The Board's Role in Risk Management

(Nine Questions Every Board Member Should Ask)

January 28, 2016

BDO KNOWLEDGE

BDO

BDO KNOWLEDGE

CPE AND SUPPORT

CPE Participation Requirements – To receive CPE credit for this webcast:

- You'll need to actively participate throughout the program.
- Be responsive to at least 75% of the participation pop-ups.
- Please refer the CPE & Support Handout in the **Handouts** section for more information about group participation and CPE certificates.

Q&A:

Submit all questions using the Q&A feature on the lower right corner of the screen. At the end of the presentation, the presenter(s) will review and answer all questions submitted.

Technical Support:

If you should have technical issues, please contact LearnLive:

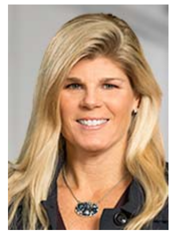
- Click on the **Live Chat** icon under the **Support tab**, OR
- Call: **1-888-228-4088**

BDO

WITH YOU TODAY

Gerard Zack
Managing Director
BDO USA, LLP

Washington, D.C.
Direct: (202) 644-5404
gzack@bdo.com



Amy Rojik
Partner
BDO USA, LLP

Boston, MA
Direct: (617) 239-7005
arojik@bdo.com

LEARNING OBJECTIVES AND AGENDA

- Understand what makes risk management so much more essential today than ever before
- Determine the best risk management governance structure for your organization (board, committee, management, etc.)
- Identify the strengths and weaknesses of your organization's risk management framework and processes
- Identify the right questions to ask in fulfilling your responsibilities as a board member

ASK YOURSELF TWO WARM-UP QUESTIONS:

1. Could all of your organization's senior managers identify the top ten risks that the organization faces, as well as the strategies being employed to address each of these risks?

2. Could all board members explain the organization's approach to risk management?

RISK

A possible event or circumstance that can have negative influences on the organization

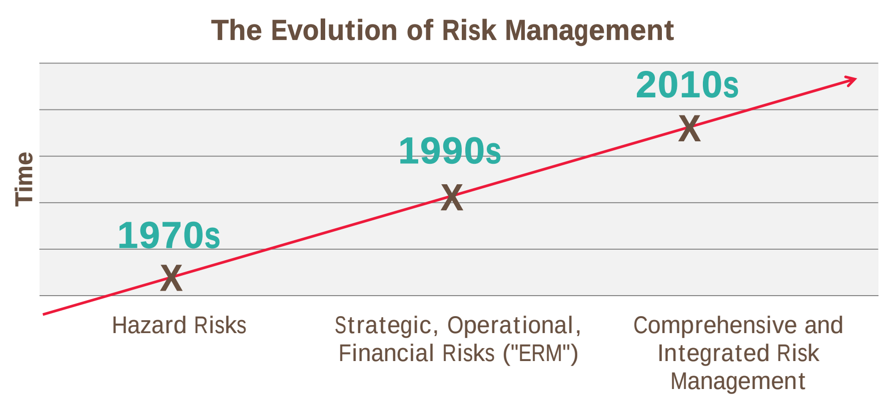
- Internal or external
- Varying degrees of control

Includes lost opportunity

INTRODUCTION TO RISK MANAGEMENT

- A Brief History of Risk Management
- Factors that Make Risk Management More Essential than Ever

A BRIEF HISTORY OF RISK MANAGEMENT



BDO KNOWLEDGE

WHAT MAKES IT SO ESSENTIAL?

1. It is the glue that connects strategy with all of our day-to-day activities
2. It is expected by stockholders, customers, regulators, auditors, and others
3. It is the key to minimizing corporate liability (e.g., vicarious liability of the organization for actions taken by employees, agents, etc.)

BDO

BDO KNOWLEDGE

DO WE NEED ANY MORE EXAMPLES OF POOR RISK MANAGEMENT?

1. Automobile and other product recalls
2. Oil spills and other man-made accidents
3. Insufficient preparation for natural disasters
4. Acquisitions gone bad
5. Accounting frauds

BDO

BDO KNOWLEDGE

ACCOUNTING FRAUDS?

- Yes – poor risk management is at the heart of most accounting frauds and other intentional acts of non-compliance
- Vast majority of accounting frauds triggered by falling short of a financial target
- Risks leading to the fraud:
  1. Unrealistic targets (a strategic or operational risk), or
  2. Under-performing (target was okay, but unforeseen operational or market risks)

BDO

BDO KNOWLEDGE

REQUIREMENTS FOR RISK MANAGEMENT

Dodd-Frank Act:

Requires board-level risk committees for public bank holding companies and certain non-public financial institutions

SEC:

Disclosure Requirement in Proxy Statements (starting 2010) requires companies to describe the board's role in the oversight of risk

COSO:

Framework for internal controls requires risk assessments

BDO

COSO – INTERNAL CONTROL

Principle 7:

"The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed."

Internal Control – Integrated Framework (2013)
Committee of Sponsoring Organizations (COSO)

COSO – INTERNAL CONTROL

Principle 8:

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

Internal Control – Integrated Framework (2013)
Committee of Sponsoring Organizations (COSO)

BDO KNOWLEDGE

MINIMIZE CORPORATE LIABILITY

"DOJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low risk area because greater attention and resources had been devoted to a higher risk area."

A Resource Guide to the U.S. Foreign Corrupt Practices Act (2012)

BDO

BDO KNOWLEDGE

MINIMIZE CORPORATE LIABILITY

"The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement or modify each requirement [of the program] to reduce the risk of criminal conduct."

United States Sentencing Guidelines
Chapter 8 – Sentencing Organizations

BDO

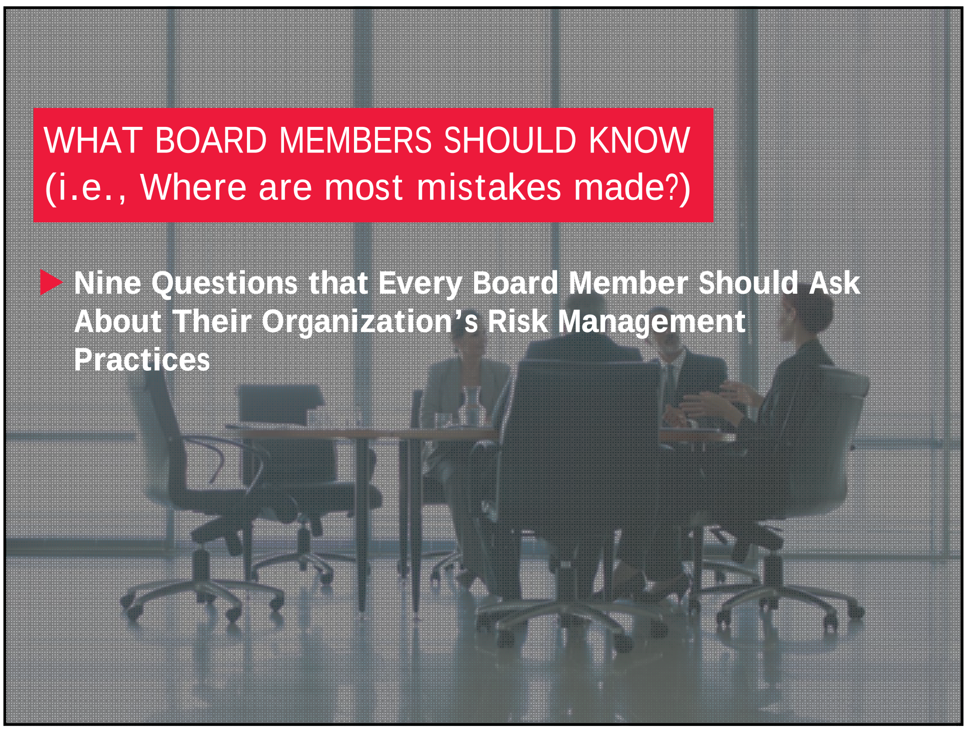
BDO KNOWLEDGE

AT THE BROADEST LEVEL, RISK MANAGEMENT IS IMPORTANT BECAUSE:

- Every entity exists to realize value for its stakeholders, and
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day

Page 17

BDO



BDO KNOWLEDGE

EVERYONE HAS A ROLE

- **Board**
  - Oversight and direction
- **Senior Management**
  - Implement, execute, monitor, report
- **Staff**
  - Roles tailored to position, risk awareness

BDO

BDO KNOWLEDGE

QUESTION NO. 1

Is there a sound governance structure in place for risk management, with well defined roles and open dialogue regarding risk

?

BDO

THE ROLE OF THE BOARD

"An area of increasing importance for boards and which is closely related to corporate strategy is oversight of the company's risk management. Such risk management oversight will involve oversight of the accountabilities and responsibilities for managing risks, specifying the types and degree of risk that a company is willing to accept in pursuit of its goals, and how it will manage the risks it creates through its operations and relationships."

G20/OECD Principles of Corporate Governance (2015)

THREE COMMON MODELS

Risk management oversight by:

1. The full board of directors
2. Adding to the responsibilities of an existing committee (e.g. audit)
3. Establishing a new standing committee solely devoted to risk management

Under all three models, day-to-day risk management should be centered around a senior management official (e.g., Chief Risk Officer)

ROLES OF THE BOARD AND MANAGEMENT

ERM Component	Board/Committee	Senior Management
ERM plan	Support, track progress	Develop and implement
Risk tolerance	Debate and approve	Establish and manage
Risk policies	Approve and monitor	Develop and implement
Risk strategies	Debate, approve, monitor	Formulate and execute
Key risks	Provide input and oversight	Manage and measure
Risk reporting	Monitor, feedback	Analysis and context

RISK COMMITTEE CHARTER

- Committee and charter referenced in the company's governing documents (articles, etc.)
- Charter includes details of committee's:
  - Membership
  - Processes (frequency of meetings, etc.)
  - Responsibilities
  - Authority
  - Reporting

BDO KNOWLEDGE

QUESTION NO. 2

Is there a clear understanding of the organization's appetite to take on risk

?

BDO

BDO KNOWLEDGE

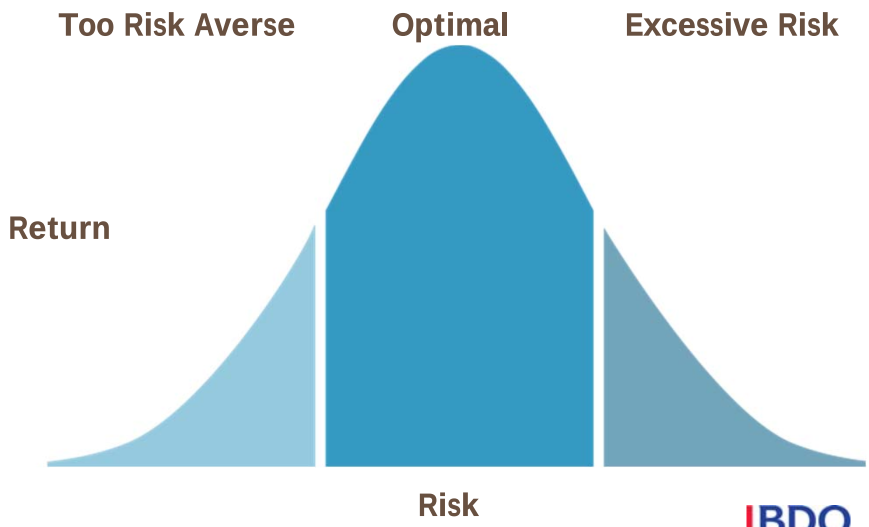
RISK APPETITE

The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. … Risk appetite guides resource allocation. … Risk appetite [assists the organization] in aligning the organization, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks.

BDO

BDO KNOWLEDGE

WHERE IS THE SWEET SPOT OF RISK AND RETURN?



Page 27

BDO

BDO KNOWLEDGE

THREE KEY STEPS TO ADOPTING RISK APPETITE

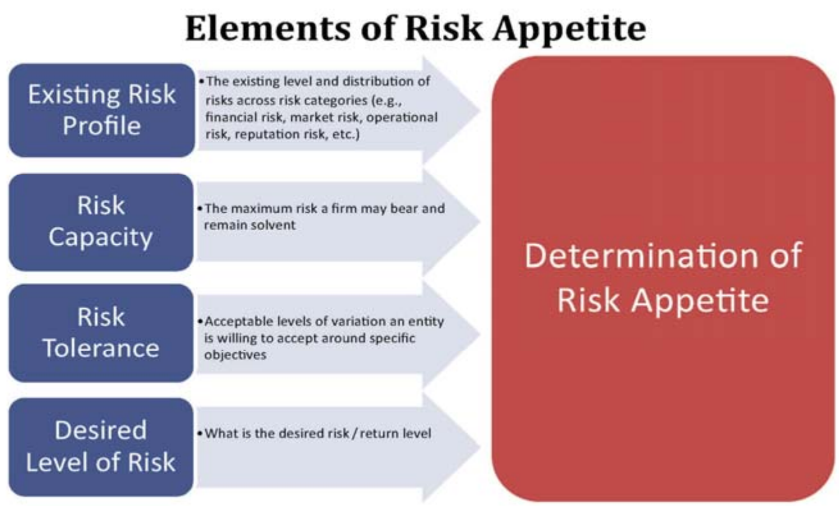
1. Management develops, with board review and concurrence, a view of the organization's overall risk appetite.
2. This view of risk appetite is translated into a written or oral form that can be shared across the organization.
3. Management monitors the risk appetite over time, adjusting how it is expressed as business and operational conditions warrant

Page 28

BDO

BDO KNOWLEDGE

HOW TO ASSESS RISK APPETITE



BDO

BDO KNOWLEDGE

QUESTION NO. 3

Is the risk assessment process linked to objectives and strategy established at the organizational and business unit levels

?

BDO

Enterprise Risk Management (ERM)

"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: *COSO Enterprise Risk Management – Integrated Framework*. 2004.

COSO = Committee of Sponsoring Organizations

(Outside the U.S. the risk management model commonly used is ISO 31000)

QUESTION NO. 4

Does the organization have a comprehensive process in place for identifying potential risks

?

BDO KNOWLEDGE

IDENTIFYING RISKS

Methods:

- Focus groups
- Interviews
- Surveys
- Monitoring of internal data
- External sources (surveys, studies, competitors, etc.)

Best Practices:

- Document inherent risks (i.e., including risks that are assumed to be well controlled)
- Centralize accumulation of identified risks
- Have a process for the identification and documentation of risks outside of the formal risk assessment process
- Don't be afraid to tackle the difficult risks!

BDO

BDO KNOWLEDGE

QUESTION NO. 5

Has the organization adopted a risk management framework that has been properly customized to its needs

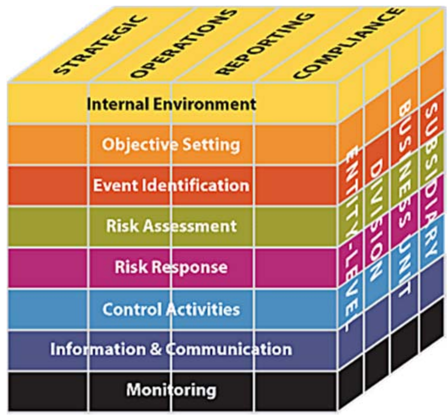
?

BDO

THE COSO ERM FRAMEWORK

Entity objectives (and risks) can be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance



Page 35

A TYPICAL FRAMEWORK & PROCESS

1. Establish risk appetite
2. Determine classification system for risks
3. Identify inherent (gross) risks
4. Assess risks using agreed-upon criteria (e.g., impact, likelihood, velocity, trend, etc.)
5. Consider effectiveness of existing controls
6. Measure residual (net) risk
7. If residual risk > tolerable risk, design and implement risk mitigation
8. Monitor and report

Page 36

EXAMPLE OF AN IMPACT ASSESSMENT SCALE FOR THE RISK OF FRAUD

BDO KNOWLEDGE

Rating	Descriptor	Definition
5	Catastrophic	• Financial loss to organization is in excess of $100 million • International long-term media coverage • Widespread employee morale issues and multiple senior leaders leave • Incident must be reported to authorities; significant sanctions and financial penalties result
4	Major	• Financial loss to organization is between $20 million and $100 million • National long-term media coverage • Widespread employee morale problems and turnover • Incident must be reported to authorities and sanctions against company result
3	Moderate	• Financial loss to organization is between $1 million and $20 million • Short-term regional or national media coverage • Widespread employee morale problems • Incident must be reported to authorities and immediate corrective action is necessary
2	Minor	• Financial loss to organization is between $10,000 and $1 million • Limited local media coverage • General employee morale problems • Incident is reportable to authorities, but no follow-up
1	Incidental	• Financial loss to organization is less than $10,000 • No media coverage • Isolated employee dissatisfaction • Event does not need to be reported to authorities

BDO

EXAMPLE: ASSESSING LIKELIHOOD

BDO KNOWLEDGE

Rating	Based on Annual Frequency		Based on Probability of Occurrence	
	Descriptor	Definition	Descriptor	Definition
5	Very frequent	More than twenty times per year	Almost certain	> 90% chance of occurrence
4	Frequent	Six to twenty times per year	Likely	65% to 90% chance of occurrence
3	Reasonably frequent	Two to five times per year	Reasonably possible	35% to 65% chance of occurrence
2	Occasional	Once per year	Unlikely	10% to 35% chance of occurrence
1	Rare	Less than once per year	Remote	< 10% chance of occurrence

BDO

BDO KNOWLEDGE

QUESTION NO. 6

How does the organization evaluate the extent to which existing controls and processes mitigate the identified risks

?

BDO

BDO KNOWLEDGE

RESIDUAL RISK

Inherent Risk − Effectiveness of Internal Controls = Residual Risk

- The effectiveness of internal controls can also be "scored" to arrive at the net/residual risk (benefit of controls should not result in net risk of zero, only to "low")
- Map risks to specific controls
- ID which controls mitigate likelihood (generally preventive and directive controls) and which mitigate impact (generally detective and corrective)

BDO

BDO KNOWLEDGE

QUESTION NO. 7

Are risk metrics properly aligned with identified risks and organizational strategy

?

Page 41

BDO

BDO KNOWLEDGE

RISK METRICS

- Link each risk to relevant data
- Internal and external data
- Categories of risk data:
  - Leading indicators
  - Internal control indicators (i.e. breakdowns in controls)
  - Event indicators
  - Lagging indicators
- Centralized vs. de-centralized data monitoring
- Dashboard reporting

Page 42

BDO

QUESTION NO. 8

How have risk awareness and risk management been embedded into the daily activities of the organization

?

Page 43

EMBED RISK MANAGEMENT VIA:

1. Training
2. Periodic communications (e-mails, newsletters, etc.)
3. Strategic planning
4. Budgeting
5. Corporate governance
6. Training programs
7. Staff meetings
8. Performance measurement and evaluation

Page 44

QUESTION NO. 9

Is there an ongoing dialogue about risk within and between each level of the organization

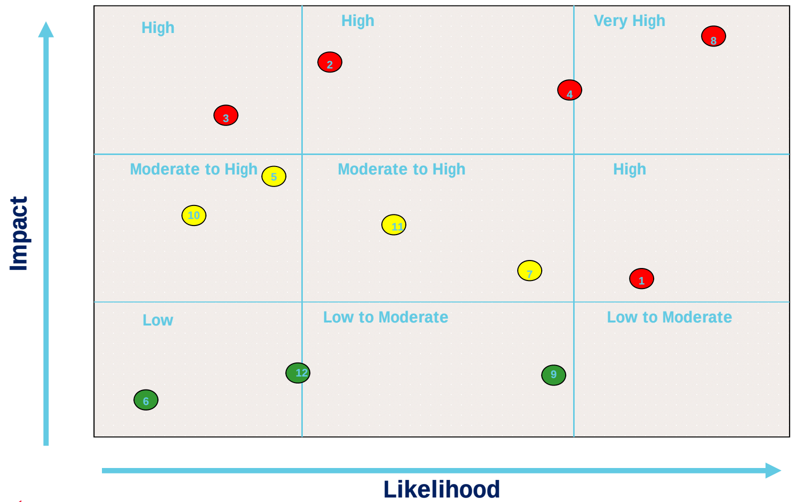
?

KEEP THE DIALOGUE OPEN

- Risk management is an ongoing process, not a periodic step
- Internal risk committee
- Brainstorm the "unknown" risks (it's easy to talk only about the "known" risks)
- Periodic reporting to board/committee
  - The board needs to know "what are our organization's most critical risks and what are we doing about them?"

EXAMPLE DASHBOARD OF A HEAT MAP

BDO KNOWLEDGE

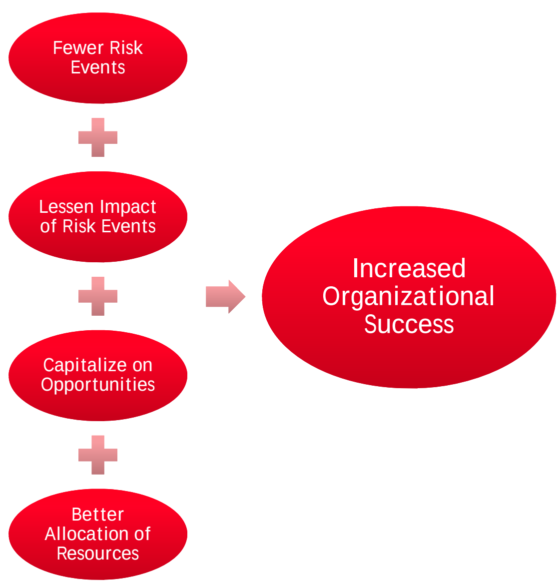


BDO

WHEN ERM WORKS PROPERLY

- It does more than enable the organization to identify risks in a more timely manner and deal with those risks
- It helps to identify opportunities for the organization
- It enhances the strategic, operational, and financial planning processes

THE RETURN ON YOUR ERM INVESTMENT



BDO KNOWLEDGE

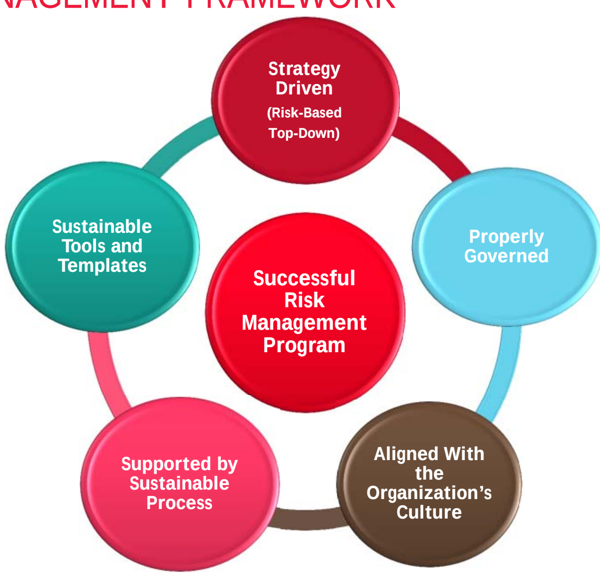
COMMON ERM ATTRIBUTES &D BEST PRACTICE RESULTS

Attribute	Best Practice Result
Program Mindset	Not a once-and done exercise
Formal Measurement	Integrated and cross-functional portfolio view of risk, no silos, with consideration to both up and downside risks
Established Scope	All key risks addressed, not just financial (e.g., operational and strategic)
Program Purpose	Long-term approach to using risk-informed decision making to govern the organization in a way that increase organizational value

BDO

BDO KNOWLEDGE

BUILDING SUSTAINABILITY INTO YOUR RISK MANAGEMENT FRAMEWORK



BDO

BDO KNOWLEDGE

GET TO KNOW BDO

BDO commits significant resources to keep our professionals and our clients up to date on current and evolving technical, governance, industry and reporting developments. Visit http://www.bdo.com for all of our offerings.

To begin receiving email notifications regarding BDO publications and event invitations (live and web-based), visit https://www.bdo.com/member/registration and create a user profile. If you already have an account on BDO's website, visit the My Profile page to login and manage your account preferences https://www.bdo.com/member/my-profile.

BDO

BDO KNOWLEDGE

GET TO KNOW BDO

INDUSTRY EXPERIENCE

Industry experience has emerged at the top of the list of what businesses need and expect from their accountants and advisors. The power of industry experience is perspective - perspective we bring to help you best leverage your own capabilities and resources.

BDO's industry focus is part of who we are and how we serve our clients, and has been for over a century. We demonstrate our experience through knowledgeable professionals, relevant client work and participation in the industries we serve.

A variety of publications and insights depicting specific industry issues, emerging trends and developments are available. For further information on the following BDO industries, please visit **https://www.bdo.com/industries**.

- Asset Management
- Broker Dealers
- Consumer Business
- Financial Services
- Gaming, Hospitality & Leisure
- Government Contracting
- Healthcare
- Insurance
- Manufacturing & Distribution
- Natural Resources
- Nonprofit & Education
- Private Equity
- Public Sector
- Real Estate & Construction
- Restaurants
- Technology & Life Sciences

BDO

EVALUATION

We continually try and improve our programming and appreciate constructive feedback.

Following the program, we will be sending out a thank you e-mail that contains a link to a brief evaluation.

Thank you in advance for your participation!

CONCLUSION

Thank you for your participation!

Certificate Availability - If you participated the entire time and responded to at least 75% of the polling questions, click the **Participation tab** to access the print certificate button.

Please exit the interface by clicking the red "X" in the upper right hand corner of your screen.

SPEAKER BIOGRAPHIES

BDO KNOWLEDGE

BIOGRAPHY

Gerard M. Zack
CFE, CPA, CIA, CRMA
BDO Consulting
Managing Director

gzack@bdo.com
Direct: 202-644-5404

Gerry Zack has more than 30 years of experience providing clients with fraud, compliance, and operational risk assessment and mitigation, enterprise risk management, internal and external audit, and investigative services. He has experience designing and delivering internal risk management and risk awareness programs for organizations, as well as anti-fraud and corruption training and education programs for a wide variety of industries and companies worldwide. In addition to serving clients, he held the position of Chief Operating Officer for an international scientific organization for two years, where he oversaw the risk management function of the organization.

Among Mr. Zack's credentials is a Certification in Risk Management Assurance. For more than 8 years, he has served on the faculty of the Association of Certified Fraud Examiners, providing anti-fraud training to companies of all sizes, including multinational organizations, and was elected to their Board of Regents for 2014 and 2015, serving as Chair for 2015. He is a frequent speaker at national conferences, including several times at AICPA industry conferences. He will be speaking on fraud risk assessments at the 2016 IIA Regional Conference in Memphis this May.