Fraud maturity model: advancing the anti-fraud management program

25th Annual ACFE Global Fraud Conference

17 June 2014

Presenter:
Beth Junell
beth.junell@ey.com

EY
Building a better working world

Discussion topics

- Role of corporate ethics and integrity
- Creating a culture of compliance
- Advancing maturity of the anti-fraud management program
- Question and answer session

Role of corporate ethics and integrity

- Compliance and integrity management are used to augment a sustainable ethical culture in the organization.
- Compliance programs should be built on the company's core values.
- Critical success factors:
  - Business integrity
  - Leadership
  - Culture

Creating a culture of compliance
Why it is so important in managing fraud

- People make decisions daily that impact the company's ethics and compliance posture.
- "Just follow the rules"
  - A company's reputation can still be harmed by conduct that is legal, but may not be seen as ethical.
  - Let's talk about the gray areas.

Unethical behaviour persists
EY's 13th Global Fraud Survey, Figures 1,5&10

	% Agree			
	North America	Developed markets	Emerging markets	All respondents
Offering entertainment to win/retain business	33	30	28	29
Personal gifts to win/retain business	5	11	17	14
Cash payments to win/retain business	1	7	16	13
Misstating company's financial performance	3	4	8	6
At least one of these can be justified	35	38	45	42

Q. Which, if any, of the following do you feel can be justified if they help a business survive an economic downturn?
Base: US 2014 (50); North America 2014 (100); developed markets 2014 (1103); emerging markets 2014 (1616); all respondents 2014 (2719)
% don't know and none of the above have been omitted to allow better comparison between responses given

Creating a culture of compliance
Ethical decision-making model

- Move toward ethical decision making
  - Focus employees on the culture of making ethical decisions tied to the company's values
  - Encourage employees to "do the right thing"
- An ethical decision-making model can guide employees when the "right" course of conduct may not be clear.
  - Is the action at issue in line with corporate values?
  - Is the action consistent with company policy?
  - Is the action legal?
  - Would I want everyone to know I took the action?
  - Would I be embarrassed if my family or friends knew?

Role of corporate compliance program
Underpin business success

- Effective compliance programs allow companies to create a culture of compliance and help employees to do the right thing.
- The ultimate outcome of an effective compliance program is a reputation for underpinning business success.

Enron Code of Ethics
Excerpted

Respect

We treat others as we would like to be treated ourselves. Ruthlessness, callousness and arrogance don't belong here.

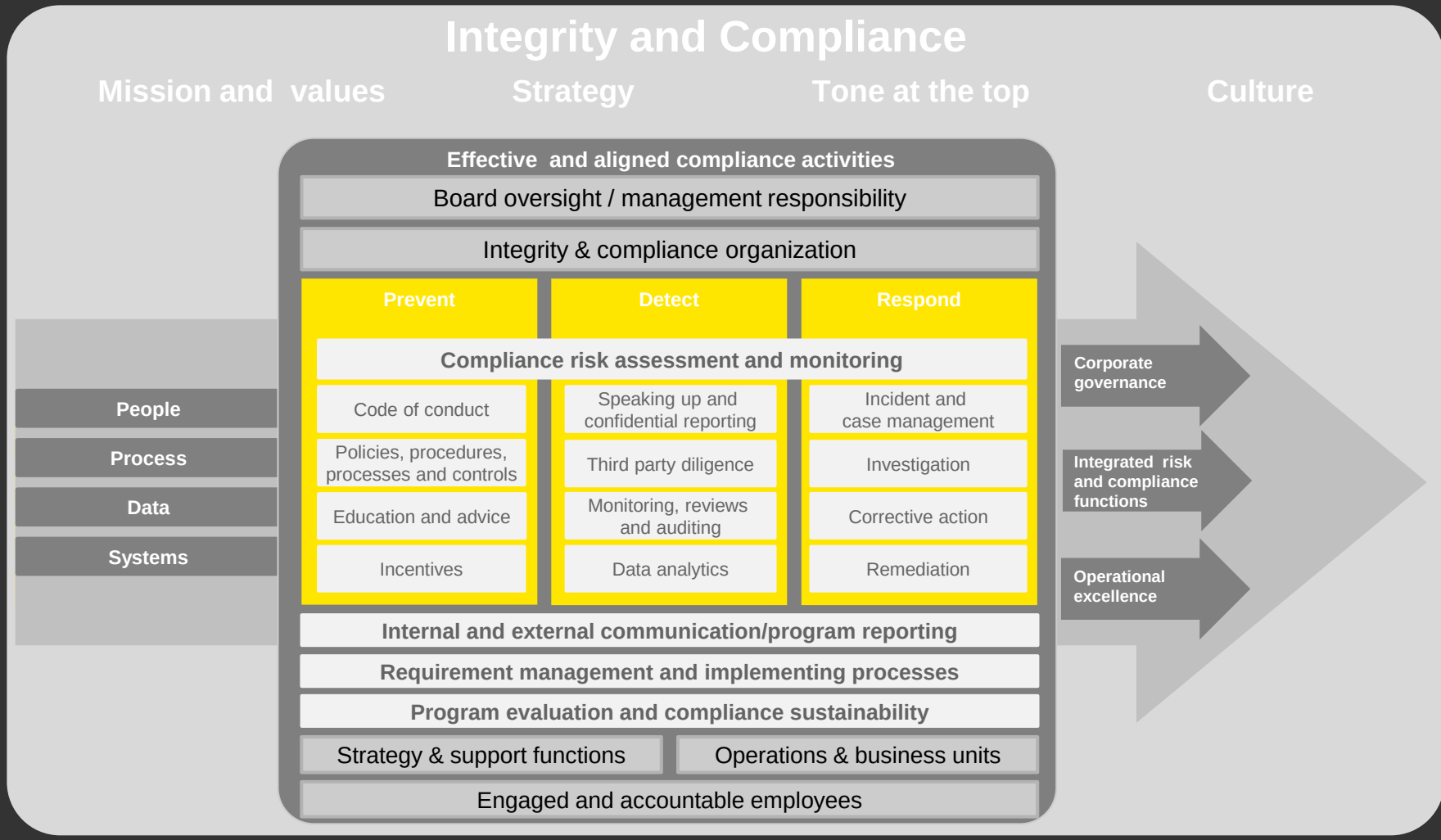
Integrity

We work with customers and prospects openly, honestly and sincerely. When we say we will do something, we will do it…

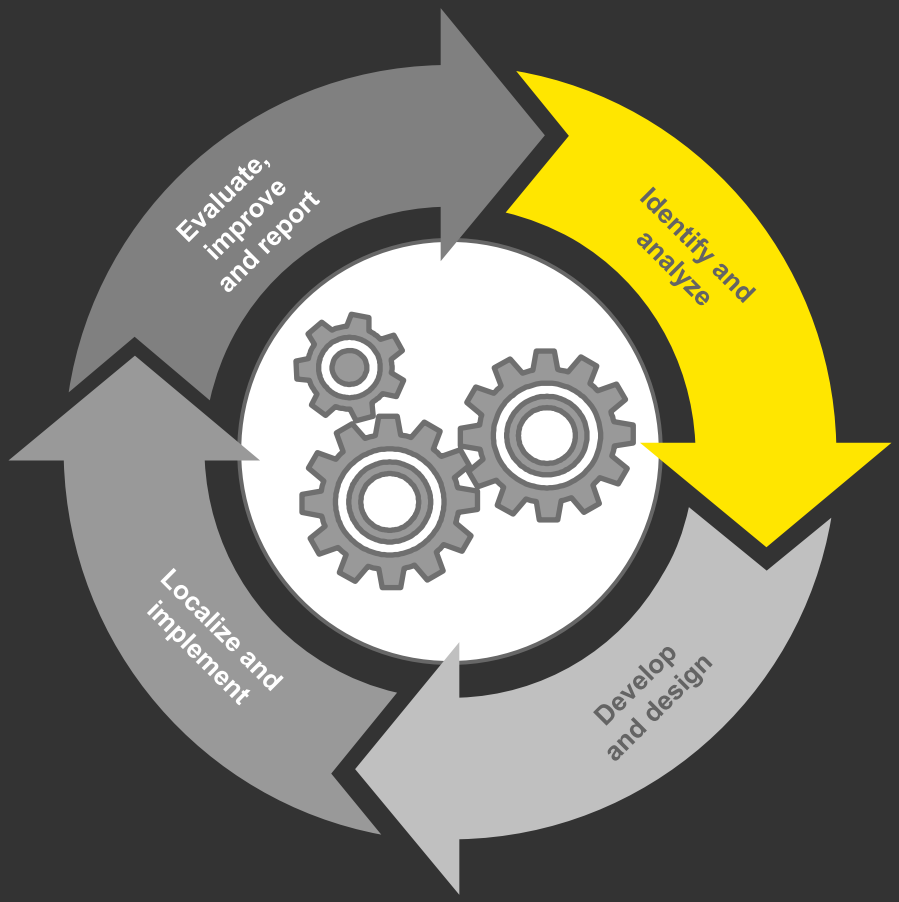
Excellence

We are satisfied with nothing less than the very best. We will continue to raise the bar for everyone.

Business integrity & corporate compliance (BI&CC) framework



Corporate compliance life cycle



Comparison of guidance

Components	COSO Integrated Control - Integrated Framework	Federal Sentencing Guidelines	DOJ/SEC FCPA guidance	UK Bribery Act Adequate Procedures	OECD Good Practice Guidance
Control environment	✓	✓	✓	✓	✓
Risk assessment	✓	✓	✓	✓	✓
Control activities	✓	✓	✓	✓	✓
Information and communication	✓	✓	✓	✓	✓
Monitoring	✓	✓	✓	✓	✓

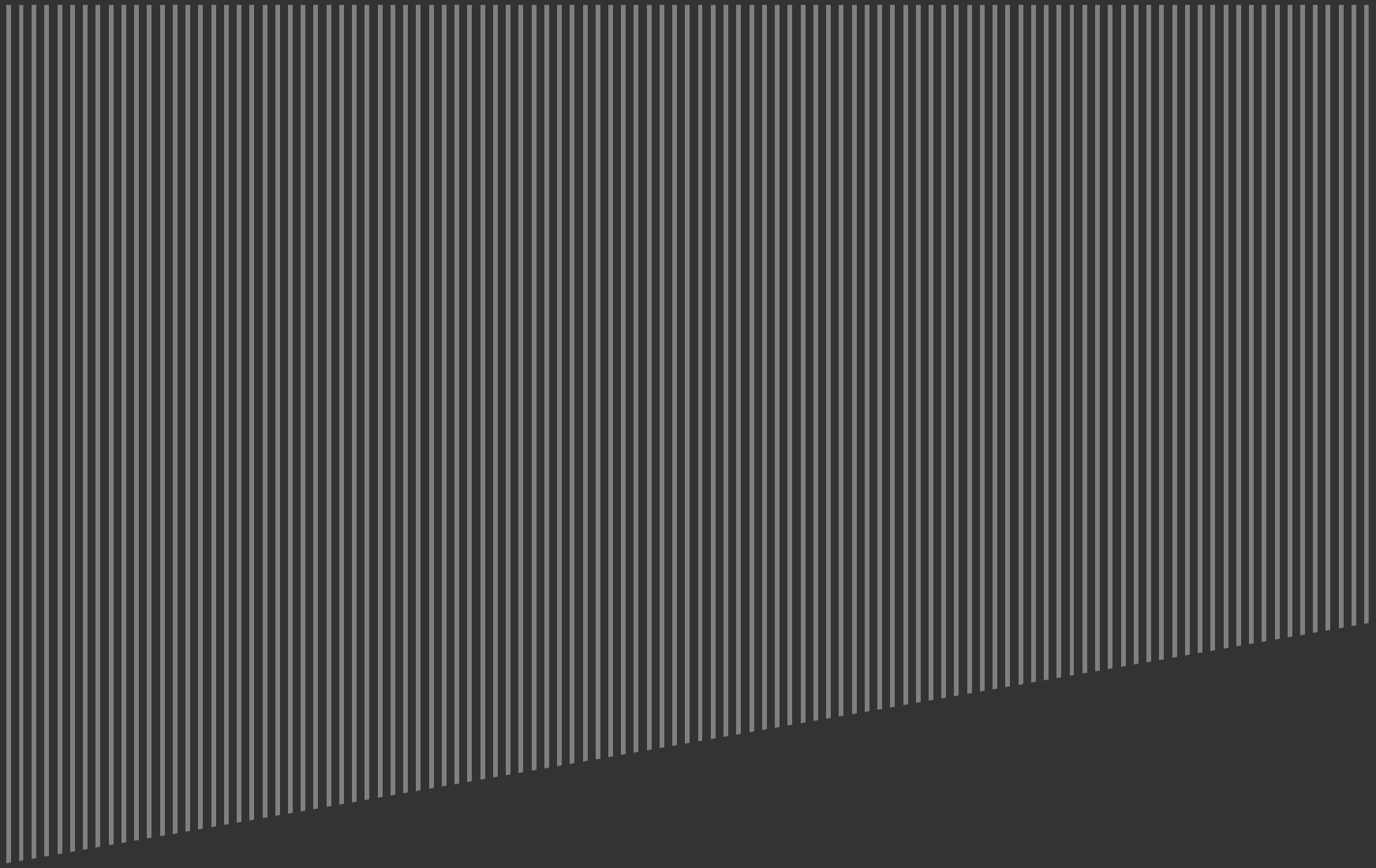
Updated COSO framework

Principles-based approach: the principles are the fundamental concepts associated with the components of internal control. It is generally expected that all principles will, to some extent, be present and functioning for an organization to have effective internal control. When a principle is not being met, some form of internal control deficiency exists.

1. Control environment	1. Demonstrates commitment to integrity and ethical values 2. Board of Directors demonstrates independence from management and exercises oversight responsibility 3. Management, with Board oversight, establishes structure, authority and responsibility 4. The organization demonstrates commitment to competence 5. The organization establishes and enforces accountability	**Principles in the framework**
2. Risk assessment	6. Specifies relevant objectives with sufficient clarity to enable identification of risks 7. Identifies and assesses risk 8. Considers the potential for fraud in assessing risk 9. Identifies and assesses significant change that could impact system of internal control	
3. Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures	
4. Information and communication	13. Obtains or generates relevant, quality information 14. Communicates internally 15. Communicates externally	
5. Monitoring	16. Selects, develops and performs ongoing and separate evaluations 17. Evaluates and communicates deficiencies	

Anti-fraud management program

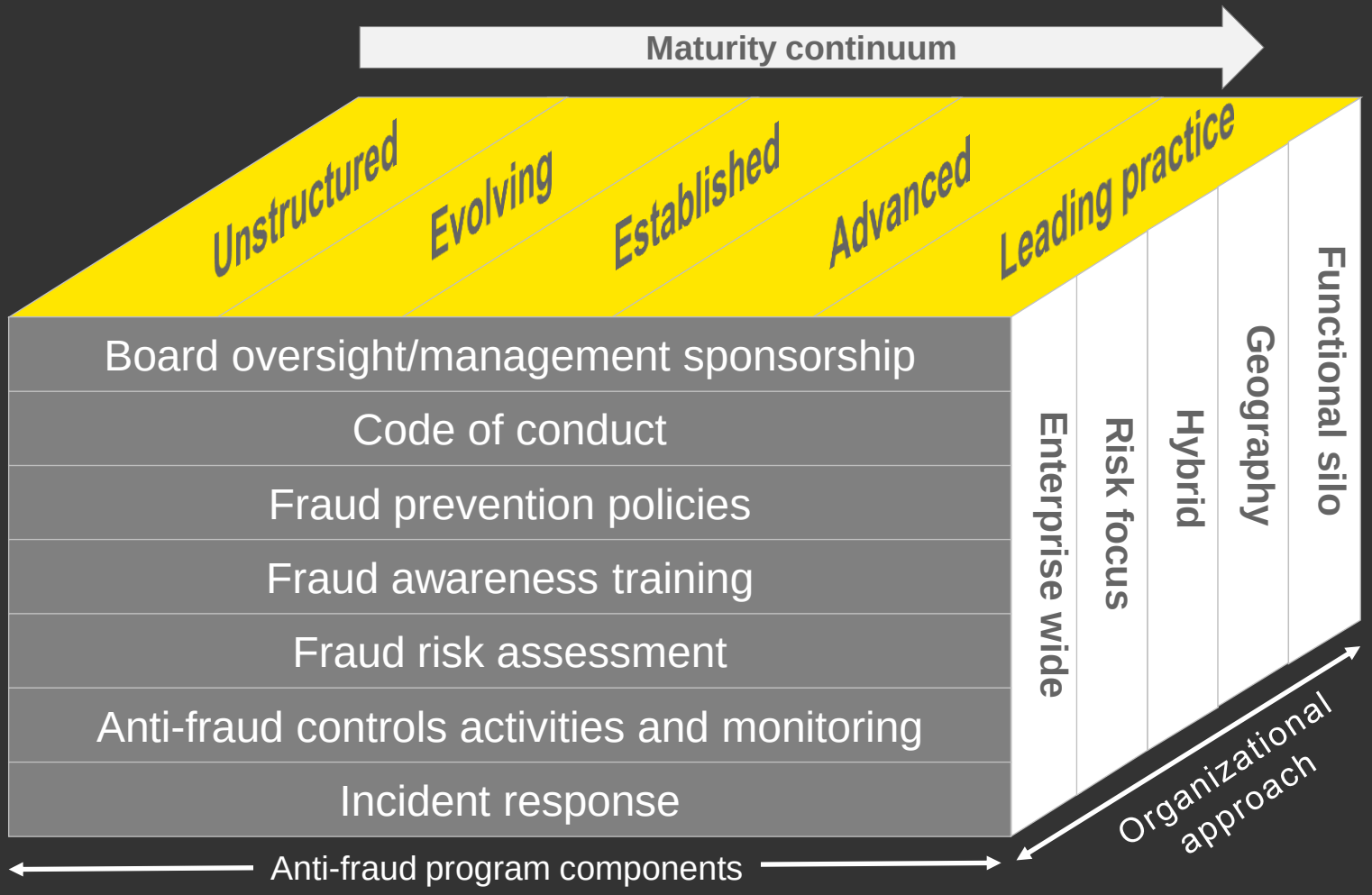
(Focusing on culture and controls to reduce risk)



Mature anti-fraud management programs build off of the BI&CC framework

- Address all core program elements
- Start with governance and tone at the top regarding the company's tolerance of fraud
- Address education of employees about fraud
- Provide reporting options and encourage reporting
- Provide non-retaliation policy
- Map fraud risks to controls
- Address control weaknesses and program gaps

Fraud risk management maturity model



ACFE 2014 Report to the Nations
Frequency of anti-fraud controls

- Presence of anti-fraud controls
  - Reduced fraud losses
  - Shorter fraud duration
- 18 anti-fraud controls in the survey
- Most are present in the BI&CC framework
- All percentages are higher in organizations with 100+ employees

- Code of conduct – 77.4%
- IA department – 70.6%
- Management review – 62.6%
- Independent audit committee – 62.0%
- Hotline – 54.1%
- Employee support programs – 52.4%
- Fraud training (management and employees separate in survey) – 47.8%
- Anti-fraud policy – 45.4%
- Dedicated fraud department, function or team – 38.6%
- Proactive data monitoring/analysis – 34.8%
- Formal fraud risk assessment – 33.5%
- Surprise audits – 33.2%
- Job rotation/mandatory vacation – 19.9%
- Rewards for whistleblowers – 10.5%

Maturity continuum defined

Anti-fraud program elements	Basic	Evolving	Established	Advanced	Leading practice
Board oversight/ management responsibility	Almost nothing exists for the element	Some parts of this element exist; application on different levels is inconsistent	Element is defined; consistently applied on some but not all levels	Element is defined with more detail and applied consistently on most levels	Element is defined in detail and consistently applied on all levels involved
Code of conduct					
Fraud prevention policies					
Fraud awareness training and communication					
Fraud risk assessment					
Controls activities and monitoring					
Incident management and response					

Board oversight/management responsibility

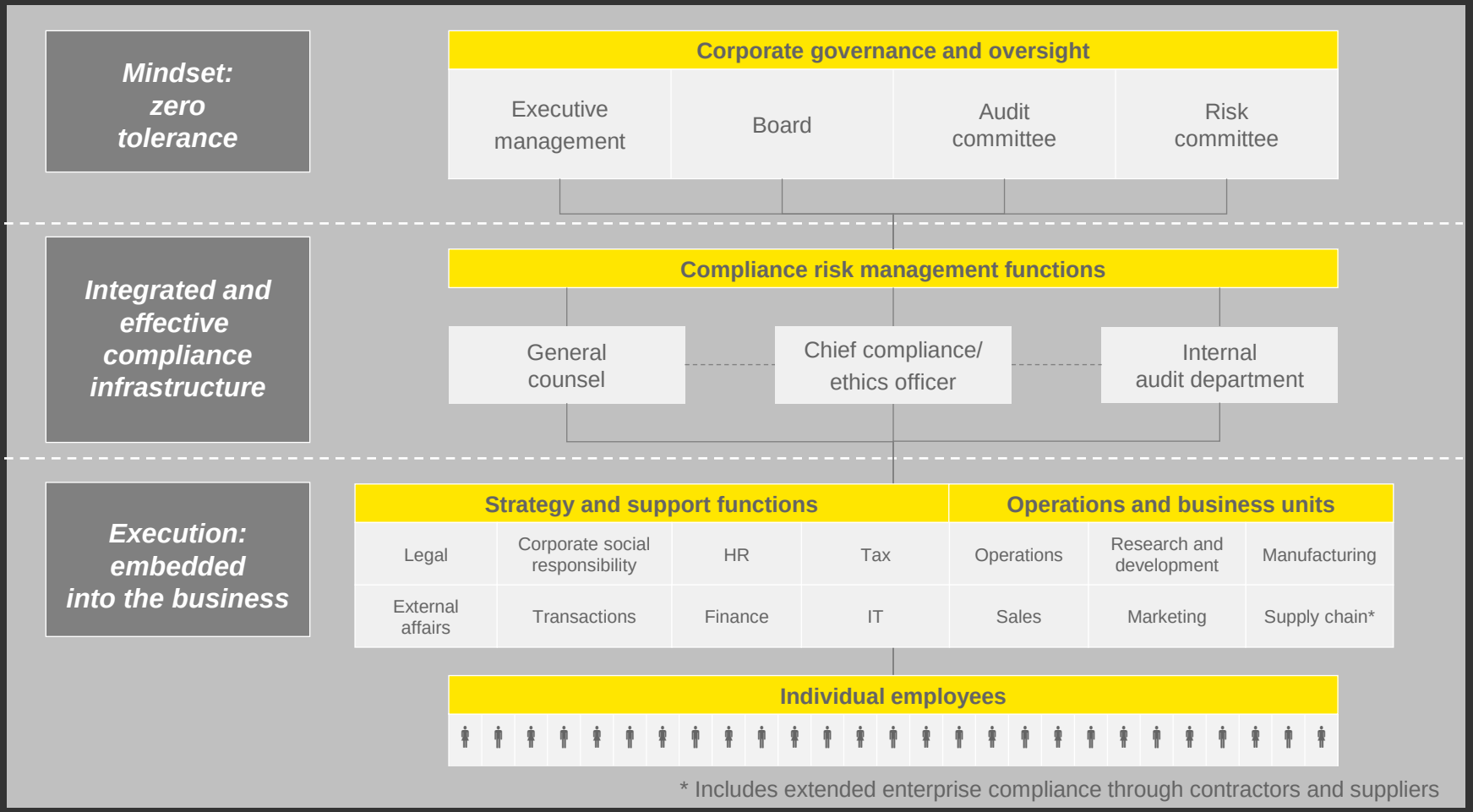
Basic

Minimal briefings to board; management delegates compliance and integrity leadership to a functional leader; no formal structures or processes

Leading practice

Compliance and integrity are embedded in the board's comprehensive risk management, governance and management review processes; management ensures an effective compliance program at all levels

Responsibility for compliance lies throughout the organization



* Includes extended enterprise compliance through contractors and suppliers

Forms of ownership of an anti-fraud program

Enterprise-wide approach

- Oversight from anti-fraud committee at executive management or board level
- Execution by:
  - Task force
  - Program management office (PMO)
  - Corporate compliance department
- Used by diversified life insurance company and an engineering, procurement and construction company

Functional-specific (silo) approach

- Ownership of fraud risk is at functional level
- Example silos:
  - Finance
  - Compliance
  - Global security
  - Geographically based
  - Business unit, division or segment based
- Most common approach

Hybrid approach

- Diversified industrial products company
  - Corporate-level oversight, e.g., chief compliance officer
  - Execution by PMOs within each major business unit or division (i.e., distinct silos)
- Apparel retail company
  - Oversight by chief financial officer
  - Execution by senior business leaders assigned to major risk category

Risk-focused approach

- Ownership of fraud risk is by risk category
- Example categories – program owner:
  - Financial reporting – CFO
  - FCPA – compliance officer
  - Loss prevention – security
  - Antitrust – legal
- Owners report separately to board-level committee
- Used by international heavy-machinery manufacturer

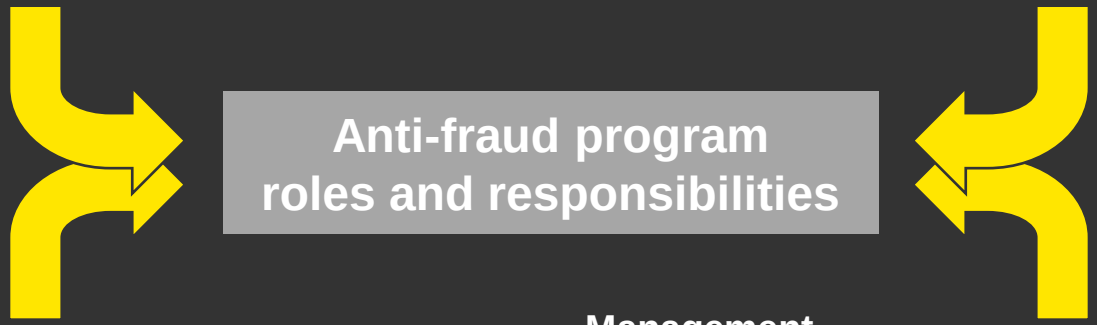
Managing fraud within the organization

Board of Directors

- Sets the proper tone
- Ensures management designs effective fraud risk management policies
- Establishes mechanisms to ensure it receives accurate and timely information
- Monitors the effectiveness of the anti-fraud program

Audit Committee

- Composed of independent board members
- Active role in the risk assessment process
- Fraud risks monitored via internal auditing
- Direct reporting channel for external audit



Internal Audit

- Ensures fraud prevention and detection controls are sufficient for identified risks
- May be responsible for investigating suspected instances of fraud
- Company charter should dictate Internal Audit's role with respect to anti-fraud development

Management

- Is responsible for design, implementation and day-to-day execution of the anti-fraud program
  - Setting the proper tone
  - Reactive
  - Proactive
- Reinforces setting the proper tone at the top
- Helps to create a culture of zero fraud tolerance

Code of conduct (tone at the top) regarding fraud

Basic

Code only addresses subjects required by corporate governance rules in legalistic terms and one language; no/minimal management communication

Leading practice

Code is recognized as a mutual commitment among the organization's stakeholders to the organization's values, standards of behavior and culture; effectiveness is measured

Code of conduct regarding fraud
Leading practices

- Recognized as a mutual commitment among the organization's stakeholders
- Periodically refreshed to reflect the organization's risks
- Specifically addresses fraud
- Translated into local languages
- Senior management makes periodic communications
- Effectiveness is measured and reported
- Actively encourages employees to "speak up"

ACFE 2014 Report to the Nations
on “speaking-up”

Tips are consistently and by far the most common detection method.

In 2014 report, 42.2% of cases showed a tip as the most common method of initial detection of occupational fraud. Management review is second at 16%.

Organizations with hotlines

- Were much more likely to catch fraud by a tip
- Detected the fraud 50% quicker
- Experienced frauds that were 41% less costly

Policies, procedures, processes and controls for fraud prevention and detection

Basic

Entity-level compliance policies for certain risks addressed in the code of conduct with limited procedural guidance for business-unit adaptation

Leading practice

Periodic assessment of policies and procedures; periodic assessment of the effectiveness of the process and control environment in the organization's operations and integrated into "life cycle" management

Anti-fraud policies and procedures
Leading practices

- Guidance for identified fraud areas/risks; expanding on Fraud Tree as applicable to the organization
  - Financial statement misstatement
  - Asset misappropriation
  - Corruption and bribery
- Related policies and procedures, for example:
  - Hiring ethical employees
  - Hiring and managing ethical third parties
- Corresponding entity-level and business-unit controls
- Communicated to employees and third parties
- Periodic assessment for effectiveness; integrated into “life cycle” management

Fraud awareness training and communication

Basic

Informal on-the-job training with no clear links to specific fraud risks/controls; limited to no ongoing communication regarding fraud risks/issues

Leading practice

Fraud awareness courses are delivered through a learning management system that sets curricula for job requirements of new and experienced personnel, assesses audience engagement, tests comprehension and tracks completion; compliance and integrity advisors build open relationships with the business

Fraud awareness training and communication
Leading practices

- Given to employees and third parties periodically
- Considers new hire, re-assignment and promotion needs
- Clear guidance on:
  - Prevention
  - Red flags
  - Reporting suspicious activity
  - Disciplinary actions
- Updated to address emerging fraud risks, issues and trends based on “life cycle” management process
- Incorporates realistic and relevant scenarios
  - Media reports
  - Actual events within the organization (sanitized)

Fraud risk assessment

Basic

No comprehensive fraud risk assessment process

Leading practice

Fraud risk assessment process and risk mitigation plans are utilized to drive resource allocation and program activities; risk monitoring provides leadership with early warning insights for improved strategic and operational decision making and management of enterprise risks

Fraud risk assessment

Leading practice: repeatable process

1 Plan — Confirm goals and schedule

- Assemble the proper team, considering:
  - Key stakeholders
  - Technical expertise
  - Industry knowledge
- Understand and refine the fraud risk universe
- Communicate the goals of the assessment to the organization

2 Assess — Assess current state of fraud risks

- Conduct interviews
- Lead facilitated sessions
- Distribute questionnaires and surveys
- Identify fraud risks present in the organization
- Assess the potential impact of risks to the organization

3 Respond — Identify gaps, strengths and recommendations

- Map identified risks to internal controls
- Assess effectiveness of the controls
- Compare to leading practices
- Perform sample testing
- Determine level of risk and assign priority ratings to risks identified

4 Report — Findings and recommendations

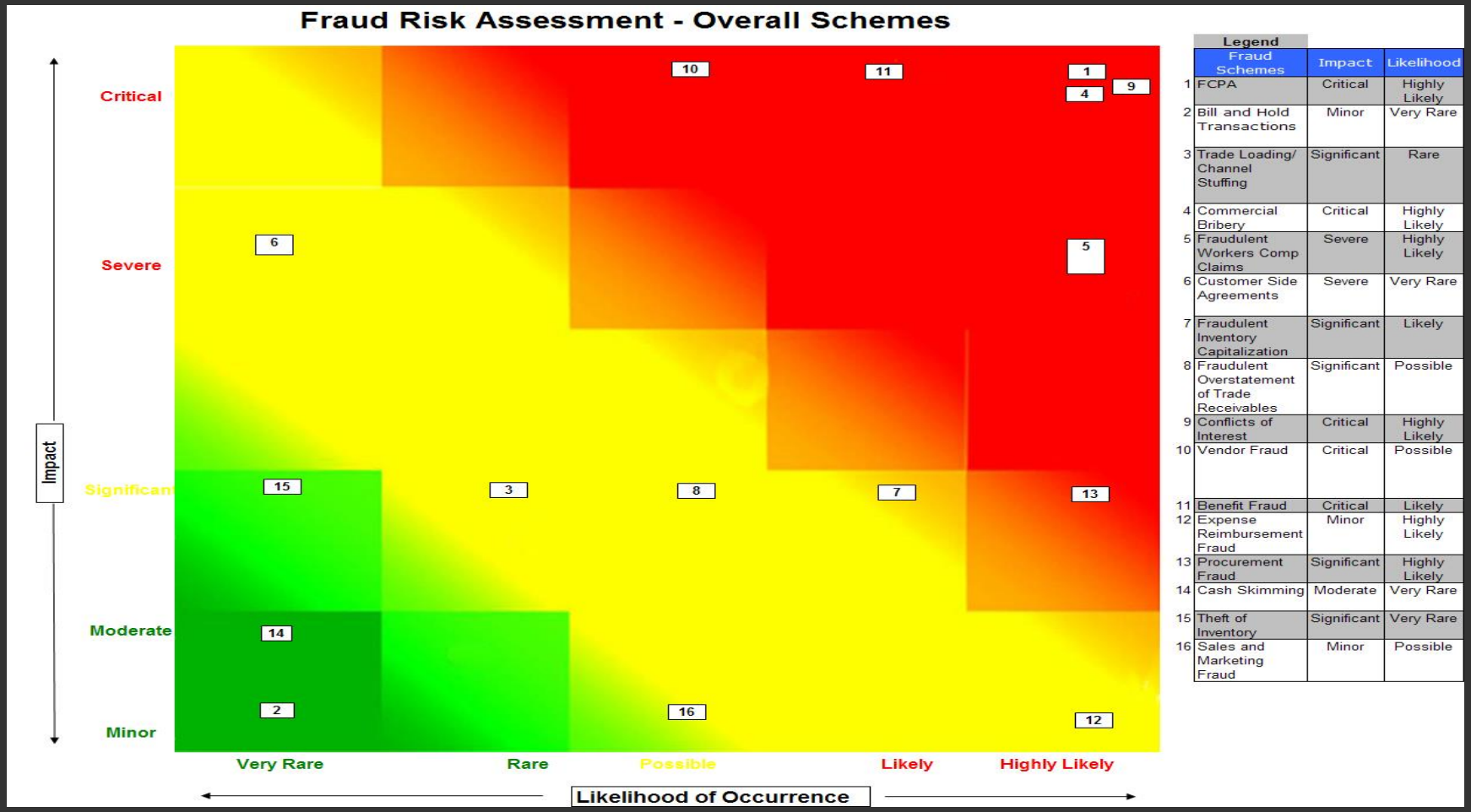
- Determine and document management's response to residual risk
  - Avoid
  - Transfer
  - Mitigate
  - Assume
- Determine plan for continuous monitoring of identified risks

Continuous coordination between management and assessment team

Fraud risk assessment
Leading practice: consider fraud risk factors

- Fraud risk universe specific to the organization
- Fraud Tree
  - Financial and non financial reporting
  - Safeguarding cash, inventory and other assets
  - Corruption, bribery and conflicts of interest
- Fraud Triangle
  - Pressures
  - Opportunities
  - Rationalizations
- Other
  - Management bias
  - Technology and management's ability to manipulate data
  - Government and regulatory enforcement actions

Fraud risk assessment
Leading practice: fraud risk ranking



Legend			
	Fraud Schemes	Impact	Likelihood
1	FCPA	Critical	Highly Likely
2	Bill and Hold Transactions	Minor	Very Rare
3	Trade Loading/ Channel Stuffing	Significant	Rare
4	Commercial Bribery	Critical	Highly Likely
5	Fraudulent Workers Comp Claims	Severe	Highly Likely
6	Customer Side Agreements	Severe	Very Rare
7	Fraudulent Inventory Capitalization	Significant	Likely
8	Fraudulent Overstatement of Trade Receivables	Significant	Possible
9	Conflicts of Interest	Critical	Highly Likely
10	Vendor Fraud	Critical	Possible
11	Benefit Fraud	Critical	Likely
12	Expense Reimbursement Fraud	Minor	Highly Likely
13	Procurement Fraud	Significant	Highly Likely
14	Cash Skimming	Moderate	Very Rare
15	Theft of Inventory	Significant	Very Rare
16	Sales and Marketing Fraud	Minor	Possible

On going anti-fraud controls activities and monitoring

Basic

No mapping of specific control activities to fraud risks exists, and there are no monitoring activities

Leading practice

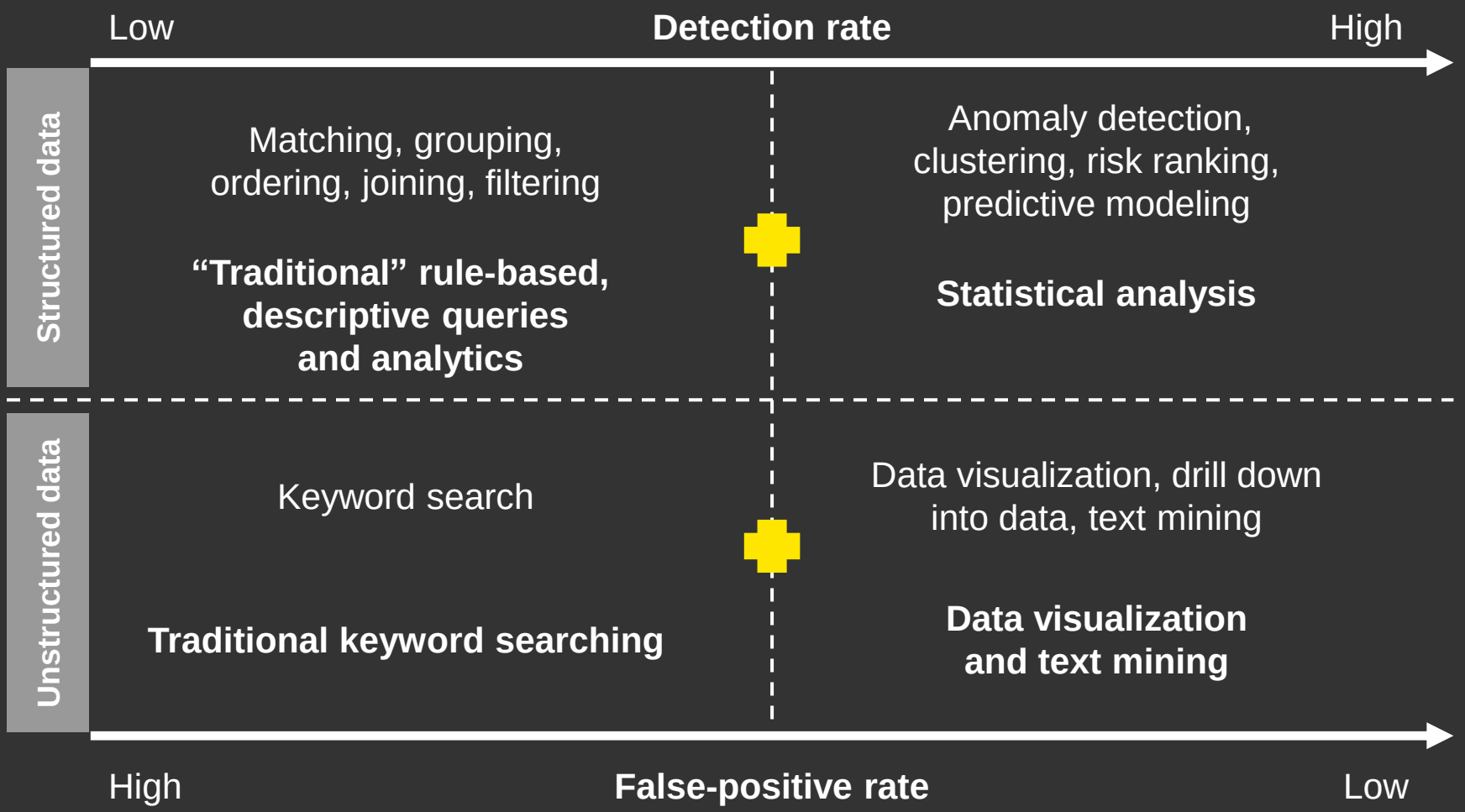
Controls are rationalized against risks to identify most efficient design; monitoring provides leadership with early warning insights for improved strategic and operational decision making and management of enterprise risks

Anti-fraud controls activities and monitoring
Leading practices

- Core work processes defined
- Fraud risk assessment mapped to anti-fraud controls identified within core work processes
- Business engages in continuous monitoring of key anti-fraud controls and “red flags” are identified
- Business conducts regular reviews of compliance with anti-fraud policies, procedures and controls
- Anti-fraud management program audited periodically
- Monitoring and auditing reports used to improve the anti-fraud management program
- Monitoring and audit utilize forensic data analytics

Forensic data analytics maturity model

Beyond traditional “rules-based queries” – consider all four quadrants



Confidential reporting and incidence response

Basic

Process for intake and tracking of issues or allegations, and incident response plan does not exist; or if it exists, corporate culture does not support openly asking questions about integrity and compliance concerns, including fraud

Leading practice

"Speak up" culture where employees have confidence in the process; systems provide robust data for updates to management and the board, with proactive use of information tied into program improvements and early warning and escalation

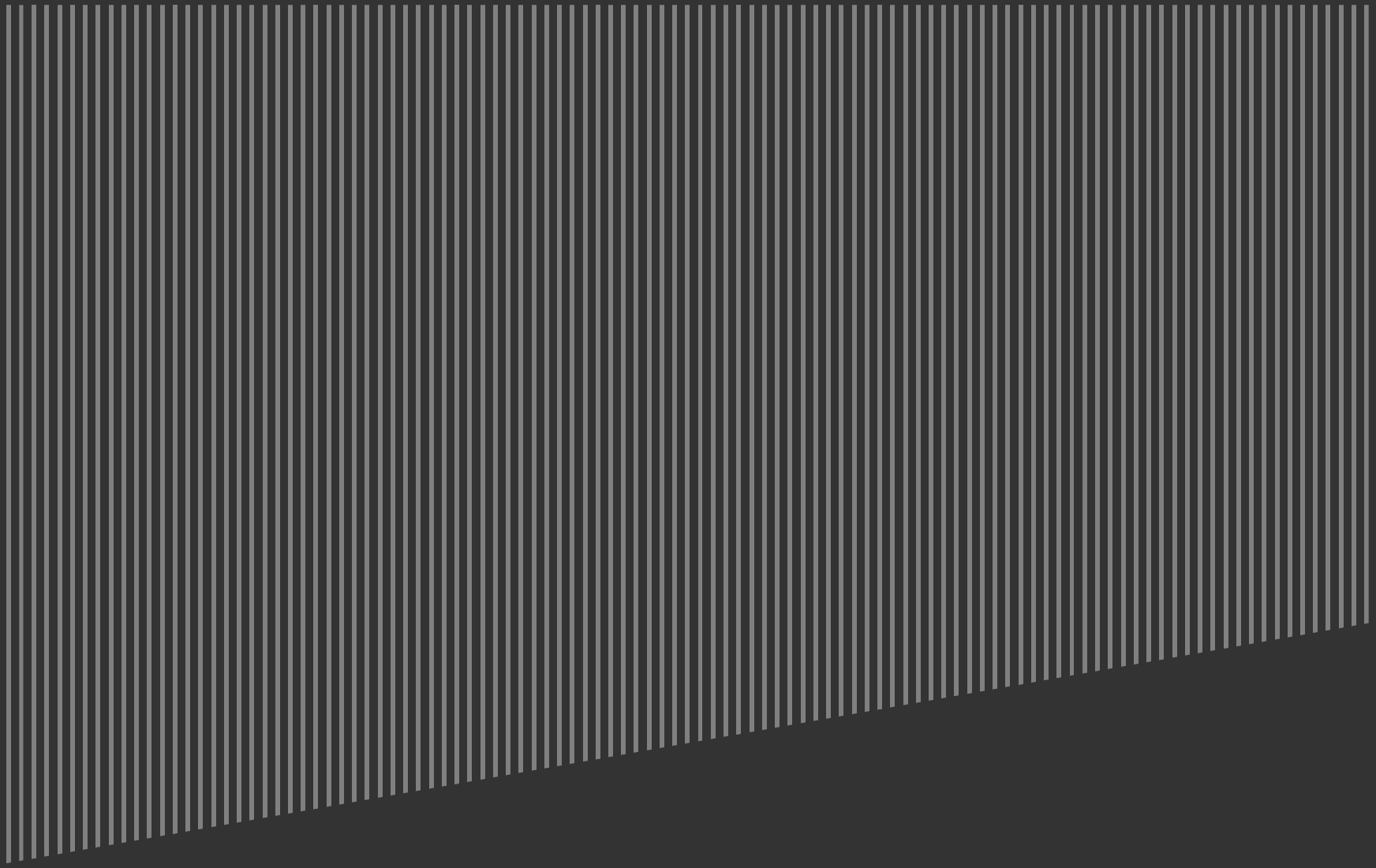
Confidential reporting and incidence response
Leading practices

- Employees encouraged to report/speak up
- Multiple localized reporting mechanisms available to employees globally
- Anonymous reporting mechanism provides for continued communication with a reporter
- Anonymity of employees respected
- Non-retaliation policy enforced at all levels
- Centralized aggregation of reporting
- Triage plan
- Incident and case management system used to track completion of each phase of case resolution, corrective action and remediation processes

Summary
Advancing maturity of the anti-fraud management program

- Anti-fraud management program, as a part of the compliance program, should be built on the company's core values
- Move toward leading practices, as appropriate for the organization
- Inclusion of fraud, specifically in all program elements
- Critical success factors
  - Business integrity, leadership and corporate culture
  - Accountability, oversight and governance
  - Monitoring and continuous improvement
- Anti-fraud management program has a perpetual life cycle

Question and answer session



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.

1405-1251556
ED None

ey.com