The Institute of Internal Auditors

Pittsburgh Chapter

Perspectives on Risk Assessment

February 2013

Ernst & Young

Quality In Everything We Do

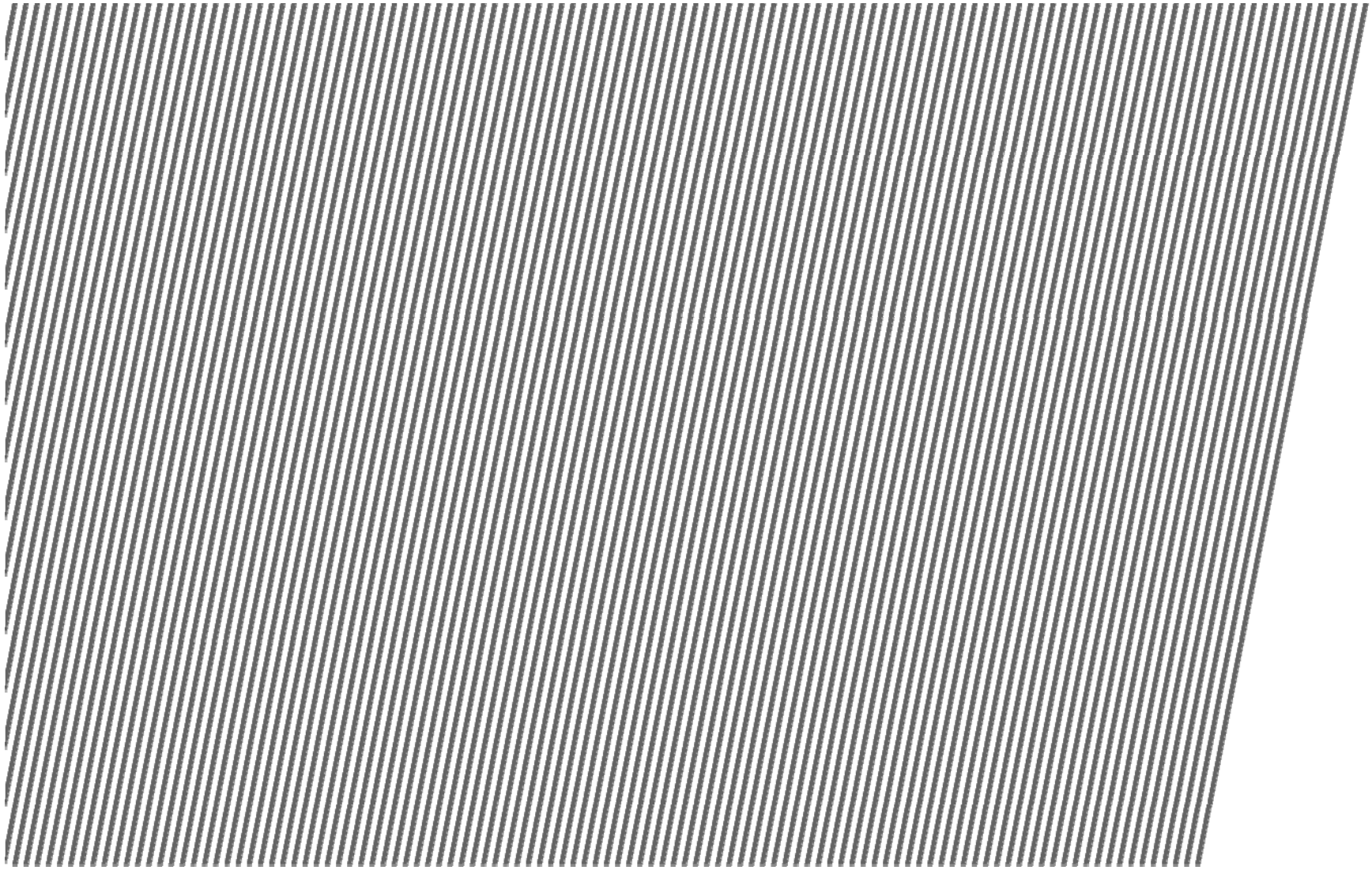
Presenter

	Name	Level	Contact Information	Experience
	Brian Portman	Senior Manager	brian.portman@ey.com +1-412-644-0495	Brian is a Pittsburgh based Senior Manager within the Financial Services Office of Ernst & Young's Advisory practice. He has over fifteen years of management experience and nine years of experience in the financial services industry serving a variety of clients, primarily in the areas of internal audit, compliance and risk management. Brian leads several internal audit co-source and outsourcing arrangements, including all aspects of the internal audit framework - risk assessment, audit planning, audit execution, reporting, issue tracking and Audit Committee reporting. Prior to joining Ernst & Young, Brian worked as a Bank Examiner with the OCC, conducting safety and soundness, compliance and specialty examinations.

Agenda

- Introduction
- Great expectations
- Key risk assessment concepts
- Top down risk assessment
- Bottoms up risk assessment
- Engagement-level risk considerations
- Continuous monitoring risk considerations
- Risk assessment process
- Key takeaways
- Appendix: Sample matrices

Great expectations



Ernst & Young
Quality In Everything We Do

Great expectations
Institute of Internal Auditors

- **2010 – Planning**

  The chief audit executive must establish a ***risk-based plan*** to determine the priorities of the internal audit activity, consistent with the organization's goals

  Interpretation
  The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's ***risk management framework, including using risk appetite levels set by management*** *for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.*

  2010.A1 – The ***internal audit activity's plan of engagements must be based on a documented risk assessment***, undertaken at least annually. The input of senior management and the board must be considered in this process.

- **2210 – Engagement Objectives**

  Objectives must be established for each engagement.

  2210.A1 – Internal auditors must conduct ***a preliminary assessment of the risks relevant to the activity under review***. Engagement objectives must reflect the results of this assessment.

Great expectations
Federal Reserve Board

Internal Audit Risk Assessment

- Assessments typically analyze the risks inherent in a given business line or process, the mitigating controls processes, and the resulting residual risk exposure to the institution
- Assessment should be well documented and dynamic, reflecting changes to the system of internal controls, infrastructure, work processes and new/changed business lines or laws and regulations.
- Risk assessments should consider thematic control issues, risk tolerance, and governance within the institution
- Assessments may be qualitative and quantitative and include factors such as impact/likelihood of an event occurring.
- Should be formally documented and supported with written analysis of the risks.
- Should include specific rationale for the overall auditable entity score
- A high-level summary of risk assessment results should be provided to the audit committee and include the most significant risks facing the institution, as well as how those risks have been addressed in the audit plan

Great expectations
Perspectives

*"Risk assessment is a process by which an **auditor identifies and evaluates** the **quantity** of the organization's risks and the **quality** of its controls over those risks "*

OCC

*"The **existence of risk is not the primary reason of concern**, rather auditors must determine if the risks are warranted. Generally, risks are warranted if they are understandable, controllable, and within the institution's capacity to withstand adverse performance"*

FFIEC

"Risk analysis is intended to provide auditors with a concise method of ***communicating and documenting judgments*** about the quantity of risk, quality of risk management, and aggregate levels of risk."

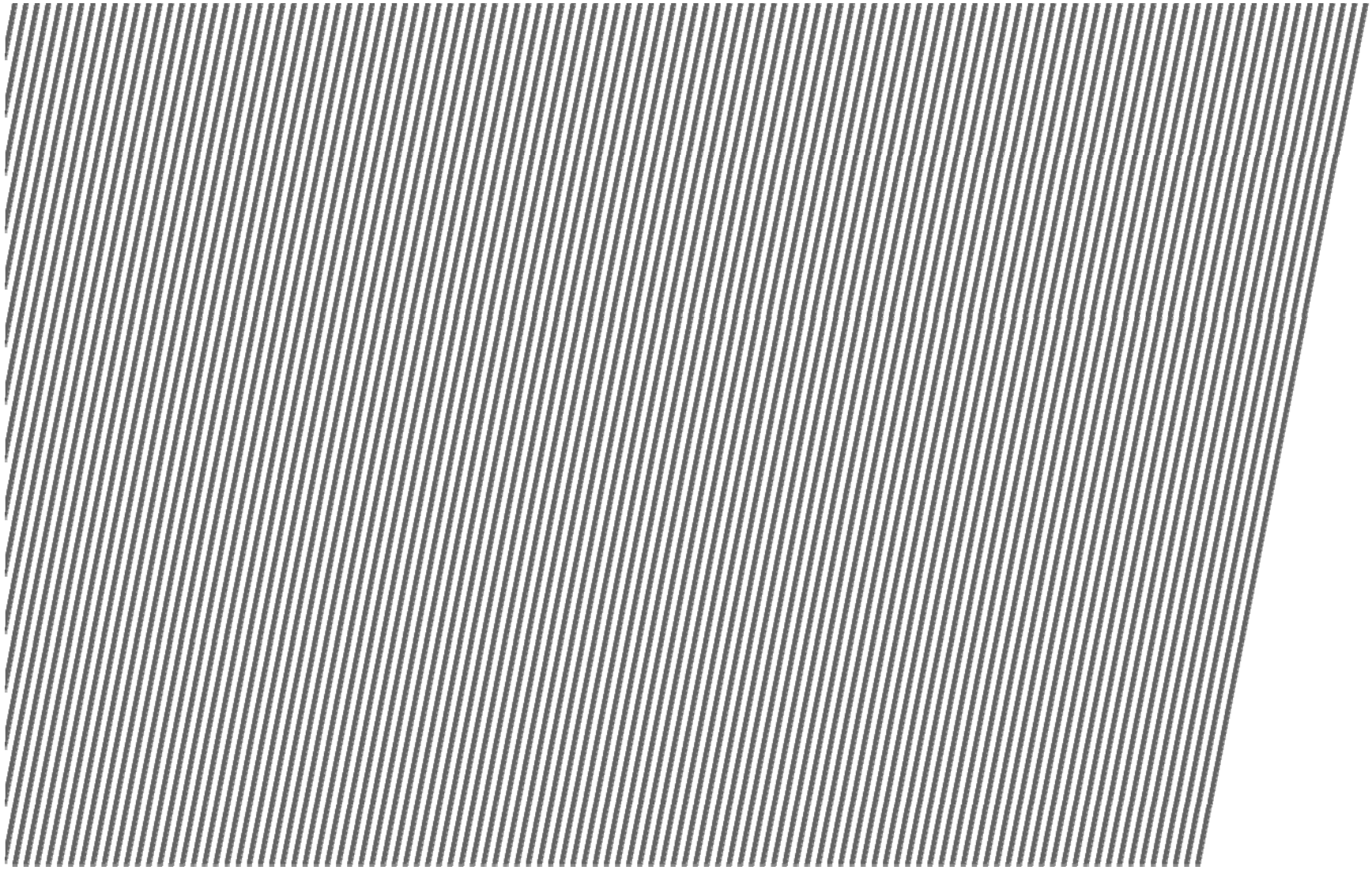
FFIEC

Great expectations
Fundamentals

All risk-based audit programs should:

- Identify all of an institution's businesses, product lines, services, and functions
- Identify the activities and compliance issues within those businesses, product lines, services, and functions that should be audited
- Include profiles of significant business units, departments, and products that identify business and control risks and document the structure of risk management and internal control systems.
- Use a measurement or scoring system to rank and evaluate business and control risks of significant business units, departments, and products
- Include board or audit committee approval of risk assessments or the aggregate result thereof and annual risk-based audit plans
- Implement the audit plan through planning, execution, reporting, and follow-up
- Have systems that monitor risk assessments regularly and update them at least annually for all significant business units, departments, and products

Key Risk Assessment Concepts

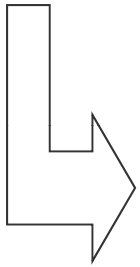


Key risk assessment concepts
Risk hierarchy

Risk Category

Facilitate the identification, measurement and reporting of risk within the business. They are used to help develop a profile of risk within business units of the company. They are the highest classification of risk within the risk universe.

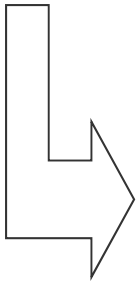
Example: Reputation Risk, Strategic Risk Operational Risk



Risk

The potential that events may have an adverse affect on the earnings. Risks are components within the risk universe where events may occur. Risks are categorized for ease of measurement and reporting. Examples:

Governance: management oversight, policy/procedures
Compliance: legal/regulatory, fraud
Operational Risk: systems, MIS, people



Risk Causes

An event or activity that could lead to the realization of a risk.

Governance: *The risk arising from the committee structure not being aligned or commensurate with the company's organizational structure and risk profile*

Operational, people: *The risk arising from inadequate staffing levels, skills sets, or succession planning resulting in ineffective execution of the strategic plan or day-to-day operations.*

Key risk assessment concepts
Risk analysis

1. **Risk identification ("what is the risk")** – a description of the risk presented
   - Example: Risk of non-compliance with regulations

2. **Risk rationale ("why does the risk exist"):** - what event(s) cause the risk to occur
   - Example: Risk of non-compliance with regulations due to reports of financial information required by regulatory agencies or tax authorities being ***incomplete, inaccurate, or untimely.***

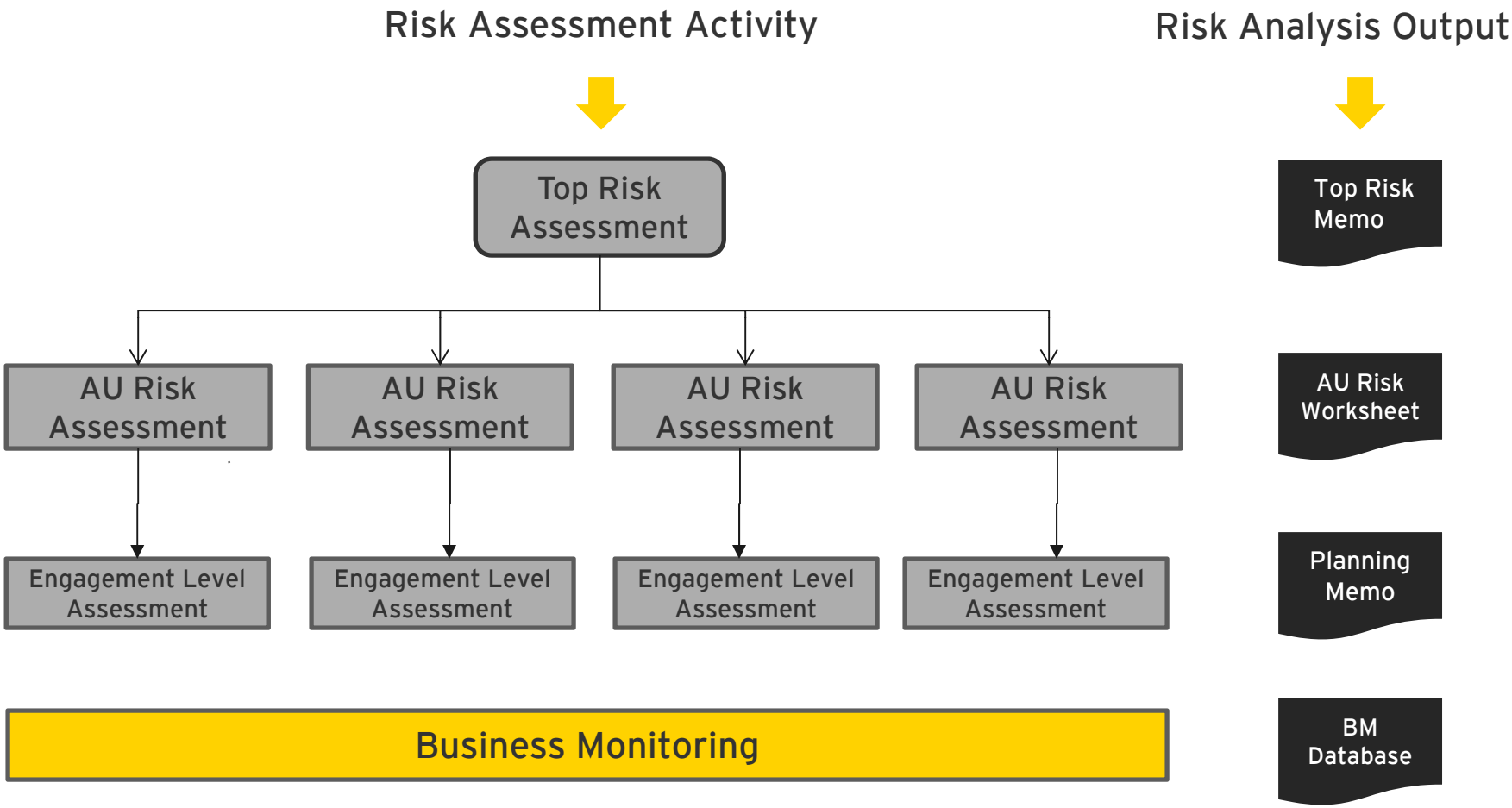
3. **Impact ("so what")** – the extent to which, if realized, the risk would affect the Company; may be expressed in qualitative or quantitative terms
   - Considerations: financial effect, reputation impacts, ability to achieve key goals and objectives
   - Example: Risk of non-compliance due to reports of financial information required by regulatory agencies or tax authorities being incomplete, inaccurate, or untimely, ***exposing the company to fines, penalties and sanctions.***

4. **Likelihood ("how often")** – probability of the risk occurring over a defined time frame
   - Consideration: often 1 year; also consider frequency of occurrence
   - Example: Risk of non-compliance due to reports of operating and financial information required by regulatory agencies or tax authorities being incomplete, inaccurate, or untimely, exposing the company to fines, penalties and sanctions. ***The likelihood of occurrence over the course of the quarter is considered to be high based on the volume of global reporting requirements***

Key risk assessment concepts
Universal considerations

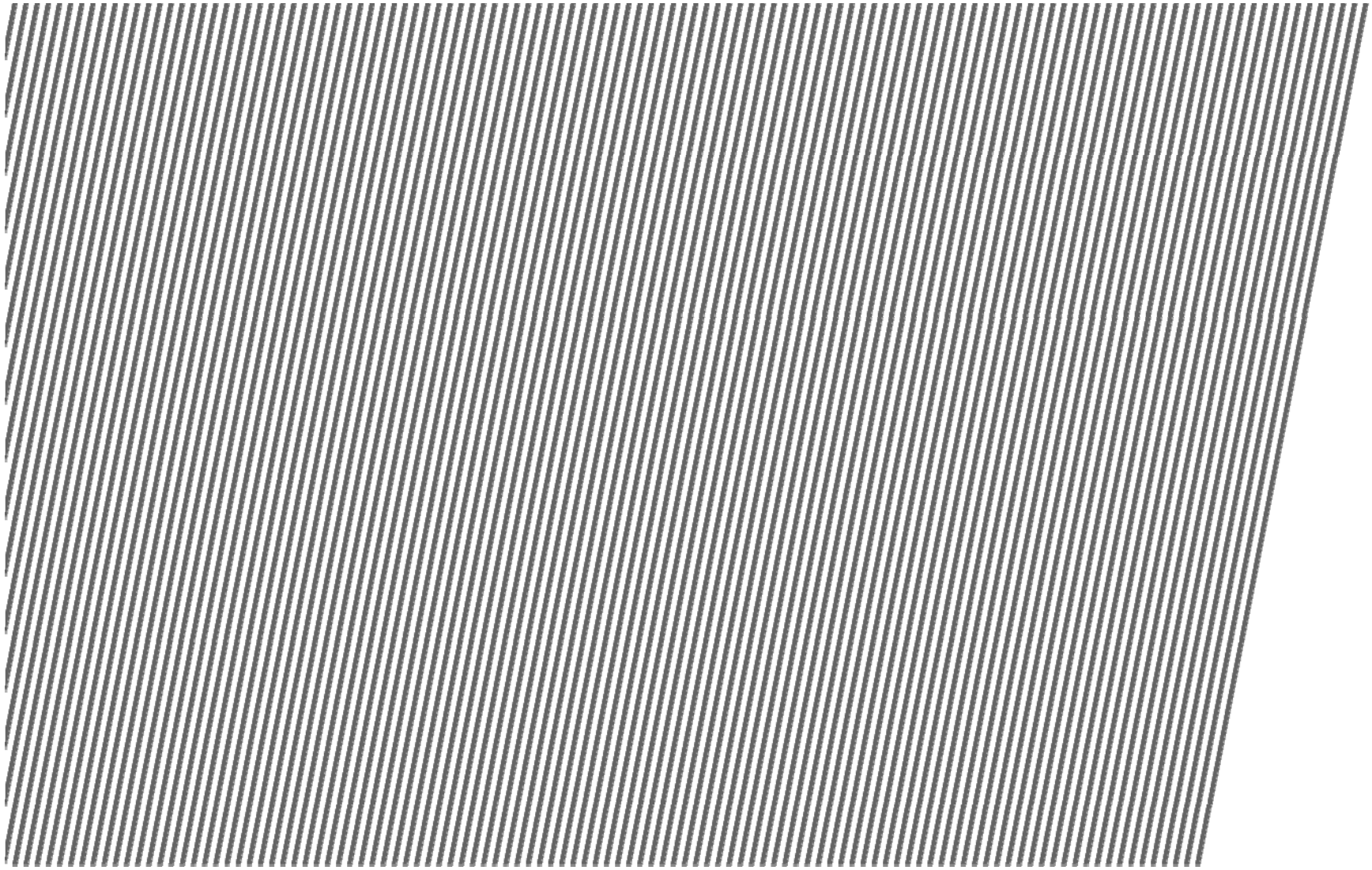
- Should include both quantitative and qualitative considerations
- Metrics alone are not "analysis" – auditors need to understand the drivers and impact beyond just the metrics e.g. what, why, so what, how often
- Need both top-down and bottoms-up assessment aspects
- Analysis may vary based on the level of assessment being performed e.g. Line of Business vs. Auditable Unit vs. Engagement
- Auditors should have a consistent frame of reference for risk measurement or scoring to rank and evaluate risks e.g., what differentiates high vs. moderate vs. low
- Incorporate forward-looking perspectives, such as risks associated with corporate objectives, growth strategies, new products, environmental and regulatory changes, etc.
- Expanding risk assessments and documentation to include IT applications and associated IT risks
- Ensuring that clear linkage exist between the auditable unit risk assessments, audit scope and objectives, and testing work

Key risk assessment concepts
Risk assessment framework



Documented risk analysis occurs within every stage of the risk assessment framework

Top Down Risk Assessment



Top down risk assessment

Key considerations

- Considers both internal and external risks
- Should include quantitative and qualitative considerations
- Helps gain an understanding of overall Enterprise-Level Risks
- Uncover issues that directly impact stakeholder value, with clear and explicit linkage to strategic issues of company
- Serve as a mechanism to understand the risk implications of the company's strategy
- Ensure the most critical risks facing the company (that may not have been identified by the bottom-up risk assessment) are identified and incorporated into the audit plan
- May result in the performance of targeted audits, horizontal audits and special projects
- Internal Audit must provide an independent view of risk, but that view can and should be formed in collaboration with management

Top down risk assessment

Overview

Purpose: Internal Audit performs activities to identify macro-level environmental, industry, and enterprise-wide areas of current or potentially emerging interest to stakeholders and develops appropriate audit strategies to address such areas.

Primary Objective: Development of the annual audit plan

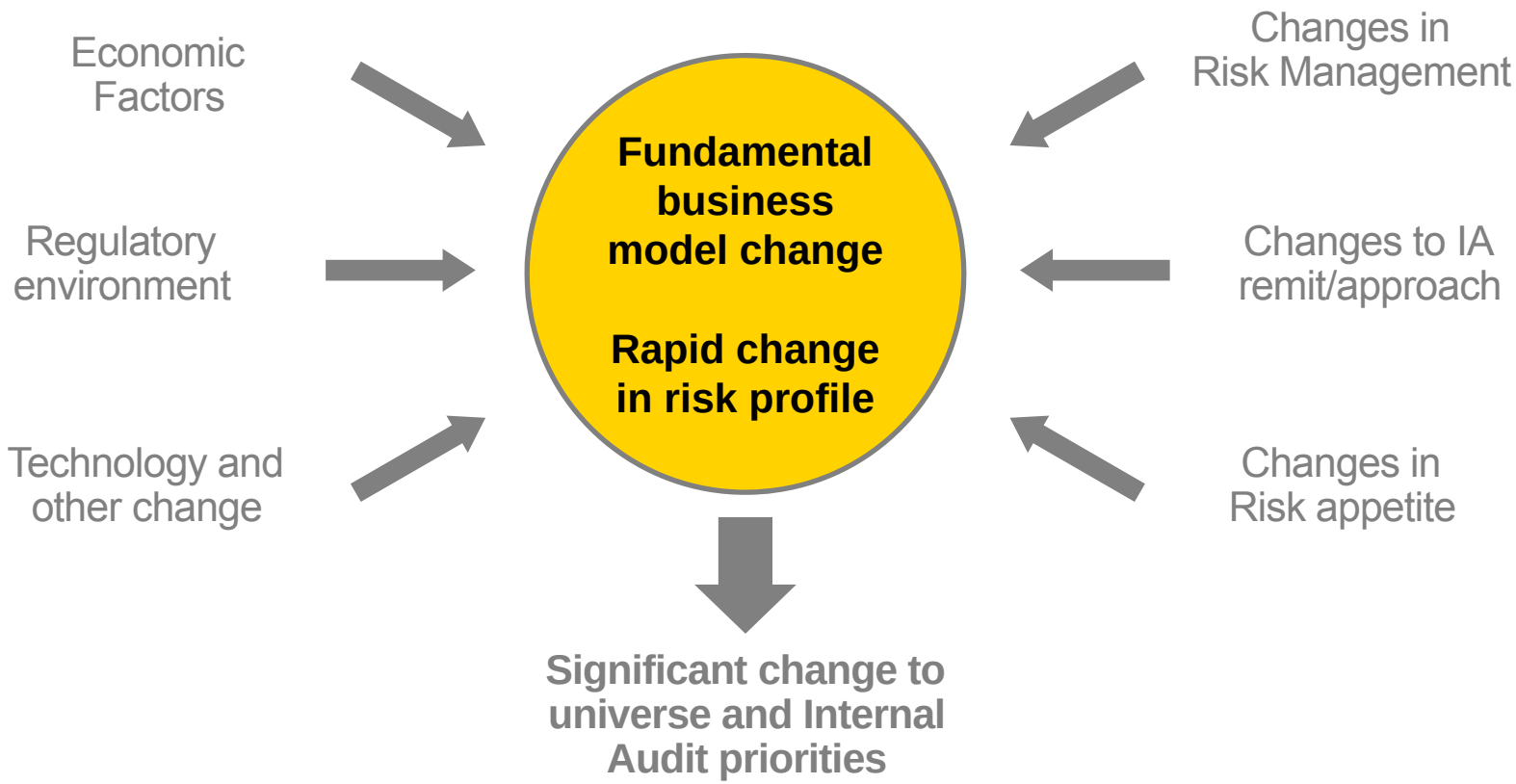
Frequency: At least annually

Key Components:

- Overall Conclusion
- Key Focus Areas for the Current Year
- Line of Business Overview
- Common Risk Factor Analysis
- Business Change Process
- Regulatory Changes
- Other Lines of Defense assessment results
- Legal Entity considerations
- Outstanding issues
- IT environment

Top down risk assessment

Business environment impact



... will result in significant change to universe and internal audit priorities

Top down risk assessment

Defining the "risks that matter"

Key Risks To Business Objectives

Key considerations

- Are we focused on the risks that matter?
- Is the scope of our assessment comprehensive?
- Do we leverage industry specific risk models?
- Do we gain insights on the risks of our key business partners and customers?
- Is our assessment approach consistent?
- Do we evaluate risk on a common basis?
- Do we recognize the impact to value drivers?
- Does our process cover emerging risks?

Top down risk assessment

Analysis considerations

Are we taking the right risks?

- How are the risks we take related to our strategies and objectives?
- Do we know the significant risks we are taking?
- Do the risks we take give us a competitive advantage?
- How are the risks we take related to activities that create value?
- Do we recognize that business is about taking risks and do we make conscious choices concerning these risks?

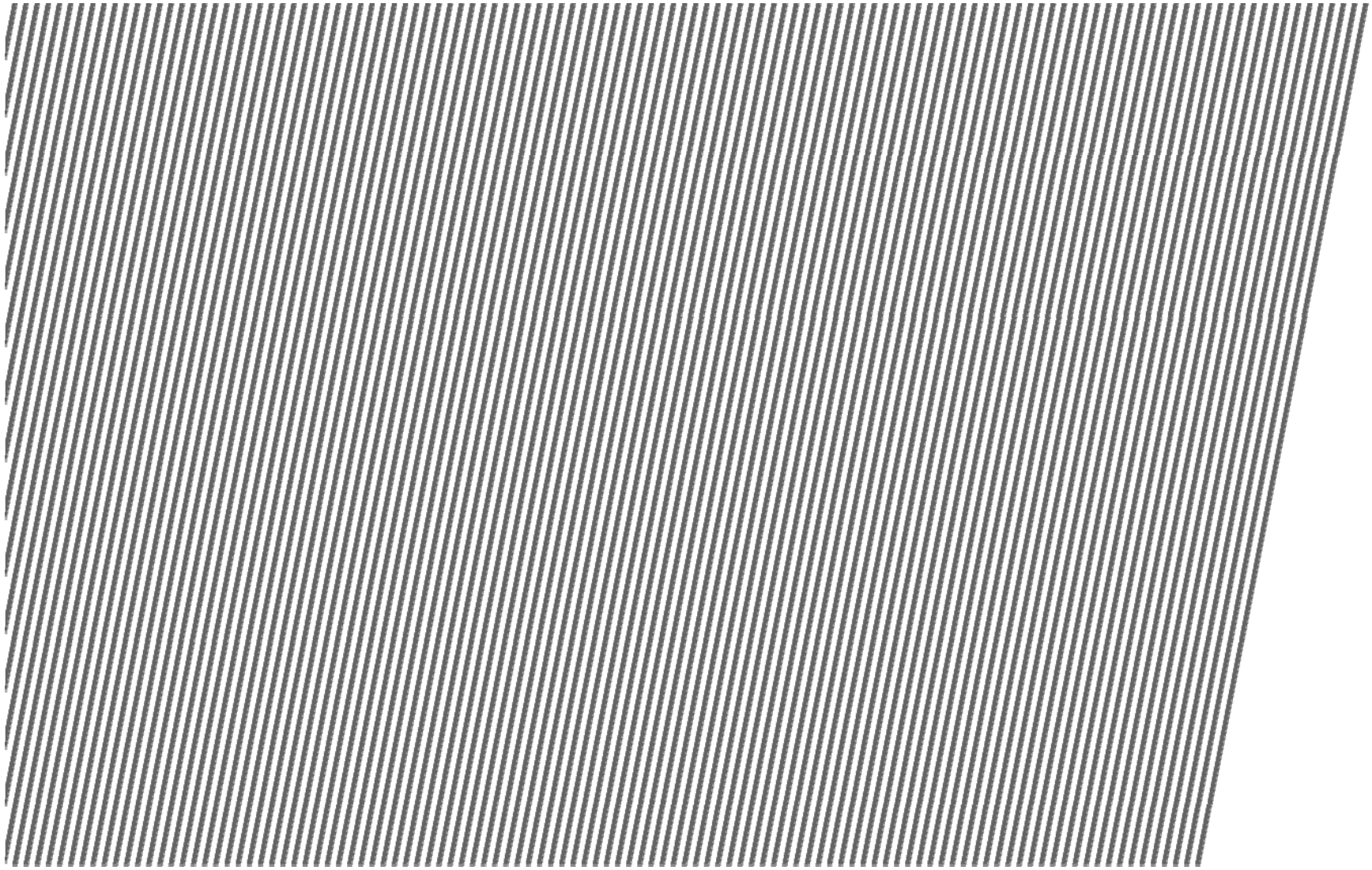
Are we taking the right amount of risk?

- Are we getting a return that is consistent with our overall level of risk?
- Does our organizational culture promote or discourage the right level of risk taking activities?
- Do we have a well defined organizational risk appetite?
- Has our risk appetite been quantified?
- Is our actual risk level consistent with our risk appetite?

Are we adequately managing our risks?

- Is our risk management process aligned with our strategic decision-making process and existing performance measures?
- Is our risk management process coordinated and consistent across the entire enterprise? Does everyone use the same definition of risk?
- Do we have gaps and/or overlaps in our risk coverage?

Bottoms Up Risk Assessment



Bottoms up risk assessment

Overview

Purpose: Internal Audit is responsible for the assessment of risks associated with Auditable Units resulting in the assignment of risk ratings to each Auditable Unit for the purpose of applying the frequency scheduling guidelines.

Primary Objective: Determine frequency of audit coverage

Frequency: Annual and ongoing

Key Components:

- Common Risk Definitions e.g. finance, compliance, operational, strategic
- Assignment of Inherent Risk, Control Factors and Residual Risk (see Appendix)
- Risk Trend e.g. constant, increasing or decreasing
- Comments/Reasons e.g. support for ratings assignments
- Governance, risk management, and oversight

Key Considerations:

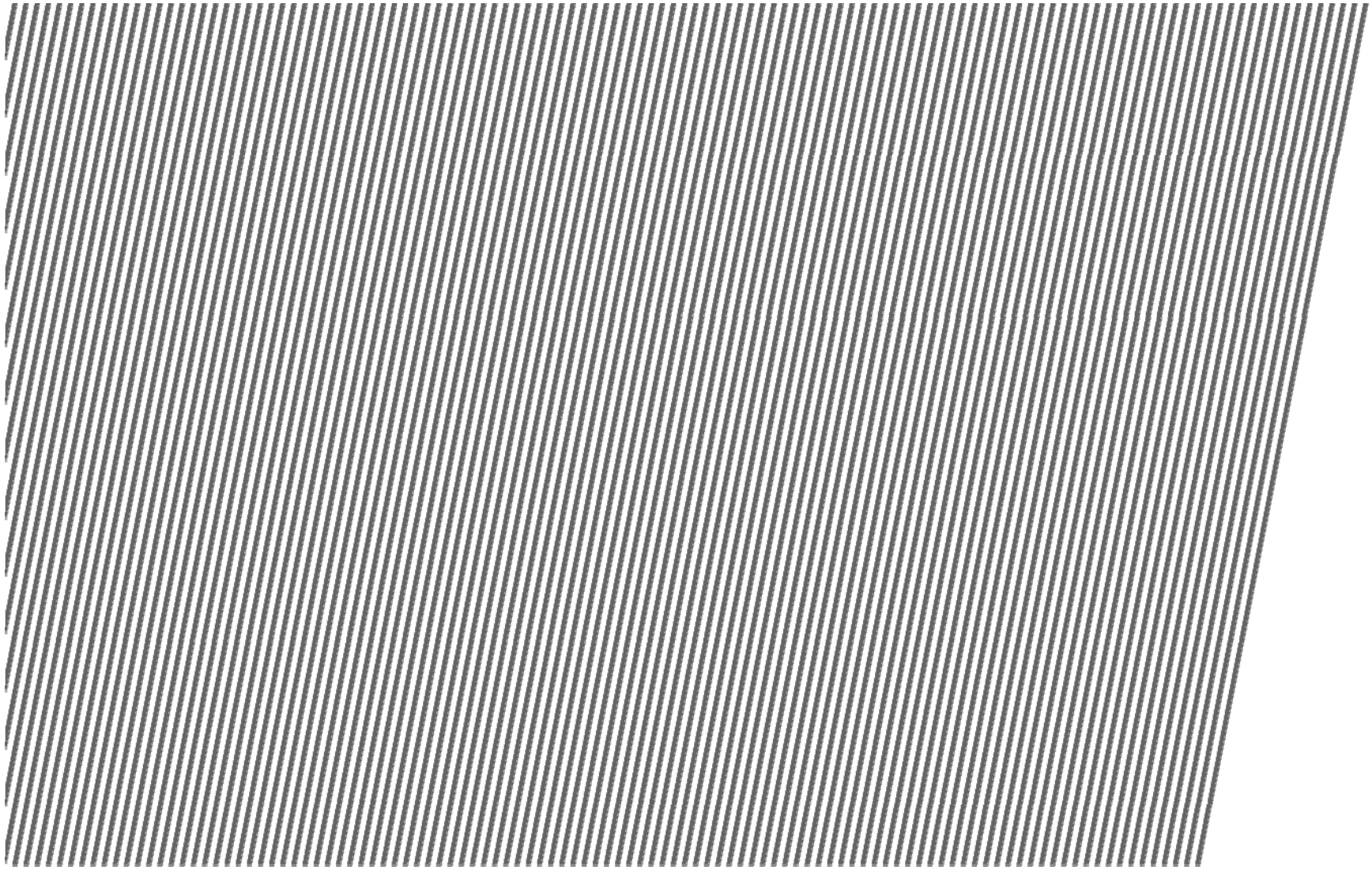
- Impact and likelihood of occurrence
- Process change factors
- Materiality factors

Bottoms up risk assessment

Analysis considerations

- What are the key business risks within the area?
- For each of those risks, what are the contributing factors and management concerns, issues, or gaps in management coverage?
- How do risks identified relate to governance, risk management and oversight?
- How does management evaluate the effectiveness of the process and related controls in managing the risks?
- Are there opportunities for improvement of processes and/or controls in managing the risk?

Engagement Level Risk Assessment



Engagement level risk assessment

Overview

Purpose: Audit Teams are responsible for the assessment of risks at the engagement level to identify and assess the appropriate design of controls and test for operating effectiveness.

Primary Objective: Determine the scope of coverage for an individual audit

Frequency: Each engagement

Key Components:

- Gain an understanding of associated business processes
- Confirm risks with business owners
- Document risks within the audit planning memo
- Governance, risk management, and oversight

Key Considerations:

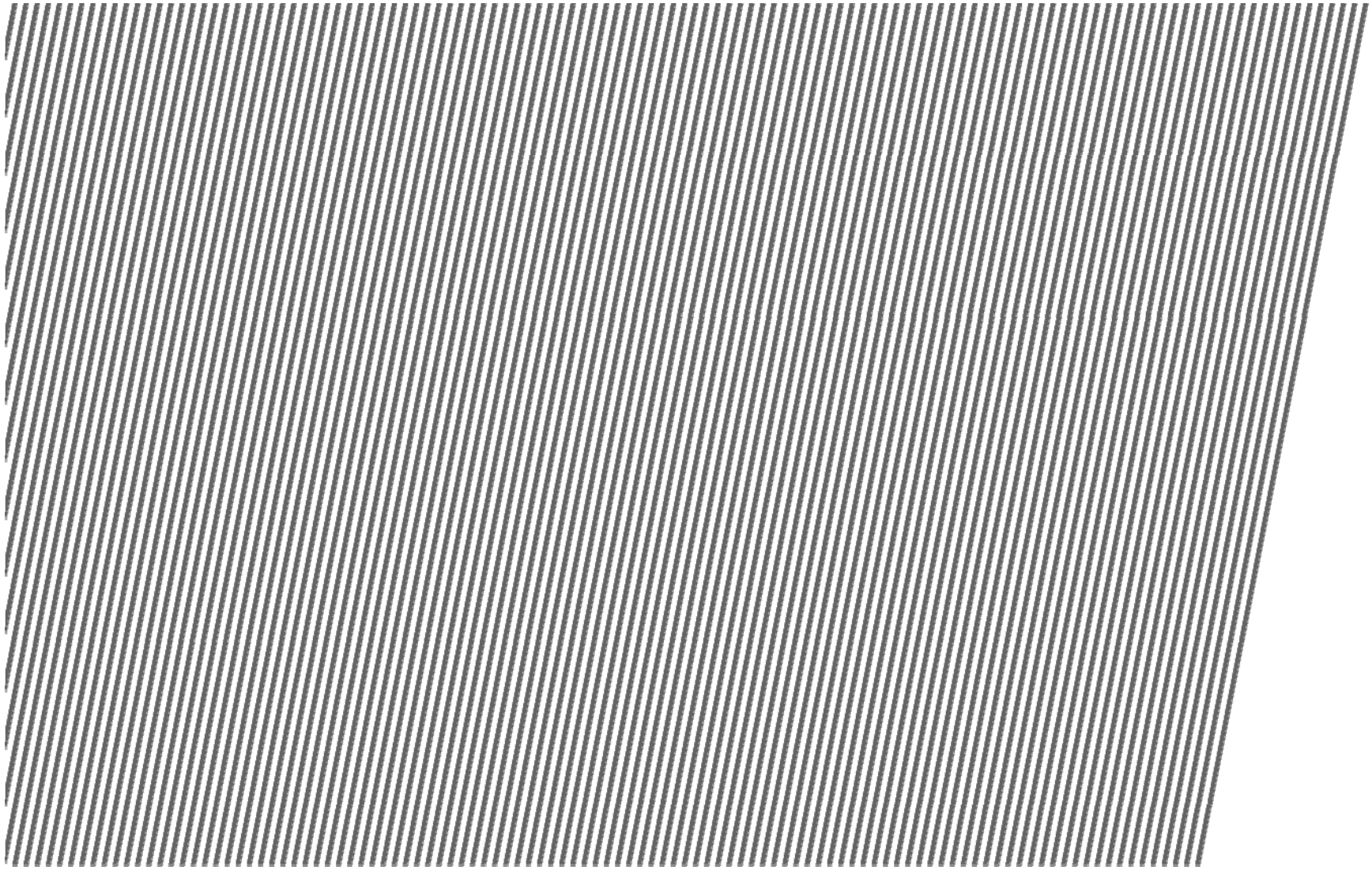
- How do these risks relate to auditable unit and/or LOB risks identified
- Risks in the context of "what could go wrong"
- Have I identified the key risks to the associated business process

Engagement level risk assessment

Analysis considerations

- What are the key risks related to each business process?
- For each of those risks, what are the contributing factors and management concerns, issues, or gaps in management coverage?
- How do risks identified relate to auditable unit or top risks?
- How does management evaluate the effectiveness of the process and related controls in managing the risks?
- Are there opportunities for improvement of processes and/or controls in managing the risk?

Continuous Monitoring Risk Assessment



Ernst & Young
Quality In Everything We Do

Continuous monitoring risk assessment

Overview

Purpose:	Audit Teams are responsible to perform certain activities designed to contribute to the identification of potential changes impacting the risk profile of the bank.
Primary Objective:	Evaluate the potential impact on current/future audit plans, scope, and coverage
Frequency:	Quarterly
Responsibility:	Audit Teams

Key Components:

- Management call program
- Analysis of quantitative and qualitative risk information
- Industry / economic considerations
- Document risks within a data repository

Key Considerations:

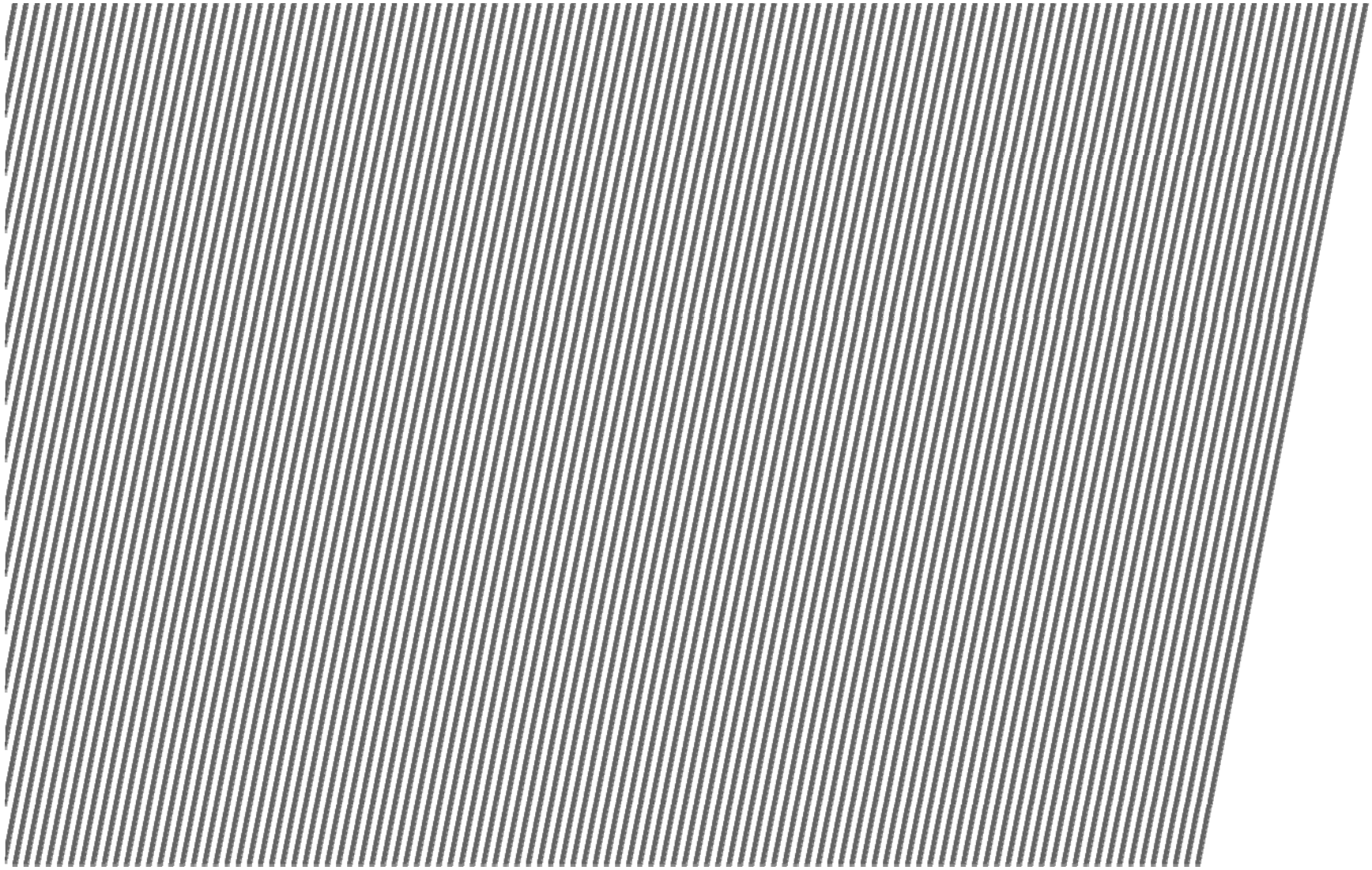
- Activity is performed at the LOB level
- Need to consider any new processes/products/systems
- Need to consider any changes to existing risk profile

Continuous monitoring risk assessment

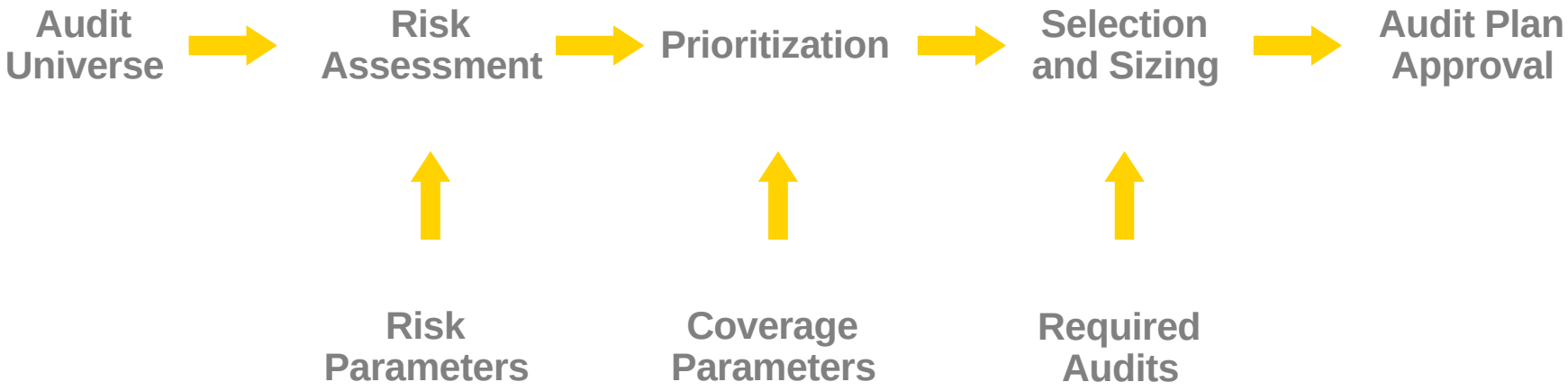
Analysis considerations

- Has the existing risk profile changed?
- Have any new risks been identified?
- Have there been any significant changes to people, processes, or systems?
- Are activity/risk trends consistent with expectations?

Risk Assessment Process

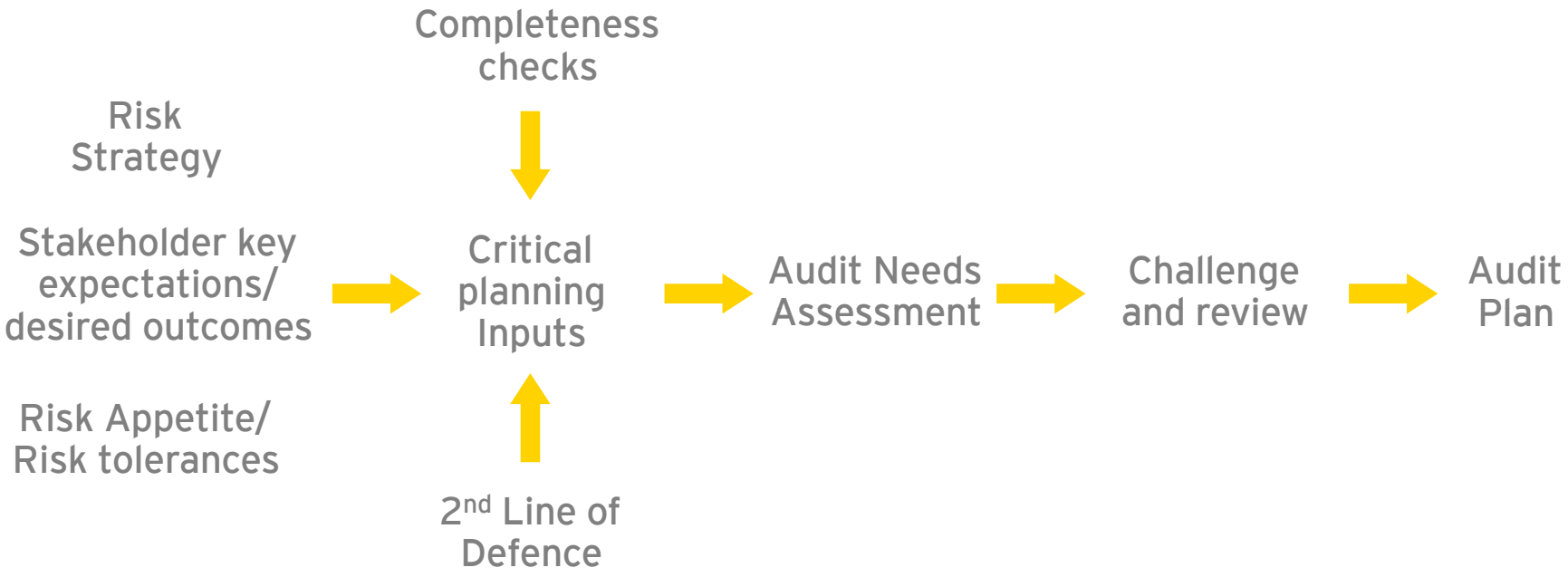


The macro Internal Audit planning process has been largely unchanged for many years...



... with refinements to meet specific needs and improve sustainability and flexibility

The current environment demands a more dynamic process



- Continuous activity with pipelines of information constantly being assessed for audit planning implications
- Strong stakeholder engagement
- Change control over the audit plan
- Completely integrated into execution

Risk assessment results

- Results should be reviewed and challenged e.g. peer review
- Results should drive frequency and intensity of audit coverage
- Assurance can be provided through multiple delivery channels e.g. end-to-end process reviews, targeted procedures, horizontals, continuous monitoring, Sox testing
- More organizations moving towards a 3+9 or 6+6 audit plan

Risk Rating	Frequency	Guideline	Intensity
Critical	06 months	500 hours	Full scope
High	12 months	400 hours	Full scope/ targeted
Moderate	24 months	300 hours	Full scope / targeted
Low	36 months	200 hours	Targeted / continuous monitoring
Very Low	48 months	100 hours	Targeted / continuous monitoring

3 + 9 Audit Plan

Example Current Annual Audit Plan

Planned Audits based on Risk Assessment

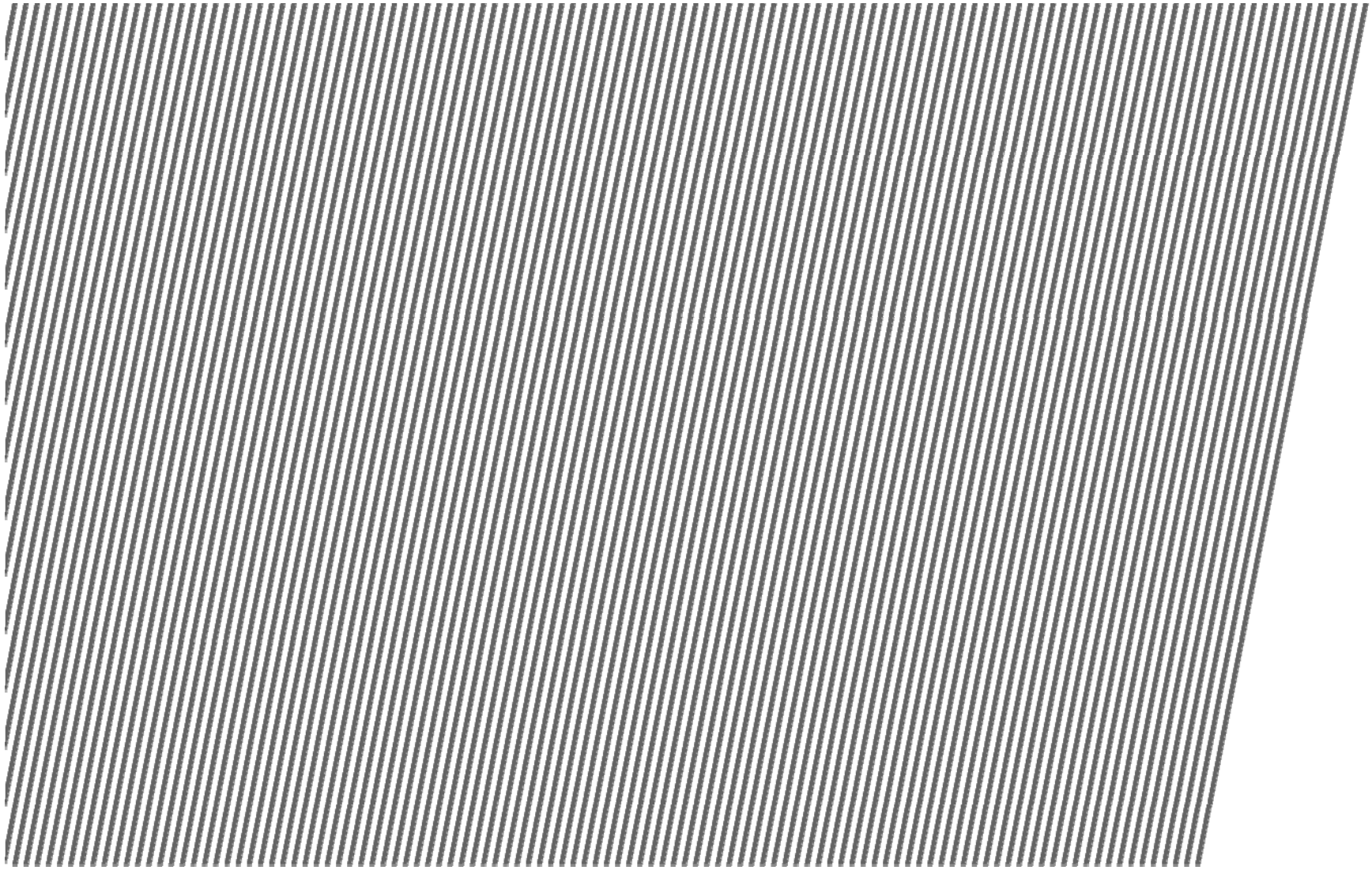
Discretionary / Special Projects

3 + 9 Quarterly Audit Plan

Audits to be executed based on results of audit needs assessment

Remaining Audit Needs that may or may not get coverage in the next 9 months

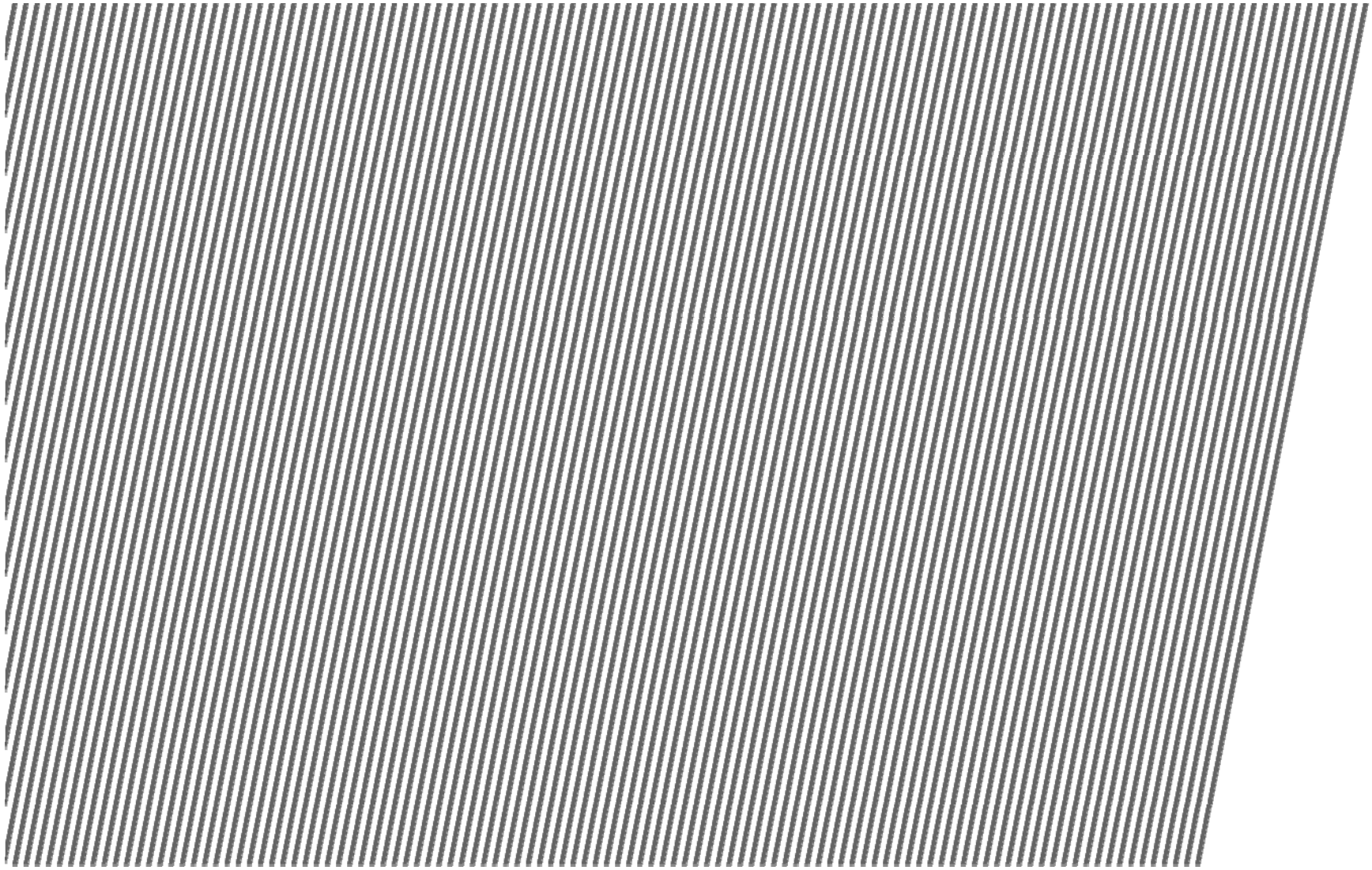
Key Takeaways



Key takeaways

- Risk assessment is NOT an annual, one-time event
- Risk assessment considerations will differ based on the level of assessment e.g. top, auditable unit, engagement, and continuous monitoring
- Risk assessment is more than simple risk identification – must include robust analysis
- Requires continuous engagement with relevant stakeholders
- Full written explanation of the Audit Plan and the thought process applied
- Risk assessment must be integrated into audit execution
- Common risk definitions support risk "convergence" with other lines of defense
- Audit's risk assessment must be independent of business or enterprise risk assessments

Appendices



Appendix A – Impact Scale

Impact		1 Minor	2 Moderate	3 Significant	4 Severe	5 Catastrophic
Financial Exposure	% Equity	x < 0.01%	0.01% ≤ x < 0.5%	0.5% ≤ x < 2%	2% ≤ x < 10%	10% ≤ x
	$ Range	x < 500 K	500 K ≤ x < 2.5 MM	2.5 MM ≤ x < 25 MM	25 MM ≤ x < 500 MM	500 MM ≤ x
	% Net Income	x < 0.5%	0.5% ≤ x < 2%	2% ≤ x < 18%	18% ≤ x < 90%	90% ≤ x
	$ Range	x < 500 K	500 K ≤ x < 2.0 MM	2.0 MM ≤ x < 20 MM	20 MM ≤ x < 100 MM	100 MM ≤ x
Brand Damage		No impact on brand.	Impact is isolated to a small group of existing customers. Damage is reversible.	Negative impact is regional, is in the public domain, but with limited publicity	Negative impact is regional with widespread publicity, or national or global, with limited publicity.	Long-term / irreparable damage. Negative impact is national or global and is widely publicized
Regulatory / Legal Action		No breaches of regulatory or contractual obligations.	Breaches of regulatory or contractual obligations are confined to an isolated incident or incidents. Not systemic.	Breach of regulatory or contractual obligations, with costs to the firm or client, and increased scrutiny from the regulator or action by the customer.	Regulatory censure or action. Significant breach of rules or contract. Possibility of action against specific member(s) of the senior management team.	Public regulatory fines or censure, or major litigation potential. Possibility of imprisonment for senior management.
Customer / Operations		Failures are isolated and limited to a small number of internal personnel.	Failure limited to a small number of customers or one business relationship.	Systemic failure impacts a specific customer group, transaction types, or agents. Excludes sales practices.	Systemic failure impacts multiple product groups, transaction types, or an entire distribution channel. Includes sales practices.	Catastrophic failure impacting broad spectrum of customer groups, and distribution channels (e.g., core system failure, systemic fraud).

(Note: This impact scale is a representative sample utilized to perform the internal audit risk assessment. The quantity of levels and definitions of each level may be modified to derive a more suitable scale based upon the maturity of the organization's current risk assessment process).

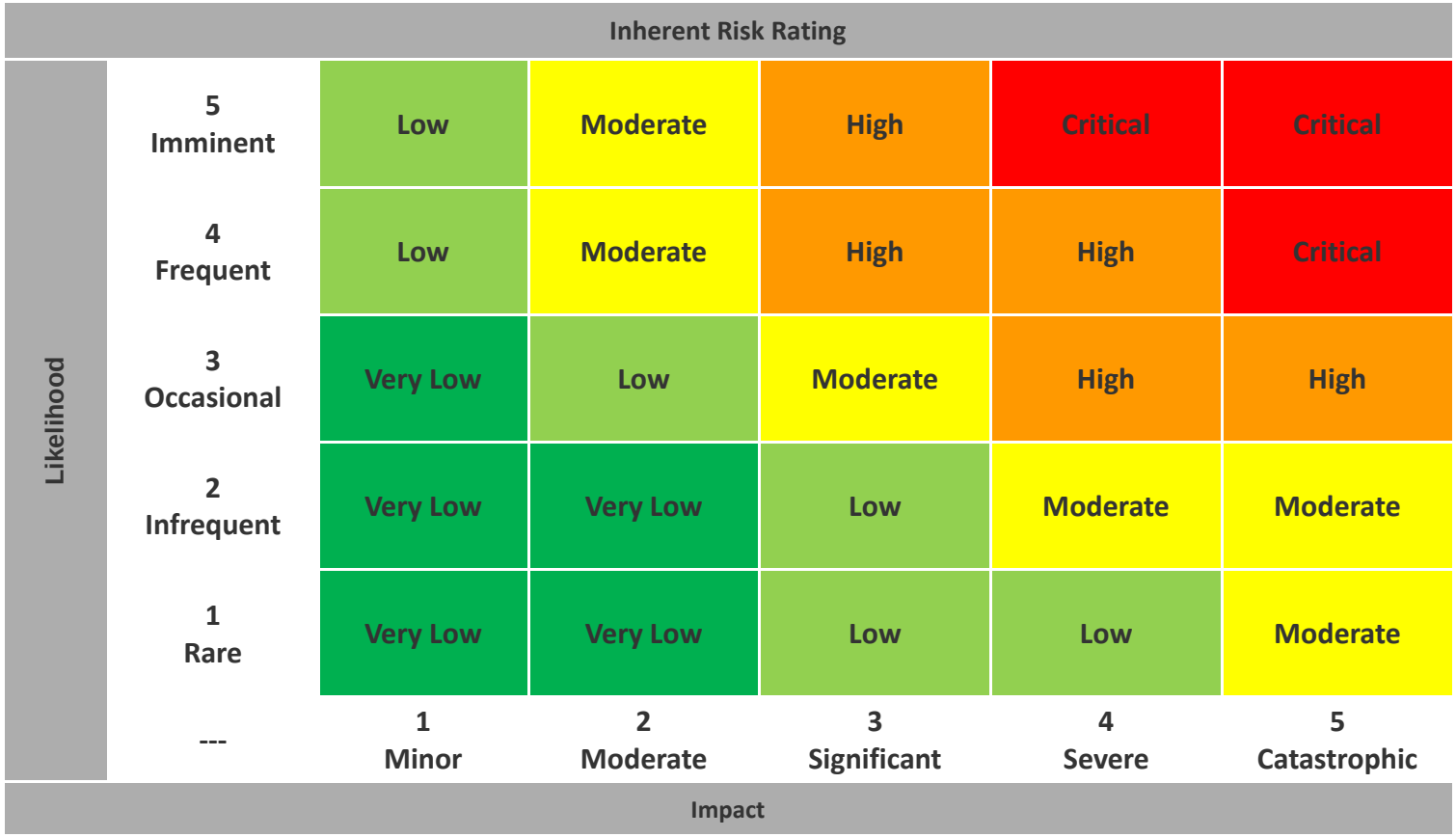
Appendix B – Likelihood and Control Scales

Likelihood	1 Rare	2 Infrequent	3 Occasional	4 Frequent	5 Imminent
Frequency	In more than / every 5 years	Within the next / every 3 to 5 years	Within the next / every 1 to 3 years	Within the next / every 1 year	Within the next / every Quarter

Control Rating	Strong	Reasonably Strong	Adequate	Marginally Adequate	Weak or Nonexistent
Description	The control processes and management's mitigating activities are strong and allow for the effective management of the risk, thereby significantly reducing the frequency and/or impact of the risk event. It does not mean that there is no exposure to risk or that the risk has been reduced to zero.	The control processes and management's mitigating activities are more than adequate and allow for the management of the risk, thereby reducing the frequency and/or impact of the risk event; however, there incremental opportunities for improvement and therefore the control cannot be considered strong.	The control processes and management's mitigating activities allow for effective management of the risk, thereby partially reducing the frequency and/or impact of the risk event occurring. There are opportunities for improvement and/or adding additional compensating controls to help mitigate the residual risk.	The control processes and management's mitigating activities allow for marginal management of the risk; there is minimal reduction in the frequency and/or severity of the risk event. Major gaps and deficiencies have been identified.	The control processes and management's mitigating activities do not allow for the effective management of the risk, there is no reduction in the frequency and/or severity of the risk event.

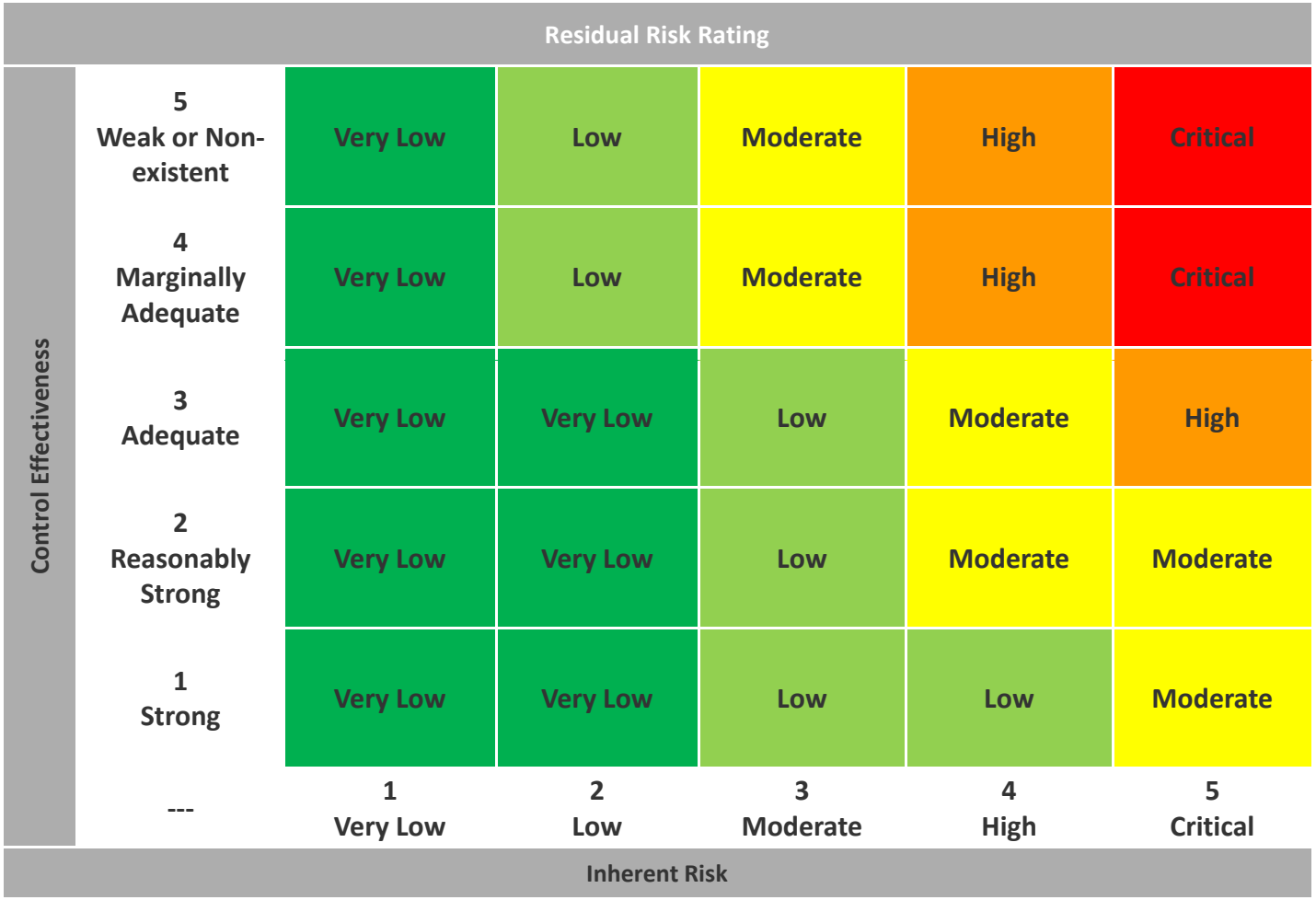
(Note: This likelihood and control effectiveness scales are representative samples utilized to perform the internal audit risk assessment. The quantity of levels and definitions of each level may be modified to derive a more suitable scale based upon the maturity of the organization's current risk assessment process).

Appendix C - Inherent Risk – Sample Matrix



(Note: This inherent risk scale is a representative sample utilized to perform the internal audit risk assessment. This is a function of the impact and likelihood scales defined within "Appendices A and B").

Appendix D - Residual Risk – Sample Matrix



(Note: This residual risk scale is a representative sample utilized to perform the internal audit risk assessment. This is a function of the control effectiveness and inherent scales defined within "Appendices B and C").