Internal Audit, Risk Management, and Other Hot Topics for Financial Services

February 5, 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Create Opportunities

Disclaimers

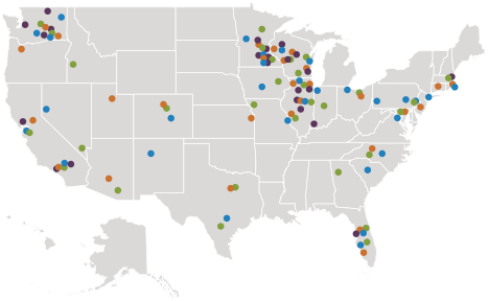
The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623**.
- Please submit your questions via the questions function at any time during the presentation.
- The **PowerPoint presentation**, as well as the **webinar recording**, will be sent to you within the next 10 business days.
- Please complete our online survey.

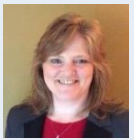
About CLA

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- More than 6,100 employees
- Offices coast to coast
- Serving 1,500+ financial institutions



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

Speaker Introductions

Today's Presenters	
	Mark Hornung – Managing Principal, Business Risk Services
	Amy Koshiol – Director, Financial Services Compliance
	John Moeller – Principal, Information Security Leader for Financial Services
	Liz Rider – Principal, Financial Services Market Leader

Today's Agenda

- Financial Risk
- Compliance Risk
- IT Risk
- Evaluating Governance
- Closing

Polling Question

Has your financial institution experienced an employee fraud at any time during the past three years?

Yes

No

ACFE Fraud Report: Fraud Statistics and Trends

Key Findings – Fraud Perpetrators*

- Losses increase based on the employee level
  - Owner/executive average loss is $703,000
  - Manager average loss is $173,000
- 95 percent of offenders are first timers
- 88 percent passed background checks (only 5 percent had some type of prior conviction)
- 39 percent demonstrated misconduct at work
  - 18 percent bullying/intimidation
  - 11 percent excessive absenteeism
  - 10 percent excessive tardiness

Financial Risks

- Instances of fraud in 2018
  - Wire transfers
  - Third party repossessed vehicles, sold, and stole proceeds
  - Suppressed transactions on members account used to hide large withdrawals
  - Abuse of accounts payable policy limits
  - ID theft, ransomware, and hacked emails

Financial Risks

- Instances of fraud in 2018
  - CLO took kick-backs from business to provide preferential deals in exchange for ignoring questionable income sources
  - Manipulation of loan due dates to mask delinquency

Financial Risks

- Instances of fraud in 2018
  - Lack of segregation of duties:
    - Transfers from customer/member accounts
    - Post to own account
    - Hide delinquencies
    - Paid personal bills
    - Cut checks to self
    - Increased pay rate

Financial Risks

- Impact of accounting changes
- Revenue recognition, leases, and CECL
- Procedures over:
  - Capturing data that might not have been reviewed in the past
  - Estimates made by management
  - Use of information technology
  - Disclosures, if necessary

Tips for Successful FDICIA/SOX 404 Projects

- Well-organized process with properly defined roles and responsibilities between management, control owners, those performing testing, and the external audit firm
- Early planning with external auditors to confirm agreement with work scope
- Address “PCAOB Hot Topics”
  - Information Provided by the Entity (IPE)
  - Electronic audit evidence (spreadsheets)
  - Completeness and accuracy of the population
  - Quality and precision of management review
  - Walkthrough requirements
  - Cloud-vendors control status (SSAE 16 reports)
  - Third party service providers
- Early and periodic key control testing
- Management oversight and monitoring throughout the project

Financial Risks

- FDICIA and SOX 404: common difficulties
  - Lack of consistent methodology
  - Assuming the existing internal audit function is already FDICIA compliant
  - Testing too many controls
  - Not sufficiently testing controls
  - Testing the process instead of the control
  - Internal audit is acting as the control
  - Waiting too long to start testing
  - Ignoring portions of the year
  - Lack of an audit trail
  - Lack of reporting

Polling Question

What is the status of the Compliance Management System (CMS) within your organization?

A. Risk-based CMS system is formally implemented and independently assessed.

B. CMS is informally implemented, and may or may not be independently assessed.

C. Compliance program is sufficient. No strategic intention to place focus on other areas of CMS.

Compliance Risks

- Compliance (Risk) Management System
  - Board and management oversight
    - Adopting clear policy statements
    - Appointing compliance officer with authority and accountability
    - Allocating sufficient resources for complexity
    - Reporting to the board
  - Compliance program
    - Policies and procedures
    - Training
    - Monitoring
    - Consumer complaint response
  - Compliance audit
    - Independent
    - Transaction testing

Compliance Risks

- Fair lending risks on the rise
  - Redlining
  - Intent to apply jointly and spousal signature requirements
  - Fair Lending Program
    - Policy, procedures, risk assessment
    - Internal controls and monitoring
    - Database and transactional testing
    - Comparative file review

Compliance Risks

- HMDA filing for 2018 data
  - Enhanced HMDA reporting increasing fair lending risks
    - Greater ability for data analytics – regulators and special interest groups
    - Know your numbers and your story
  - Filing deadline 3/1/2019
    - Ensure information is scrubbed and accurate
    - Regulators giving a break on data; however, inaccurate data may reflect poorly on fair lending

Polling Question

Has your financial institution run an external IT penetration test over the past year?

Yes

No

IT Risks

- Penetration Testing and Phishing Attacks
  - Cybercriminals are very sophisticated and have monetized their strategies
  - Banks are not doing enough testing and the right kind of testing
  - Weaknesses in patching and password strength are still being exploited
- Strengthen Testing Processes and Frequency
  - Outsource network application and operating system patching via managed services
  - Scan networks monthly for vulnerabilities, outsource reviewing the results
  - Add social engineering tests that the bank can run by using tools from KnowB4, PhishMe, and others
  - Stop relying upon annual external vulnerability scans and run full penetrations tests based upon email phishing
  - Do not forget about social engineering tests (pretext calling and onsite face to face tests)

IT Risks

- Vendor Management Requirements from Federal Financial Institutions Examination Council (FFIEC)
  - Existence and corporate history
  - Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate
  - Other companies using similar services from the provider that may be contacted for reference
  - Financial status, including reviews of audited financial statements
  - Strategy and reputation
  - Service delivery capability, status, and effectiveness
  - Technology and systems architecture
  - Internal controls environment, security history, and audit coverage
  - Legal and regulatory compliance including any complaints, litigation, or regulatory actions
  - Reliance on and success in dealing with third party service providers
  - Insurance coverage
  - Ability to meet disaster recovery and business continuity requirements

IT Risks

- Cloud Migration Strategies
  - — Start with a Cloud Readiness Assessment (CRA)
    - Moving to the cloud can be an emotional decision. Is bank leadership ready?
    - Identify the types of cloud environments that are relevant. Hardware as a Service (HaaS), Infrastructure as a Service (IaaS), Public and Private cloud, and Vendor hosted applications
    - Identify application performance requirements, Wide Area Network speed, Vendor support, Vendor security and history of providing cloud services
    - Compare 5-year costs for bank owned hardware and applications hosted in-house versus bank owned hardware and software hosted in a datacenter versus outsourced fully to the cloud
  - — Identify how roles change for internal IT staff
    - Their positions do not go away when the server stack moves to the cloud
    - Outsource day-to-day activities so IT can focus on strategic initiatives
  - — Identify Financial Impact of moving to the cloud
    - Capital expenses move to operating expenses
    - Total costs may go up so identify the new benefits to justify this

Polling Question

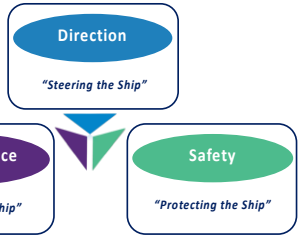
Has your financial institution established an approach to evaluate the quality of your enterprise risk management program?

Yes

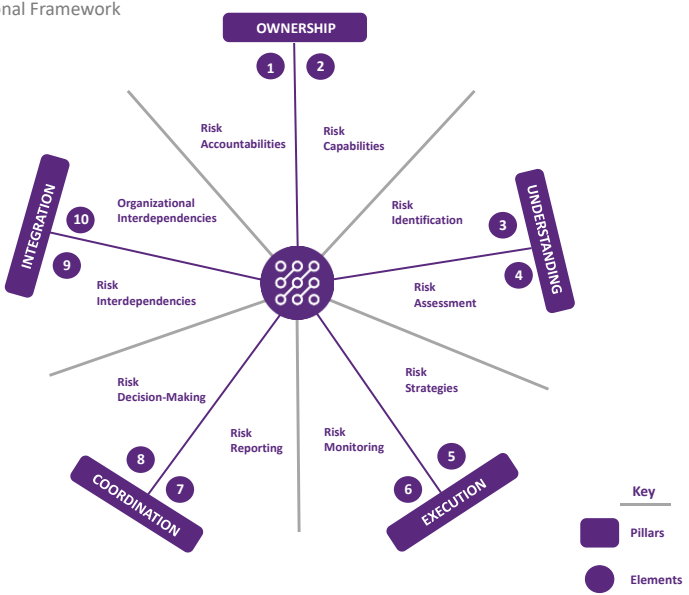
No

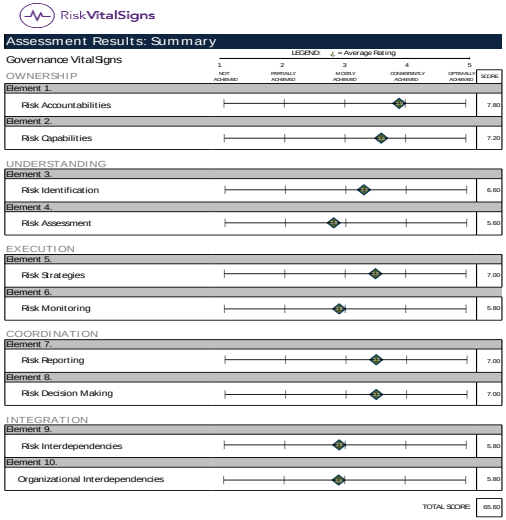
Governance – ERM Leading Practices

Evaluating the Quality of your ERM Program



RiskVitalSigns
Foundational Framework




RiskVitalSigns

Assessment Results: Summary

Governance VitalSigns

LEGEND: ∠ = Average Rating

	1 NOT ACHIEVED	2 PARTIALLY ACHIEVED	3 MOSTLY ACHIEVED	4 CONSISTENTLY ACHIEVED	5 OPTIMALLY ACHIEVED	SCORE
OWNERSHIP						
Element 1.						
Risk Accountabilities				∠		7.80
Element 2.						
Risk Capabilities				∠		7.20
UNDERSTANDING						
Element 3.						
Risk Identification			∠			6.60
Element 4.						
Risk Assessment			∠			5.60
EXECUTION						
Element 5.						
Risk Strategies				∠		7.00
Element 6.						
Risk Monitoring			∠			5.80
COORDINATION						
Element 7.						
Risk Reporting				∠		7.00
Element 8.						
Risk Decision Making				∠		7.00
INTEGRATION						
Element 9.						
Risk Interdependencies			∠			5.80
Element 10.						
Organizational Interdependencies			∠			5.80

TOTAL SCORE: 65.60

Governance – Analyzing Culture

Definition of Firm Culture*

Set of norms, practices, and expected behaviors that influence how all employees make and implement decisions in the course of conducting business:

Evaluation of Firm Culture*

1. Consider whether *control functions are valued* within the organization including having key policies and processes by which the firm establishes cultural values;
2. Consider whether policy or control *breaches are tolerated*;
3. Consider whether the organization *proactively seeks to identify risk and compliance events*;
4. Consider whether immediate *managers are effective role models* of firm culture; and
5. Consider whether *sub-cultures that may not conform* to overall corporate culture are identified and addressed.

*FINRA's 2016 Regulatory and Examination Priorities

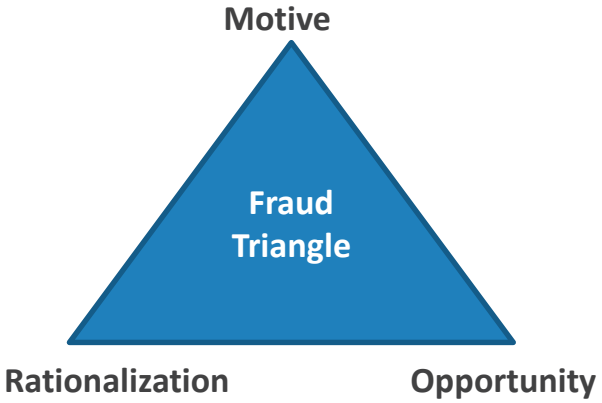
Governance – Evaluating Tone at the Top

Motive: the need for committing fraud ***(personal situation)***

Rationalization: the mindset of the fraudster that justifies them to commit fraud ***(ethics)***

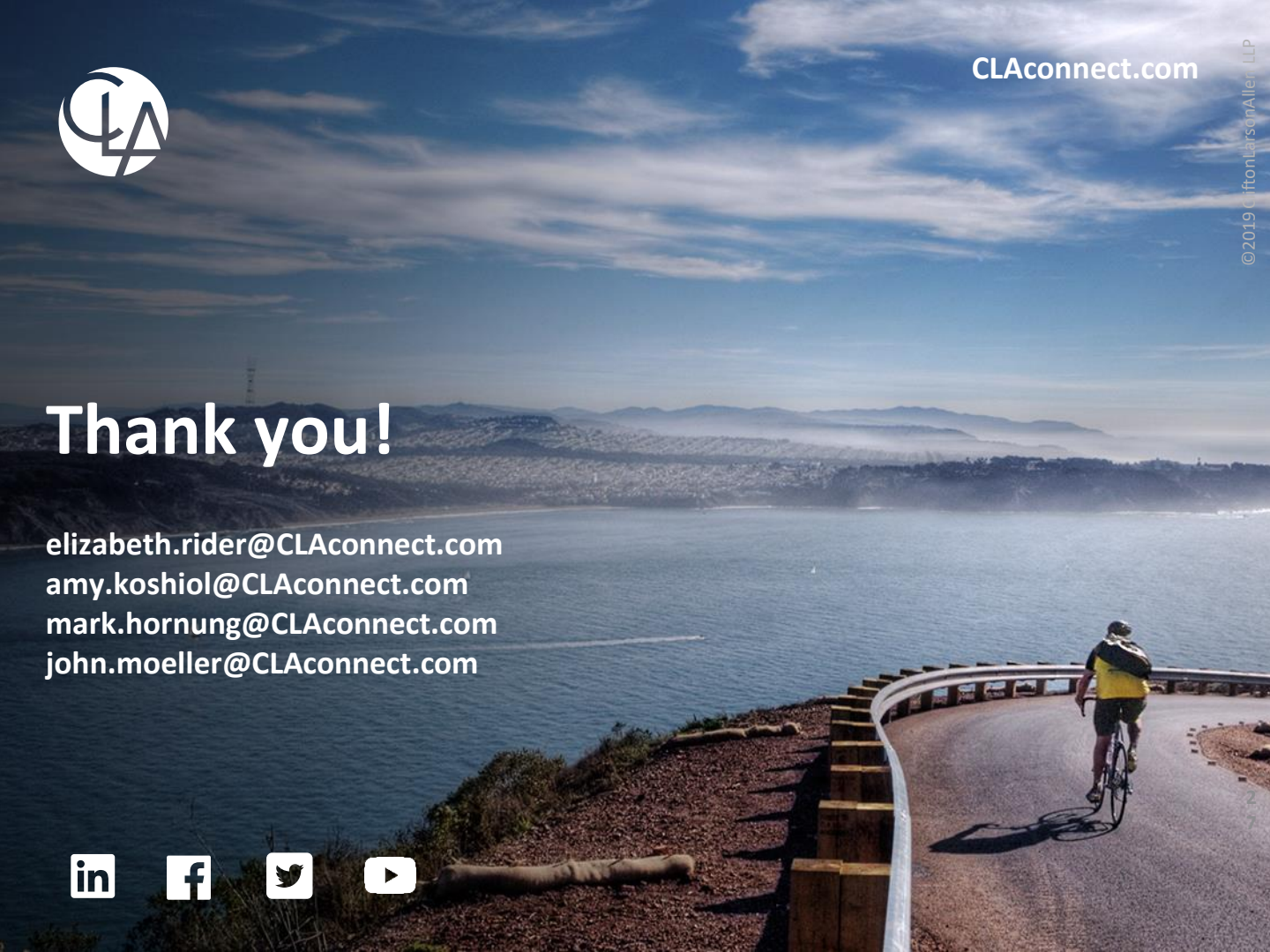
Opportunity: the situation that enables fraud to occur ***(anti – fraud internal controls)***

Guiding Employee Behaviors



Evaluate culture/ethics/reputation risks in each audit by considering activities related to:		
• Social Ethics / Social Media	• Ethics Evaluation	• Sustainability/Environmental Impact
• Diversity & Inclusion	• Discrimination	• Code of Conduct and Hotline
• Sexual Harassment	• Bonus Structures	• Employee surveys
• Conflicts of Interest	• Information security	• Cross-generational workforce

*Donald Ray Cressey authored the fraud triangle. He was a criminologist who made innovative contributions to the study of organized crime, prisons, criminology, the sociology of criminal law, white-collar crime.



CLAconnect.com

Thank you!

elizabeth.rider@CLAconnect.com
amy.koshiol@CLAconnect.com
mark.hornung@CLAconnect.com
john.moeller@CLAconnect.com