Financial Crimes Governance and Risk Assessment

CEFLI Notes

We'll start shortly after the top of the hour.

Important Information for attendees of the live session:

1. The **presentation deck** will be emailed to you within about 24 hours.
2. A **Certificate of Attendance** template will be included in the email. *CEFLI's materials **are not** filed for CLE or CE with State Bar or other organizations.*

CEFLI Premier Partners

CEFLI Affiliate Members

Gold:

Bronze:

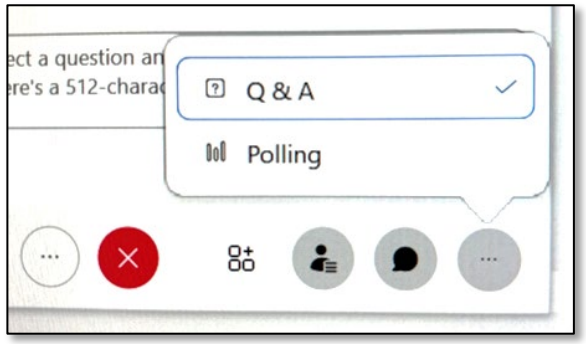
CEFLI Reminders

This Presentation

- Access to the recording and slides
- Certificate of Attendance

Submitting Questions

Please use the Q&A Feature (***not*** the Chat feature)

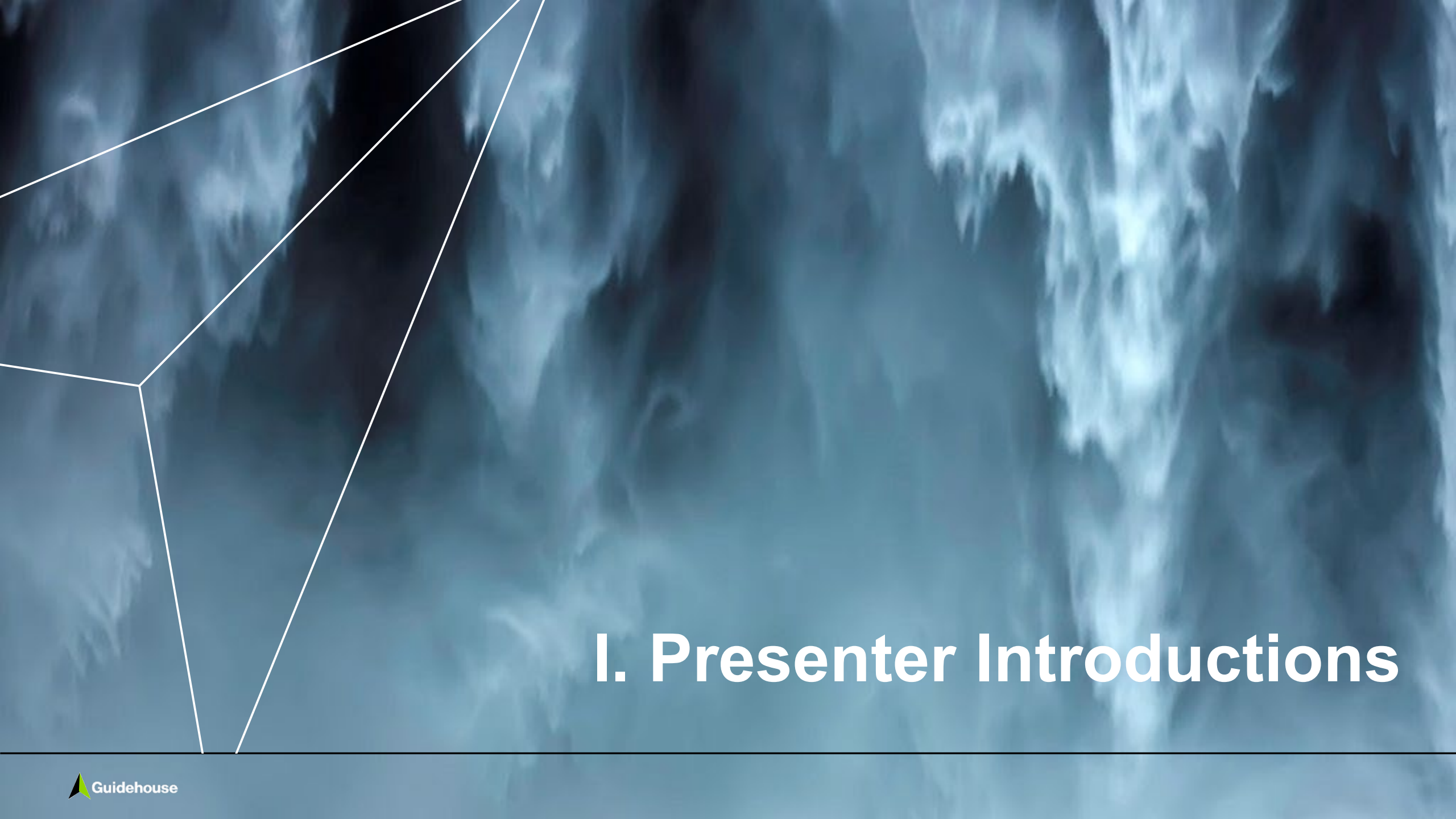


CEFLI's Antitrust Policy

The Compliance and Ethics Forum for Life Insurers (CEFLI) is committed to adhering strictly to the letter and spirit of the antitrust laws. Meetings conducted under CEFLI's auspices are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.

Under no circumstances shall CEFLI meetings be used as a means for competing companies or firms to reach any understanding -- expressed or implied -- which restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition. Accordingly, appropriate objection will be made to any presentation or colloquy that presents a risk from the standpoint of the antitrust laws.

Agenda



I. Presenter Introductions

A. Presenter Introductions

Samantha Welch

Partner
Financial Services
Samantha.Welch@guidehouse.com

Gene Bolton

Director
Financial Services
Gene.Bolton@guidehouse.com

II. Training Objective

A. Training Objective

With a risk-based approach to financial crimes, one size does not fit all. This webinar will explore the essential components of a financial crimes operating model and provide practical advice for maintaining a financial crimes program that is fit for the size and complexity of the institution. Critical to this effort is the financial institution's risk assessment process. The webinar will delve into assessing the varying financial crimes risks, and critical components of the risk assessment process.

Training Overview

PART I **Critical Elements of a Financial Crimes Governance Framework**	1. Documenting the Operating Model and Three Lines of Defense (3LOD) 2. Senior Management and Board Reporting 3. Culture of Compliance 4. Workforce Planning 5. Ongoing Monitoring and Additional Oversight Considerations
PART 2 **Tips for Developing Financial Crimes Risk Assessments**	1. Different Assessments for Different Financial Crimes 2. Spotlight on BSA / AML and Sanctions Risk Assessments a. Inherent Risk b. Controls c. Residual Risk 3. Using the Risk Assessment to Tailor Your Program

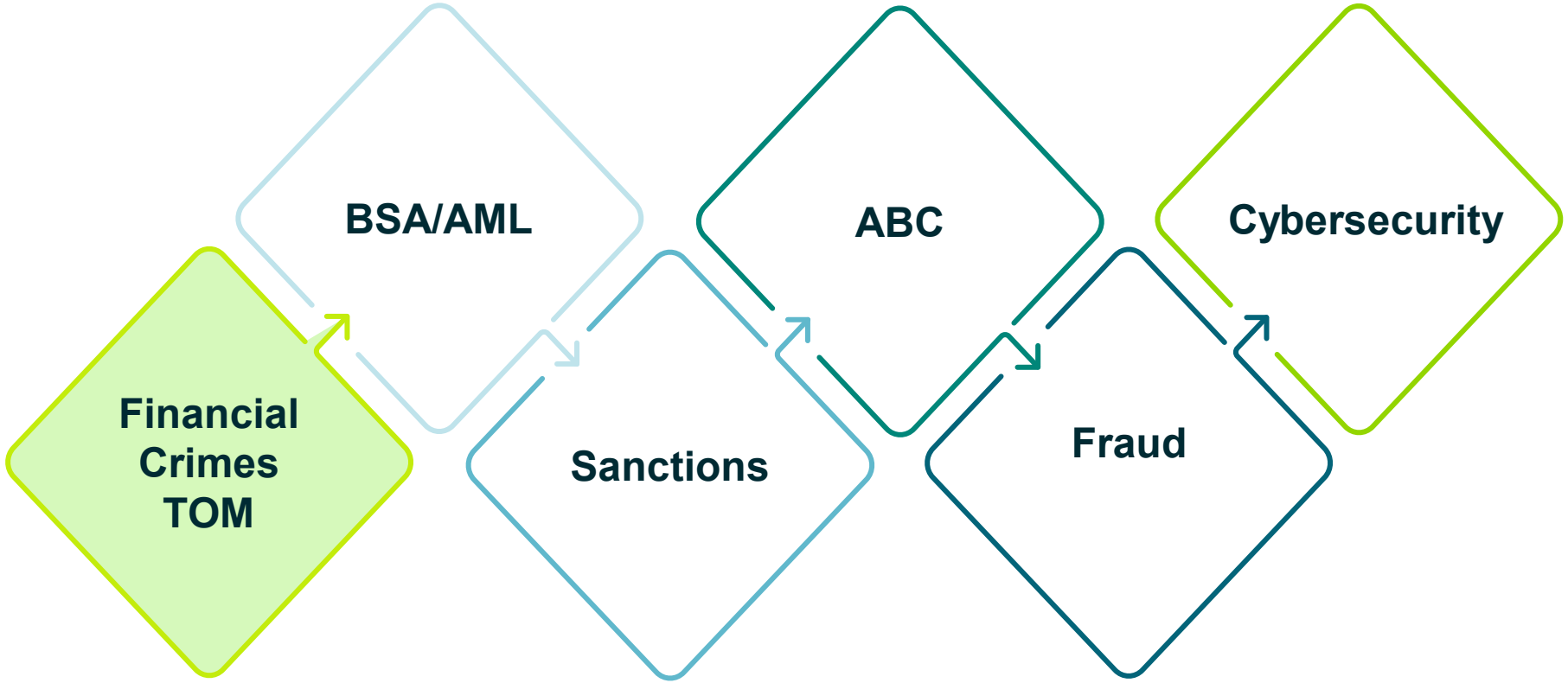
III. Financial Crimes Governance Framework

A. Holistic View of Financial Crimes

A holistic risk management program should address each of the financial crimes risks applicable to the insurance company.

The operating model should consider *how* and *where* financial crimes risk is best managed and align to an enterprise risk management framework.

Financial crime risks are typically not all handled in the same manner across the different functional areas.



B. Three Lines of Defense

Three Lines of Defense (3LOD)

The Financial Crimes Operating Model should document the roles and responsibilities for each line of defense including critical hand-offs and accountability for material decisions.

A. 1LOD – Business Line Management and Operations

B. 2LOD – Compliance and Risk Management

C. 3LOD – Internal Audit and External Independent Testing

Tips for implementation:

- Training should be tailored to the recipient's role, including their responsibilities for compliance
- Job descriptions and performance management metrics should consider compliance
- Identify key decision points using RACI
- Identify a POC / Liaison in the 1LOD

C. Culture of Compliance

The level of oversight needed by the 2LOD is influenced by the Culture of Compliance. Typically, firms with a strong culture of compliance have risk management embedded into front office policies and procedures. Firms that do not have a strong culture of compliance rely more heavily on the 2LOD to provide greater oversight.

1.

Senior Management Commitment

Start with Senior Management to set the tone at the top, but also include middle management. Senior Management should communicate the Board's risk appetite and ensure policies and procedures are aligned.

2.

Reporting Mechanisms

The firm's reporting, or 'whistleblower' hotline should allow for anonymous reporting and have clear anti-retaliation clauses for good faith reporting.

Investigation procedures should be documented and followed regardless of employee level.

3.

Incentive Structure

Consider whether incentive policies are structured to promote compliance. Fraud can occur when incentives do not consider the best interest of the customer.

Additionally, consider how disaplianry actions are handled.

D. Senior Management and Board Reporting

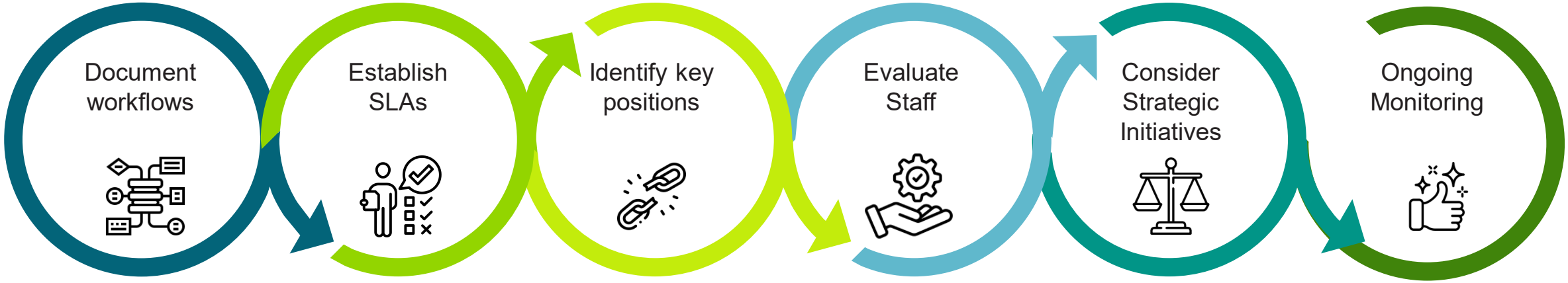
Senior Management and the Board are ultimately responsible for risk management. To discharge these obligations, they must have a level of understanding of both the risks inherent in the business, as well as the controls implemented or needed to mitigate those risks.

Well defined Key Risk Indicators (KRI) are critical for oversight. Determine the scope / particular area you are measuring, and what level of information is needed.

KRIs are different than Key Performance Indicators (KPI). KPIs measure operational efficiency and can be used to measure employee performance. KRIs measure the amount of risk in the ecosystem and are used to identify patterns and trends vs the firm's risk appetite on an ongoing basis.

E. Workforce Planning

Consider both qualitative (skills) and quantitative (number) factors when determining your resourcing needs. Typically, the less technology you employ, the more reliance you will have on human capital.



1	2	3	4	5	6
Document the key processes and workflows.	Measure handle times and SLAs.	Identify key positions and necessary skill sets to fulfill them.	Evaluate current staff and resource mix to determine gaps in skills/ numbers.	Resource needs should be part of any new business evaluation.	Consider resource needs based on changes to business and technology/ process changes.

F. Ongoing Monitoring and Additional Oversight Considerations

Common pitfalls and helpful tips

Risk Assessment

Ongoing Monitoring

Know Your Product and Process

New Business Process

Review Acquisition Targets

Communication and Training

Centralize Documentation

Governance Policies

IV. Financial Crimes Risk Assessments

A. Regulatory Background

1. Risk Assessment Use

A robust risk assessment helps insurance companies promptly and accurately identify financial crimes risks and vulnerabilities, and apply appropriate controls to mitigate those risks, or identify unacceptable risks to avoid.

2. Different Risks Require Different Approaches

- Anti-Money Laundering / Terrorist Financing
- Sanctions
- Anti-Bribery and Corruption
- Fraud

A. Regulatory Background

3. International and US Regulatory Framework

US BSA/AML/OFAC

a. 31 CFR § 1025.210 - Anti-money laundering programs for insurance companies: (b) (1) *Incorporate policies, procedures, and internal controls based upon the insurance company's assessment of the money laundering and terrorist financing risks associated with its covered products.*

b. July 2024 FinCEN NPRM: Imposes mandatory risk assessment process: (1) AML/CFT Priorities; (2) products, services, distribution channels, customers, intermediaries, and geographic locations; and (3) reports pursuant to 31 CFR chapter X (e.g., SARs, CTRs).

c. Certain states require risk assessments.

d. Risk assessments should serve as the foundation for designing policies, procedures and internal controls ("risk-based approach").

e. OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program, including conducting a sanctions risk assessment.

f. DoJ - Resource Guide to the U.S. Foreign Corrupt Practices Act

g. DoJ - Evaluation of Corporate Compliance Programs

International Standards

a. The European Banking Authority ("EBA") expects that European Union ("EU") central banks and EU member country financial regulators require financial institutions to identify ML/TF risks in their sectors.

b. Though not an EBA requirement, periodic risk assessments are strongly encouraged and EBA Guidance requires a risk-based approach to compliance.

c. The Wolfsberg Group and Financial Action Task Force ("FATF") published guidance on the risk-based approach required for ML/TF.

d. Non-US regulators require institutions to conduct Risk Assessments (e.g., FINTRAC, CBI)

B. Methodology

Risk assessments should be customized to an insurance company's business and operations, including the financial crime risks associated with products and services, customer/user base, delivery channels, intermediaries/ counterparties, operations, and geographic locations in which it operates.

A Identify Available Data and Business/ Assessment Units

B Determine Relevant Risk Categories

C Identify Inherent Risk Scoring Methods

D Identify Control Rating Methods

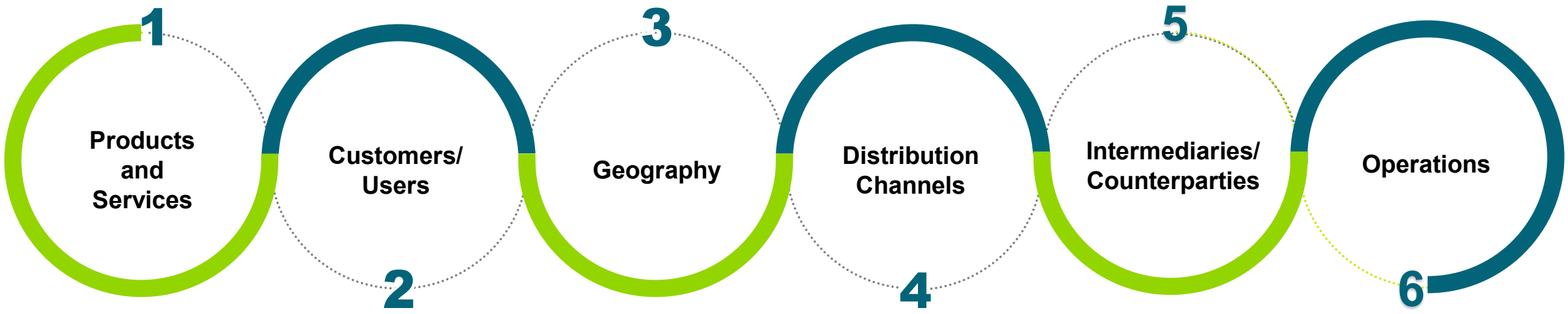
E Identify Residual Risk(s) Rating Methods

F Prepare Legal Entity and Enterprise Wide BSA/AML Risk Assessment Report

G Document Action Plans and Recommendations

C. Data

The first step of the risk assessment is to develop a wish list to understand what client data is available to risk score. This can help identify and consider relevant money laundering, terrorist financing and sanctions risks in areas such as:



D. Inherent Risk

Inherent Risk is the risk of money laundering/ terrorist financing or potential sanctions violations occurring through the organization without consideration of controls to alter its impact. Inherent risks are determined using the following techniques:

A. Process Steps

1. Data collection	2. Data analysis
3. Interviews	4. Qualitative analysis of inherent risk
5. Quantification of inherent risk	6. Validation of inherent risk with senior management

B. Example of Inherent Risks

Risk Category	Inherent Risk Rating
Customers	High
Products and Services	Medium
Geography	Low
Delivery Channel	Low
Overall	**Medium**

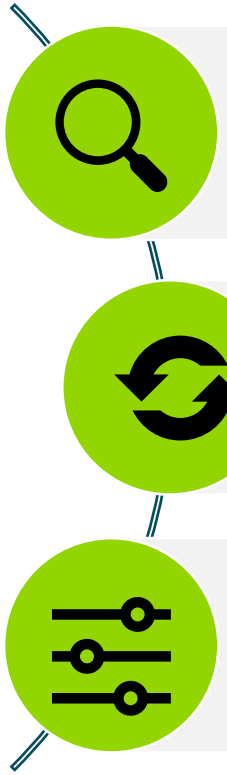
E. Control Assessment

Control evaluations are essential to understand the extent to which the control environment is reasonably designed and implemented to mitigate specific risks.

Risk Category	Control Rating
Know Your Customer	Needs Improvement
Transaction Monitoring	Adequate
Governance	Strong
Screening	Strong

Key Consideration

Third Party Administrators



Identify current controls (e.g., transaction monitoring, KYC, training) designed to mitigate risk, map them to inherent risk categories, and assess design and effectiveness

Refresh control inventories to include relevant testing results and new controls

Use the control ratings to determine the degree to which current controls mitigate inherent risks

F. Residual Risk

Subtract inherent risk score from control score to calculate a residual risk rating.

- Leadership may adjust residual risk scores based on qualitative information
- Results should be approved and accepted by the appropriate governing body
- Management should develop action plans based on residual risk
- The company should use the results to assess whether it is operating within its risk appetite


Questions

Closing CEFLI Reminders

Post Presentation

Registrants who attended the live session will receive:

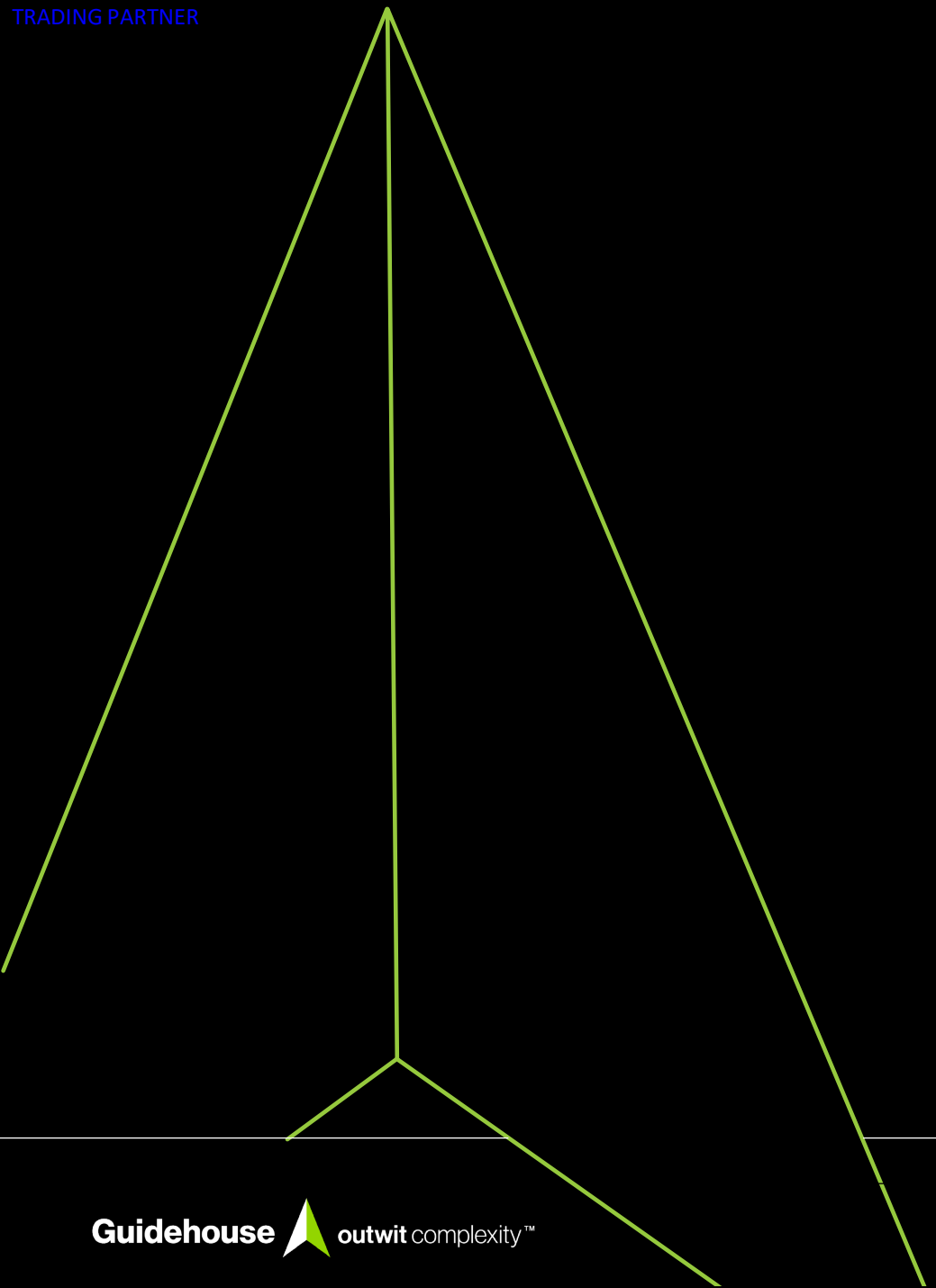
- Access to a short post-event survey
- A Certificate of Attendance (live attendees) form

All Registrants will receive:

- A PDF of the presentation deck
- A link to the recorded event

While CEFLI does not file its materials with any Compliance, Ethics, Fraud or State Bar Associations, it provides a Certificate of Attendance template to individuals who attend CEFLI's live events. The form, and the information below may be helpful to Member who elect to self submit for potential CLE or CE credit consideration from the organizations they are involved with. More information about CEFLI can be found at: https://cefli.org/about-cefli/

- CEFLI Webinars are conducted via Cisco Webex and CEFLI is the sponsor of the webinars.
- Participants are required to register, to join a live session.
- CEFLI provides a Certificate of Attendance only to individuals who *attended* the live event.
- While CEFLI does not utilize bios for Webinar speakers, it references its presenters by name, title and affiliation, within the presentation materials and on each Certificate of Attendance. Its participants are industry experts in their respective fields.
- The topics covered address life/annuity compliance and ethics matters (no sales/ marketing content).
- CEFLI Does not have a way of knowing how many attorneys attend its events.
- While CEFLI does not utilize a timed agenda, its webinars are one-hour in duration.
- Participants may ask questions during an event using the Q&A feature in the Webex.
- CEFLI is a compliance and ethics organization whose mission is to support compliance, ethics, legal and risk management professionals in the life insurance industry.



Thank You