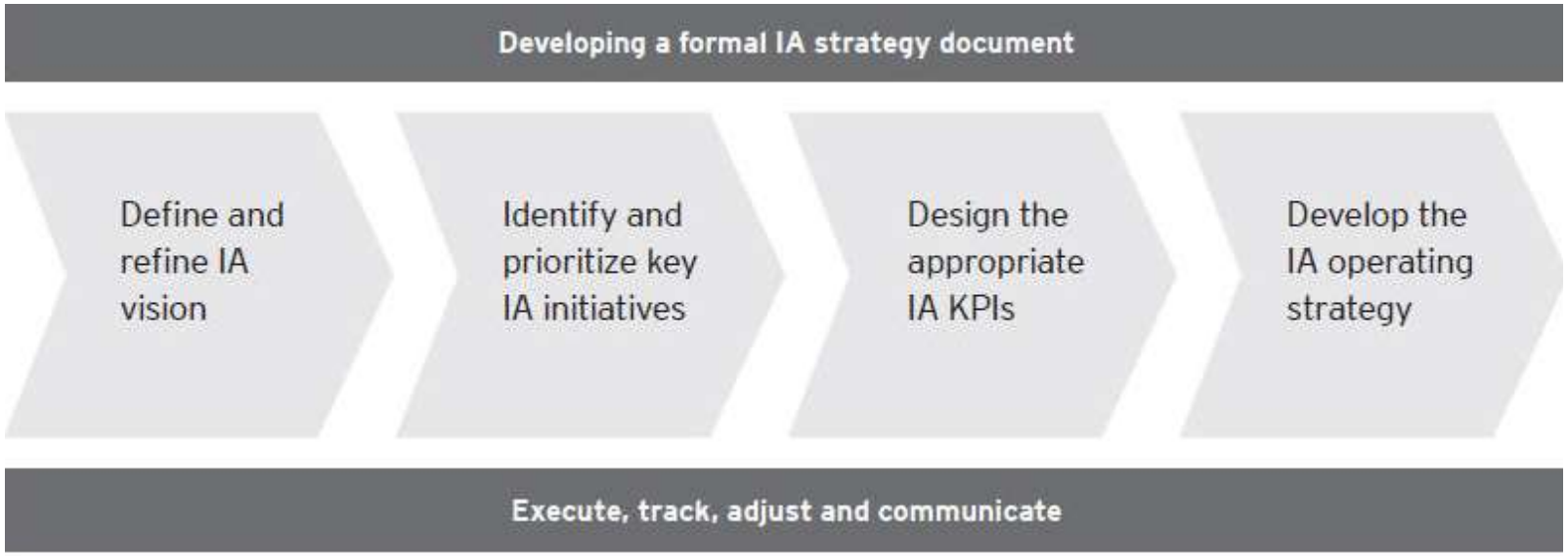
e.g., incident tracking, fact pact reviews, scenario analysis, workflow monitoring, etc.

- **Risk assessment results**
  - Annual audit plan
  - Risk heat map



© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Internal audit's role in risk management



- Risks identified are ranked and mapped back to management's ERM framework in order to decide which risks will be included in the IA audit plan.
- The audit plan is created with the consideration of management's risk appetite and the risk rankings in mind to develop a comprehensive testing approach/plan.
- Industry also plays a large part in what belongs in the audit plan. Some industries, such as banking or healthcare, have unique regulatory requirements (separate from risks identified) which belong in the audit plan as well.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

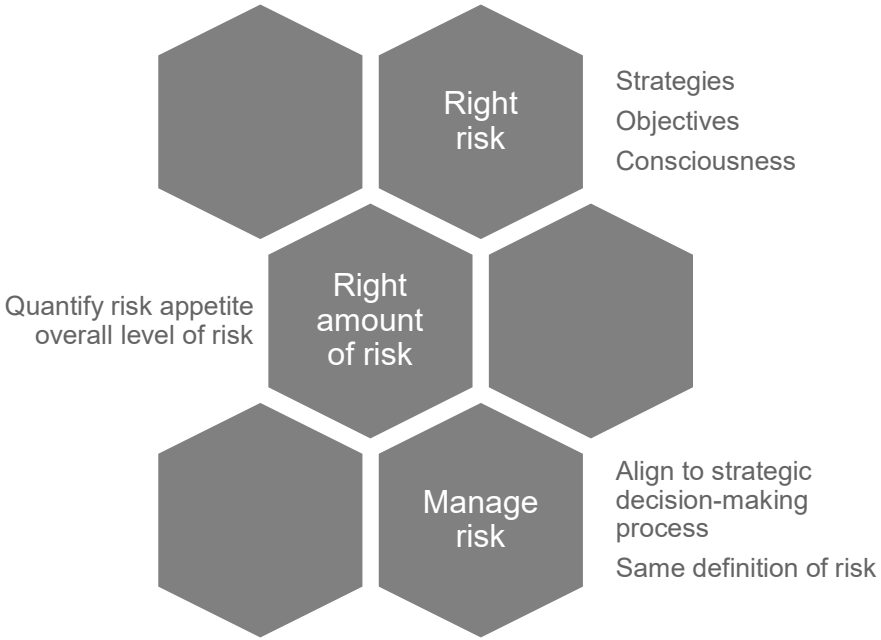
Internal audit's role in risk management (cont'd..)

- Internal audit activity
  - Alerts management to new risks or inadequately mitigated risks.
  - Evaluates risk management process
  - Provides recommendations and action plans for risk responses (e.g. accept, transfer, avoid)
- The internal audit actively performs its own risk assessments
  - Discussions with the board permit alignment of recommended risk responses with the risk appetite
- Assurance roles provided by the internal audit activity
  - Giving assurance on the risk management process
  - Evaluating the risk management process
  - Reviewing the management of key risks
    - E.g. When management decides to accept risk, the CAE must determine whether this is appropriate. If the CAE concludes that management has accepted a level of risk that is unacceptable, then CAE must discuss with senior management and may need to report to the board.

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Keys to success

- Buy-in from senior leaders on risk prioritization and rankings is essential for support of the audit plan and future actionable items
- Consistent application of rating criteria
  - Inherent vs. residual ratings
    - Apply ratings with a baseline of effective controls, and then adjust rating up (worsening) if controls exceptions or gaps are known or discovered



© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

Hot topics and emerging risk considerations

The pace of change today is faster than it has ever been ever before – yet it is slower than it will ever be again in the future. We continue to adapt the audit plans accordingly to stay in front of new risks – while not losing sight of the traditional risk areas of the past. What emerging risks do you believe warrant increased attention today?

- Technology architecture
- Scaling of Robotics Process Automation (RPA) technologies
- Internet of Things (IoT) – connected assets
- Information protection, data governance and classification
- IT security including ransomware response planning
- Cloud technology migration plans
- ERP upgrades and other new technology releases
- EU General Data Protection Regulation (GDPR)

- Leases
- Revenue recognition
- Accounting policy governance over acquisitions
- Non-financial reporting
- Identity and access management controls
- IT segregation of duties
- Mergers, divestitures and acquisition integration
- Digital supply chain optimization
- Business continuity and crisis response planning
- Large capital programs
- Third-party risks

- Taxes, tariffs and duties
- Non-GAAP reporting
- Financial statement close
- Planning and forecasting
- Cash flow forecasting
- Cost reduction programs
- Payables management optimization
- Derivatives and hedging/foreign exchange
- Financial metrics and KPI monitoring
- Risk culture reviews
- Fraud, corruption and FCPA compliance

- Human capital and cross border succession planning
- Workforce training
- Reputational risk scans/crisis management
- Executive compensation and proxy disclosures
- Pay parity assessments
- VAT/GST sales tax
- Indirect tax
- Corporate tax planning, transfer pricing and provisions
- Business partner compliance
- Shared service centers

© EYGM Limited 2018. All rights reserved. Confidential & Proprietary. Subject to Contract.

EY

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2015 Ernst & Young LLP.
All Rights Reserved.

1508-1612242
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Sarbanes-Oxley (SOX) 101
(Internal Controls)

EY
Building a better working world

Table of Contents

1 Introduction

2 Setting the Context

3 Control Execution

4 Audits

5 SOX Program Structure

Table of Contents

1 **Introduction**
What is Sarbanes-Oxley (SOX)?

2 **Setting the Context**

3 **Control Execution**

4 **Audits**

5 **SOX Program Structure**

What is SOX?

- The Sarbanes-Oxley Act (SOX) (named after senators Sarbanes and Oxley) was passed in 2002 as a result of several corporate scandals that occurred in earlier years, including Enron, WorldCom and Parmalat

The Benefits

- Provides assurance to management on the accuracy of the financial statements
- Reinforces internal controls
- Identifies weaknesses and leads to rapid remediation due to firm timelines
- Meets our obligation to our shareholders

Paradigm Shift

- Increase the accountability of management
- Improve Corporate Governance
- Oversight of Public Accounting firms
- Restore investor confidence in capital markets

Application Scoping

- Driven by business processes
- IT applications used for financial reporting or calculations in support of key business controls need to be visited from a scoping perspective

Affects all companies with debt or equity listed on the US stock exchange

Table of Contents

1 Introduction

2 Setting the Context
Why should you care?

3 Control Execution

4 Audits

5 SOX Program Structure

Stock Impact of SOX

Overview:

As a shareholder, non-compliance with SOX can have a significant impact on your stock price!

-4.06%

Stock Impact - Material Weakness:

Average 60 day stock price impact resulting from material weakness classification resulting from lack of internal control.

-3.02%

Stock Impact – Deficiencies:

Average 60 day stock price impact resulting from reported deficiencies resulting from lack of internal control.

Metrics defined above were concluded by **www.CFO.com** in the following article:
http://ww2.cfo.com/risk-compliance/2005/07/how-markets-punish-material-weaknesses/

Risk & Controls: Definitions

What is a **risk**?	Anything that can impede the achievement of management objectives
What is a **control objective**?	Control objectives are a category of controls that would satisfy an objective, i.e. controls around managing access, managing changes, managing IT operations
What is a **control**?	Any action taken by management to manage or address the risks identified in a process
What is an **IT general control?**	IT General Controls are common controls that can be applied to IT systems such as applications, operating systems, databases, and supporting IT infrastructure.

Example of Control Objective: Restrict Access to Appropriate Users

Control Objective 1:

Password Setting

Control Objective 2:

New User Access Provisioning

Control Objective 3:

User Access Review

Risks and Controls - Examples

Risk:

Inadequate authentication and security settings

Risk:

Inappropriate access to users in the IT environment without proper authorization

Risk:

Users of the IT environment are not authorized, because requests for removal of unneeded access of IT personnel are not made timely or access action requests fulfilled inaccurately or ultimately

Example of Control Objectives: Restrict Access to Appropriate Users

Control 1:

Password Settings are reviewed against Passord Policy. Any deviations are corrected and exceptions to deviations are approved

Control 2:

Appropriate approvals are obtained prior to provisioning access to new users

Control 3:

Access to existing users on the system are reviewed on a periodic basis. Inapropriate access is identified and removed

Operational vs. SOX Risk

Operational Risk

Are risks that are procedural in nature and would impact the **day-to-day operations** of the enterprise.

Example:

Risk of insufficient customer identity verification.

SOX Risk

Are risks that are financial in nature and would impact the **financial statements** of the enterprise.

Example:

Risk of unauthorized personnel creating fictitious orders.

Classification of Controls

1

Manual Controls

Performed manually; Not performed by the system and not reliant on system generated information

2

IT Dependent Manual Controls

Manual controls that use system-produced information. Since the manual control relies on system-produced information or reports, it is important that controls are in place to ensure that the system-produced information is complete and accurate

3

Application Controls

Performed solely by the computer with no manual intervention

Manual Controls

IT-Dependent Manual Controls

Application Controls

PREVENT — **Control Objectives** — DETECT

Preventive Control
Controls designed to avoid errors in transactions before they occur

Example: User's access is approved by an appropriate individual prior to access being provisioned

Detective Control
Controls designed to find errors in transactions after they have occurred, typically performed on a periodic basis

Example: All user's access are reviewed every quarter to determine appropriateness.

In-Scope Applications

Overview:

An IT application which supports a key business process or business control in a material manner.

An example of an In-Scope Application: **Billing Application**		An example of **IT General Control (ITGC):**
Business Process	In-Scope Application's Role	
Manage Customer Billing The primary purpose of this process pertains to effective management of the customer's billing account as it relates to the products purchased and consumed throughout the appropriate billing cycle. This process focuses on managing changes to the customer's billing account (for example, customer billing address, etc.) as it relates to the customer's service portfolio, such as ensuring that the correct purchased products are assigned to the customer's billing account for accurate billing.	**Billing Application Customer Billing:** Billing Application is responsible for creating customer invoices.	**Access** to existing users **on the system** are **reviewed** on a **periodic basis.** Inappropriate access identified is removed.

Supporting Tools

Overview:

A tool which supports key IT SOX control in a material manner.

An example of an In-Scope Supporting Tool: **OIM**		An example of **IT General Control (ITGC):**
IT SOX Control **Control Description:** On a semi-annual basis, individuals with Admin access to the OIM application are reviewed to ensure access is appropriate based on the user's job responsibilities. Inappropriate access identified as part of the review is removed.	→	Supporting Tool's Role **OIM's Role:** OIM receives information of full time employees, contractors, service partners etc. from source systems, and provisions access to Active Directory, Billing Application, POS and SAP	**Administrative access** to users **on the supporting tool** are **reviewed** on a **periodic basis.** Inappropriate access identified is removed.

Corporate Governance – Three lines of defense

First line of defense

Business

- Define product- and flow-specific controls
- Assess control effectiveness
- Provide inputs for control definitions and thresholds
- Monitor and escalate business level control breaches

Technology - Application Support

- Implement business and system controls
- Monitor business and system controls
- Establish Change Management controls
- Implement infrastructure controls and provide support
- Provide incident management support
- Execute incident management activities

Second line of defense

Governance Risk and Compliance

- Provide regulatory oversight for control definition and implementation
- Provide market risk oversight for controls, and evaluate adequacy and effectiveness
- Provide operational risk oversight for controls and evaluate adequacy and effectiveness
- Provide regulatory advice on technology related controls

Third line of defense

Internal Audit

- Perform periodic control audits across all applicable categories of controls
- Monitor key risk indicators on an ongoing basis

Table of Contents

1 Introduction

Setting the Context 2

3 Control Execution
Requirements & Operation

Audits 4

5 SOX Program Structure

Requirements for SOX Compliance

SOX Section 302	SOX Section 404	SOX Section 906	PCAOB Auditing Standard 5	SEC Guidance
Management responsibility over financial and non – financial information in annual and quarterly reports	Incorporation of controls designed to ensure integrity of annual financial statements	Section 906 enumerates the penal clauses for incorrect reporting of financial information by certifying officers	AS5 provides governance and guidance for audit of internal controls having effect on financial reporting	SEC guidance uses a top-down, risk-based approach to identify and focus on areas of highest risks leading to material misstatement of financial statements

The Public Company Accounting Oversight Board

Control Execution & Ownership

Control VP

- Accountable for overseeing the control operation and execution.
- Ensure all processes that fall under the Control VP have the Control Owner and Control Operator take responsibility and accountability for ensuring operation of the controls and remediation in case of deficiency

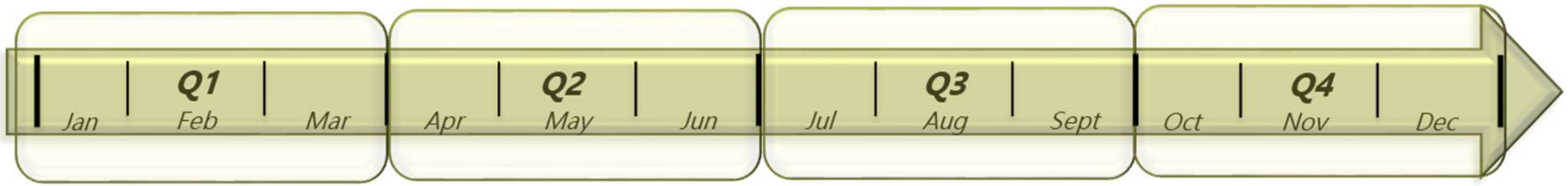
Control Owner

- Individual who confirms the control is an accurate reflection of the current processes in place.
- Accountable to ensure remediation of controls identified with deficiency and communicates with the SOX Governance on remediation plan
- Certifies that controls have been operating as required in the quarterly SOX 302 attestation

Control Operator

- Operates the control based on the agreed-upon frequency
- Responsible to make sure the Control Owner is aware of any issues or observations identified during the control observation and loop in SOX Governance as required.
- Responsible to respond to deficiencies and action on the remediation plan

Control Frequency and Audit Calendar



Half 1 **Half 2**

Periodic Controls

Review controls are performed at a point-in-time and may include the following frequencies:

- **Annual** - The control is executed once a year
- **Semi-Annual** - The control is executed twice a year, once every 6 months
- **Quarterly** - The control is executed 4 times in a year, once every quarter
- **Monthly** - The control is executed once a month
- **Weekly** - The control is executed once a week

Event Driven / Continuous

The execution of this control is not performed on a defined schedule:

- **Event Driven** – The execution of this control is triggered by an event where the frequency is undefined and variable
- **Automated/Continuous** – The control is continuously executed in an automated manner

Common Focus Areas in Control Execution

Establish Completeness of Population

- Provide sufficient evidence to show that the population or the report extract used in the operation of the control is complete and accurate
- Ensure all applications relevant to the control have been included.
- Perform a check against the Master Database and Master Server listing to ensure all in-scope databases/servers relevant to the control have been included in the control execution.
- Ensure all scripts used in generating key reports during the control execution have been baselined. Any changes to the script require it to be re-baselined.

Precision of Review

- Provide attention to detail in the review process and determine whether access and the roles associated to the user is appropriate and that no terminated users are attested to keep access.

Segregation of Duties (SOD)

- Verify that reviewer is not reviewing his/her own access to prevent a segregation of duties conflict
- Obtain approval from a level higher to avoid SOD conflict

Human Error and Sensitive Info Disclosure

- Provide attention to detail on manual errors in formulas as they could lead to failure in operating the control correctly.
- Sensitive information such as passwords should be securely concealed and not be included in the evidence package

Execution Timeliness

- Timeliness in execution and completion of controls should be kept in mind, especially for time sensitive controls such as Weekly, Monthly, Quarterly or Semi-Annual controls

Table of Contents

1 Introduction

Setting the Context 2

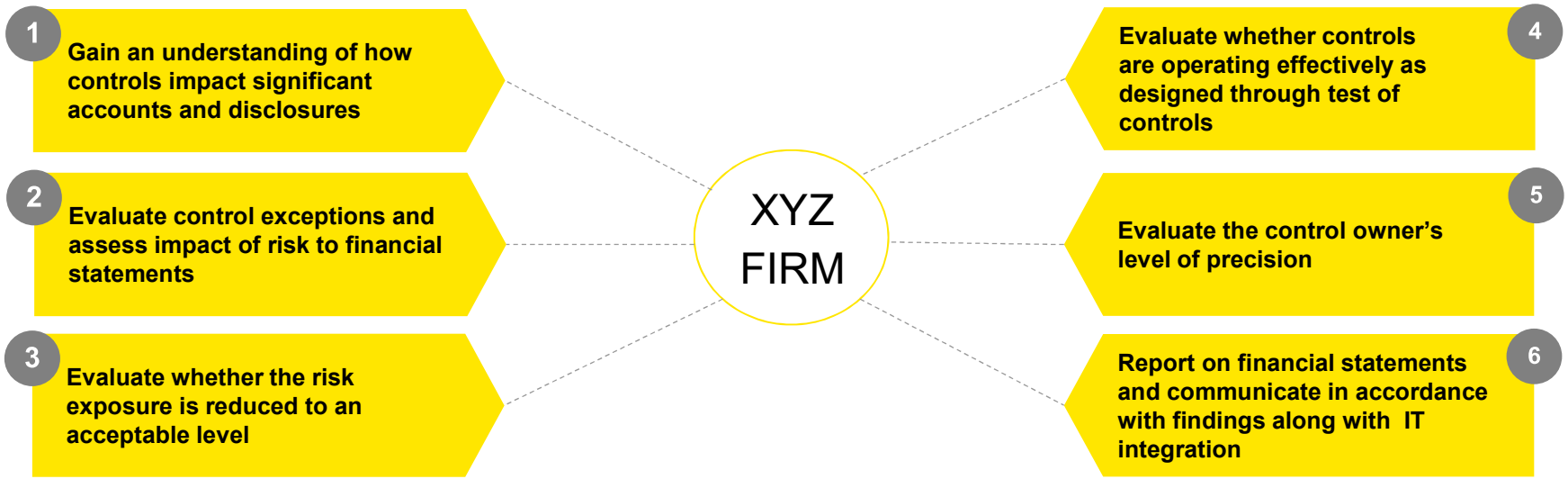
3 Control Execution

Audits 4
Purpose & Resulting conclusions

5 SOX Program Structure

Auditor's Responsibilities

Our auditor's must obtain **reasonable assurance** about whether the financial statements as a whole are free of material misstatement, whether due to fraud or error, thereby enabling auditors to express an opinion on whether the financial statements are prepared and presented fairly, in all material respects, in accordance with an applicable financial reporting framework.



Control Exception, Deficiency & Remediation

When a control deviation occurs, the following classifications and processes may result:

Exception

- An internal control exception occurs when the control that was tested did not operate as intended

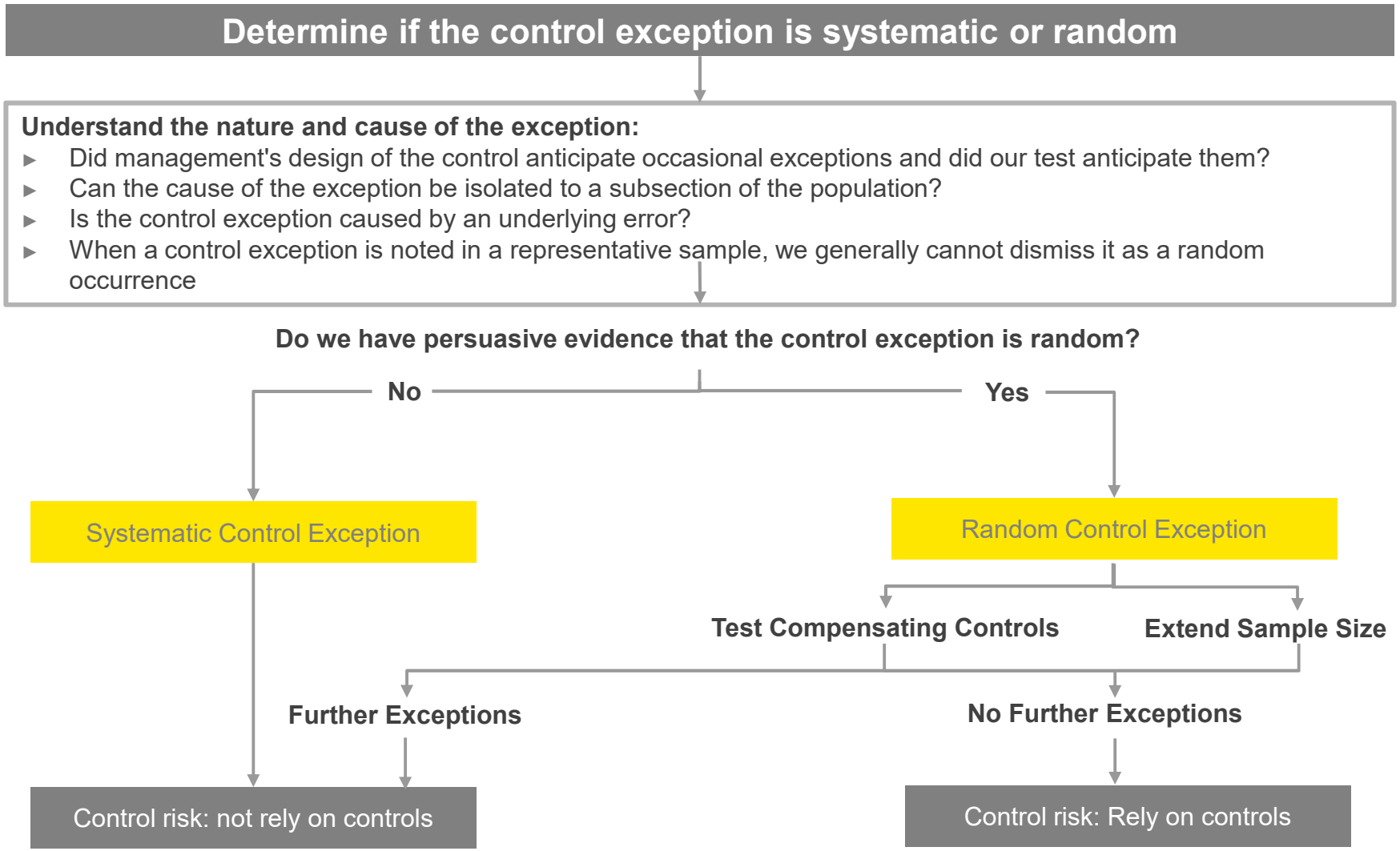
Deficiency

- When the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis

Remediation

- The process of fixing a control so that the exceptions and deficiencies identified may not re-occur

Evaluating Exceptions



Control Deficiency – Next Steps

Assess

- Identify and evaluate possible responses to risk and impact on financial statements
- Evaluate options in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood

Remediate

- Work with Control Owners and Operators to identify root cause leading to the deficiency
- Formalize a remediation plan
- Implement remediation plan
- Verify control is operating effectively
- Work with Governance/Internal Audit/External Audit to confirm Control Remediation

Monitor

- Monitor controls to make sure they continue to operate effectively since agreed upon remediation date

Control Deficiency Aggregations

1. **What is a Deficiency?**
When the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis

2. **What is a Significant Deficiency?**
A control deficiency, or combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected

3. **What is a Material Weakness?**
A significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected

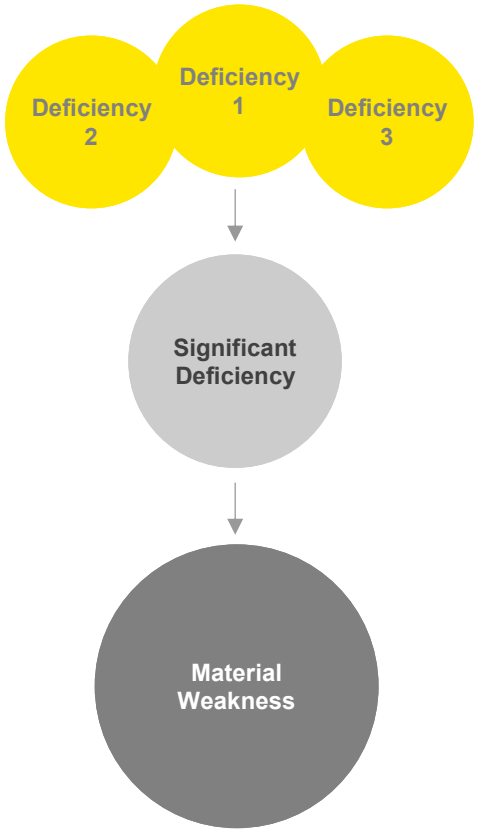


Table of Contents

1 Introduction

2 Setting the Context

3 Control Execution

4 Audits

5 SOX Program Structure
Introduction to the Team & Roles

SOX Program Structure

Control Execution & Ownership	SOX Governance / Compliance Team	Audit Groups
Control VP's	SOX Governance Team	Internal Audit
Control Owners		External Auditor
Control Operators		

SOX Governance's Responsibilities

Leadership

- Responsible for setting the "tone at the top" that affects integrity and ethics and other factors of a positive control environment

Direction

- Provide leadership and direction for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions

Accountability

- Accepts responsibility for the effectiveness of internal control over information technology
- Accountable when a control is determined deficient
- Ensuring timely completion of periodic review controls

Accountability

- Assess the impact of risk as a result from control deficiency
- Support the control operators and owners in the remediation process

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2017 Ernst & Young LLP.
All Rights Reserved.

SCORE no. 01606-171US

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com