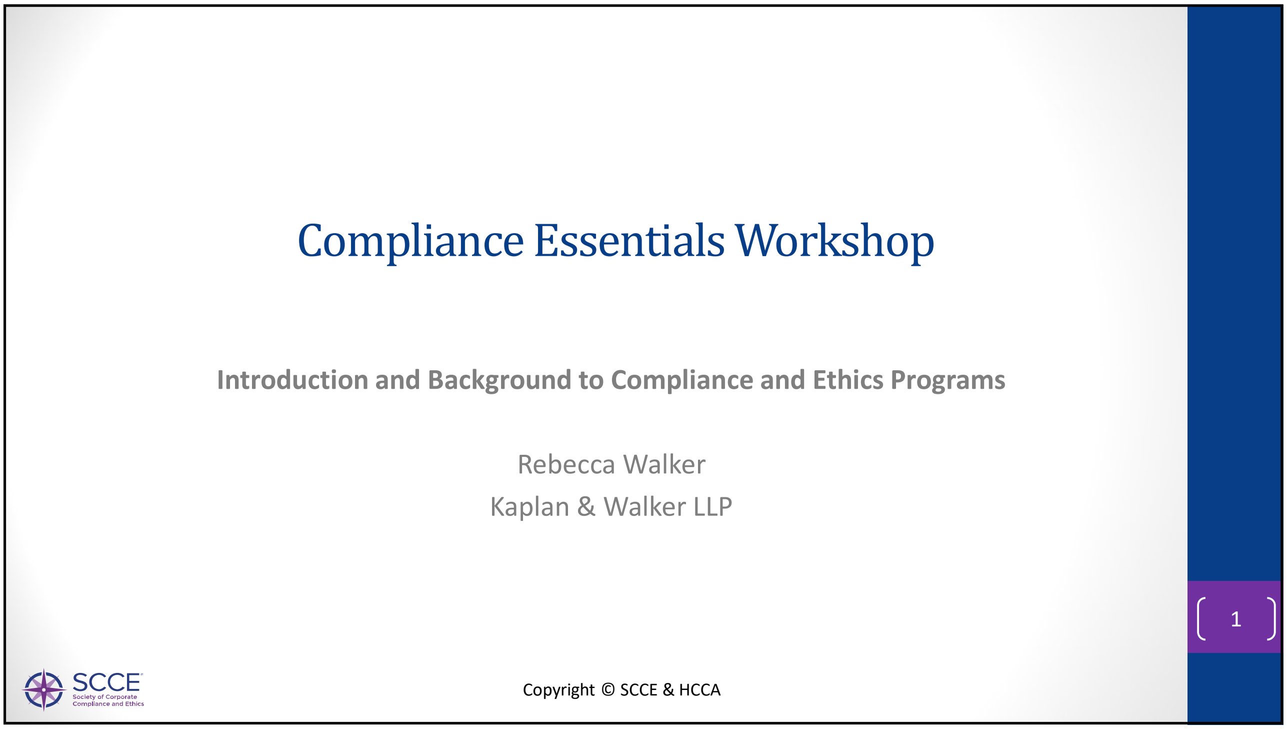
SCCE Compliance & Ethics Essentials Workshop

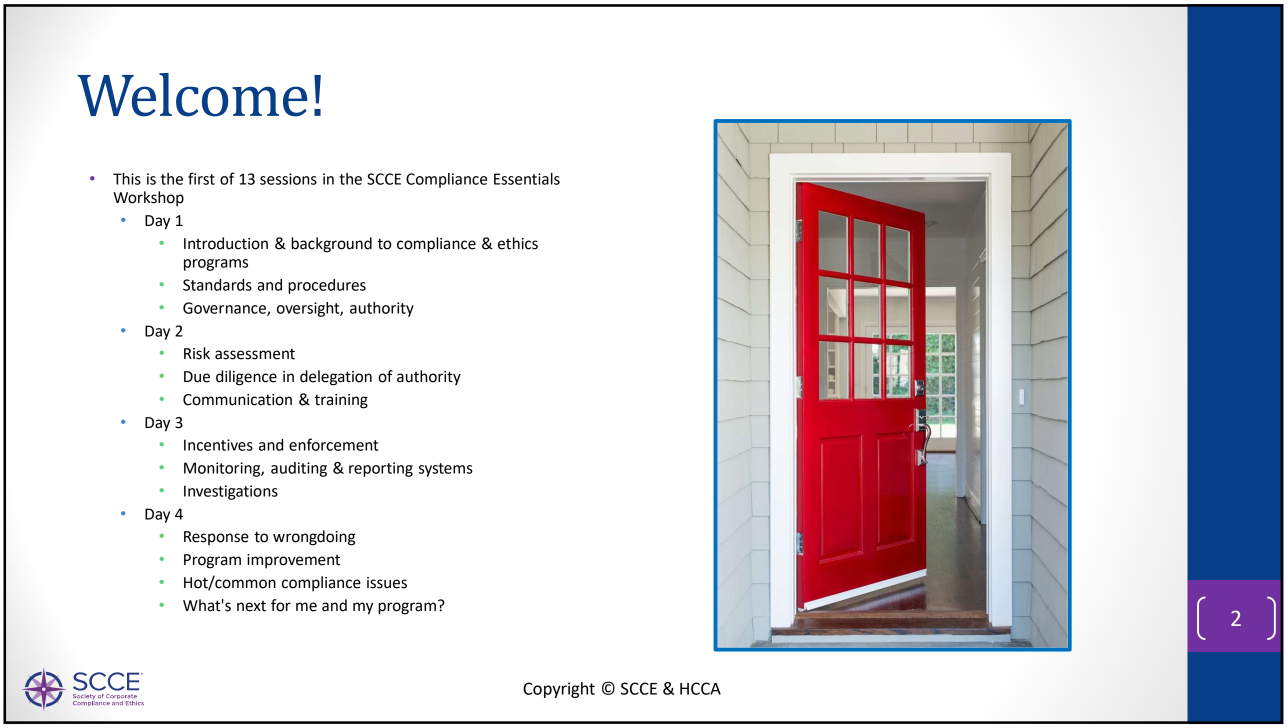
All PDF Presentations Combined



Compliance Essentials Workshop

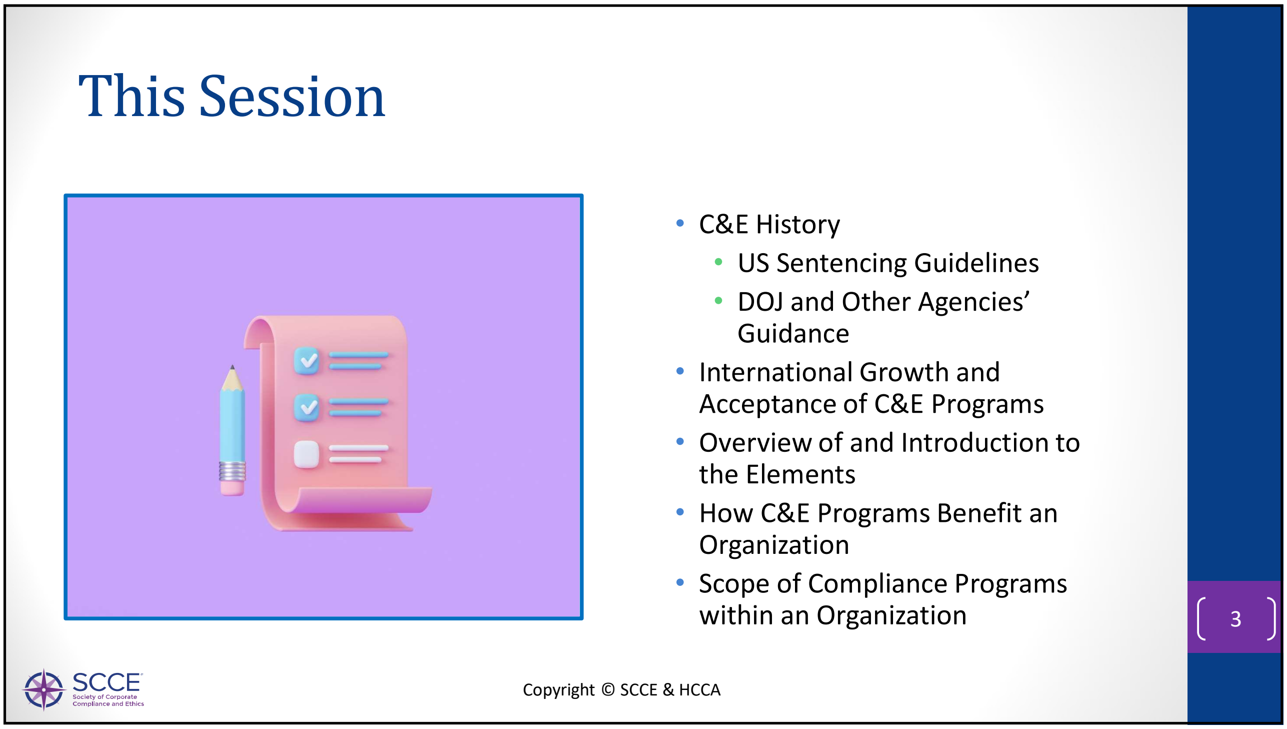
Introduction and Background to Compliance and Ethics Programs

Rebecca Walker
Kaplan & Walker LLP



Welcome!

- This is the first of 13 sessions in the SCCE Compliance Essentials Workshop
  - Day 1
    - Introduction & background to compliance & ethics programs
    - Standards and procedures
    - Governance, oversight, authority
  - Day 2
    - Risk assessment
    - Due diligence in delegation of authority
    - Communication & training
  - Day 3
    - Incentives and enforcement
    - Monitoring, auditing & reporting systems
    - Investigations
  - Day 4
    - Response to wrongdoing
    - Program improvement
    - Hot/common compliance issues
    - What's next for me and my program?



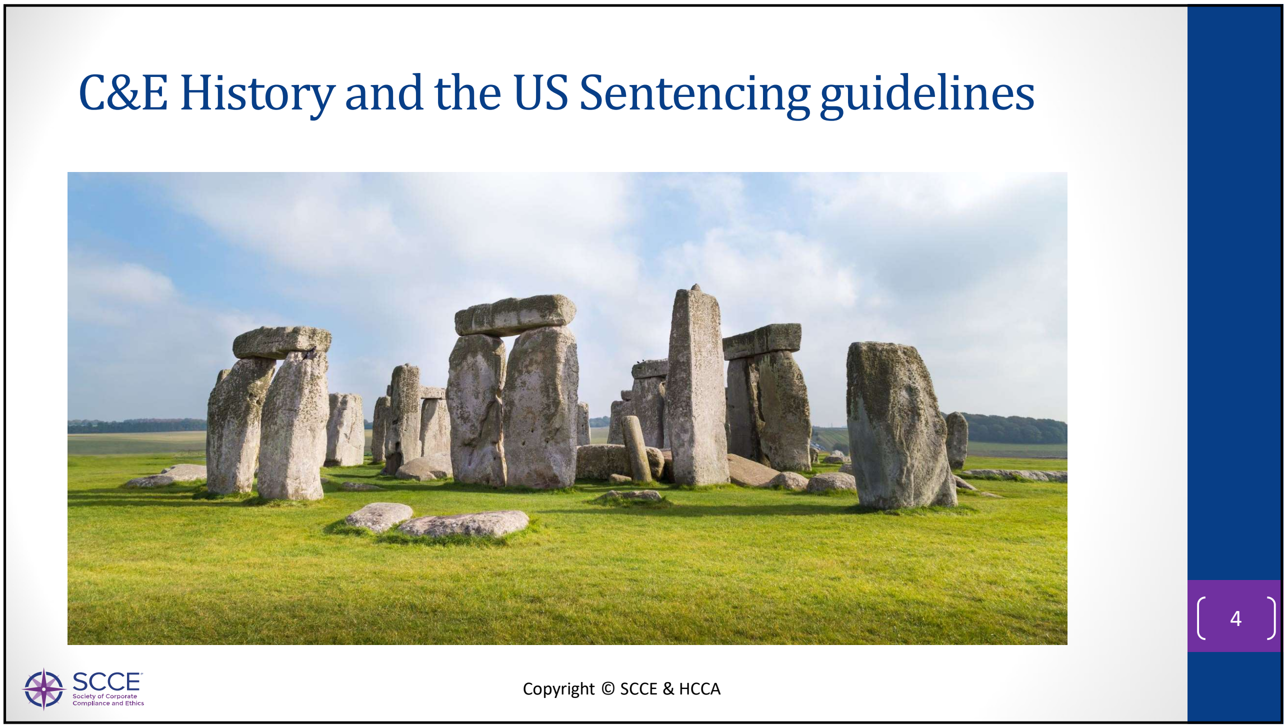
This Session

- C&E History
  - US Sentencing Guidelines
  - DOJ and Other Agencies' Guidance
- International Growth and Acceptance of C&E Programs
- Overview of and Introduction to the Elements
- How C&E Programs Benefit an Organization
- Scope of Compliance Programs within an Organization

3

SCCE Society of Corporate Compliance and Ethics

3

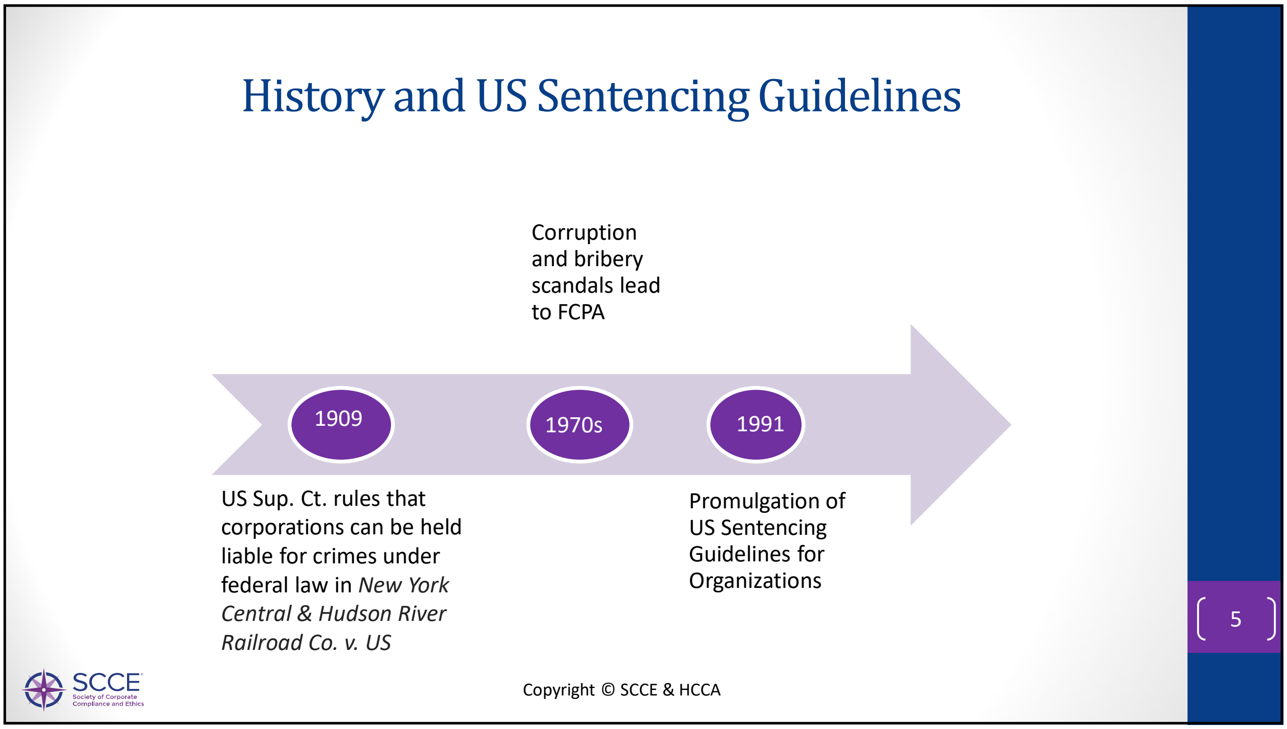


C&E History and the US Sentencing guidelines

4

SCCE Society of Corporate Compliance and Ethics

4



History and US Sentencing Guidelines

Corruption and bribery scandals lead to FCPA

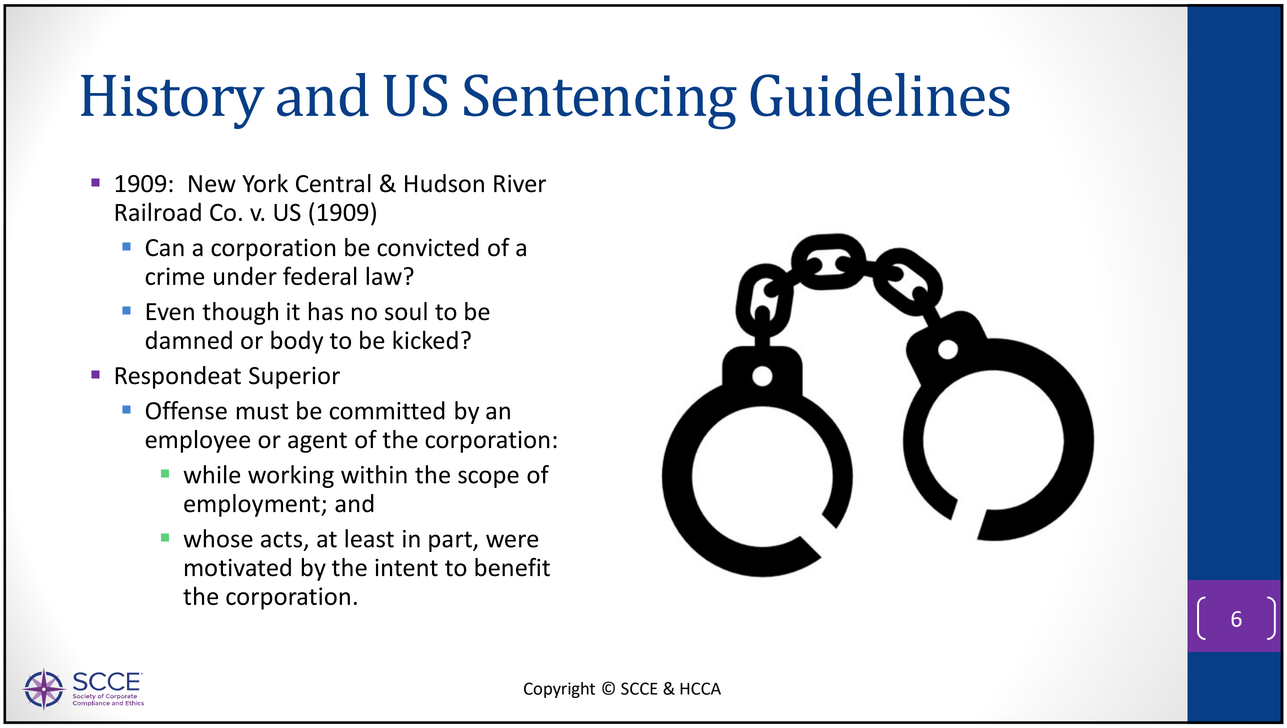
1909

1970s

1991

US Sup. Ct. rules that corporations can be held liable for crimes under federal law in *New York Central & Hudson River Railroad Co. v. US*

Promulgation of US Sentencing Guidelines for Organizations

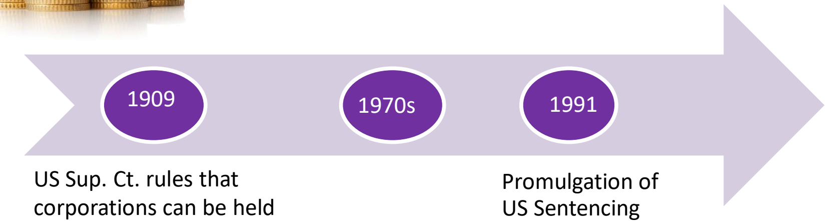


History and US Sentencing Guidelines

- 1909: New York Central & Hudson River Railroad Co. v. US (1909)
  - Can a corporation be convicted of a crime under federal law?
  - Even though it has no soul to be damned or body to be kicked?
- Respondeat Superior
  - Offense must be committed by an employee or agent of the corporation:
    - while working within the scope of employment; and
    - whose acts, at least in part, were motivated by the intent to benefit the corporation.

History and US Sentencing Guidelines

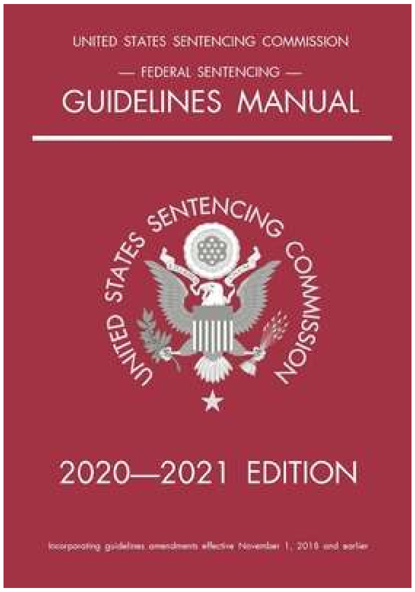
Corruption and bribery scandals lead to FCPA



US Sup. Ct. rules that corporations can be held liable for crimes under federal law in *New York Central & Hudson River Railroad Co. v. US*

Promulgation of US Sentencing Guidelines for Organizations

SCCE Society of Corporate Compliance and Ethics



UNITED STATES SENTENCING COMMISSION

— FEDERAL SENTENCING —

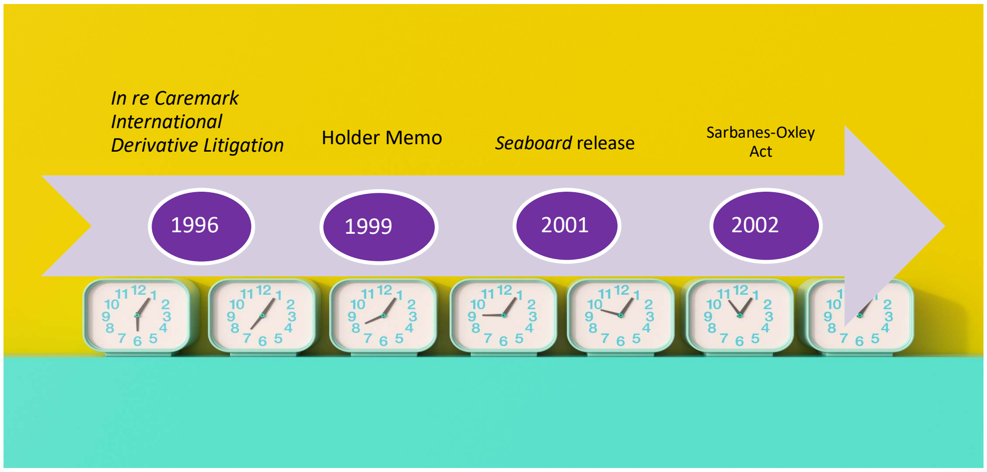
GUIDELINES MANUAL

2020—2021 EDITION

Incorporating guidelines amendments effective November 1, 2018 and earlier

SCCE Society of Corporate Compliance and Ethics

History and US Sentencing Guidelines



9

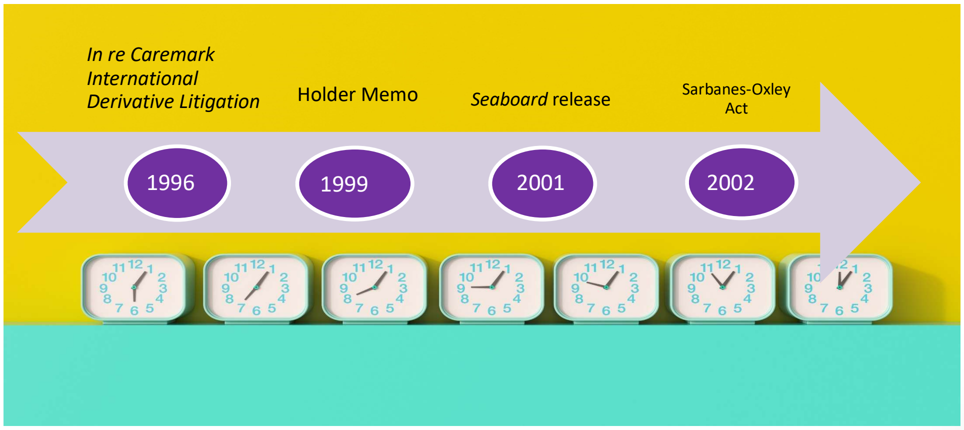
History and US Sentencing Guidelines

?

- 1996: In re Caremark International Derivative Litigation (Del Chancery Court)
  - "I note the potential impact of the federal organizational sentencing guidelines on any business organization. Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account this development and the enhanced penalties and the opportunities for reduced sanctions that it offers."
  - "Thus, I am of the view that a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."
- The standard for liability is very high.
  - "The theory here advanced is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."

10

History and US Sentencing Guidelines



In re Caremark International Derivative Litigation

1996

Holder Memo

1999

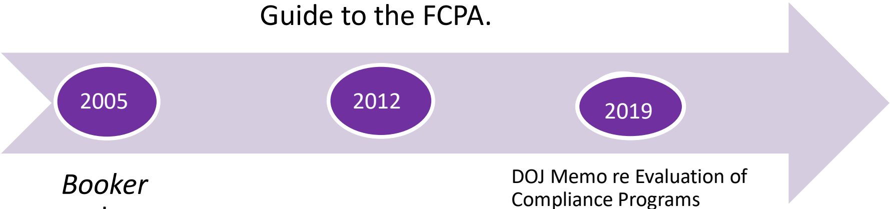
Seaboard release

2001

Sarbanes-Oxley Act

2002

History and US Sentencing Guidelines



2005

Booker and *Fanfan*

2012

DOJ Morgan Stanley declination

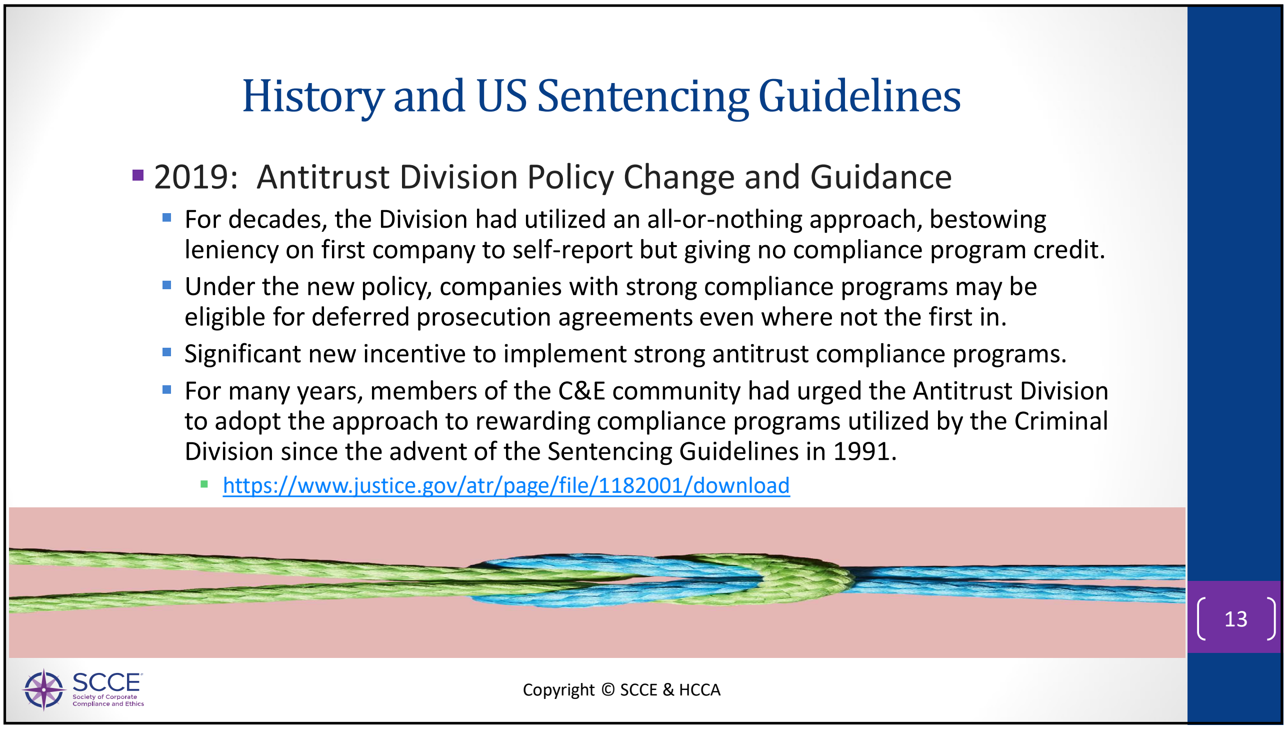
DOJ/SEC Resource Guide to the FCPA.

2019

DOJ Memo re Evaluation of Compliance Programs

Antitrust Division announces new policy re compliance program credit

Marchand v. Barnhill and In re Clovis Oncology

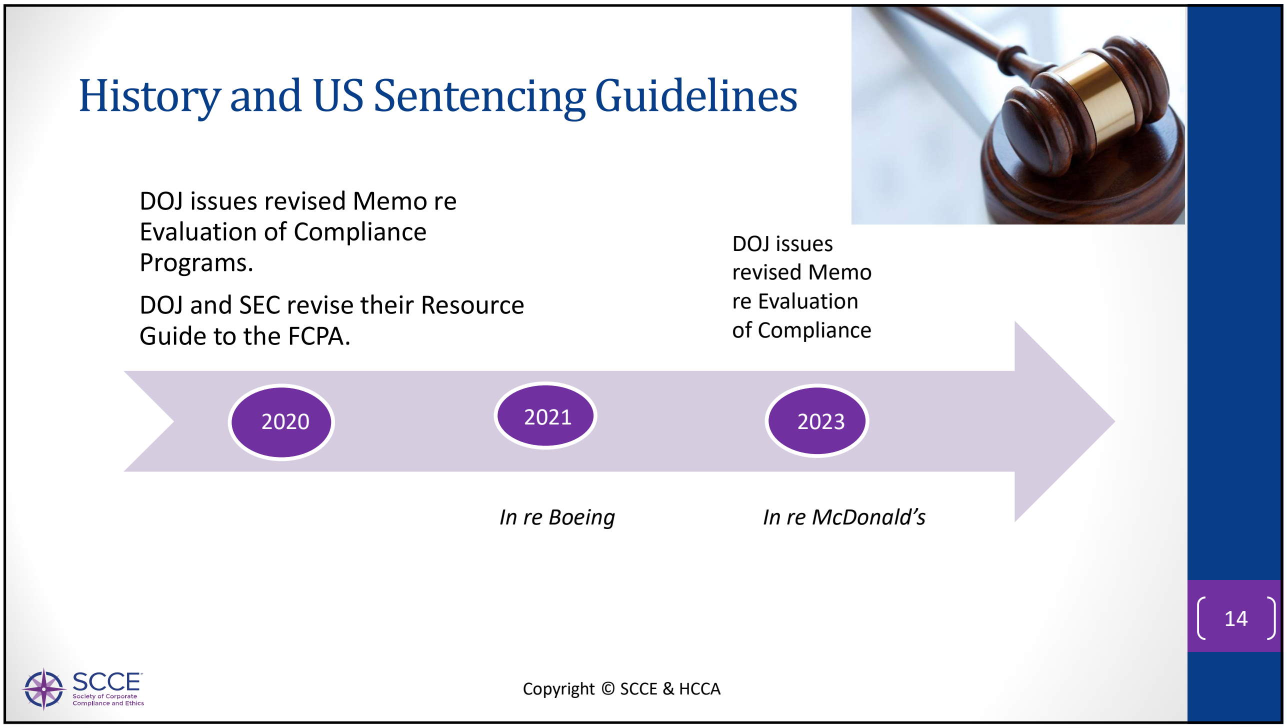


History and US Sentencing Guidelines

- 2019: Antitrust Division Policy Change and Guidance
  - For decades, the Division had utilized an all-or-nothing approach, bestowing leniency on first company to self-report but giving no compliance program credit.
  - Under the new policy, companies with strong compliance programs may be eligible for deferred prosecution agreements even where not the first in.
  - Significant new incentive to implement strong antitrust compliance programs.
  - For many years, members of the C&E community had urged the Antitrust Division to adopt the approach to rewarding compliance programs utilized by the Criminal Division since the advent of the Sentencing Guidelines in 1991.
    - https://www.justice.gov/atr/page/file/1182001/download

13

13



History and US Sentencing Guidelines

DOJ issues revised Memo re Evaluation of Compliance Programs.

DOJ and SEC revise their Resource Guide to the FCPA.

2020

2021

In re Boeing

DOJ issues revised Memo re Evaluation of Compliance

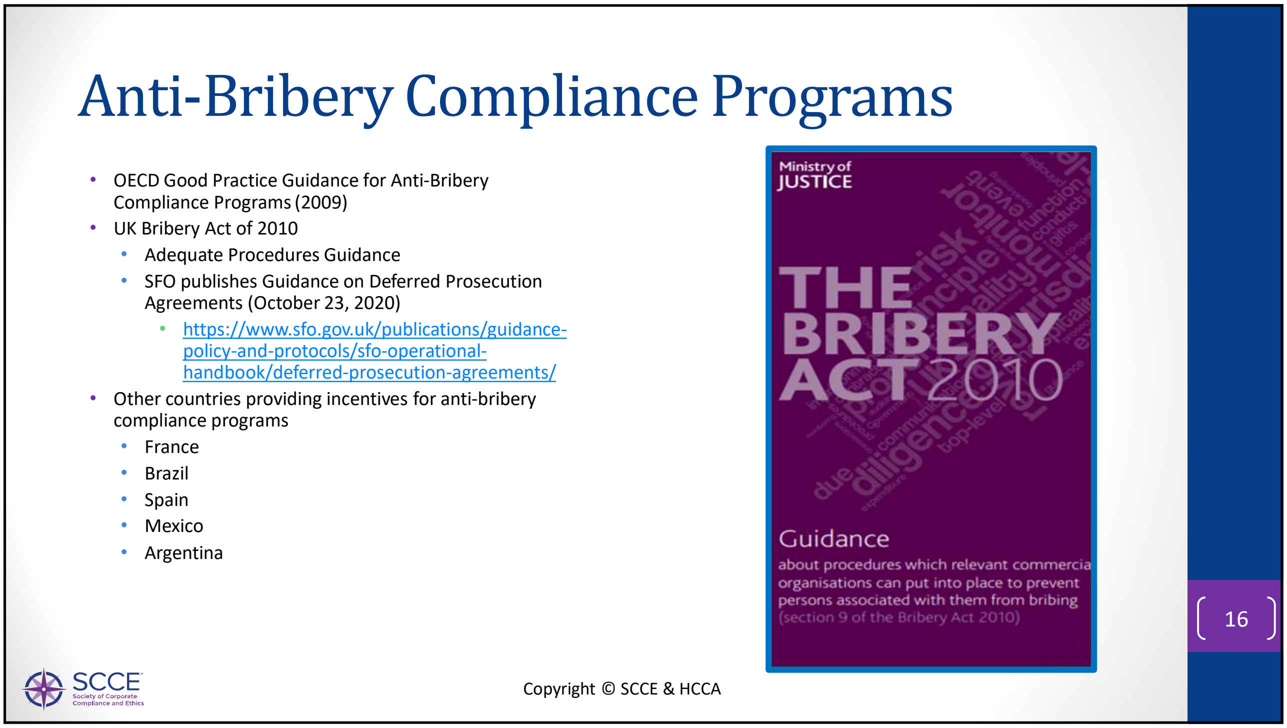
2023

In re McDonald's

14

14

INTERNATIONAL GROWTH AND ACCEPTANCE OF C&E PROGRAMS



Anti-Bribery Compliance Programs

- OECD Good Practice Guidance for Anti-Bribery Compliance Programs (2009)
- UK Bribery Act of 2010
  - Adequate Procedures Guidance
  - SFO publishes Guidance on Deferred Prosecution Agreements (October 23, 2020)
    - https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/
- Other countries providing incentives for anti-bribery compliance programs
  - France
  - Brazil
  - Spain
  - Mexico
  - Argentina

Ministry of JUSTICE

THE BRIBERY ACT 2010

Guidance

about procedures which relevant commercia organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)

Competition Law Incentives

- Incentives for competition law compliance program guidance
  - Australia
  - Brazil
  - Israel
  - Italy
  - Malaysia
  - Spain
  - Mexico
  - Canada
  - Switzerland
  - South Africa
  - Singapore
  - United Kingdom

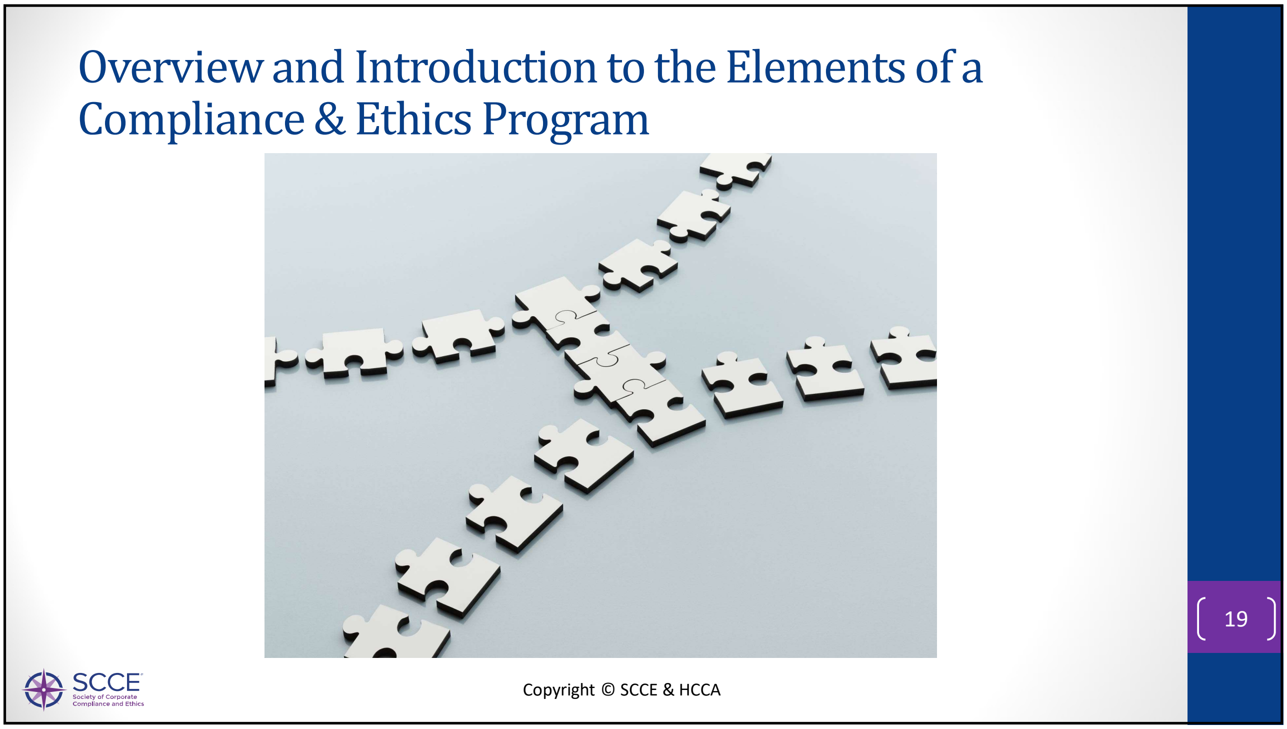
17

EU Whistleblower Directive

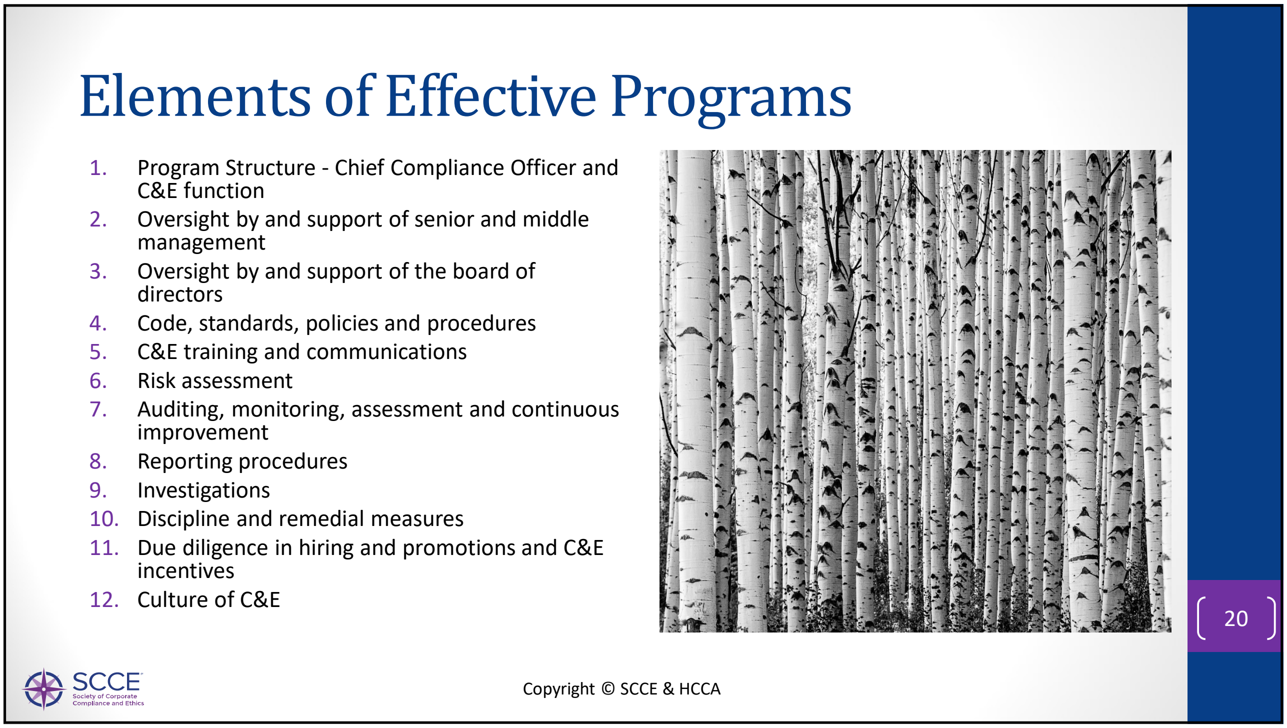
?

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L1937
- National laws must require companies with more than 50 employees to implement reporting channels and protect against retaliation.
- Topics of reporting include, e.g., public procurement, financial services, money laundering, terrorist financing, product safety and compliance, protection of the environment, protection of privacy and personal data.

18

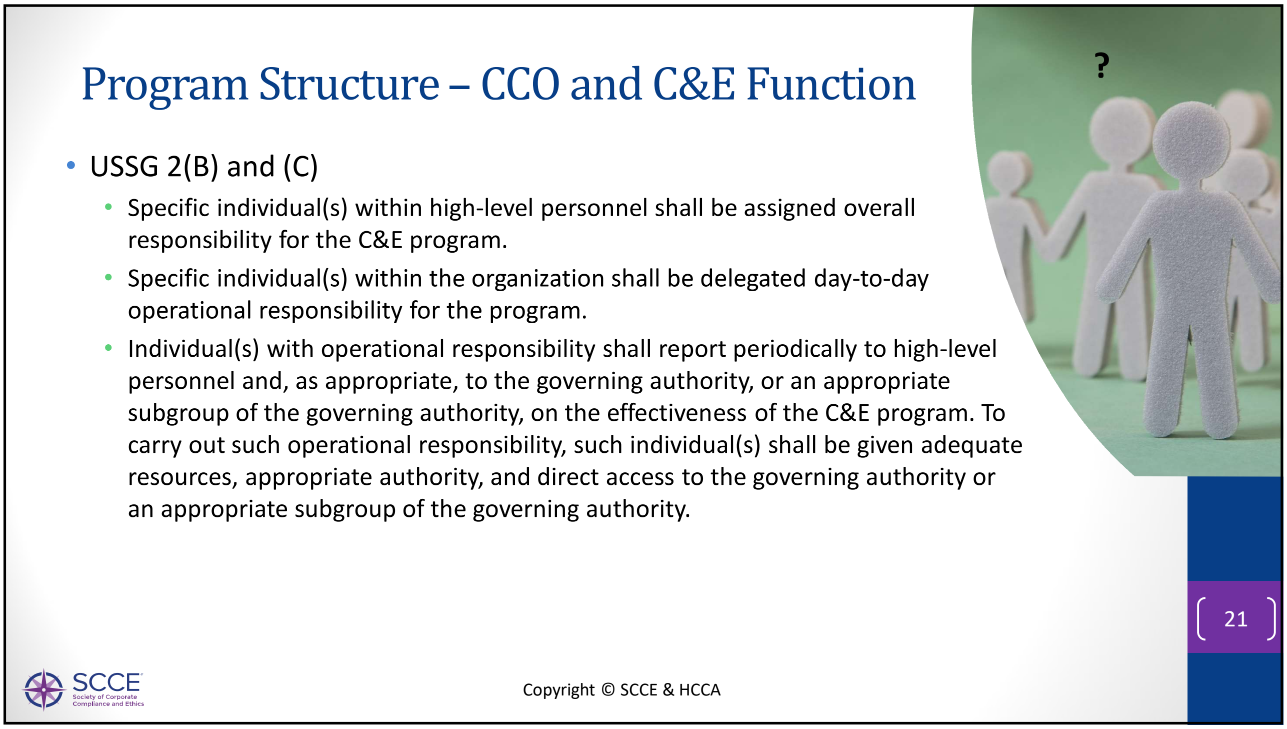


Overview and Introduction to the Elements of a Compliance & Ethics Program



Elements of Effective Programs

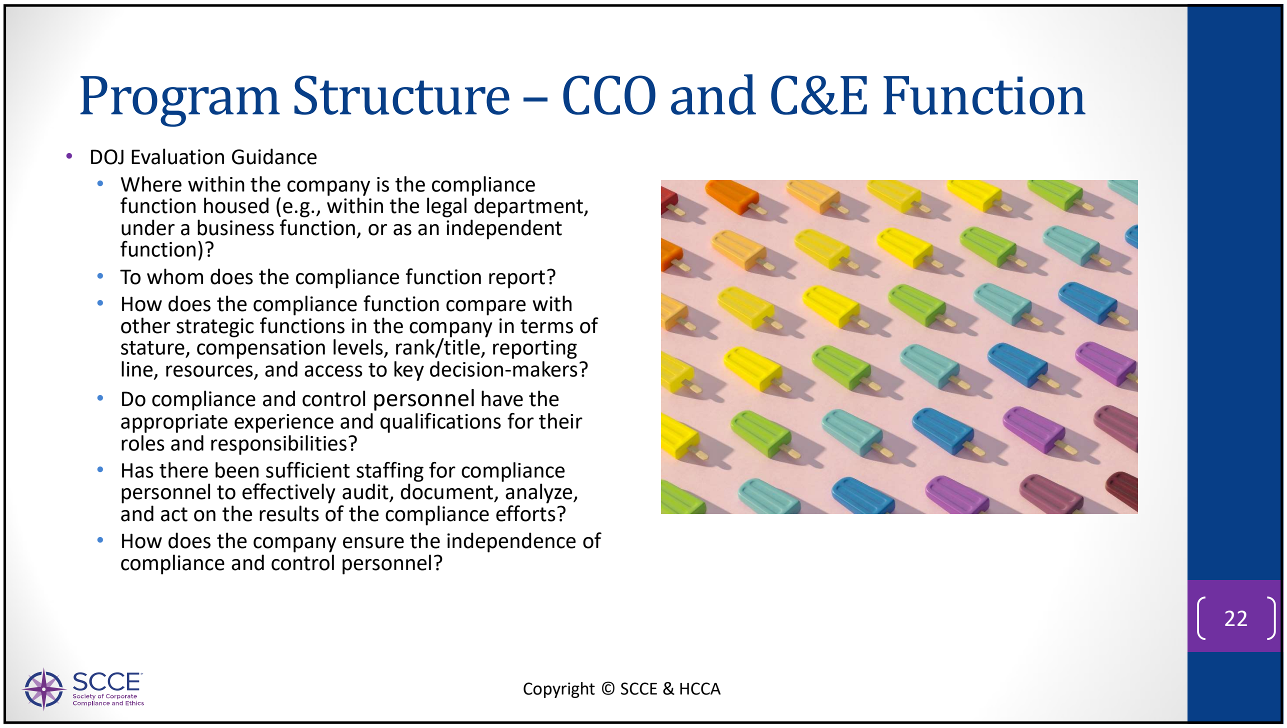
1. Program Structure - Chief Compliance Officer and C&E function
2. Oversight by and support of senior and middle management
3. Oversight by and support of the board of directors
4. Code, standards, policies and procedures
5. C&E training and communications
6. Risk assessment
7. Auditing, monitoring, assessment and continuous improvement
8. Reporting procedures
9. Investigations
10. Discipline and remedial measures
11. Due diligence in hiring and promotions and C&E incentives
12. Culture of C&E



Program Structure – CCO and C&E Function

- USSG 2(B) and (C)
  - Specific individual(s) within high-level personnel shall be assigned overall responsibility for the C&E program.
  - Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the program.
  - Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the C&E program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

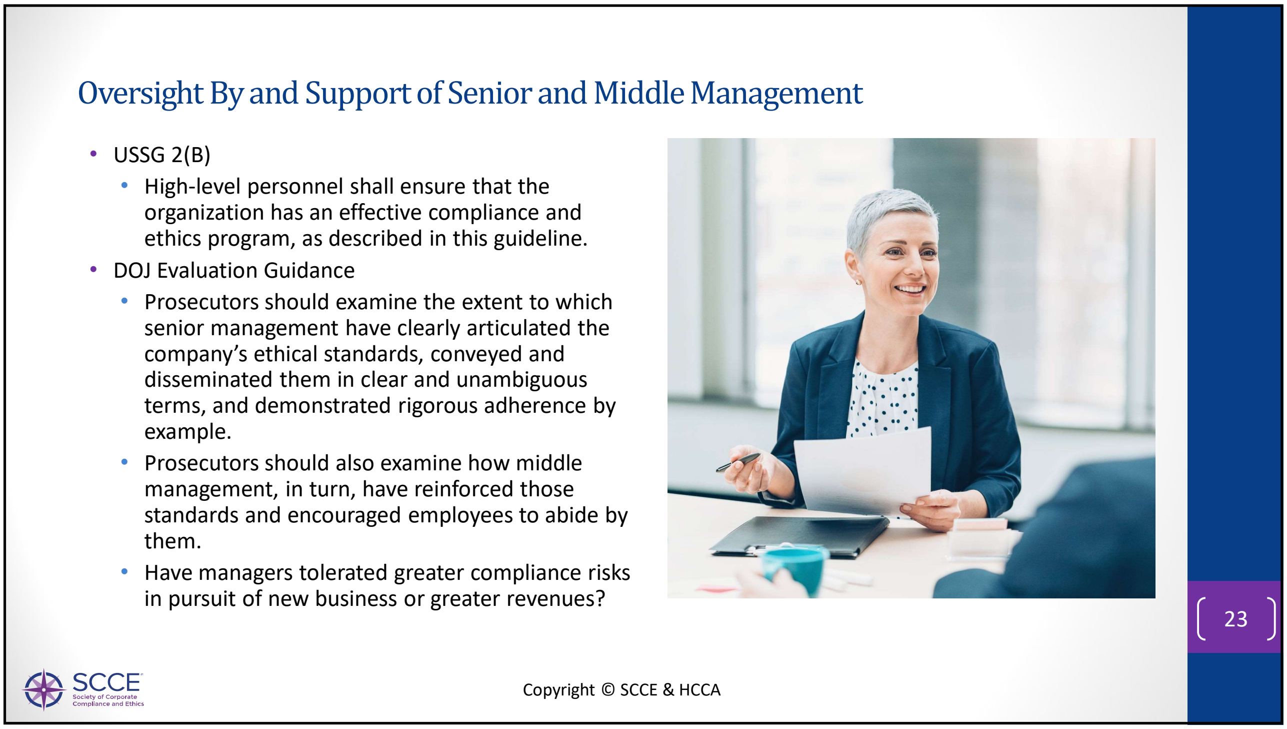
SCCE Society of Corporate Compliance and Ethics



Program Structure – CCO and C&E Function

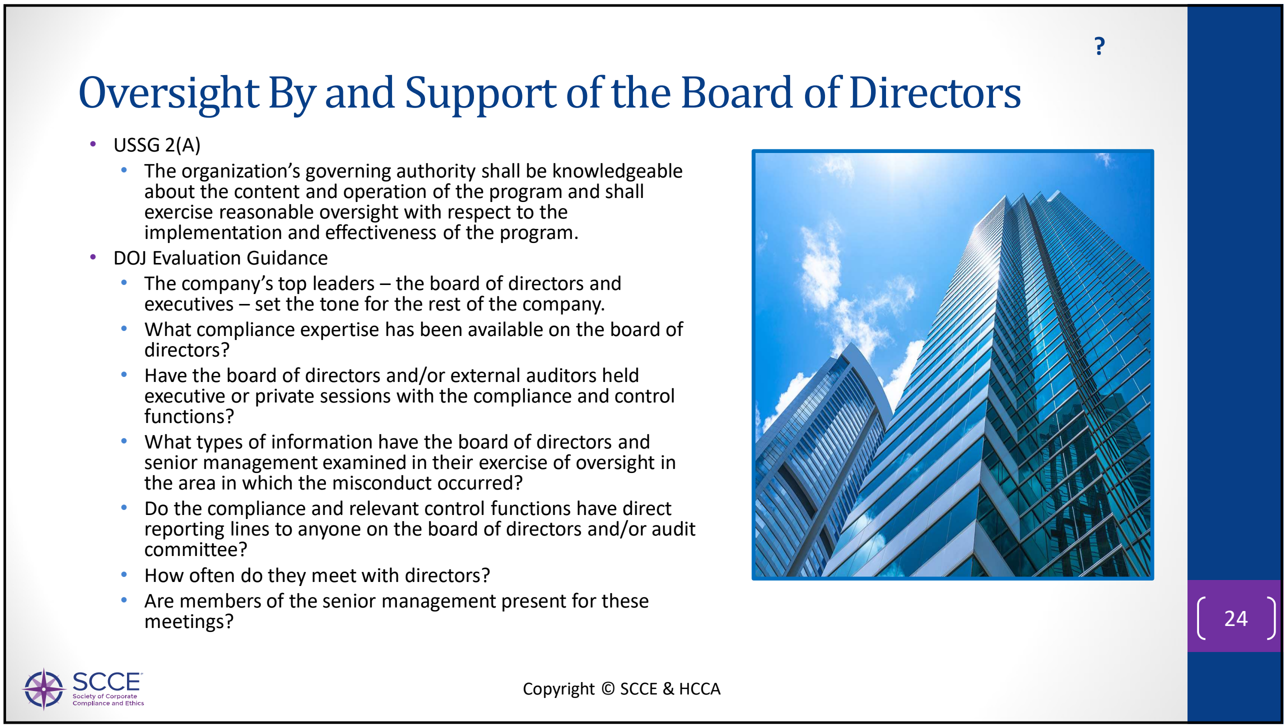
- DOJ Evaluation Guidance
  - Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function)?
  - To whom does the compliance function report?
  - How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers?
  - Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities?
  - Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts?
  - How does the company ensure the independence of compliance and control personnel?

SCCE Society of Corporate Compliance and Ethics



Oversight By and Support of Senior and Middle Management

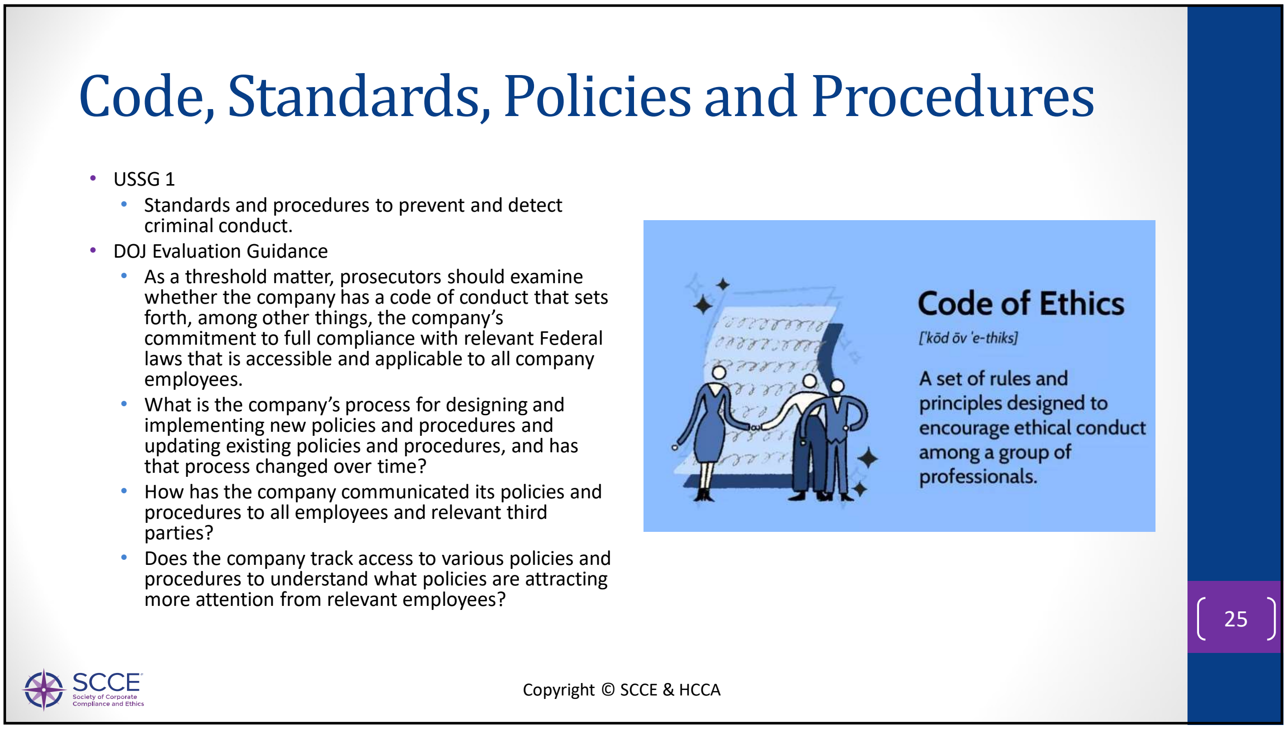
- USSG 2(B)
  - High-level personnel shall ensure that the organization has an effective compliance and ethics program, as described in this guideline.
- DOJ Evaluation Guidance
  - Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example.
  - Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them.
  - Have managers tolerated greater compliance risks in pursuit of new business or greater revenues?



?

Oversight By and Support of the Board of Directors

- USSG 2(A)
  - The organization's governing authority shall be knowledgeable about the content and operation of the program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the program.
- DOJ Evaluation Guidance
  - The company's top leaders – the board of directors and executives – set the tone for the rest of the company.
  - What compliance expertise has been available on the board of directors?
  - Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions?
  - What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?
  - Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee?
  - How often do they meet with directors?
  - Are members of the senior management present for these meetings?



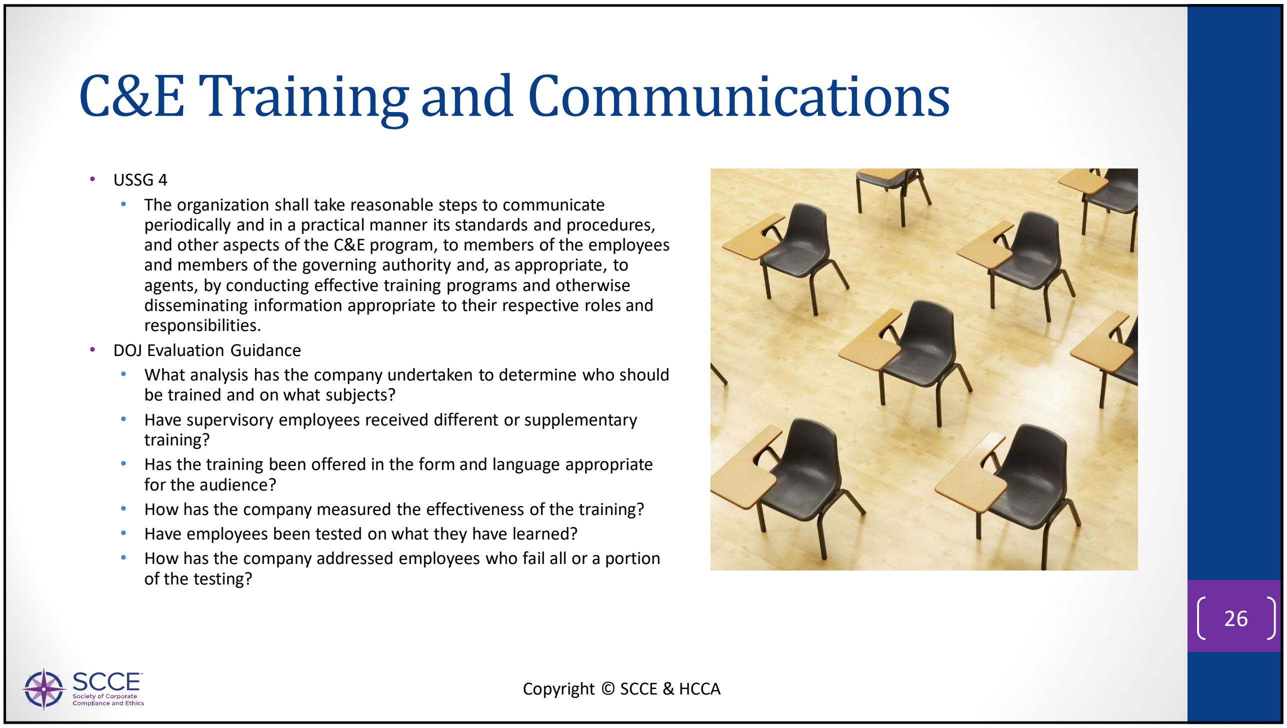
Code, Standards, Policies and Procedures

- USSG 1
  - Standards and procedures to prevent and detect criminal conduct.
- DOJ Evaluation Guidance
  - As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all company employees.
  - What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time?
  - How has the company communicated its policies and procedures to all employees and relevant third parties?
  - Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

Code of Ethics

['kōd ōv 'e-thiks]

A set of rules and principles designed to encourage ethical conduct among a group of professionals.



C&E Training and Communications

- USSG 4
  - The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the C&E program, to members of the employees and members of the governing authority and, as appropriate, to agents, by conducting effective training programs and otherwise disseminating information appropriate to their respective roles and responsibilities.
- DOJ Evaluation Guidance
  - What analysis has the company undertaken to determine who should be trained and on what subjects?
  - Have supervisory employees received different or supplementary training?
  - Has the training been offered in the form and language appropriate for the audience?
  - How has the company measured the effectiveness of the training?
  - Have employees been tested on what they have learned?
  - How has the company addressed employees who fail all or a portion of the testing?

C&E Risk Assessment

- USSG
  - The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each Program element to reduce the risk of criminal conduct identified through this process.
- DOJ Evaluation Guidance
  - What methodology has the company used to identify, analyze, and address the particular risks it faces?
  - Is the risk assessment current and subject to periodic review?
  - Is the periodic review limited to a “snapshot” in time or based upon continuous access to operational data and information across functions?
  - Has the periodic review led to updates in policies, procedures, and controls?
  - Do these updates account for risks discovered through misconduct or other problems with the compliance program?
  - How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices?

Auditing, Monitoring, Assessment and Continuous Improvement

- USSG 3
  - The organization shall take reasonable steps (A) to ensure that the organization’s compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct and
  - (B) to evaluate periodically the effectiveness of the C&E program.
- DOJ Evaluation Guidance
  - One hallmark of an effective compliance program is its capacity to improve and evolve.
  - Prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale.
  - Has the company reviewed and audited its compliance program in the area relating to the misconduct?
  - What testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake?
  - Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?

Reporting Procedures

- USSG 5(C)
  - Have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization’s employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.
- DOJ Evaluation Guidance
  - Does the company have an anonymous reporting mechanism and, if not, why not?
  - How is the reporting mechanism publicized to the company’s employees and other third parties?
  - Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it?
  - How has the company assessed the seriousness of the allegations it received?
  - Has the compliance function had full access to reporting and investigative information?

Investigations

- USSG
  - Not specifically mentioned in the USSG definition.
- DOJ Evaluation Guidance
  - How does the company ensure that investigations are properly scoped?
  - What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented?
  - Does the company apply timing metrics to ensure responsiveness?
- DOJ/SEC Resource Guide to the FCPA
  - “The truest measure of an effective compliance program is how it responds to misconduct. Accordingly, for a compliance program to be truly effective, it should have a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company’s response, including any disciplinary or remediation measures taken.”

Discipline and Remedial Measures

- USSG
  - (6) The program shall be promoted and enforced consistently throughout the organization through (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.
  - (7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.
- DOJ Evaluation Guidance
  - Are the actual reasons for discipline communicated to employees? If not, why not?
  - Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency?

Due Diligence in Hiring and Promotions and C&E Incentives

- USSG
  - (3) Use reasonable efforts not to include within the substantial authority personnel anyone whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective C&E program.
  - (6) The program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the program.
- DOJ Evaluation Guidance
  - Some companies have found that providing positive incentives – personnel promotions, rewards, and bonuses for improving and developing a C&E program or demonstrating ethical leadership – have driven compliance.
  - Some companies have even made compliance a significant metric for management bonuses and/or have made working on compliance a means of career advancement.
  - Has the company considered the implications of its incentives and rewards on compliance?
  - Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations?

Culture of C&E

- USSG
  - Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.
- DOJ Evaluation Guidance
  - How often and how does the company measure its culture of compliance?
  - Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance?
  - What steps has the company taken in response to its measurement of the compliance culture?

33

SCCE Society of Corporate Compliance and Ethics

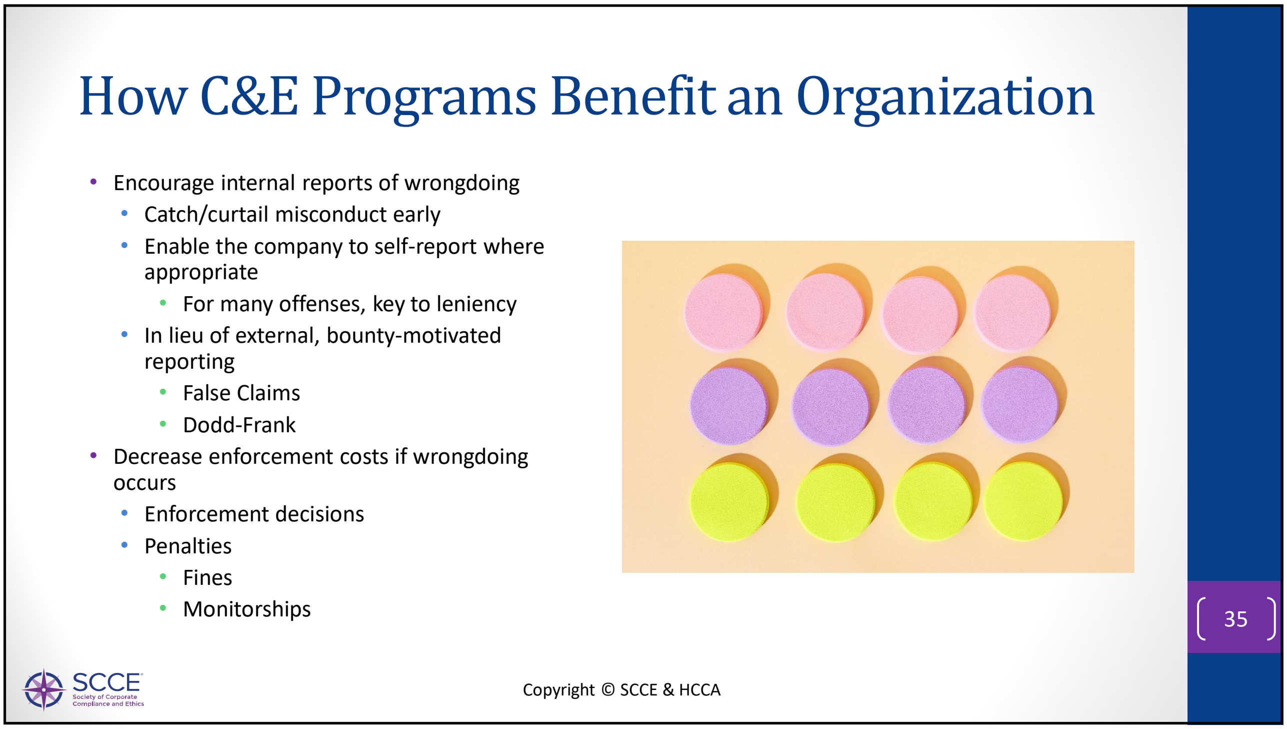
33

How C&E Programs Benefit an Organization

34

SCCE Society of Corporate Compliance and Ethics

34



How C&E Programs Benefit an Organization

- Encourage internal reports of wrongdoing
  - Catch/curtail misconduct early
  - Enable the company to self-report where appropriate
    - For many offenses, key to leniency
  - In lieu of external, bounty-motivated reporting
    - False Claims
    - Dodd-Frank
- Decrease enforcement costs if wrongdoing occurs
  - Enforcement decisions
  - Penalties
    - Fines
    - Monitorships

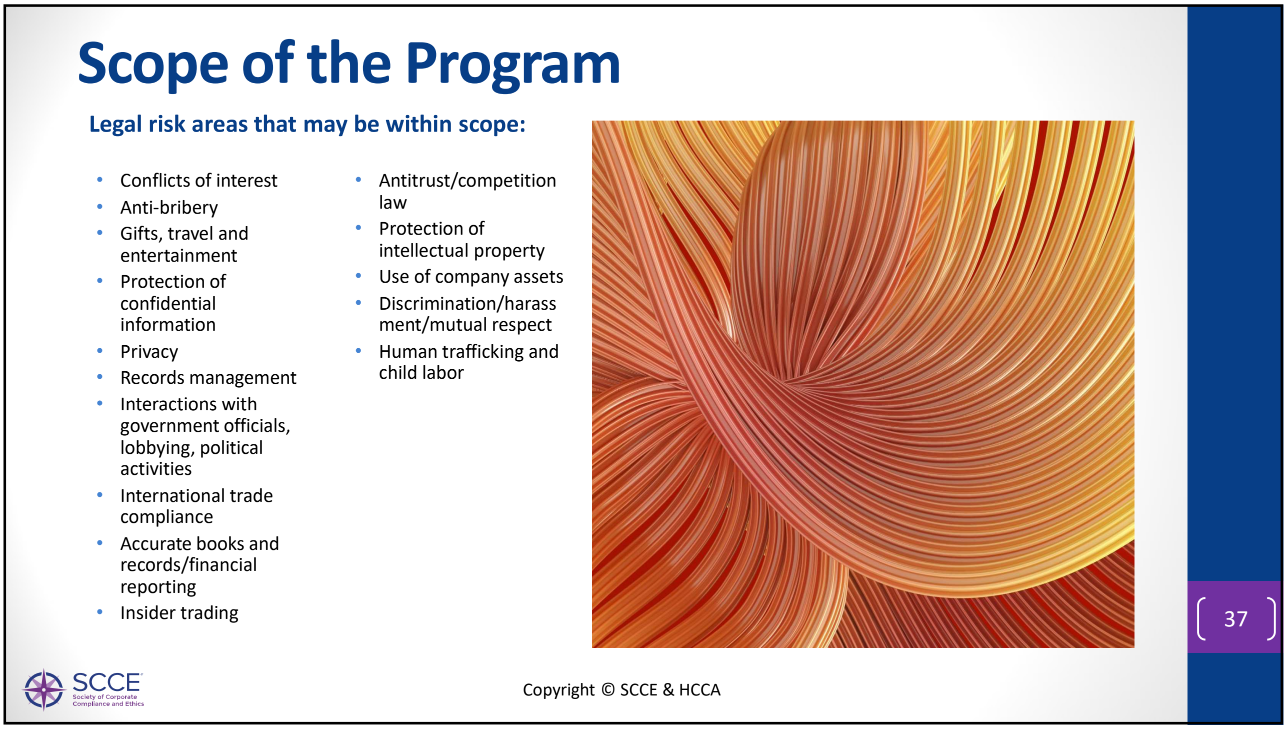
35

35

Scope of a Program

36

36



Scope of the Program

Legal risk areas that may be within scope:

- Conflicts of interest
- Anti-bribery
- Gifts, travel and entertainment
- Protection of confidential information
- Privacy
- Records management
- Interactions with government officials, lobbying, political activities
- International trade compliance
- Accurate books and records/financial reporting
- Insider trading
- Antitrust/competition law
- Protection of intellectual property
- Use of company assets
- Discrimination/harassment/mutual respect
- Human trafficking and child labor

37

37

Questions ?

38

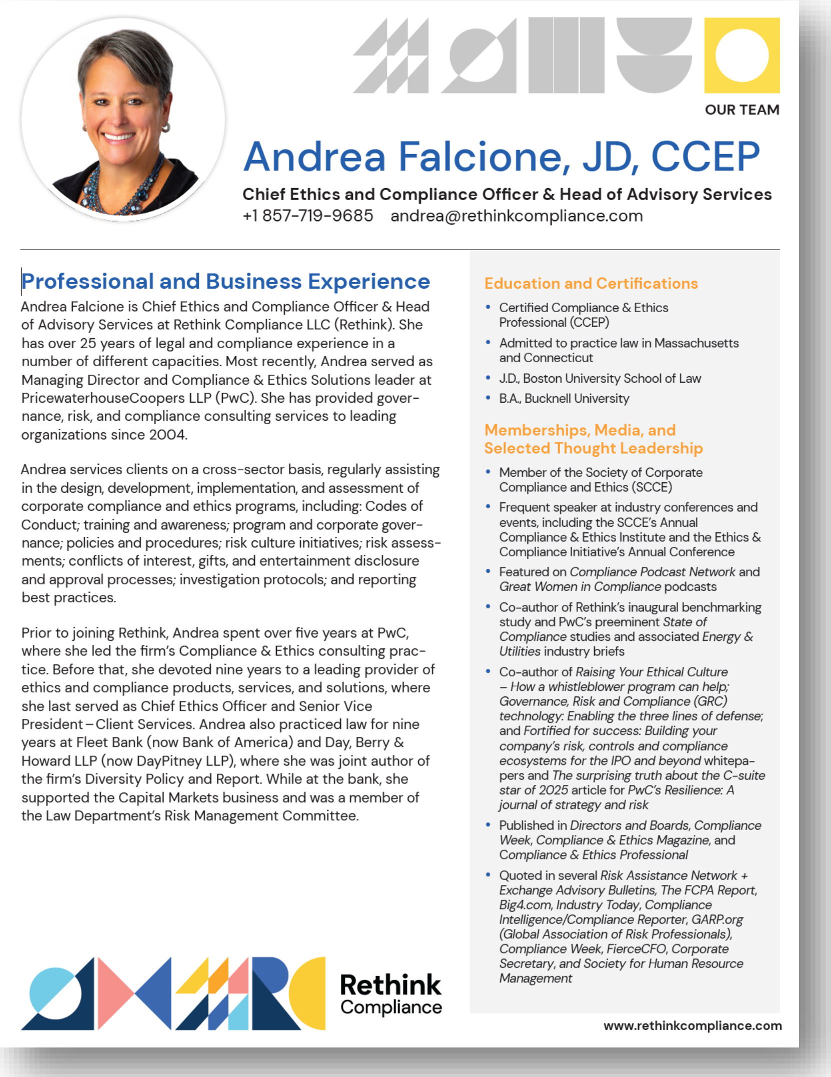
38

SCCE Compliance & Ethics Essentials Workshop

Standards and Procedures (Element no. 1)

Andrea Falcione

Introductions



OUR TEAM

Andrea Falcione, JD, CCEP

Chief Ethics and Compliance Officer & Head of Advisory Services
+1 857-719-9685 andrea@rethinkcompliance.com

Professional and Business Experience

Andrea Falcione is Chief Ethics and Compliance Officer & Head of Advisory Services at Rethink Compliance LLC (Rethink). She has over 25 years of legal and compliance experience in a number of different capacities. Most recently, Andrea served as Managing Director and Compliance & Ethics Solutions leader at PricewaterhouseCoopers LLP (PwC). She has provided governance, risk, and compliance consulting services to leading organizations since 2004.

Andrea services clients on a cross-sector basis, regularly assisting in the design, development, implementation, and assessment of corporate compliance and ethics programs, including: Codes of Conduct; training and awareness; program and corporate governance; policies and procedures; risk culture initiatives; risk assessments; conflicts of interest, gifts, and entertainment disclosure and approval processes; investigation protocols; and reporting best practices.

Prior to joining Rethink, Andrea spent over five years at PwC, where she led the firm's Compliance & Ethics consulting practice. Before that, she devoted nine years to a leading provider of ethics and compliance products, services, and solutions, where she last served as Chief Ethics Officer and Senior Vice President – Client Services. Andrea also practiced law for nine years at Fleet Bank (now Bank of America) and Day, Berry & Howard LLP (now DayPitney LLP), where she was joint author of the firm's Diversity Policy and Report. While at the bank, she supported the Capital Markets business and was a member of the Law Department's Risk Management Committee.

Education and Certifications

- Certified Compliance & Ethics Professional (CCEP)
- Admitted to practice law in Massachusetts and Connecticut
- J.D., Boston University School of Law
- B.A., Bucknell University

Memberships, Media, and Selected Thought Leadership

- Member of the Society of Corporate Compliance and Ethics (SCCE)
- Frequent speaker at industry conferences and events, including the SCCE's Annual Compliance & Ethics Institute and the Ethics & Compliance Initiative's Annual Conference
- Featured on *Compliance Podcast Network* and *Great Women in Compliance* podcasts
- Co-author of Rethink's inaugural benchmarking study and PwC's preeminent *State of Compliance* studies and associated *Energy & Utilities* industry briefs
- Co-author of *Raising Your Ethical Culture – How a whistleblower program can help; Governance, Risk and Compliance (GRC) technology: Enabling the three lines of defense;* and *Fortified for success: Building your company's risk, controls and compliance ecosystems for the IPO and beyond* whitepapers and *The surprising truth about the C-suite star of 2025* article for *PwC's Resilience: A journal of strategy and risk*
- Published in *Directors and Boards, Compliance Week, Compliance & Ethics Magazine,* and *Compliance & Ethics Professional*
- Quoted in several *Risk Assistance Network + Exchange Advisory Bulletins, The FCPA Report, Big4.com, Industry Today, Compliance Intelligence/Compliance Reporter, GARP.org (Global Association of Risk Professionals), Compliance Week, FierceCFO, Corporate Secretary, and Society for Human Resource Management*

Rethink Compliance

www.rethinkcompliance.com

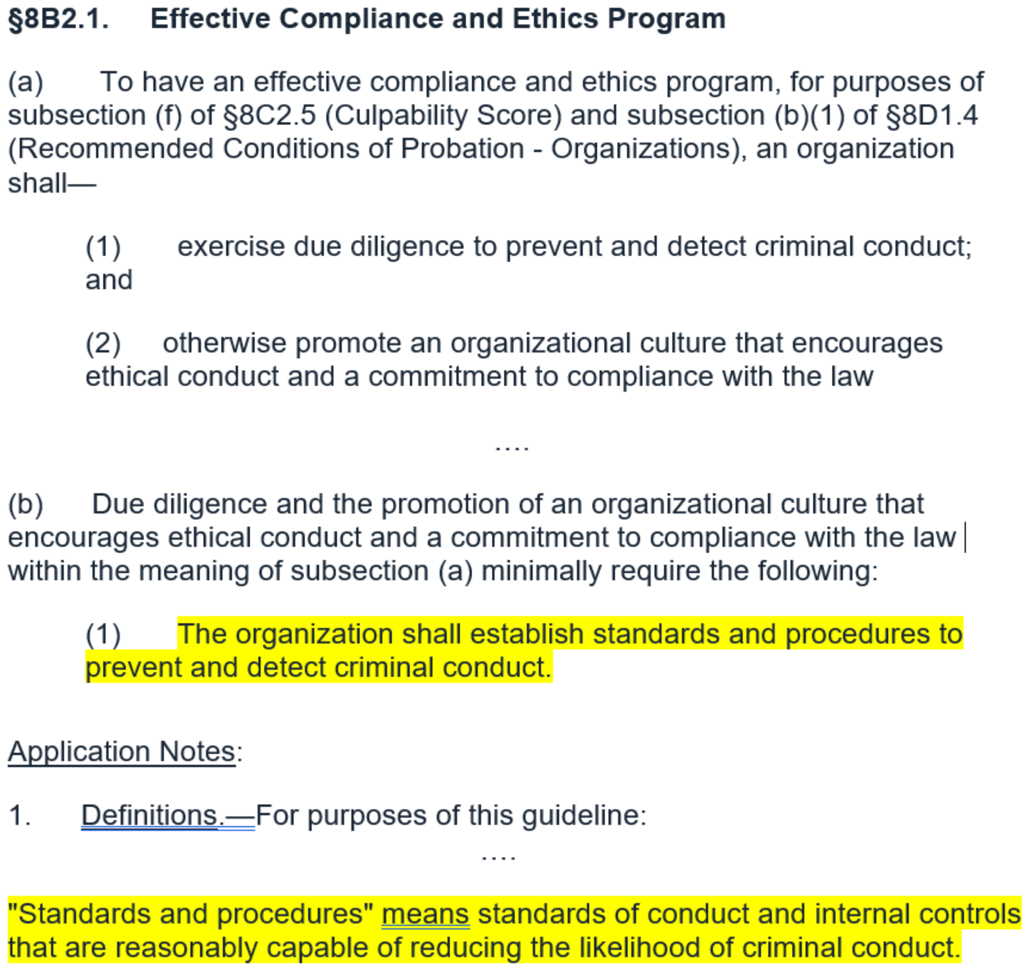
What we will cover today

- Standards and Procedures (Element No. 1): 2 min.
- Code of Ethics / Conduct: 35 min.
- Policies v. procedures: 20 min.
- Structural v. substantive: 5 min.
- Format, style, references, etc.: 3 min.
- Documentation for each element of a CEP: 10 min.
- From policies / procedures to a culture of compliance: 15 min.
- TOTAL SESSION TIME: 90 minutes

2 minutes

STANDARDS AND PROCEDURES (ELEMENT NO. 1)

Sentencing Guidelines



§8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (b)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law

. . . .

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

Application Notes:

1. Definitions.—For purposes of this guideline:

. . . .

"Standards and procedures" means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct.

Source: U.S. Federal Sentencing Guidelines for Organizations

35 minutes

CODE OF ETHICS / CONDUCT

SCCE
Society of Corporate Compliance and Ethics

"Detail of mock-up of cornerstone for McKim Building at Milford Quarry" by Boston Public Library is licensed under CC BY 2.0.

Foundation or cornerstone of a CEP

What’s required?

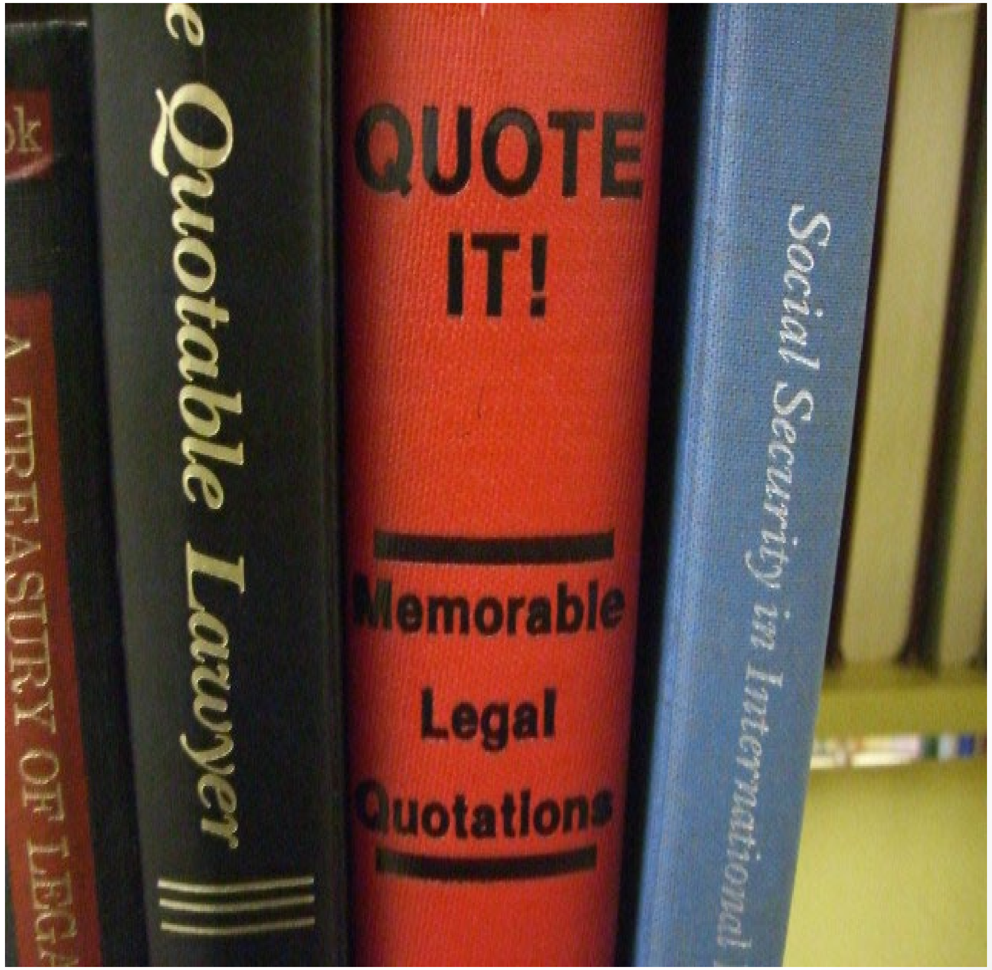
- Applies to directors, officers, *and* employees alike
- Covers basic business integrity topics, such as:
  - ✓ Conflicts of interest and corporate opportunities
  - ✓ Confidentiality and data protection
  - ✓ Competition and fair dealing
  - ✓ Employee rights
  - ✓ Use of company assets
  - ✓ Insider trading
  - ✓ Compliance with laws, rules, and regulations in general
  - ✓ Reporting illegal or unethical behavior
- Contains standards and procedures facilitating the effective operation of the Code, including a fair process for enforcement
- Includes anti-retaliation protections
- Is clear and objective

Leading practices

- ✓ Be thorough, but think beyond a list of topics
- ✓ Tie the Code to business or culture
- ✓ Values-, constituent-, or rules-based?
- ✓ Legacy, branding, imagery – what resonates?
- ✓ Use positive language
- ✓ Get user feedback

Leading practices (cont.)

Think like a LAWYER, talk like a HUMAN ….



"QUOTE IT! Memorable Legal Quotations'; 'Quotable Lawyer'" by umjanedoan is licensed under CC BY 2.0.

An example

The old way …

Fair competition, or antitrust, laws are designed to encourage fair competition in the marketplace. They protect both companies and consumers from unfair competitive practices.

As a large, global company, we must be very aware of our often dominant position in the marketplace. We are committed to complying with both the letter and the spirit of fair competition laws.

Our Company believes in vigorous competition, but we do not use illegal or unethical means to gain an advantage over a competitor. In this section, you'll learn what this means and what behavior is expected of you in this respect.

The new way …

The competition laws help support a free and fair marketplace.

We’re a large company in a high-visibility industry.

We **need** to follow these laws.

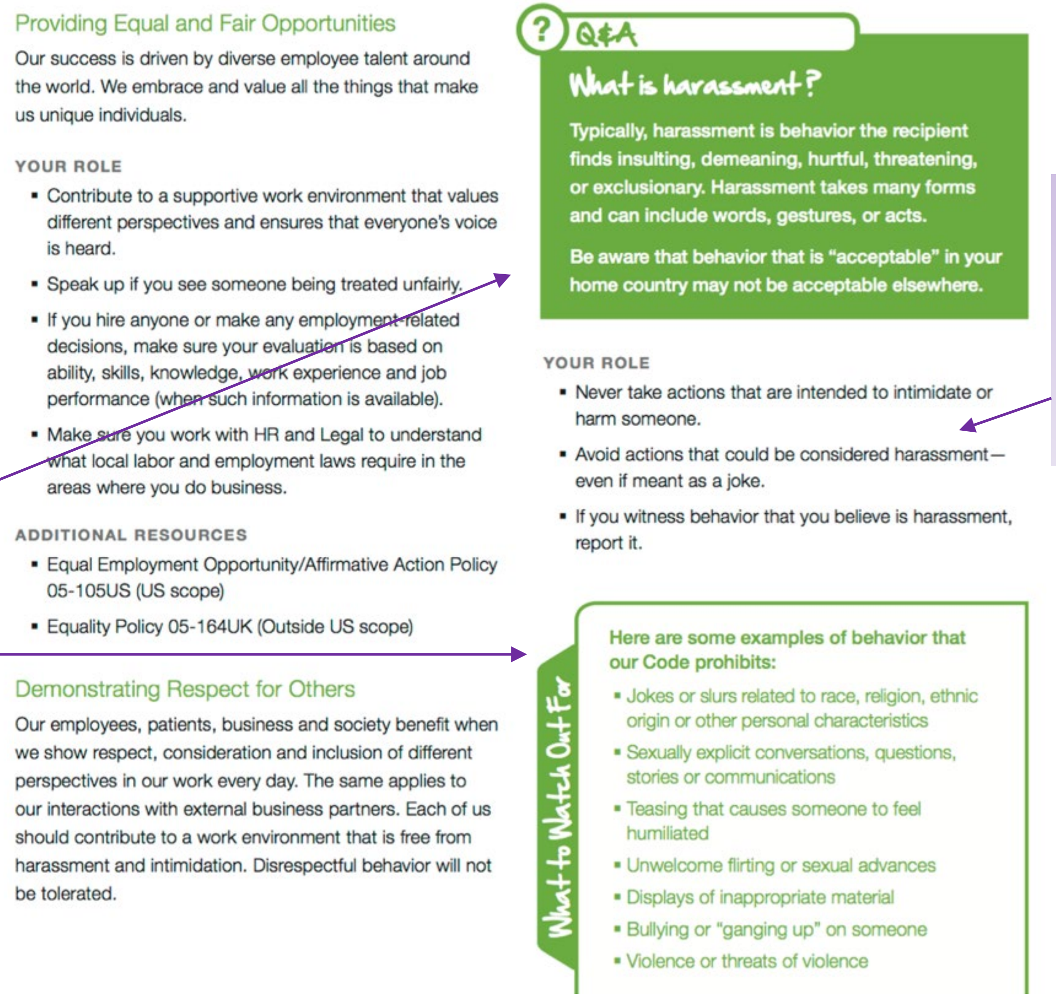
We will never take illegal or unethical actions, even if it helps us win.

Here are some key concepts....

A better example

Use a plainspoken approach to the Code. Write the way people speak!

Write in a layout-friendly style, using callouts and sidebars to help bring Code material to life.



Providing Equal and Fair Opportunities

Our success is driven by diverse employee talent around the world. We embrace and value all the things that make us unique individuals.

YOUR ROLE

- Contribute to a supportive work environment that values different perspectives and ensures that everyone's voice is heard.
- Speak up if you see someone being treated unfairly.
- If you hire anyone or make any employment-related decisions, make sure your evaluation is based on ability, skills, knowledge, work experience and job performance (when such information is available).
- Make sure you work with HR and Legal to understand what local labor and employment laws require in the areas where you do business.

ADDITIONAL RESOURCES

- Equal Employment Opportunity/Affirmative Action Policy 05-105US (US scope)
- Equality Policy 05-164UK (Outside US scope)

Demonstrating Respect for Others

Our employees, patients, business and society benefit when we show respect, consideration and inclusion of different perspectives in our work every day. The same applies to our interactions with external business partners. Each of us should contribute to a work environment that is free from harassment and intimidation. Disrespectful behavior will not be tolerated.

? Q&A

What is harassment?

Typically, harassment is behavior the recipient finds insulting, demeaning, hurtful, threatening, or exclusionary. Harassment takes many forms and can include words, gestures, or acts.

Be aware that behavior that is "acceptable" in your home country may not be acceptable elsewhere.

YOUR ROLE

- Never take actions that are intended to intimidate or harm someone.
- Avoid actions that could be considered harassment—even if meant as a joke.
- If you witness behavior that you believe is harassment, report it.

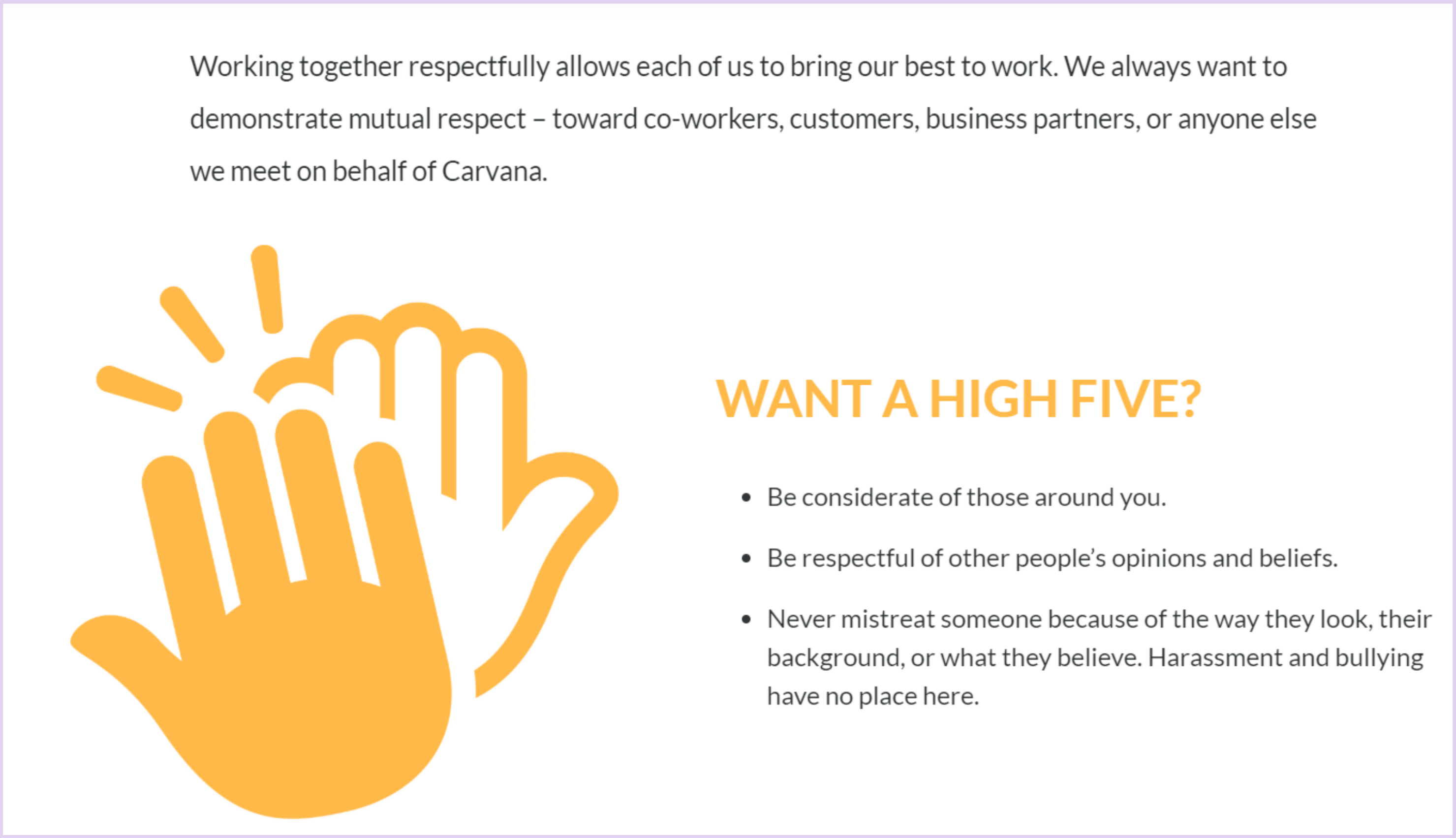
What to Watch Out For

Here are some examples of behavior that our Code prohibits:

- Jokes or slurs related to race, religion, ethnic origin or other personal characteristics
- Sexually explicit conversations, questions, stories or communications
- Teasing that causes someone to feel humiliated
- Unwelcome flirting or sexual advances
- Displays of inappropriate material
- Bullying or "ganging up" on someone
- Violence or threats of violence

Focus on specific behaviors – helping your constituents understand not what the law SAYS, but what the law MEANS.

An even better example



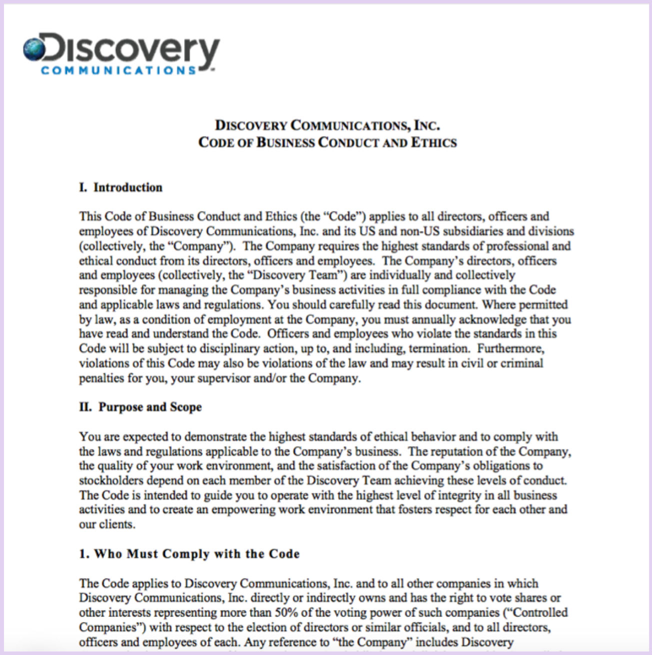
Working together respectfully allows each of us to bring our best to work. We always want to demonstrate mutual respect – toward co-workers, customers, business partners, or anyone else we meet on behalf of Carvana.

WANT A HIGH FIVE?

- Be considerate of those around you.
- Be respectful of other people's opinions and beliefs.
- Never mistreat someone because of the way they look, their background, or what they believe. Harassment and bullying have no place here.

Code evolution

2010-2016: From contracts to marketing documents



Discovery COMMUNICATIONS

DISCOVERY COMMUNICATIONS, INC.
CODE OF BUSINESS CONDUCT AND ETHICS

I. Introduction

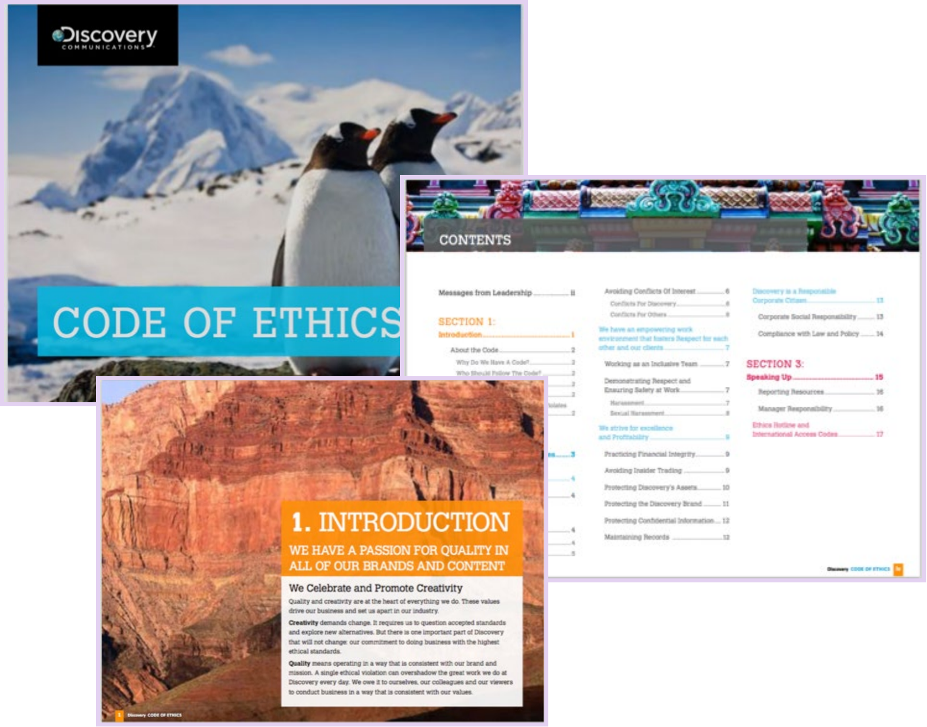
This Code of Business Conduct and Ethics (the "Code") applies to all directors, officers and employees of Discovery Communications, Inc. and its US and non-US subsidiaries and divisions (collectively, the "Company"). The Company requires the highest standards of professional and ethical conduct from its directors, officers and employees. The Company's directors, officers and employees (collectively, the "Discovery Team") are individually and collectively responsible for managing the Company's business activities in full compliance with the Code and applicable laws and regulations. You should carefully read this document. Where permitted by law, as a condition of employment at the Company, you must annually acknowledge that you have read and understand the Code. Officers and employees who violate the standards in this Code will be subject to disciplinary action, up to, and including, termination. Furthermore, violations of this Code may also be violations of the law and may result in civil or criminal penalties for you, your supervisor and/or the Company.

II. Purpose and Scope

You are expected to demonstrate the highest standards of ethical behavior and to comply with the laws and regulations applicable to the Company's business. The reputation of the Company, the quality of your work environment, and the satisfaction of the Company's obligations to stockholders depend on each member of the Discovery Team achieving these levels of conduct. The Code is intended to guide you to operate with the highest level of integrity in all business activities and to create an empowering work environment that fosters respect for each other and our clients.

1. Who Must Comply with the Code

The Code applies to Discovery Communications, Inc. and to all other companies in which Discovery Communications, Inc. directly or indirectly owns and has the right to vote shares or other interests representing more than 50% of the voting power of such companies ("Controlled Companies") with respect to the election of directors or similar officials, and to all directors, officers and employees of each. Any reference to "the Company" includes Discovery



Messages from Leadership ii
SECTION 1:
Introduction 1
About the Code 2
Why Do We Have A Code? 2
Who Should Follow The Code? 2
Avoiding Conflicts Of Interest 6
Conflicts For Discovery 6
Conflicts For Others 8
We have an empowering work environment that fosters Respect for each other and our clients 7
Working as an Inclusive Team 7
Demonstrating Respect and Ensuring Safety at Work 7
Harassment 7
Sexual Harassment 8
We strive for excellence and Profitability 9
Practicing Financial Integrity 9
Avoiding Insider Trading 9
Protecting Discovery's Assets 10
Protecting the Discovery Brand 11
Protecting Confidential Information 12
Maintaining Records 12
Discovery is a Responsible Corporate Citizen 13
Corporate Social Responsibility 13
Compliance with Law and Policy 14
SECTION 3:
Speaking Up 15
Reporting Resources 16
Manager Responsibility 16
Ethics Hotline and International Access Codes 17

1. INTRODUCTION

WE HAVE A PASSION FOR QUALITY IN ALL OF OUR BRANDS AND CONTENT

We Celebrate and Promote Creativity

Quality and creativity are at the heart of everything we do. These values drive our business and set us apart in our industry.

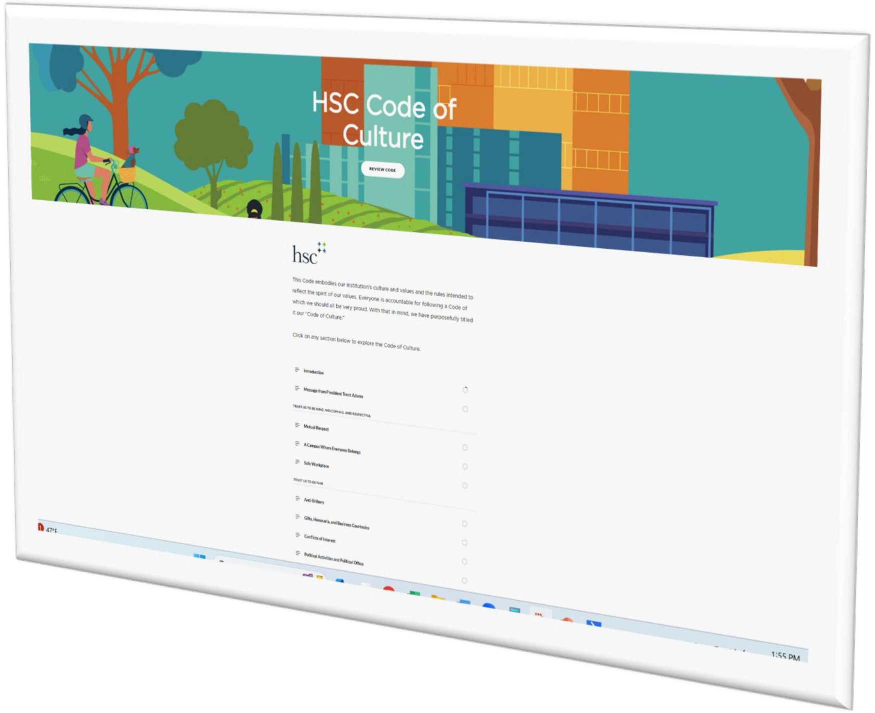
Creativity demands change. It requires us to question accepted standards and explore new alternatives. But there is one important part of Discovery that will not change: our commitment to doing business with the highest ethical standards.

Quality means operating in a way that is consistent with our brand and mission. A single ethical violation can overshadow the great work we do at Discovery every day. We owe it to ourselves, our colleagues and our viewers to conduct business in a way that is consistent with our values.

SCCE Society of Corporate Compliance and Ethics

Code evolution (cont.)

Today: microsites, digital magazines, apps


HSC Code of Culture

REVIEW CODE

hsc

This Code embodies our institution's culture and values and the rules intended to reflect the spirit of our values. Everyone is accountable for following a Code of which we should all be very proud. With that in mind, we have purposefully titled it our "Code of Culture."

Click on any section below to explore the Code of Culture.

- Introduction
- Message from President Trent Adams

TRUST US TO BE KIND, WELCOMING, AND RESPECTFUL

- Mutual Respect
- A Campus Where Everyone Belongs
- Safe Workplace

TRUST US TO BE FAIR

- Anti-Bribery
- Gifts, Honoraria, and Business Courtesies
- Conflicts of Interest
- Political Activities and Political Office

SHIONOGI INC.

Succeedir
Togeth

Our Guide to Ethical Business Conduct at Shio

3

The most pharmac of the ma

e consistently
iding in 1878,
nes to protect

research-driven
ed by healthcare
society at large.

all Shionogi Inc.
ers build.

e operate, reflect
y we have to our-
ess with integrity
nd regulations.

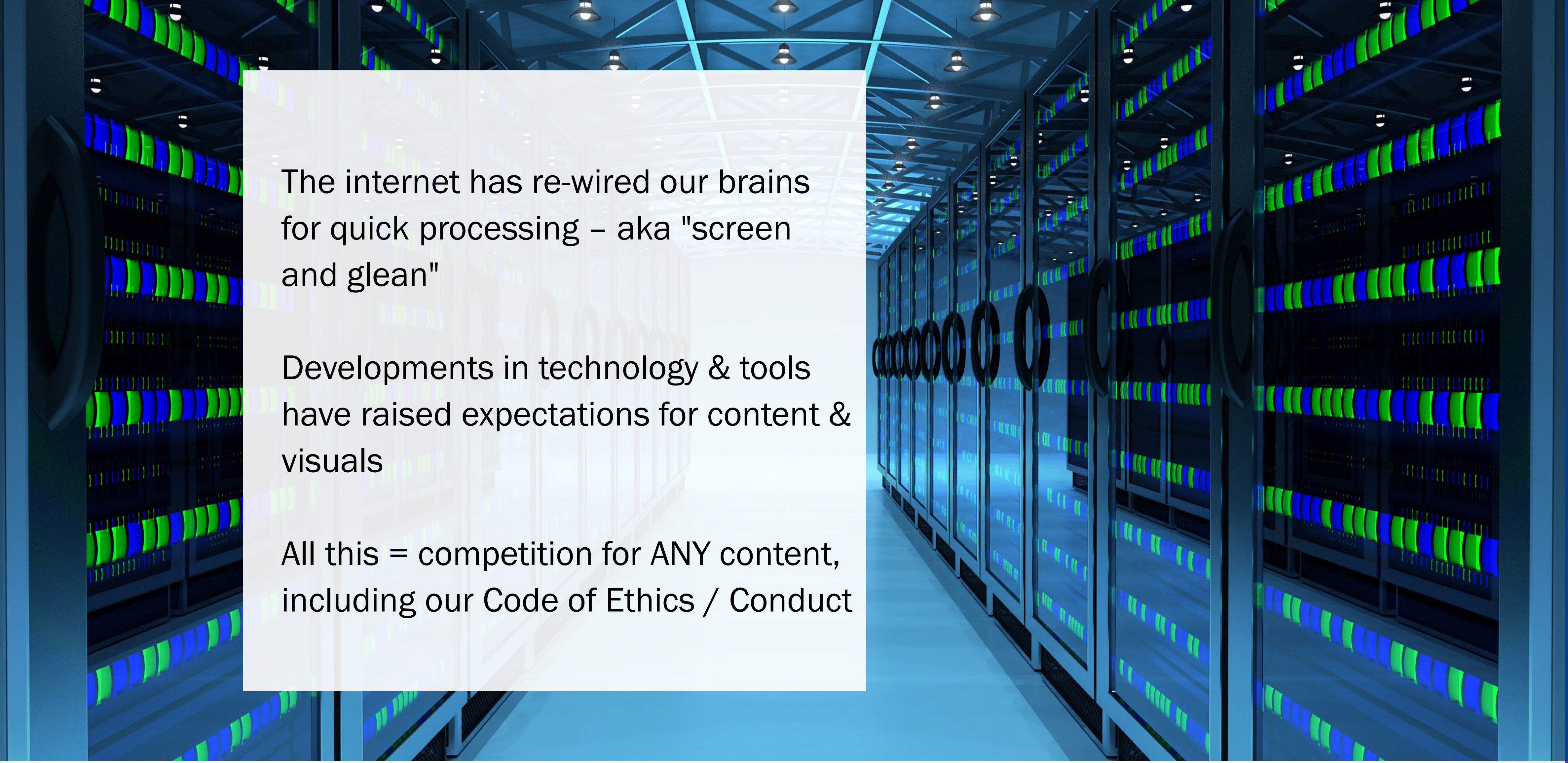
To view these Codes, click the graphics above.

Why are Codes changing?

Because …

- Regulator expectations (DOJ Guidance, anyone??)
- Tools and technology
- Your audience

… have all changed!



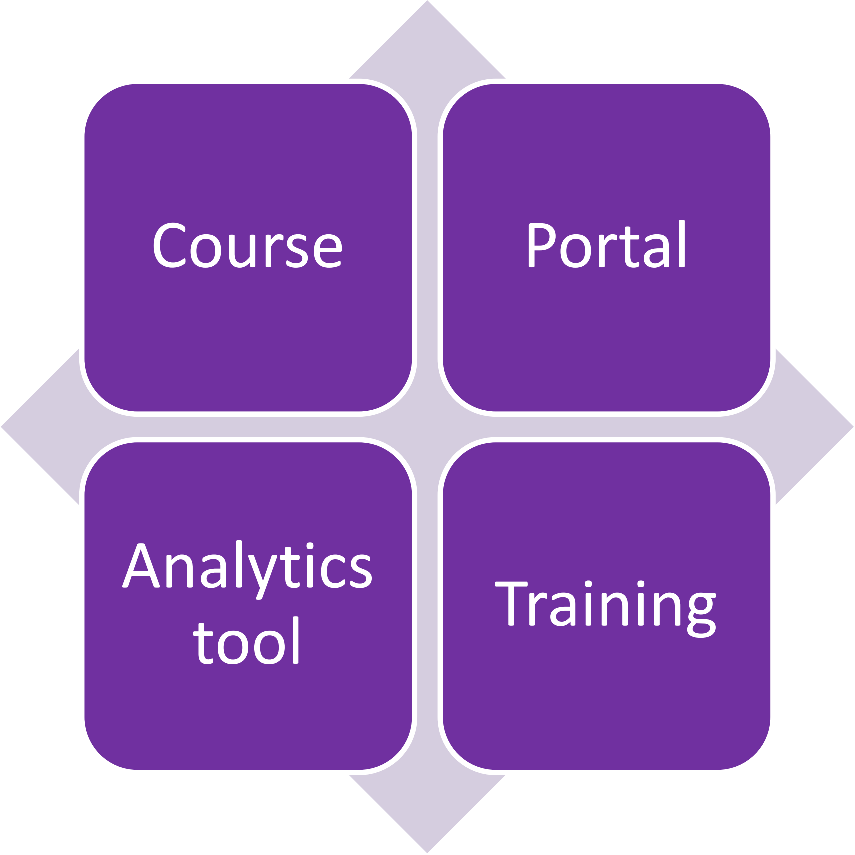
The internet has re-wired our brains for quick processing – aka "screen and glean"

Developments in technology & tools have raised expectations for content & visuals

All this = competition for ANY content, including our Code of Ethics / Conduct

How has our audience changed?

Additional benefits



Course

Portal

Analytics tool

Training

A strategic approach to communications can amplify the impact of your Code

Develop a Code communications strategy

20 minutes

POLICIES V. PROCEDURES

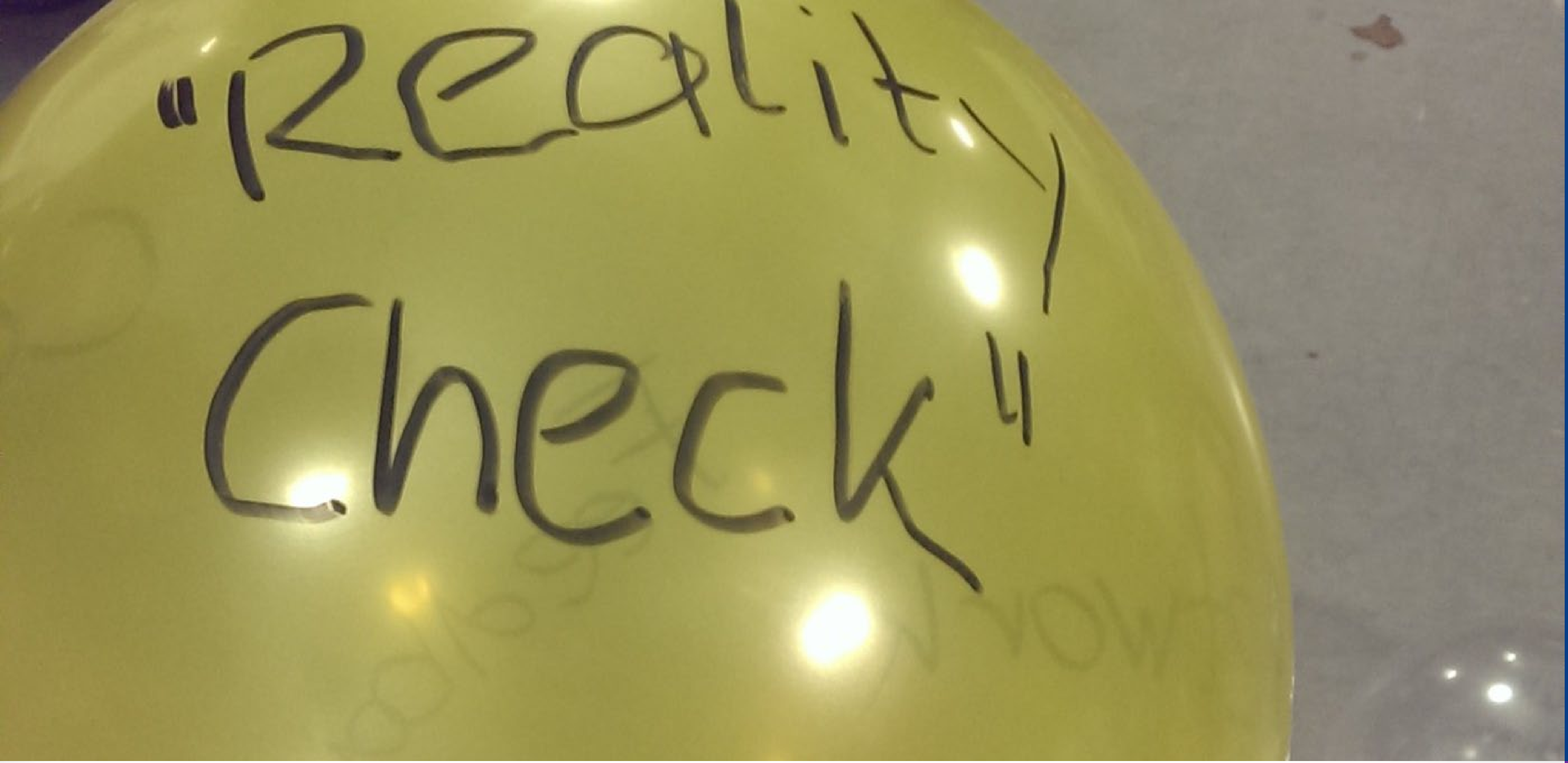
What’s the difference?

Policies …

- Describe guiding principles
- Set the company’s direction and tone and support its corporate values
- Should be universally applicable across all operations, all over the world
- Address legal, statutory, or ethical risk
- Help guide employee decision-making

Procedures, on the other hand …

- Provide additional guidance or information
- Help to further explain a policy
- Describe specific steps to accomplish an end result required by a policy
- Support the principles set forth in a related policy
- Should always be tied to at least one relevant policy



"Reality Check" by Solvetogether.org is licensed under CC BY-SA 2.0.

The current state of affairs …

Leading practices

What are your expectations for accountability???

SCCE
Society of Corporate Compliance and Ethics

Leading practices (cont.)

- Develop a plan
- Be realistic
- Understand stakeholders’ needs
- Seek user feedback

Leading practices (cont.)

Remember:
shorter is better!

Leading practices (cont.)

Recognize the need for P&P management protocols

1. Templatize
Approach to new P&P creation

2. Describe
Process for new P&P creation

3. Categorize
P&P by operational vs. legal risk

4. Update
Frequency of P&P review

5. Evaluate
Review and approval processes

Leading practices (cont.)

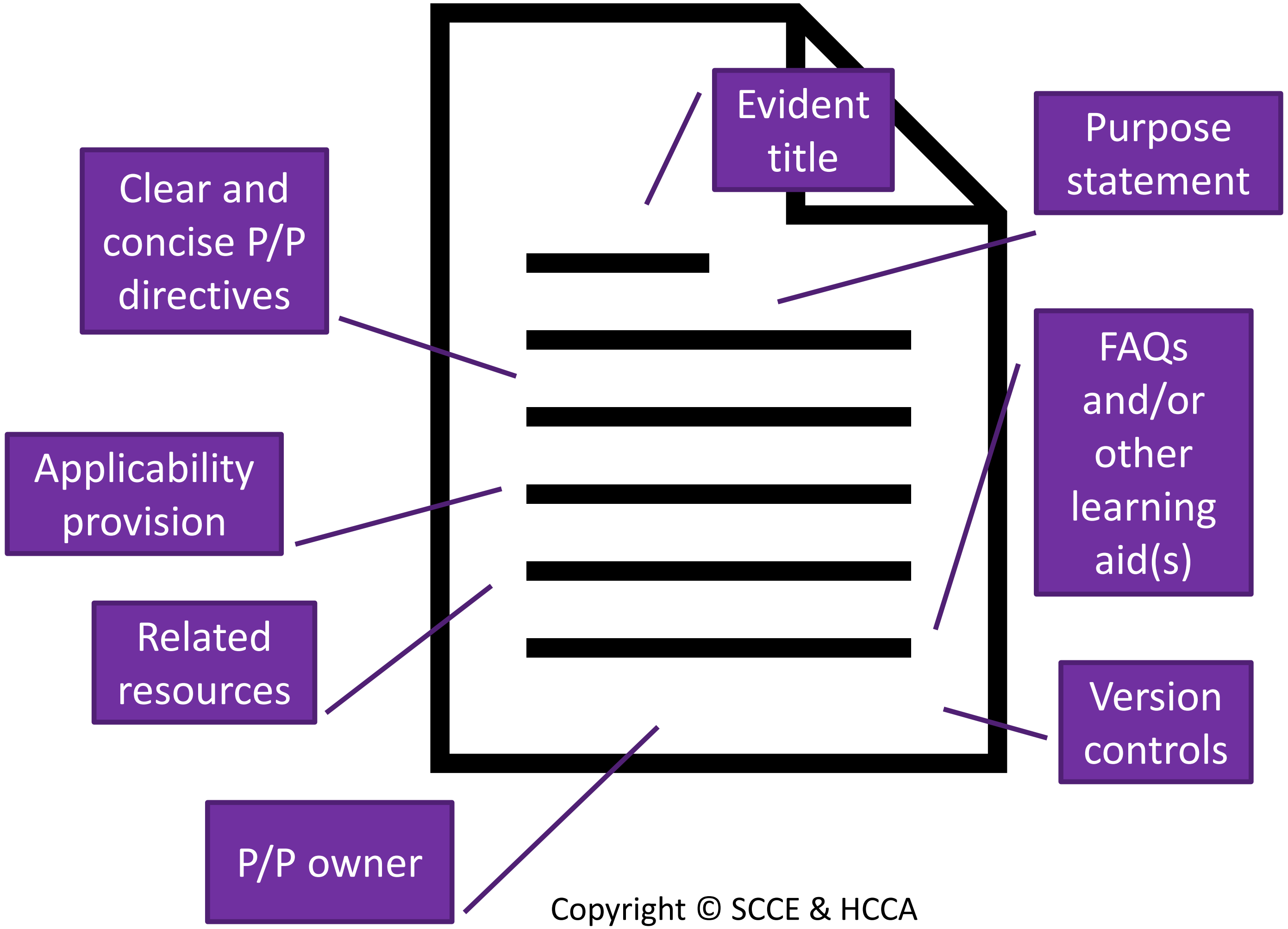
Important elements of P&P management

- Establish a business case
- Assess impacts on other policies
- Identify policy owner
- Define scope and applicability
- Ensure accuracy and comprehension of content
- Identify education and awareness opportunities
- Provide review, approval and reassessment processes

5 minutes

STRUCTURAL V. SUBSTANTIVE

Structural v. Substantive



SCCE
Society of Corporate Compliance and Ethics

3 minutes

FORMAT, STYLE, REFERENCES, ETC.

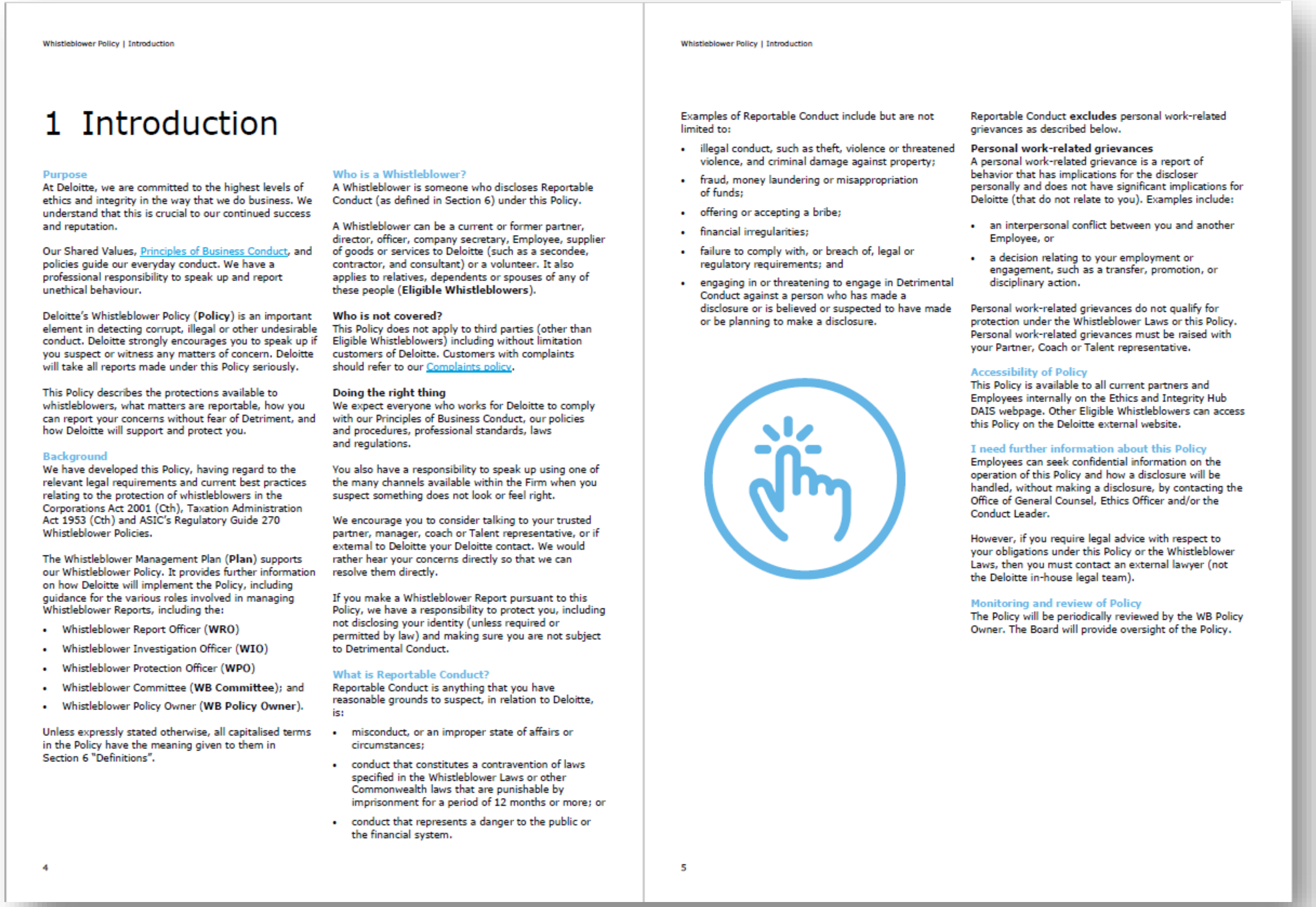
SCCE Society of Corporate Compliance and Ethics

Format, style, references, etc.

P&Ps ≠ Codes!

But maybe they should!

An example



1 Introduction

Purpose

At Deloitte, we are committed to the highest levels of ethics and integrity in the way that we do business. We understand that this is crucial to our continued success and reputation.

Our Shared Values, Principles of Business Conduct, and policies guide our everyday conduct. We have a professional responsibility to speak up and report unethical behaviour.

Deloitte's Whistleblower Policy (**Policy**) is an important element in detecting corrupt, illegal or other undesirable conduct. Deloitte strongly encourages you to speak up if you suspect or witness any matters of concern. Deloitte will take all reports made under this Policy seriously.

This Policy describes the protections available to whistleblowers, what matters are reportable, how you can report your concerns without fear of Detriment, and how Deloitte will support and protect you.

Background

We have developed this Policy, having regard to the relevant legal requirements and current best practices relating to the protection of whistleblowers in the Corporations Act 2001 (Cth), Taxation Administration Act 1953 (Cth) and ASIC's Regulatory Guide 270 Whistleblower Policies.

The Whistleblower Management Plan (**Plan**) supports our Whistleblower Policy. It provides further information on how Deloitte will implement the Policy, including guidance for the various roles involved in managing Whistleblower Reports, including the:

- Whistleblower Report Officer (**WRO**)
- Whistleblower Investigation Officer (**WIO**)
- Whistleblower Protection Officer (**WPO**)
- Whistleblower Committee (**WB Committee**); and
- Whistleblower Policy Owner (**WB Policy Owner**).

Unless expressly stated otherwise, all capitalised terms in the Policy have the meaning given to them in Section 6 "Definitions".

Who is a Whistleblower?

A Whistleblower is someone who discloses Reportable Conduct (as defined in Section 6) under this Policy.

A Whistleblower can be a current or former partner, director, officer, company secretary, Employee, supplier of goods or services to Deloitte (such as a secondee, contractor, and consultant) or a volunteer. It also applies to relatives, dependents or spouses of any of these people (**Eligible Whistleblowers**).

Who is not covered?

This Policy does not apply to third parties (other than Eligible Whistleblowers) including without limitation customers of Deloitte. Customers with complaints should refer to our Complaints policy.

Doing the right thing

We expect everyone who works for Deloitte to comply with our Principles of Business Conduct, our policies and procedures, professional standards, laws and regulations.

You also have a responsibility to speak up using one of the many channels available within the Firm when you suspect something does not look or feel right.

We encourage you to consider talking to your trusted partner, manager, coach or Talent representative, or if external to Deloitte your Deloitte contact. We would rather hear your concerns directly so that we can resolve them directly.

If you make a Whistleblower Report pursuant to this Policy, we have a responsibility to protect you, including not disclosing your identity (unless required or permitted by law) and making sure you are not subject to Detrimental Conduct.

What is Reportable Conduct?

Reportable Conduct is anything that you have reasonable grounds to suspect, in relation to Deloitte, is:

- misconduct, or an improper state of affairs or circumstances;
- conduct that constitutes a contravention of laws specified in the Whistleblower Laws or other Commonwealth laws that are punishable by imprisonment for a period of 12 months or more; or
- conduct that represents a danger to the public or the financial system.

Examples of Reportable Conduct include but are not limited to:

- illegal conduct, such as theft, violence or threatened violence, and criminal damage against property;
- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities;
- failure to comply with, or breach of, legal or regulatory requirements; and
- engaging in or threatening to engage in Detrimental Conduct against a person who has made a disclosure or is believed or suspected to have made or be planning to make a disclosure.

Reportable Conduct **excludes** personal work-related grievances as described below.

Personal work-related grievances

A personal work-related grievance is a report of behavior that has implications for the discloser personally and does not have significant implications for Deloitte (that do not relate to you). Examples include:

- an interpersonal conflict between you and another Employee, or
- a decision relating to your employment or engagement, such as a transfer, promotion, or disciplinary action.

Personal work-related grievances do not qualify for protection under the Whistleblower Laws or this Policy. Personal work-related grievances must be raised with your Partner, Coach or Talent representative.

Accessibility of Policy

This Policy is available to all current partners and Employees internally on the Ethics and Integrity Hub DAIS webpage. Other Eligible Whistleblowers can access this Policy on the Deloitte external website.

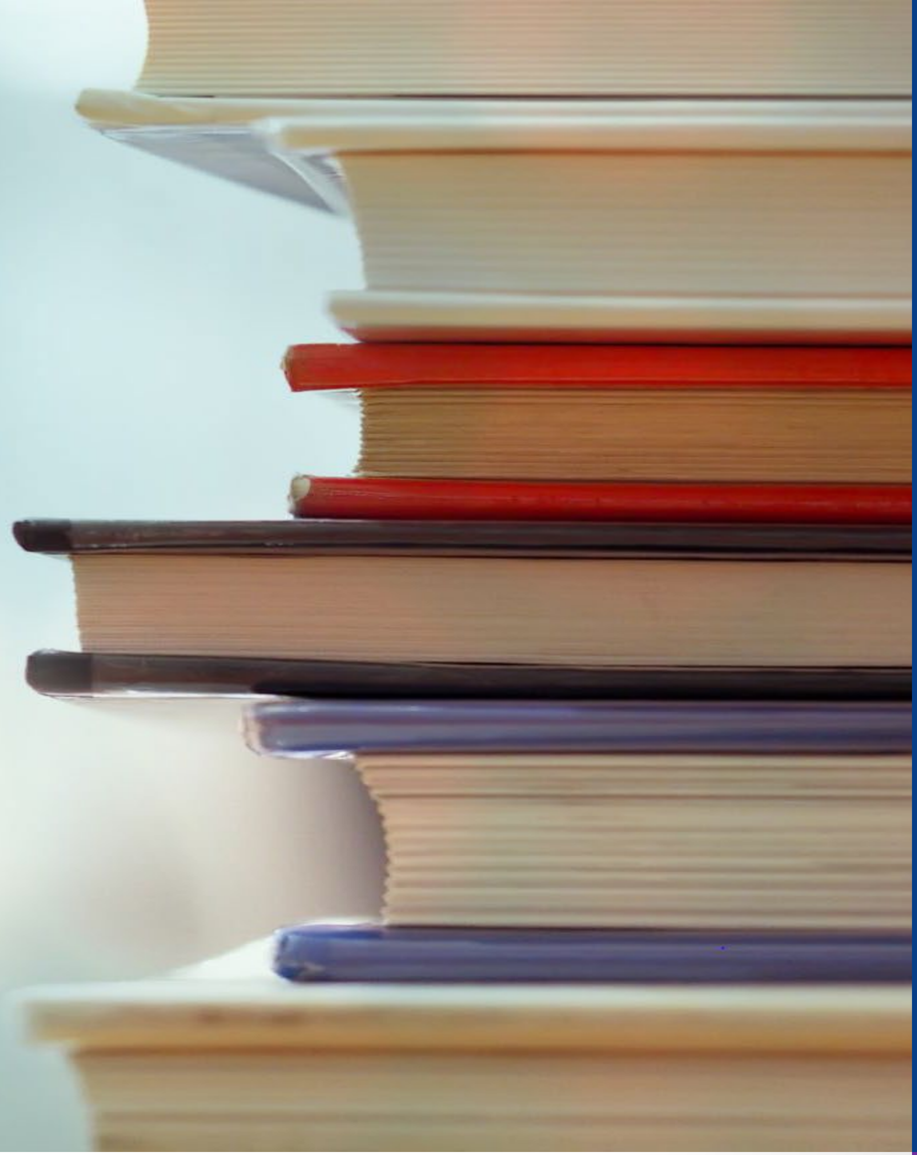
I need further information about this Policy

Employees can seek confidential information on the operation of this Policy and how a disclosure will be handled, without making a disclosure, by contacting the Office of General Counsel, Ethics Officer and/or the Conduct Leader.

However, if you require legal advice with respect to your obligations under this Policy or the Whistleblower Laws, then you must contact an external lawyer (not the Deloitte in-house legal team).

Monitoring and review of Policy

The Policy will be periodically reviewed by the WB Policy Owner. The Board will provide oversight of the Policy.



As with all things CEP-related, you need a plan

Do a policy cross walk

Work with your SMEs

Get MarComm’s help

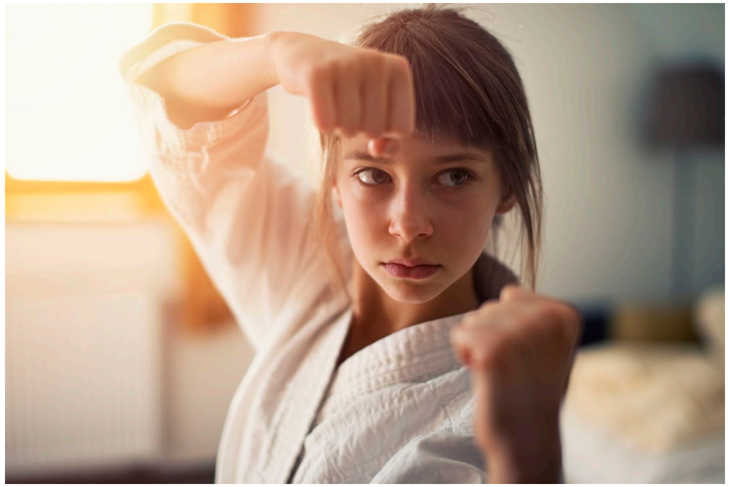
Decide which P&Ps merit attestation

Communication and education

10 minutes

DOCUMENTATION FOR EACH ELEMENT OF A CEP

Why document?



"DOJ seal" by Mike Licht, NotionsCapital.com is licensed under CC BY 2.0.

Litigation by Nick Youngson CC BY-SA 3.0 Alpha Stock Images

"Discipline" by Grotuk is licensed under CC BY 2.0.d

Why document? (cont.)

Elements no. 2 and 3

Governance, oversight, and authority

- Governing authority charter (*e.g.,* Board of Directors or a committee of the Board of Directors)
- Compliance Committee charter (*i.e.,* management committee)
- Program description / charter
- Org charts
- Job descriptions
- RACI matrices
- Delegations of authority
- Program / information flows
- Budget requests / grants
- Technology resources

Due diligence in delegation of authority

- List of substantial authority personnel
- Background checks
- Personnel / performance management records
- HR complaints (if any)
- Substantiated compliance violations or ethical lapses
- Third-party due diligence process, RACI matrix, technology resources, and results
- M&A compliance due diligence checklist, RACI matrix, and results

Elements no. 4 and 5

Communication and training

- Annual communication plan
- Annual training plan
- Communications content and formats
- Training content and formats
- Training completion rates, test scores, etc.
- Click rates for non-mandatory initiatives
- Vendor selection process and criteria
- Relationship to risk assessment results
- Effectiveness measures and other data analytics

Monitoring, auditing, and reporting systems

- Controls testing plan and results
- Annual compliance audit plan, report, and management response (including third-party compliance audits)
- Ongoing compliance monitoring protocols
- Relationship to risk assessment results
- Hotline / whistleblower program audit plan and results
- Year-over-year trend analyses
- Data analytics
- Regulatory change monitoring process

Elements no. 6 and 7

Incentives and enforcement

- Individual contributor, management, and business unit compliance and ethics KPIs
- Evidence of management's active support for and promotion of CEP
- Performance evaluation processes and aggregated compliance-related KPI data
- Description of incentives programs and compliance analysis thereof
- Description of compliance and ethics-related incentives
- Disciplinary process, trends, aggregated data, and indicators of consistency in application, including for third parties

Response to wrongdoing

- Root cause analyses process
- Root cause analyses results
- Program design and remediation indicators
- Program design and remediation plans and results
- Year-over-year trend analyses

SCCE Society of Corporate Compliance and Ethics

Elements no. 8a and 8b

Risk assessment

- Risk identification, culture, and assessment process and methodology
- Risk identification, culture, and assessment results
- Inherent v. residual risk
- Controls mapping
- Risk ranking methodology
- Risk assessment response
- Technology enablement
- Risk reporting

Program improvement

- Internal and external program assessment methodology and results
- Program benchmarking methodology and results

15 minutes

FROM POLICIES / PROCEDURES TO A CULTURE OF COMPLIANCE

SCCE Society of Corporate Compliance and Ethics

Framing the issue

Policies and procedures

- Are, of course, necessary
- But they are not sufficient to ensure compliance
- WHY, you ask? Because…

Human nature and motivation

- Are nuanced and complex!

What we know

"Culture eats strategy for breakfast."

- Peter Drucker

An example

A useful definition

What is culture then?

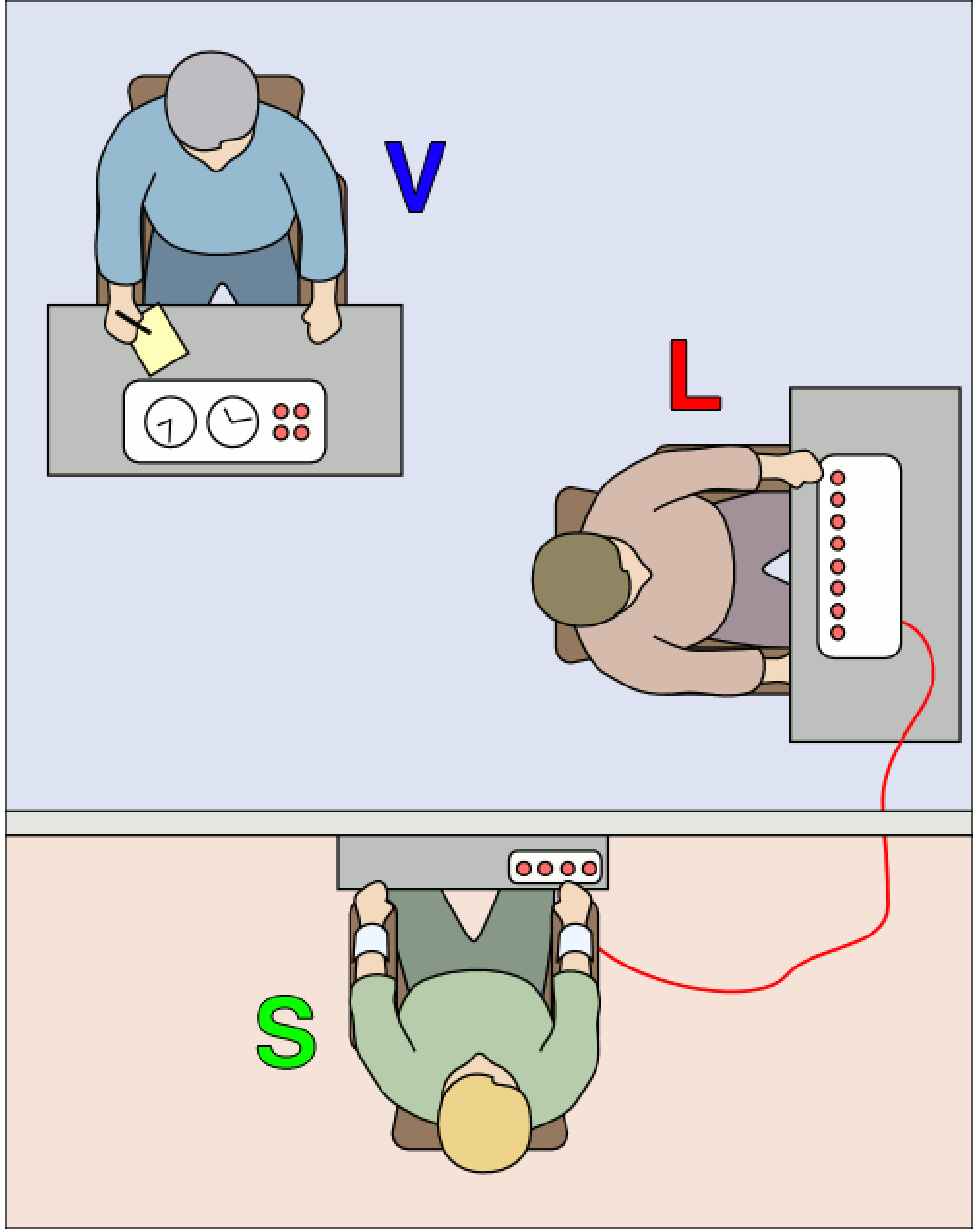
- "**Culture** (/ˈkʌltʃər/) is an umbrella term which encompasses the social behavior and norms found in human societies, as well as the knowledge, beliefs, arts, laws, customs, capabilities, and habits of the individuals in these groups.
- Humans acquire culture through the learning processes of enculturation and socialization ….
- A cultural norm codifies acceptable conduct in society; it serves as a guideline for behavior, dress, language, and demeanor in a situation, which serves as a template for expectations in a social group.

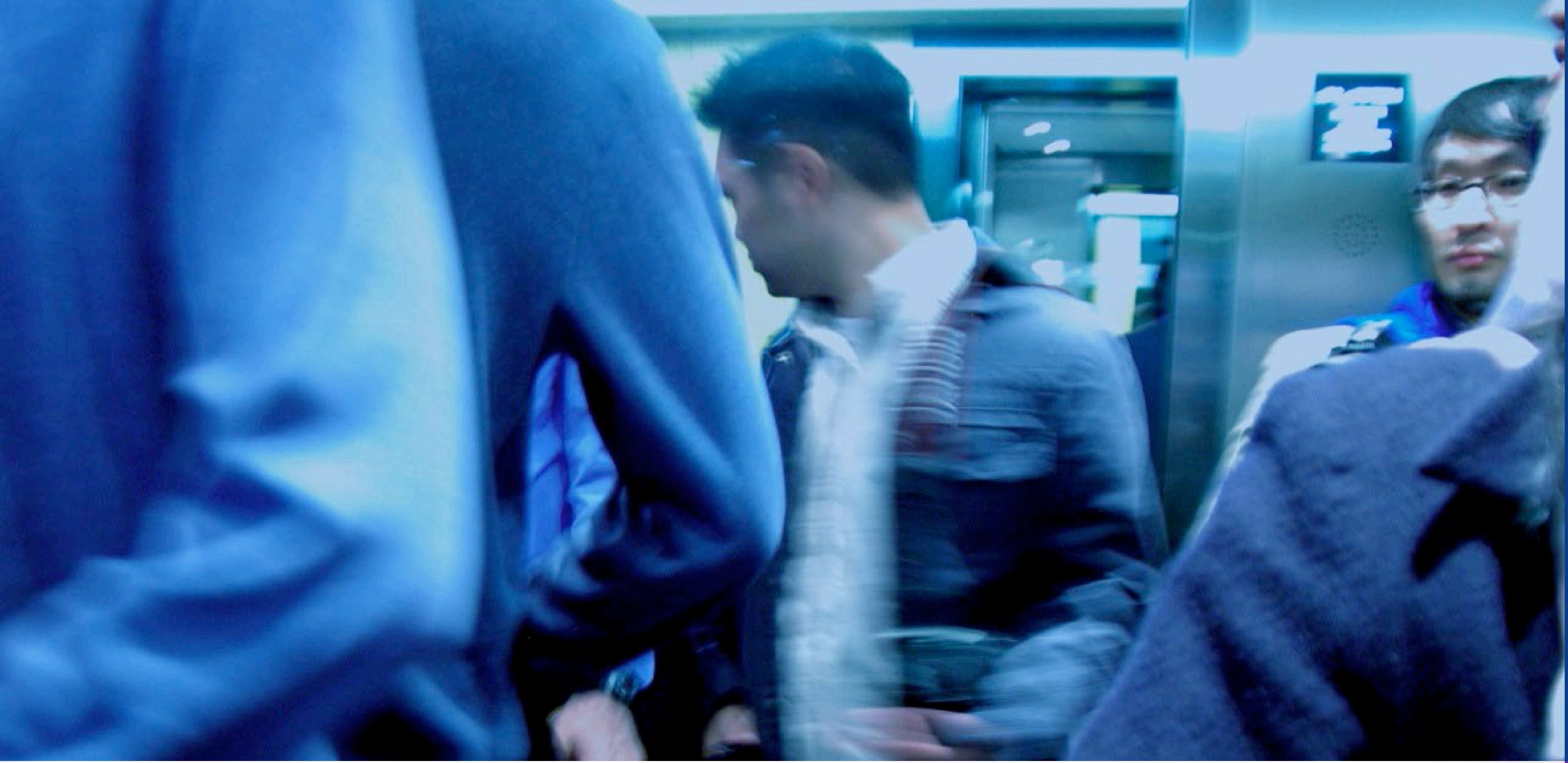
Source: Wikipedia

Decision Making by Nick Youngson CC BY-SA 3.0 Alpha Stock Images

How do we make decisions?

SCCE Society of Corporate Compliance and Ethics


V
L
S



"elevator crowd" by Gideon Tsang is licensed under CC BY-SA 2.0.

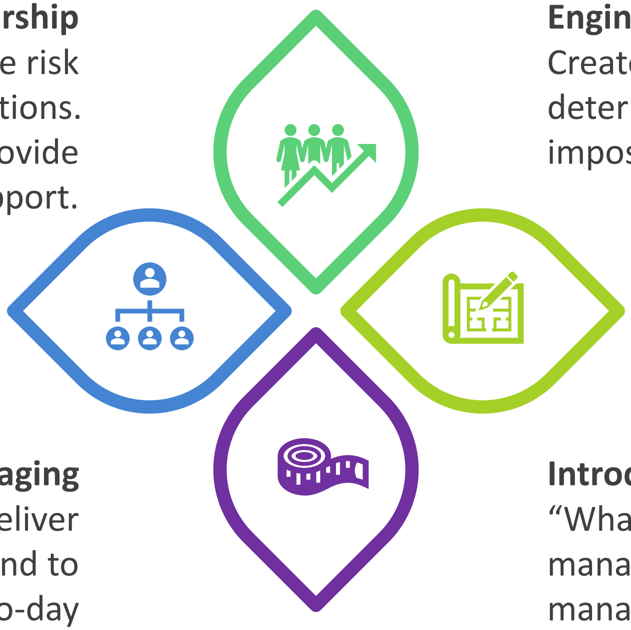
The elevator experiment

So, how can we impact culture?

Implement Systems Thinking:
Determine how you can operationalize compliance!

Give the Business Ownership
Shift responsibility for compliance risk management to the business functions. Compliance function should provide oversight and support.

Engineer Out Violations
Create obstacles and built-in deterrence. What if it were simply impossible to break the law or policy?



Get Managers Involved in Messaging
Equip and require managers to deliver compliance messages and respond to questions regarding day-to-day compliance issues in operations.

Introduce Data and Measurement
"What gets measured gets managed." Score departments, managers, and individuals based on compliance success.

So, how can we impact culture?

Learn from Marketing and Advertising:
Know where your audience is and where you want to move them!

Start with Audience Insights
Start by learning what matters most to your audience, not what matters to you.

Become a Mind Reader
Speak to your audience about what they find important, ideally using the words and phrases THEY use.

Ask: What's Interesting Here?
Only the strongest, most interesting content survives. Be concise, catchy, engaging, and well-crafted.

Drive and Measure Behavior
Know the change you want to see and how you'll measure it and build those into your initiatives.

So, how can we impact culture?

Use Persuasion and Influence techniques:
Information alone won’t change behavior. You have to make your audience care!

Go Beyond Information
Knowing right doesn’t always mean doing right.

Connect with People
Most of us make decisions based on emotions and justify with logic.

Create Feedback Loops
People support what they create (or influence).

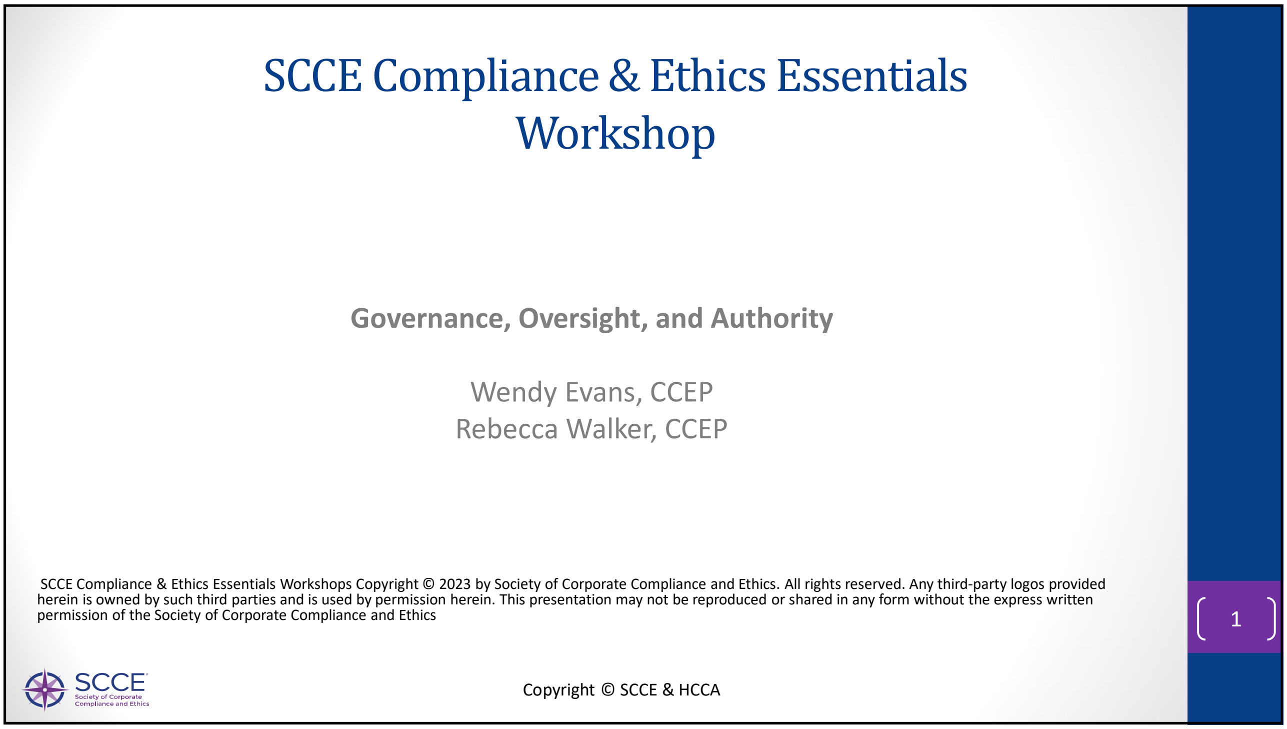
Use Key Messages
Once you know your audience, you can put your message in their terms.

Be Thoughtful
Take advantage of the way the human brain works to make your message “sticky.”

Say it Again
Messages are more effective when they are repeated.

THANK YOU!

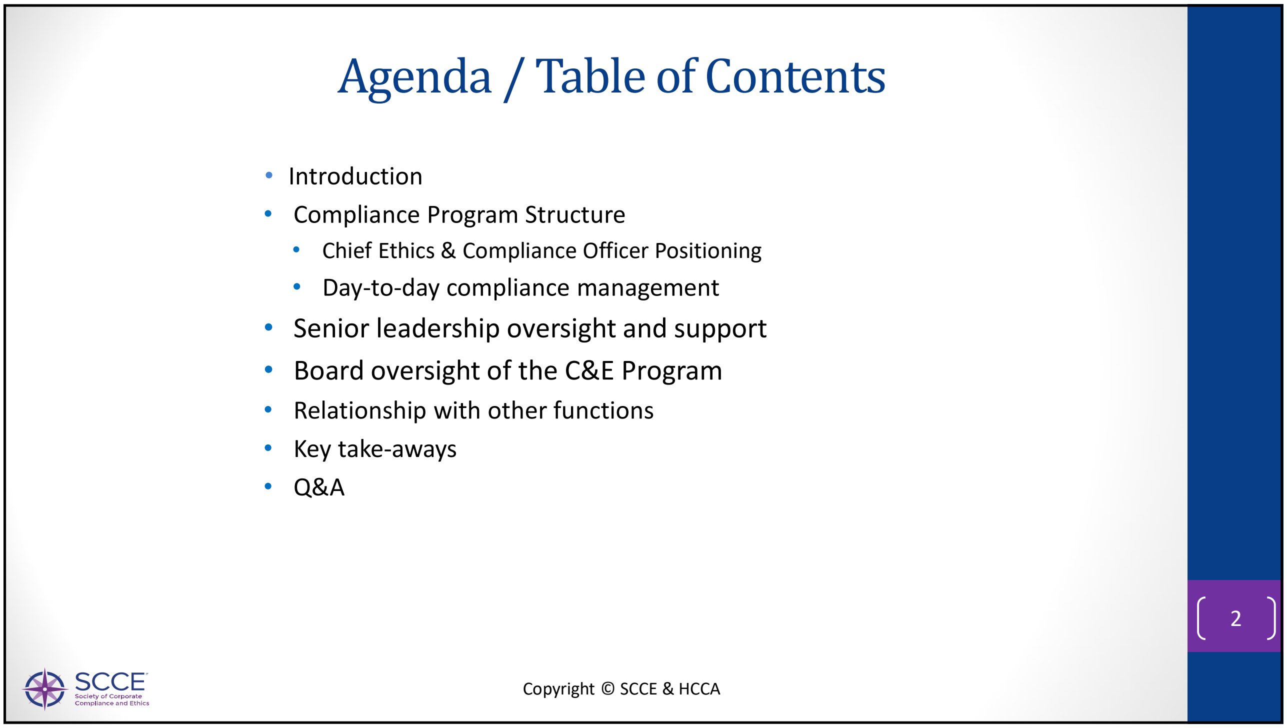
SCCE®
Society of Corporate
Compliance and Ethics



SCCE Compliance & Ethics Essentials Workshop

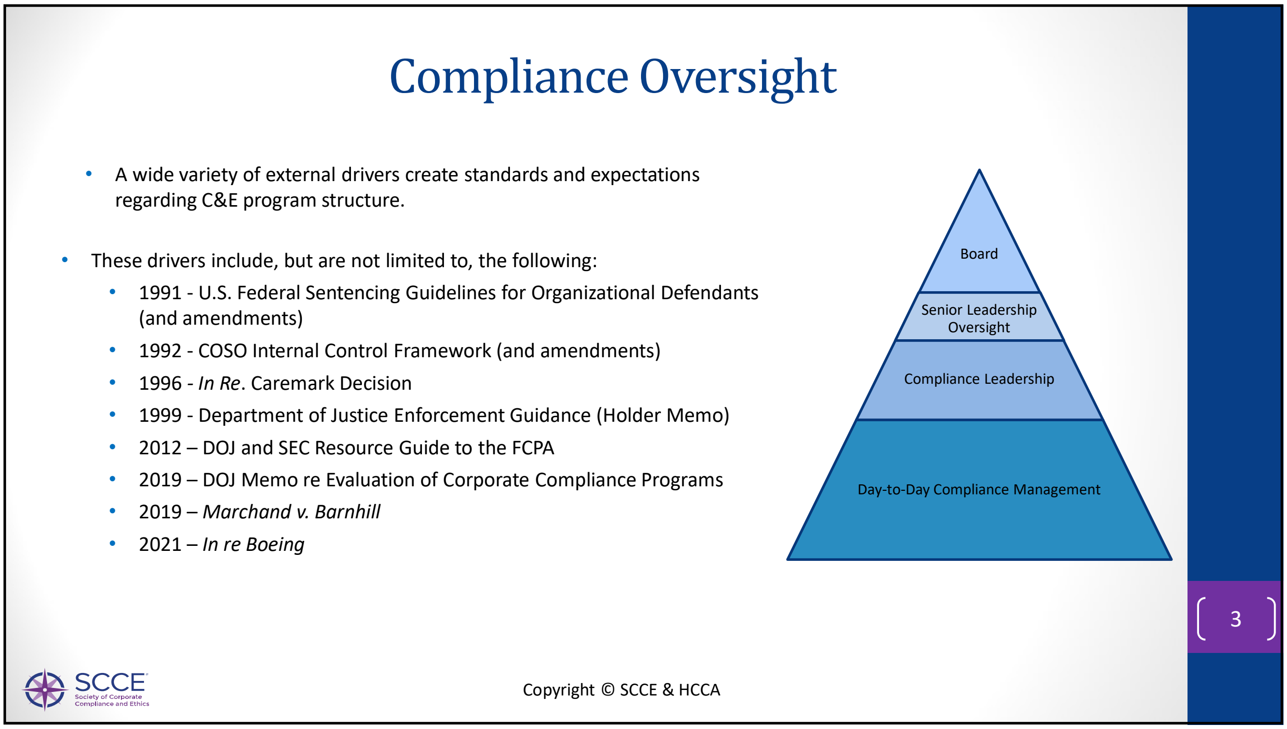
Governance, Oversight, and Authority

Wendy Evans, CCEP
Rebecca Walker, CCEP



Agenda / Table of Contents

- Introduction
- Compliance Program Structure
  - Chief Ethics & Compliance Officer Positioning
  - Day-to-day compliance management
- Senior leadership oversight and support
- Board oversight of the C&E Program
- Relationship with other functions
- Key take-aways
- Q&A



Compliance Oversight

- A wide variety of external drivers create standards and expectations regarding C&E program structure.

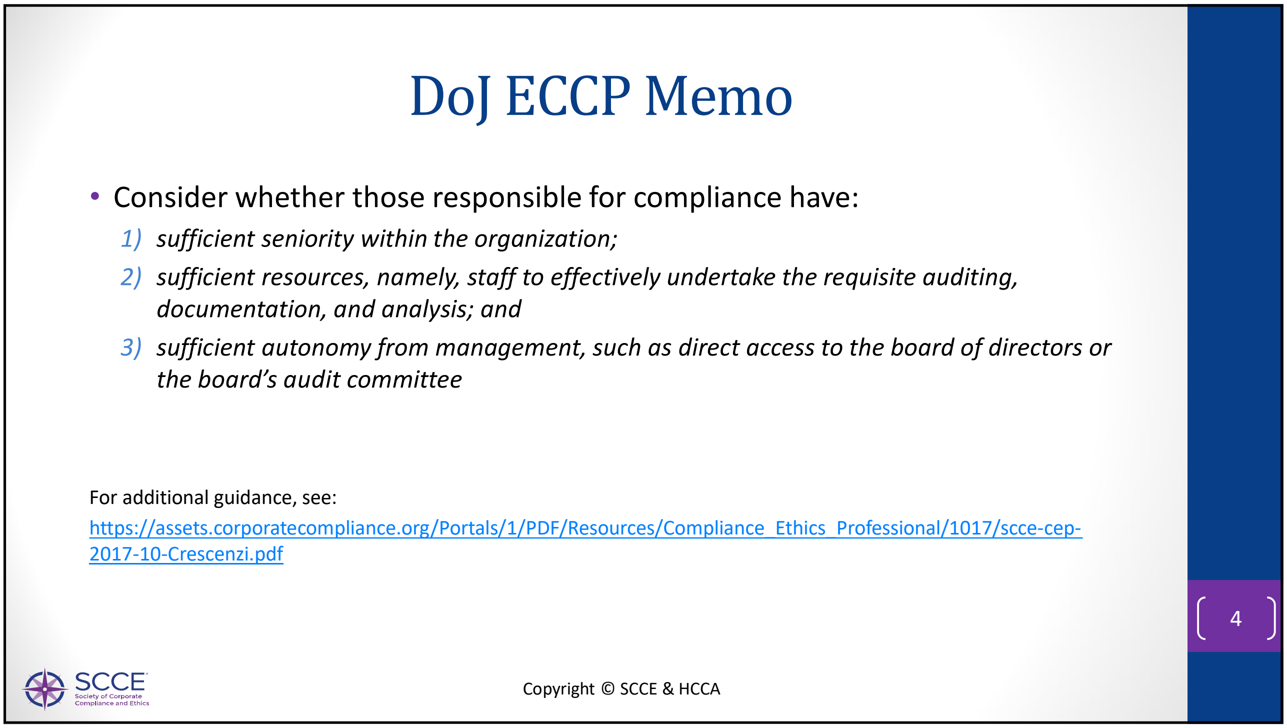
- These drivers include, but are not limited to, the following:
  - 1991 - U.S. Federal Sentencing Guidelines for Organizational Defendants (and amendments)
  - 1992 - COSO Internal Control Framework (and amendments)
  - 1996 - *In Re*. Caremark Decision
  - 1999 - Department of Justice Enforcement Guidance (Holder Memo)
  - 2012 – DOJ and SEC Resource Guide to the FCPA
  - 2019 – DOJ Memo re Evaluation of Corporate Compliance Programs
  - 2019 – *Marchand v. Barnhill*
  - 2021 – *In re Boeing*

Board

Senior Leadership Oversight

Compliance Leadership

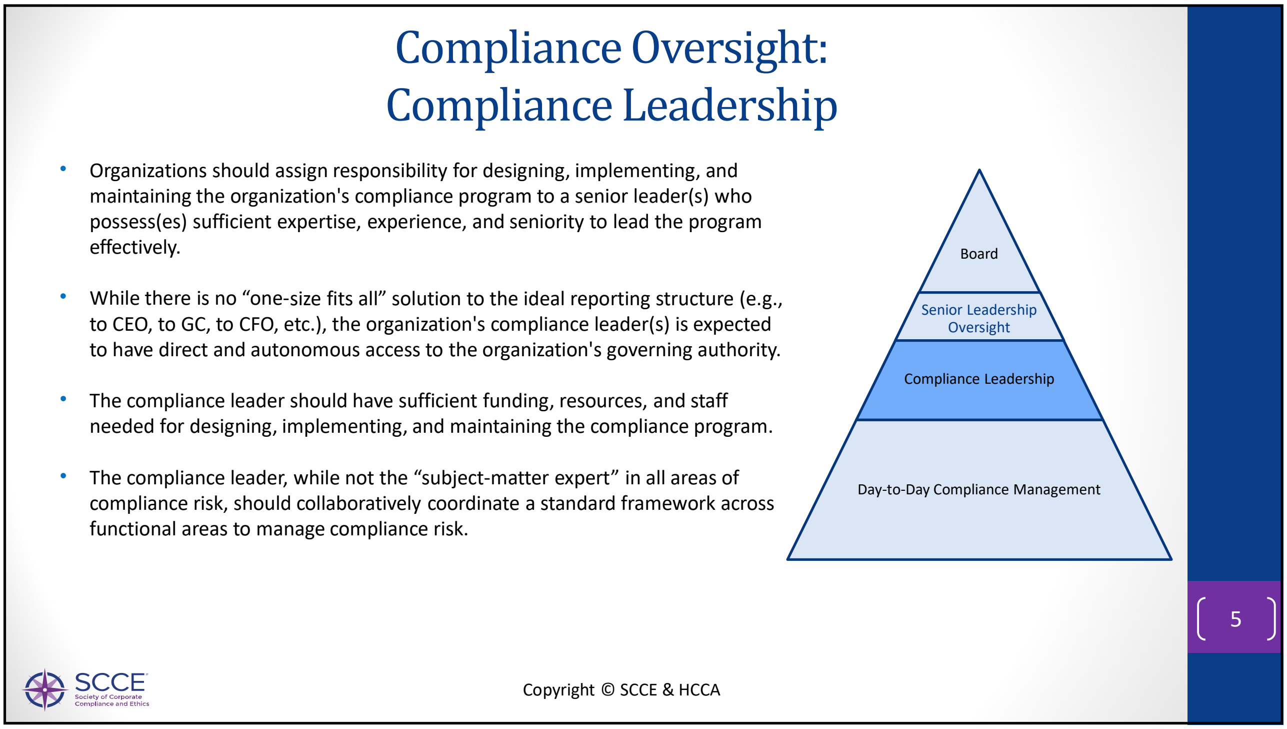
Day-to-Day Compliance Management



DoJ ECCP Memo

- Consider whether those responsible for compliance have:
  1) *sufficient seniority within the organization;*
  2) *sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and*
  3) *sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee*

For additional guidance, see: https://assets.corporatecompliance.org/Portals/1/PDF/Resources/Compliance_Ethics_Professional/1017/scce-cep-2017-10-Crescenzi.pdf



Compliance Oversight: Compliance Leadership

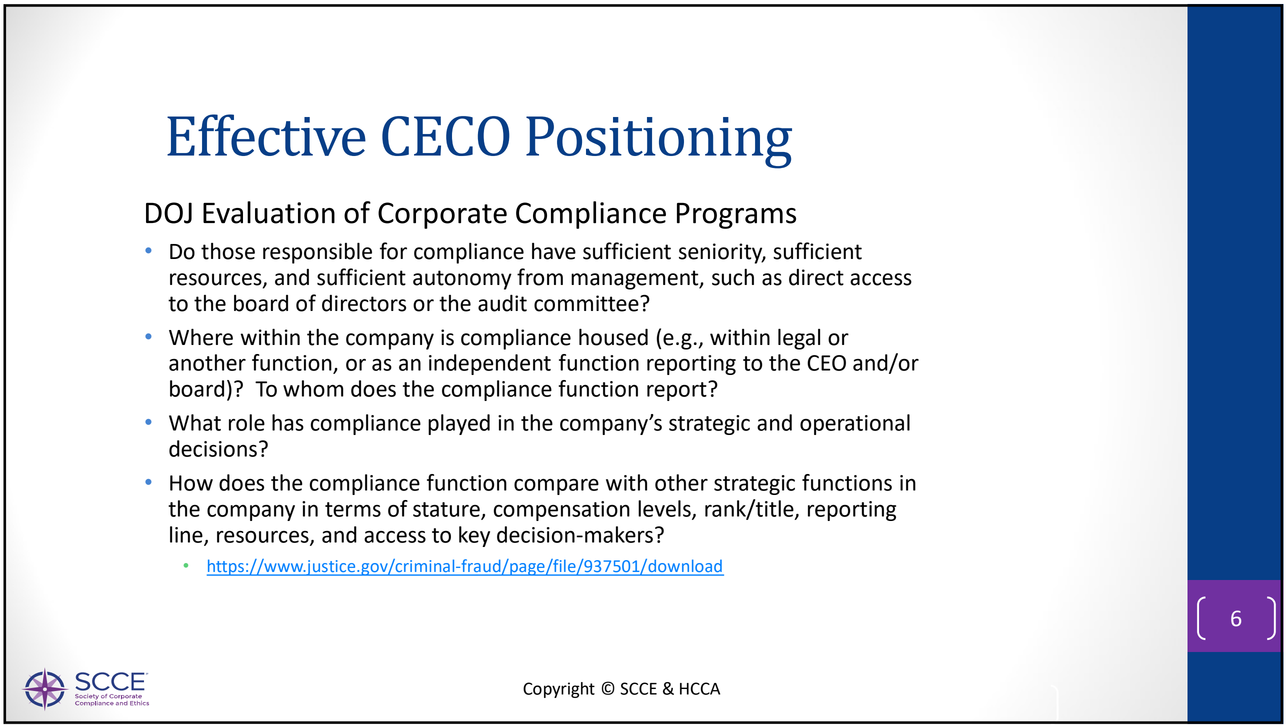
- Organizations should assign responsibility for designing, implementing, and maintaining the organization's compliance program to a senior leader(s) who possess(es) sufficient expertise, experience, and seniority to lead the program effectively.
- While there is no “one-size fits all” solution to the ideal reporting structure (e.g., to CEO, to GC, to CFO, etc.), the organization's compliance leader(s) is expected to have direct and autonomous access to the organization's governing authority.
- The compliance leader should have sufficient funding, resources, and staff needed for designing, implementing, and maintaining the compliance program.
- The compliance leader, while not the “subject-matter expert” in all areas of compliance risk, should collaboratively coordinate a standard framework across functional areas to manage compliance risk.

Board

Senior Leadership Oversight

Compliance Leadership

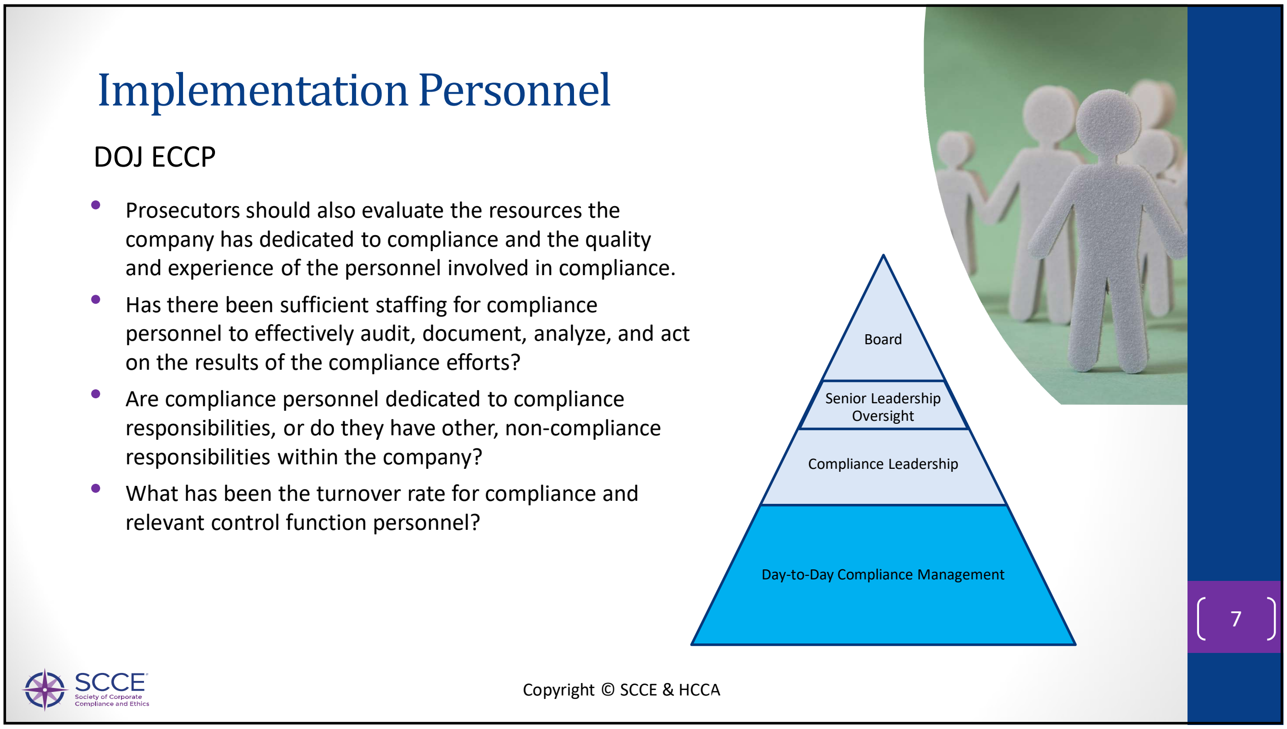
Day-to-Day Compliance Management



Effective CECO Positioning

DOJ Evaluation of Corporate Compliance Programs

- Do those responsible for compliance have sufficient seniority, sufficient resources, and sufficient autonomy from management, such as direct access to the board of directors or the audit committee?
- Where within the company is compliance housed (e.g., within legal or another function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report?
- What role has compliance played in the company’s strategic and operational decisions?
- How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers?
  - https://www.justice.gov/criminal-fraud/page/file/937501/download



Implementation Personnel

DOJ ECCP

- Prosecutors should also evaluate the resources the company has dedicated to compliance and the quality and experience of the personnel involved in compliance.
- Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts?
- Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company?
- What has been the turnover rate for compliance and relevant control function personnel?

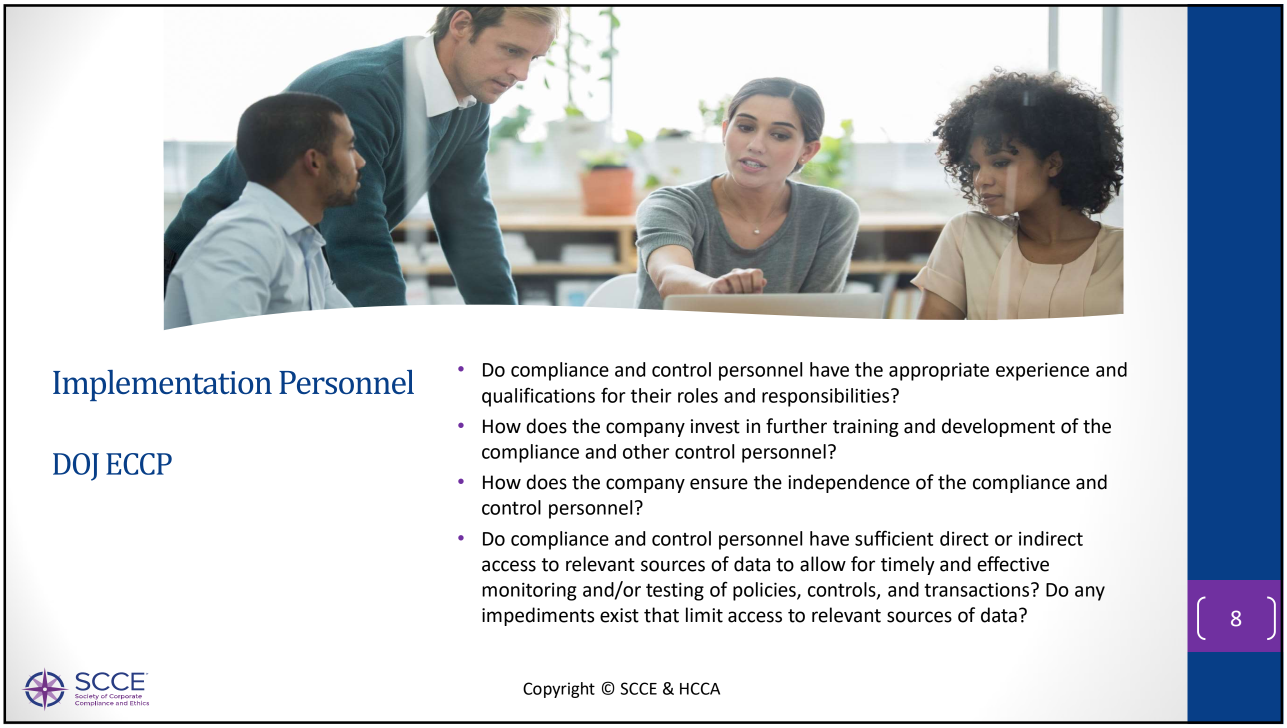
Board

Senior Leadership Oversight

Compliance Leadership

Day-to-Day Compliance Management

SCCE Society of Corporate Compliance and Ethics



Implementation Personnel

DOJ ECCP

- Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities?
- How does the company invest in further training and development of the compliance and other control personnel?
- How does the company ensure the independence of the compliance and control personnel?
- Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data?

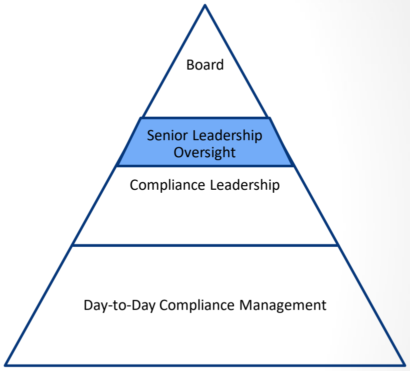
SCCE Society of Corporate Compliance and Ethics

Compliance Oversight: Senior Leadership

The Sentencing Guidelines provide that high-level personnel of the organization "shall ensure that the organization has an effective compliance and ethics program."

ECCP questions regarding leadership oversight of the compliance program:

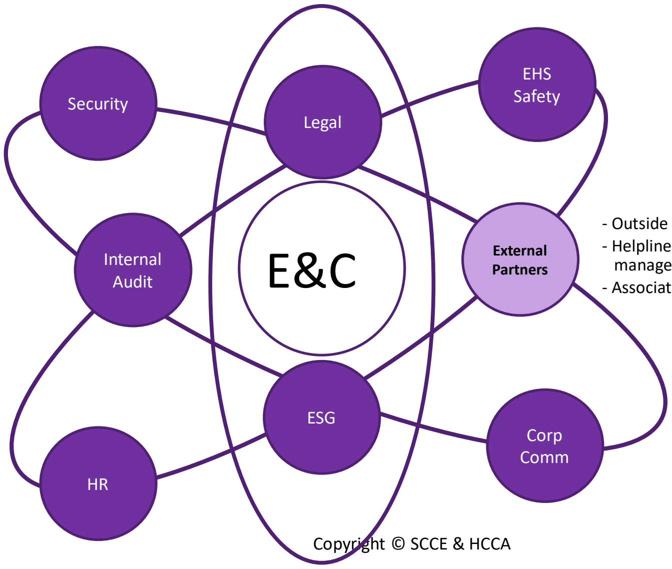
- How have senior leaders, through their words and actions, encouraged or discouraged compliance?
- Have managers tolerated greater compliance risks in pursuit of new business or greater revenues?
- Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?
- What actions have senior leaders and middle-management stakeholders taken to demonstrate their commitment to compliance or compliance personnel?



Senior Leadership Oversight

- Executive officers – like directors – have a fiduciary duty to oversee the organization's compliance and ethics program.
- In re McDonald's Corp. (Del 2023)
  - "This decision clarifies that corporate officers owe a duty of oversight. The same policies that motivated Chancellor Allen to recognize the duty of oversight for directors apply equally, if not to a greater degree, to officers. The Delaware Supreme Court has held that under Delaware law, corporate officers owe the same fiduciary duties as corporate directors, which logically include a duty of oversight. Academic authorities and federal decisions have concluded that officers have a duty of oversight."

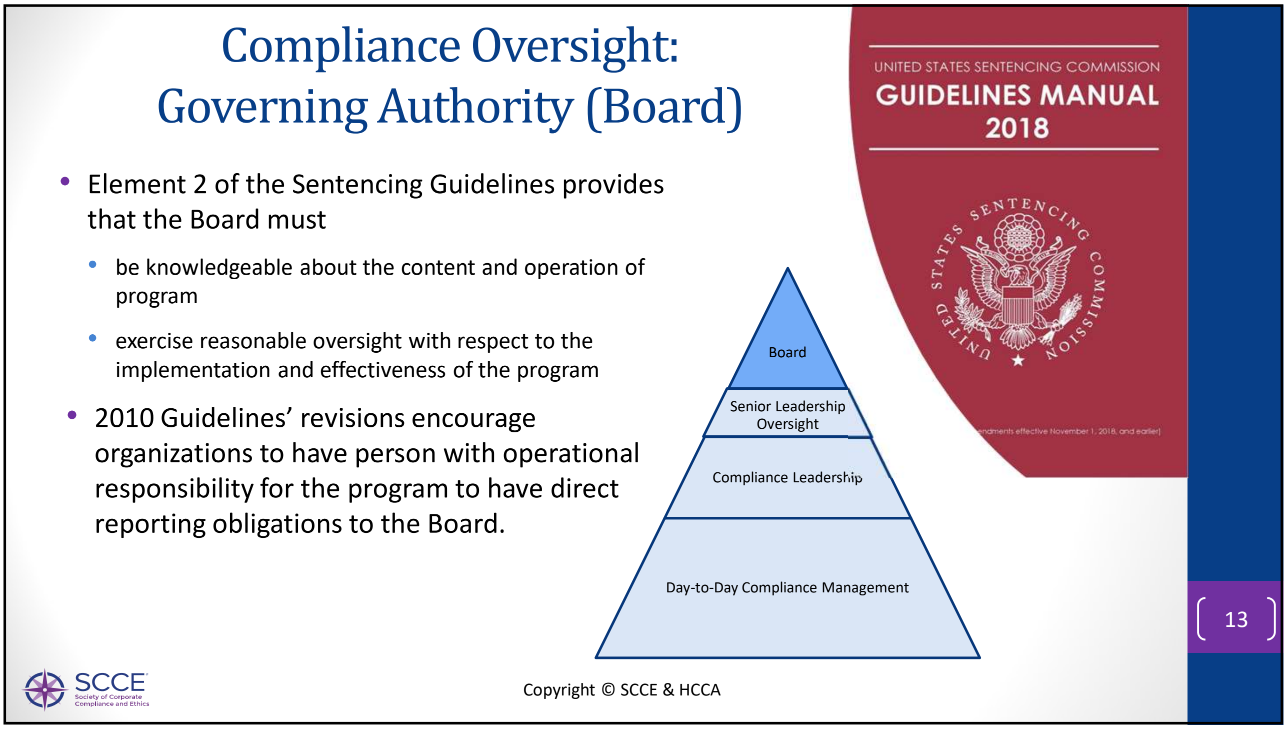
Leveraging Relationship with Other Functions



- Outside Counsel
- Helpline, training, risk management vendors
- Associations & networks

Management Oversight: Compliance Committees

- OIG General Compliance Program Guidance (Oct 2023)
  - The Compliance Committee's purpose is to aid and support the compliance officer in implementing, operating, and monitoring the Compliance Program. The Compliance Committee should meet no less than quarterly. Having a regularly scheduled meeting may enhance routine attendance.
  - According to OIG Guidance, primary duties of the Committee should include:
    - analyzing the legal and regulatory requirements applicable to the entity
    - assessing, developing, and regularly reviewing policies and procedures
    - monitoring and recommending internal systems and controls
    - assessing education and training needs and effectiveness, and regularly reviewing required training
    - developing a disclosure program and promoting compliance reporting
    - assessing effectiveness of the disclosure program and other reporting mechanisms
    - conducting annual risk assessments
    - developing the compliance workplan
    - evaluating the effectiveness of the compliance workplan and any action plans for risk remediation
    - evaluating the effectiveness of the compliance program.



Compliance Oversight: Governing Authority (Board)

- Element 2 of the Sentencing Guidelines provides that the Board must
  - be knowledgeable about the content and operation of program
  - exercise reasonable oversight with respect to the implementation and effectiveness of the program
- 2010 Guidelines’ revisions encourage organizations to have person with operational responsibility for the program to have direct reporting obligations to the Board.

UNITED STATES SENTENCING COMMISSION
GUIDELINES MANUAL
2018

UNITED STATES SENTENCING COMMISSION

endments effective November 1, 2018, and earlier)

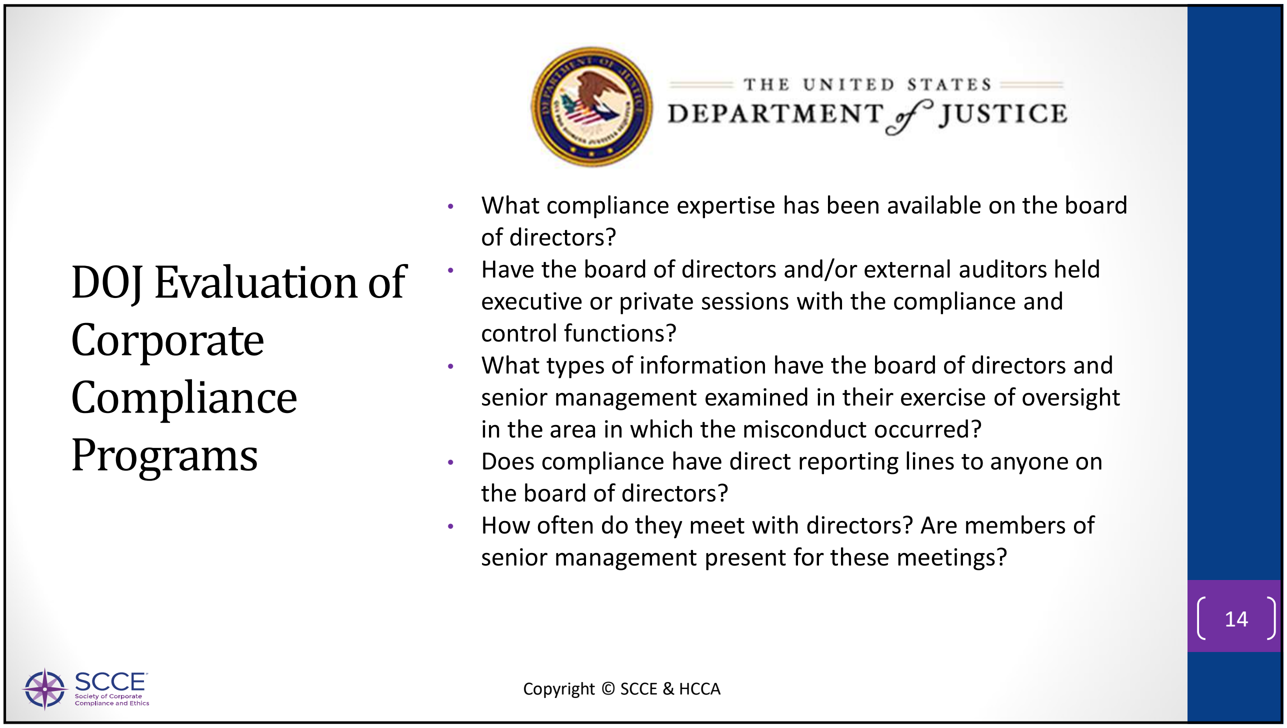
Board

Senior Leadership Oversight

Compliance Leadership

Day-to-Day Compliance Management

SCCE Society of Corporate Compliance and Ethics

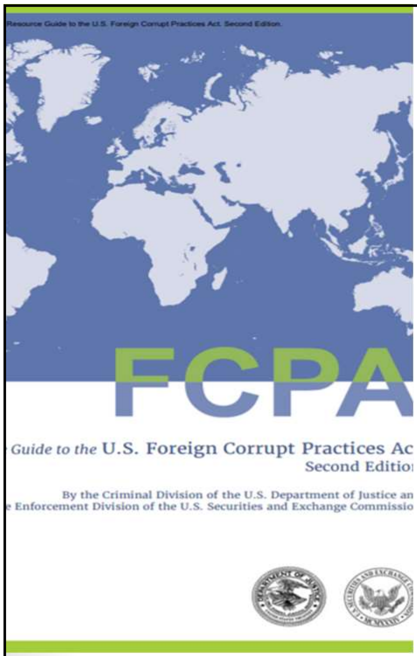


THE UNITED STATES DEPARTMENT of JUSTICE

DOJ Evaluation of Corporate Compliance Programs

- What compliance expertise has been available on the board of directors?
- Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions?
- What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?
- Does compliance have direct reporting lines to anyone on the board of directors?
- How often do they meet with directors? Are members of senior management present for these meetings?

SCCE Society of Corporate Compliance and Ethics



Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition.

FCPA

Guide to the U.S. Foreign Corrupt Practices Ac
Second Editio

By the Criminal Division of the U.S. Department of Justice an
e Enforcement Division of the U.S. Securities and Exchange Commissio

DOJ & SEC Resource Guide to the FCPA

- Within a business organization, compliance begins with the board of directors and senior executives setting the proper tone for the rest of the company.
- DOJ and SEC consider the commitment of corporate leaders to a “culture of compliance.”
- Adequate autonomy generally includes direct access to an organization’s governing authority, such as the board of directors and committees of the board of directors (e.g., the audit committee).
- A compliance program should apply from the board room to the supply room—no one should be beyond its reach. DOJ and SEC will thus consider whether, when enforcing a compliance program, a company has appropriate and clear disciplinary procedures, whether those procedures are applied reliably and promptly, and whether they are commensurate with the violation.

SCCE Society of Corporate Compliance and Ethics

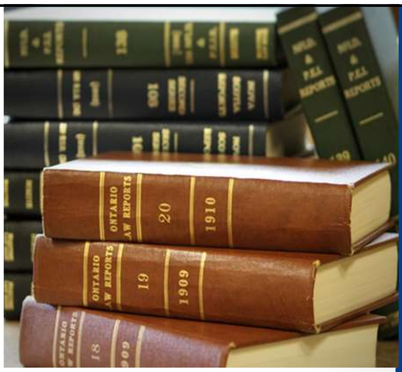
Delaware Case Law

- 1996: In re Caremark International Derivative Litigation (Del Chancery Court)
  - “Thus, I am of the view that a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.”
- The standard for liability is high.
- 2006: Stone v. Ritter

SCCE Society of Corporate Compliance and Ethics

Delaware Case Law

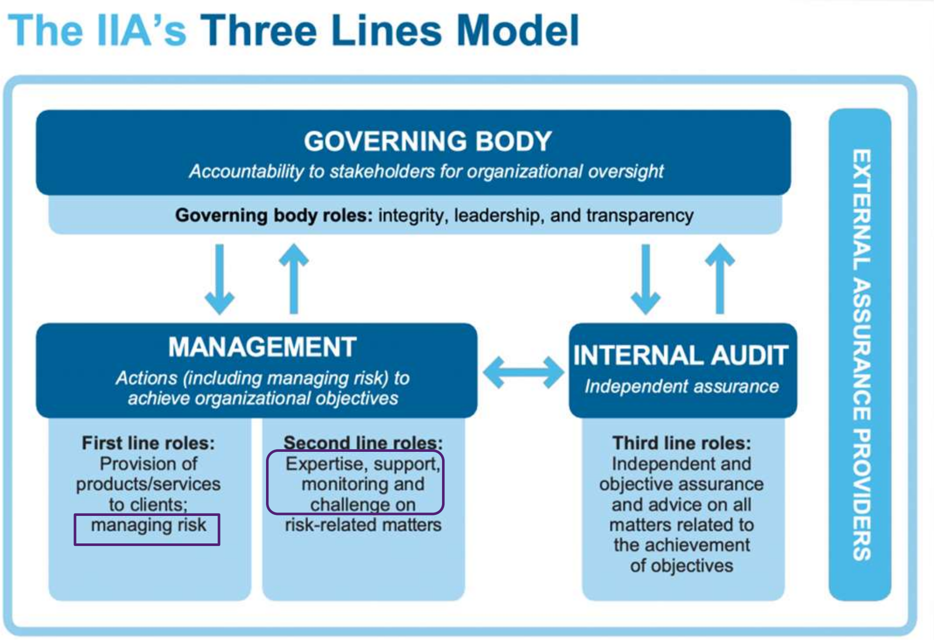
- *Marchand v. Barnhill* 212 A.3d 805 (Del. Supreme Court June 2019)
  - Importance of monitoring and oversight
    - In critical risk areas
    - Re reporting and investigations
- *In re Clovis Oncology* (Del. Chancery Court October 2019)
  - Systems to monitor for red flags
  - Oversight in highly-regulated areas
- *In re Boeing* (Del. Chancery Court September 2021) https://courts.delaware.gov/Opinions/Download.aspx?id=324120
  - *Caremark*'s bottom-line requirement: "the board must make a good faith effort—i.e., try—to put in place a reasonable board-level system of monitoring and reporting."



17

17

As compared to the IIA Three Lines Model



The IIA's Three Lines Model

GOVERNING BODY

Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT

Actions (including managing risk) to achieve organizational objectives

INTERNAL AUDIT

Independent assurance

First line roles: Provision of products/services to clients; managing risk

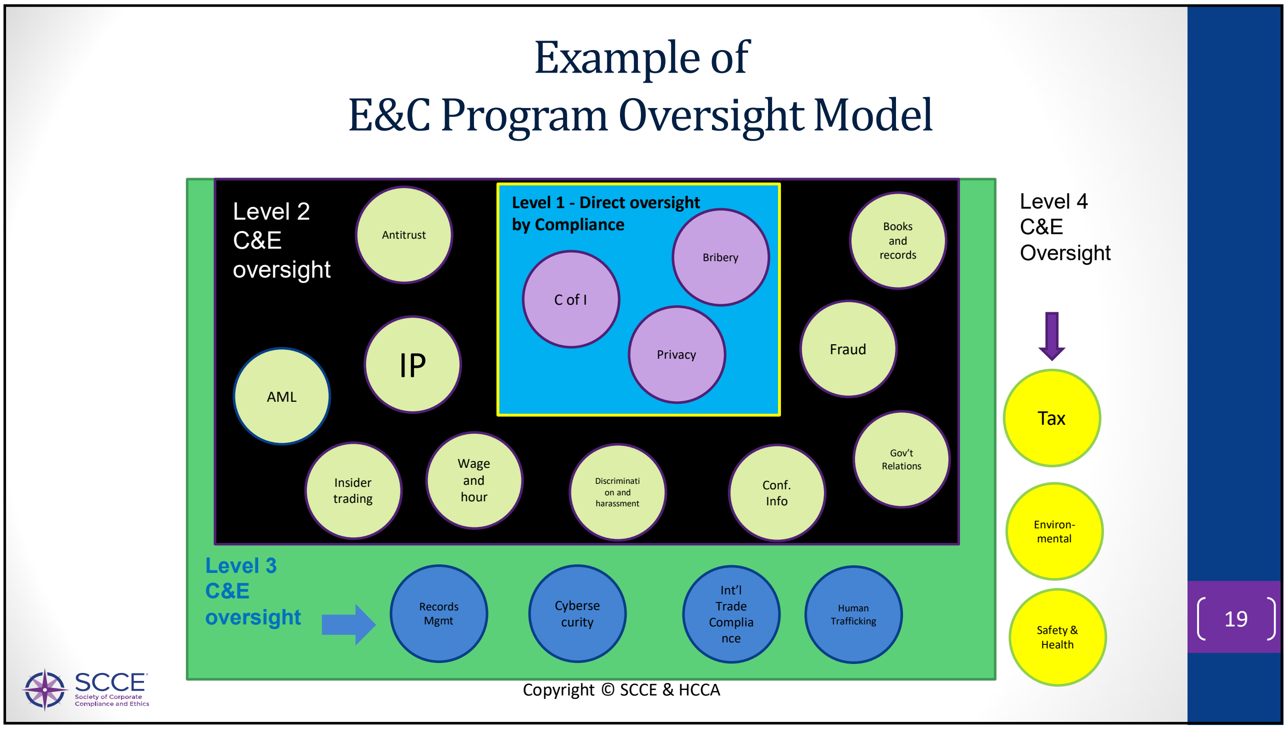
Second line roles: Expertise, support, monitoring and challenge on risk-related matters

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

18

18



Example of
E&C Program Oversight Model

Level 2
C&E
oversight

Antitrust

IP

AML

Insider trading

Wage and hour

Discrimination and harassment

Conf. Info

Gov't Relations

Fraud

Books and records

Level 1 - Direct oversight by Compliance

C of I

Bribery

Privacy

Level 3
C&E
oversight

Records Mgmt

Cyberse curity

Int'l Trade Complia nce

Human Trafficking

Level 4
C&E
Oversight

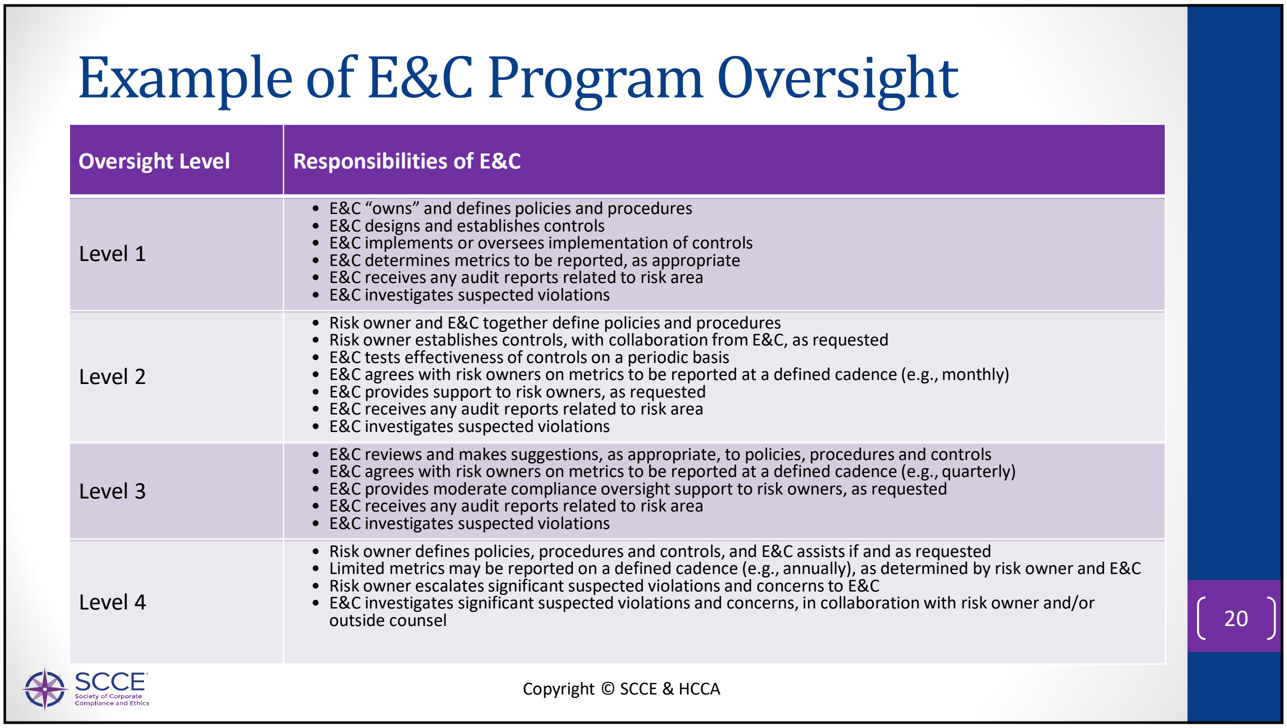
Tax

Environ-mental

Safety & Health

Copyright © SCCE & HCCA

19

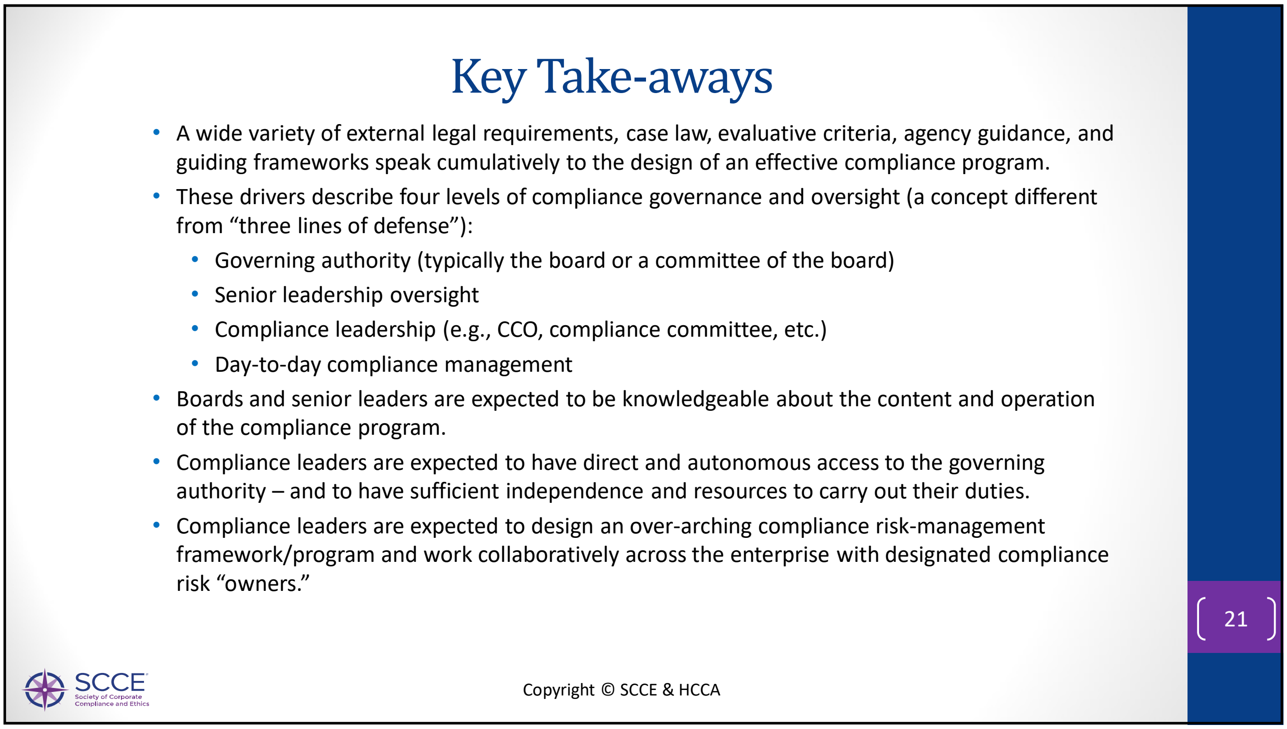


Example of E&C Program Oversight

Oversight Level	Responsibilities of E&C
Level 1	• E&C “owns” and defines policies and procedures • E&C designs and establishes controls • E&C implements or oversees implementation of controls • E&C determines metrics to be reported, as appropriate • E&C receives any audit reports related to risk area • E&C investigates suspected violations
Level 2	• Risk owner and E&C together define policies and procedures • Risk owner establishes controls, with collaboration from E&C, as requested • E&C tests effectiveness of controls on a periodic basis • E&C agrees with risk owners on metrics to be reported at a defined cadence (e.g., monthly) • E&C provides support to risk owners, as requested • E&C receives any audit reports related to risk area • E&C investigates suspected violations
Level 3	• E&C reviews and makes suggestions, as appropriate, to policies, procedures and controls • E&C agrees with risk owners on metrics to be reported at a defined cadence (e.g., quarterly) • E&C provides moderate compliance oversight support to risk owners, as requested • E&C receives any audit reports related to risk area • E&C investigates suspected violations
Level 4	• Risk owner defines policies, procedures and controls, and E&C assists if and as requested • Limited metrics may be reported on a defined cadence (e.g., annually), as determined by risk owner and E&C • Risk owner escalates significant suspected violations and concerns to E&C • E&C investigates significant suspected violations and concerns, in collaboration with risk owner and/or outside counsel

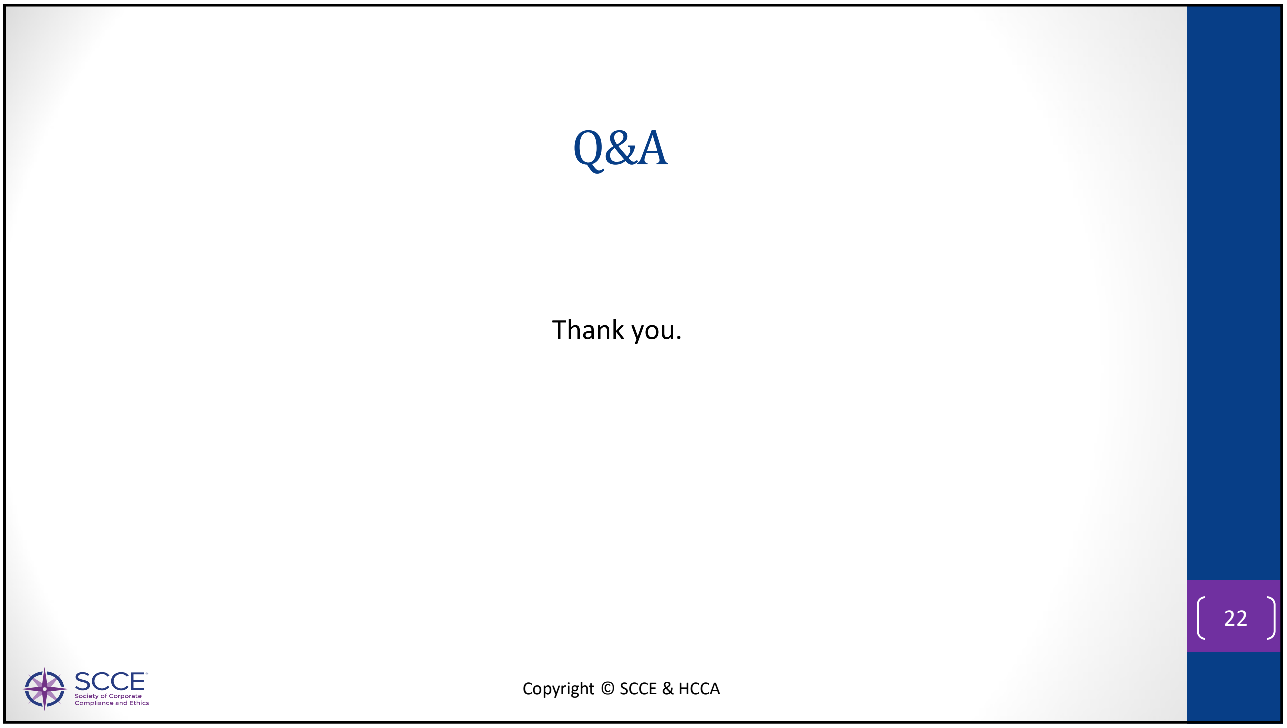
Copyright © SCCE & HCCA

20



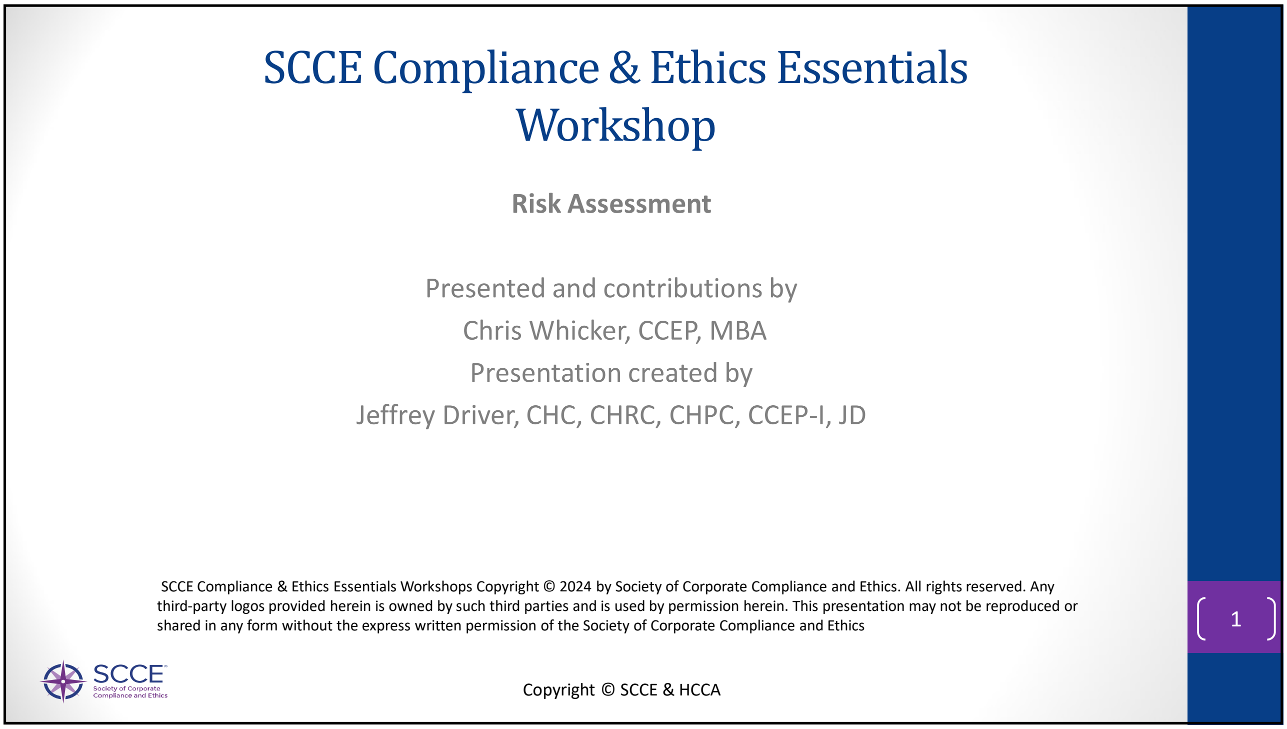
Key Take-aways

- A wide variety of external legal requirements, case law, evaluative criteria, agency guidance, and guiding frameworks speak cumulatively to the design of an effective compliance program.
- These drivers describe four levels of compliance governance and oversight (a concept different from “three lines of defense”):
  - Governing authority (typically the board or a committee of the board)
  - Senior leadership oversight
  - Compliance leadership (e.g., CCO, compliance committee, etc.)
  - Day-to-day compliance management
- Boards and senior leaders are expected to be knowledgeable about the content and operation of the compliance program.
- Compliance leaders are expected to have direct and autonomous access to the governing authority – and to have sufficient independence and resources to carry out their duties.
- Compliance leaders are expected to design an over-arching compliance risk-management framework/program and work collaboratively across the enterprise with designated compliance risk “owners.”



Q&A

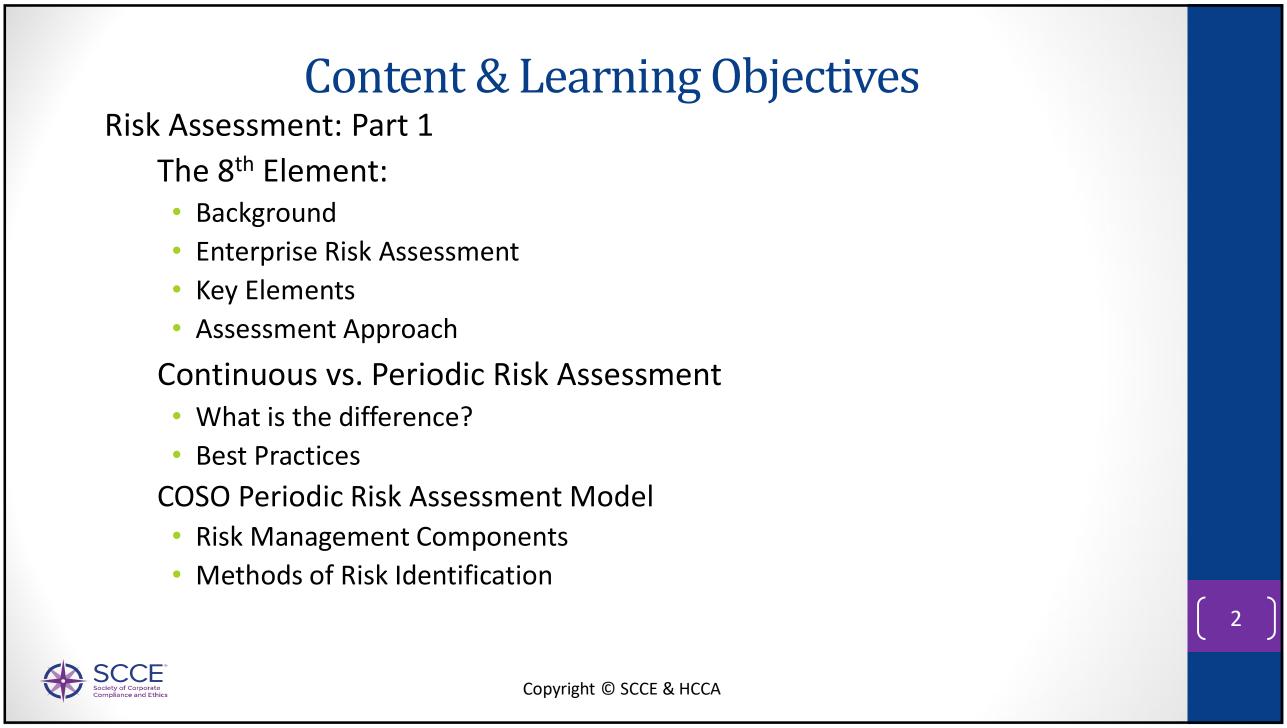
Thank you.



SCCE Compliance & Ethics Essentials Workshop

Risk Assessment

Presented and contributions by
Chris Whicker, CCEP, MBA
Presentation created by
Jeffrey Driver, CHC, CHRC, CHPC, CCEP-I, JD



Content & Learning Objectives

Risk Assessment: Part 1

The 8th Element:

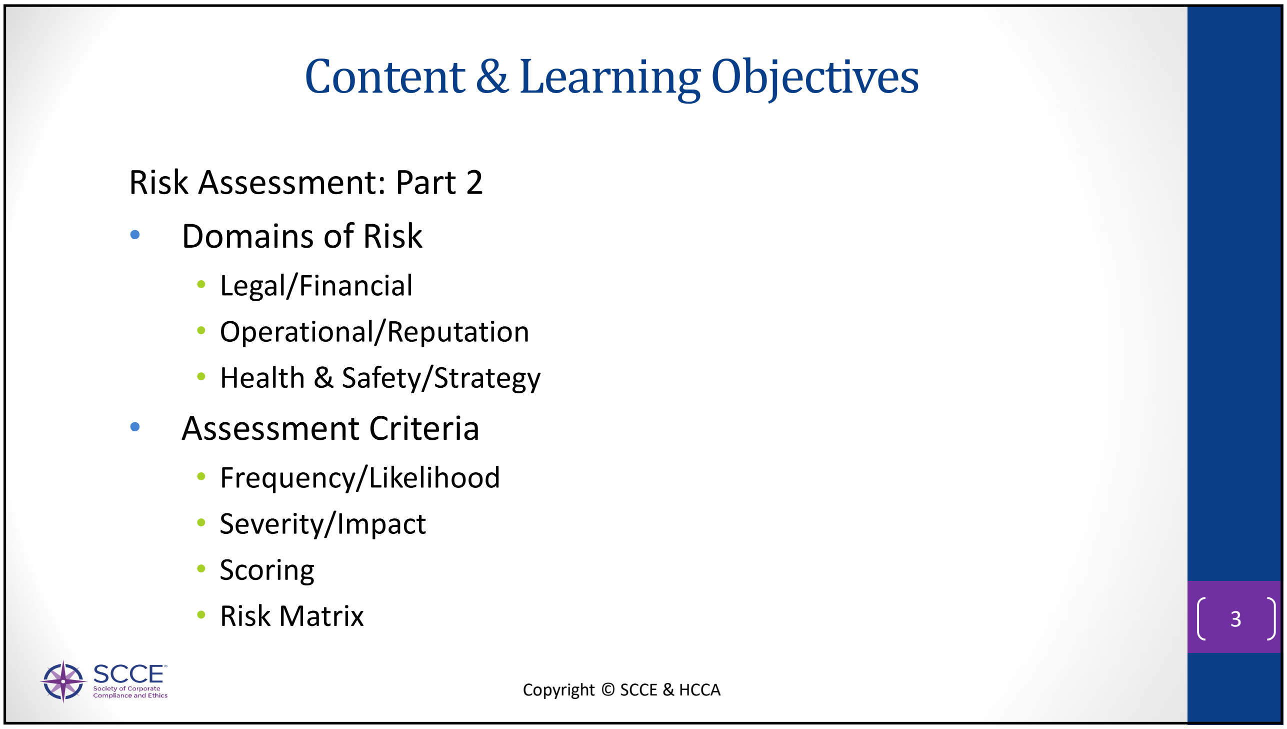
- Background
- Enterprise Risk Assessment
- Key Elements
- Assessment Approach

Continuous vs. Periodic Risk Assessment

- What is the difference?
- Best Practices

COSO Periodic Risk Assessment Model

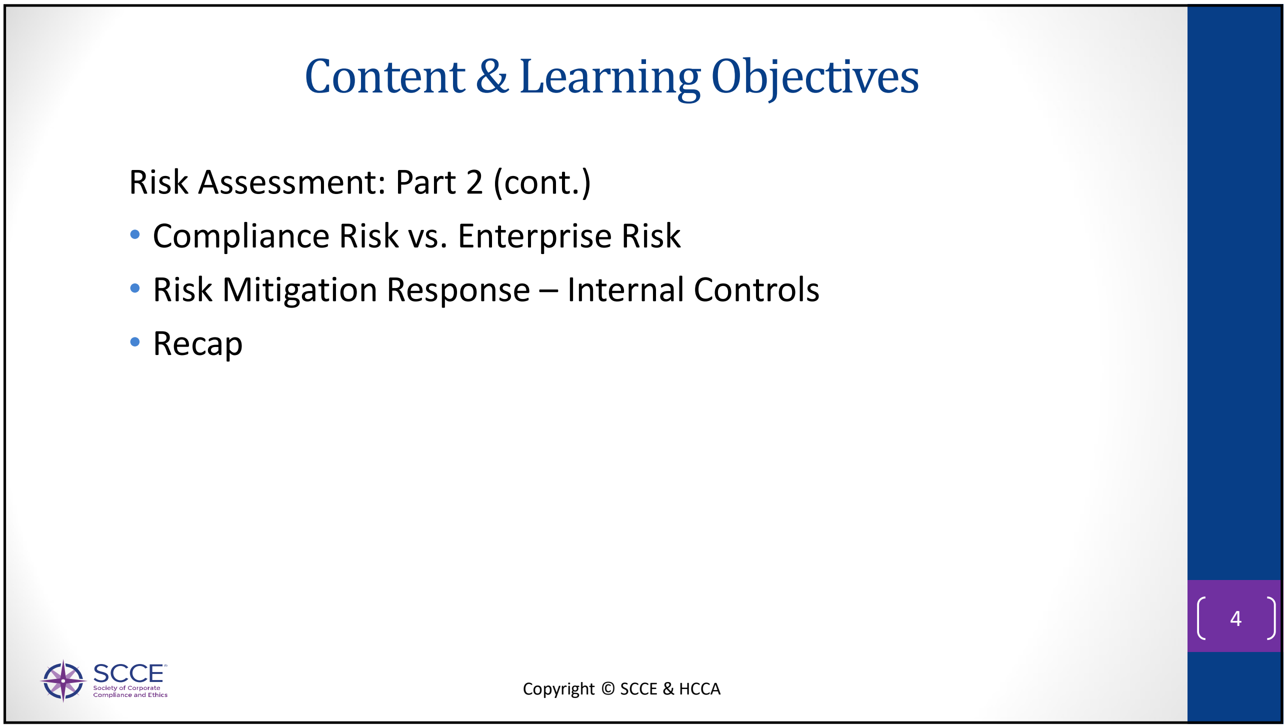
- Risk Management Components
- Methods of Risk Identification



Content & Learning Objectives

Risk Assessment: Part 2

- Domains of Risk
  - Legal/Financial
  - Operational/Reputation
  - Health & Safety/Strategy
- Assessment Criteria
  - Frequency/Likelihood
  - Severity/Impact
  - Scoring
  - Risk Matrix



Content & Learning Objectives

Risk Assessment: Part 2 (cont.)

- Compliance Risk vs. Enterprise Risk
- Risk Mitigation Response – Internal Controls
- Recap

7 Elements of an Effective Compliance & Ethics Program

These 7 elements are identified in the US Sentencing Guidelines as essential to an effective compliance and ethics program. Use them as a road map to establishing and maintaining compliance and ethics at your organization.

01 Standards of conduct, policies, and procedures — Put these policies in writing and use them as the foundation for your entire program.

02 Compliance officer and committee — Delegate an individual or group with operational responsibility, autonomy, and authority.

03 Communication and education — Create effective, ongoing training methods and establish open lines of communication.

04 Internal monitoring and auditing — Use internal tools to evaluate program effectiveness and detect criminal conduct.

05 Reporting and investigating — Encourage employees to raise concerns and have investigative procedures in place.

06 Enforcement and discipline — Establish appropriate incentives for compliance and disciplinary actions for violations.

07 Response and prevention — Resolve identified problems promptly and add related issues to monitoring activities.

Learn more about the 7 elements of compliance and more in SCCE's *Compliance 101, second edition*. Order online at corporatecompliance.org/books

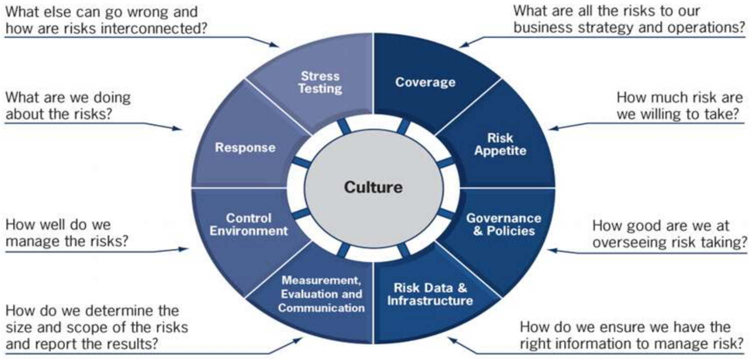
The Eighth Element: Risk Assessment

- Not included in 7 Elements of an Effective Compliance and Ethics Program
- Referenced in Chapter 8 of 2004 Federal Sentencing Guidelines Manual as part of guidance for an Effective Compliance and Ethics Program
- Chapter 8, Sec. 8B2. 1(c), pg. 477.
  - *In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process*
- Risk Assessments should be performed by organizations that have a mission, strategy, objectives and make decisions based on risk

  Benefits
  - Evaluates impact of external/internal events, specific to domains of risk
  - Allows management to put practices in place to manage risks going forward
  - Integrates risk in the culture and in the execution of strategy
  - Principles apply to all levels of the organization and all functions
  - Enhances monitoring and fosters continuous improvement
- Federal Sentencing Guidelines state that an organization should periodically assess risk of criminal conduct and should take the appropriate steps to design, implement, or modify requirements to reduce this risk

Enterprise Risk Management

WHAT IS ERM? **It is the capability to effectively answer the following quesions:**


What else can go wrong and how are risks interconnected?
What are all the risks to our business strategy and operations?
Stress Testing
Coverage
What are we doing about the risks?
How much risk are we willing to take?
Response
Risk Appetite
Culture
Control Environment
Governance & Policies
How well do we manage the risks?
How good are we at overseeing risk taking?
Measurement, Evaluation and Communication
Risk Data & Infrastructure
How do we determine the size and scope of the risks and report the results?
How do we ensure we have the right information to manage risk?

- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

https://www.coso.org/_files/ugd/3059fc_ae81f45d98474c9188045cbacbd510bf.pdf

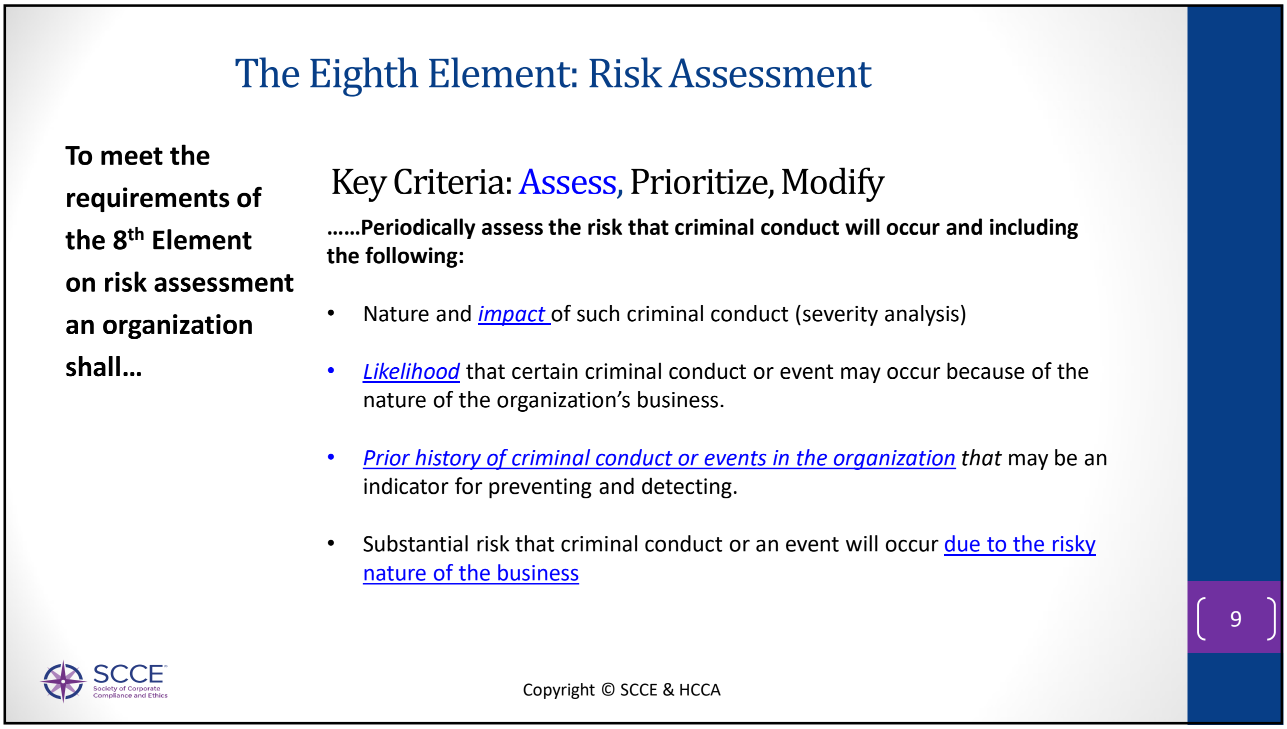
SCC Society of Co Compliance a

The Eighth Element: Risk Assessment

Key Elements

- Concise and easy to follow methodology
- Comprehensive coverage across all functions
- Appropriately defined thresholds
- Established risk domains
- Regular cadence for both continuous and periodic assessments
- Consistent and applicable method for identifying risk
- Includes Risk Criteria/Risk Scoring/Risk Matrix
- Incorporates response to risk assessment that evaluates 7 elements

SCCE Society of Corporate Compliance and Ethics



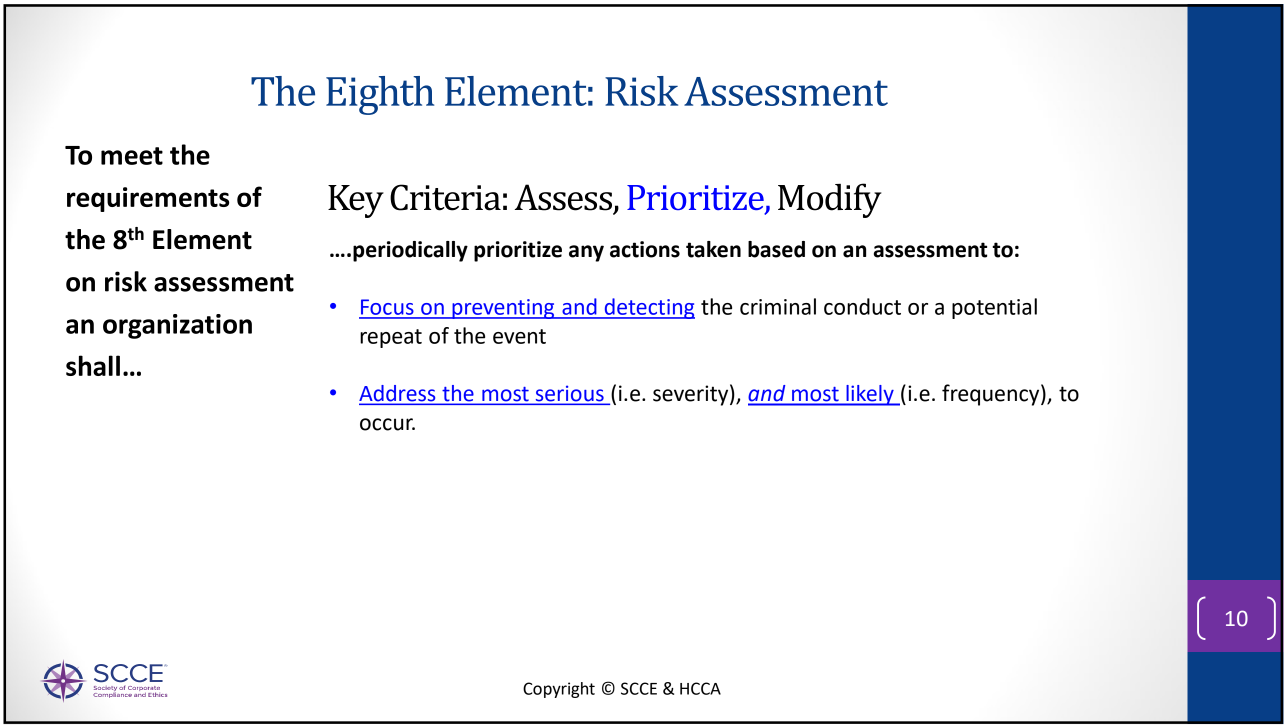
The Eighth Element: Risk Assessment

To meet the requirements of the 8th Element on risk assessment an organization shall…

Key Criteria: Assess, Prioritize, Modify

……Periodically assess the risk that criminal conduct will occur and including the following:

- Nature and *impact* of such criminal conduct (severity analysis)
- *Likelihood* that certain criminal conduct or event may occur because of the nature of the organization's business.
- *Prior history of criminal conduct or events in the organization that* may be an indicator for preventing and detecting.
- Substantial risk that criminal conduct or an event will occur due to the risky nature of the business



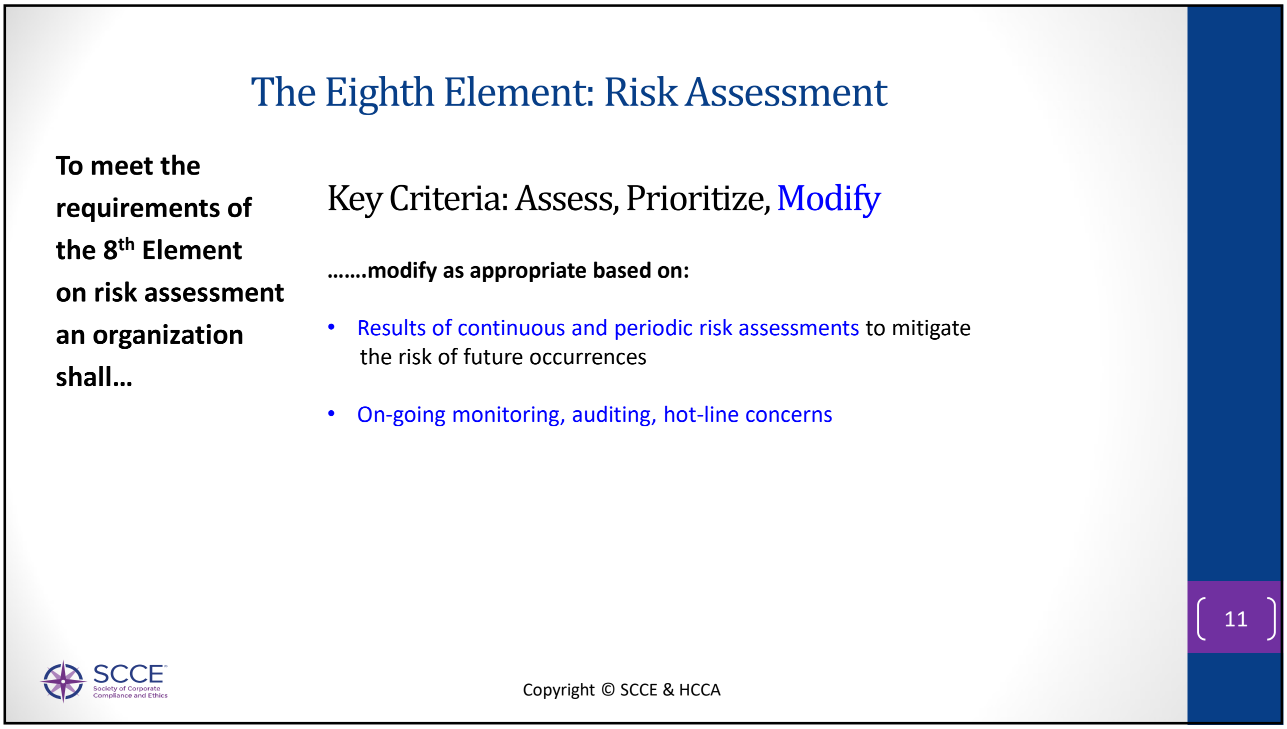
The Eighth Element: Risk Assessment

To meet the requirements of the 8th Element on risk assessment an organization shall…

Key Criteria: Assess, Prioritize, Modify

….periodically prioritize any actions taken based on an assessment to:

- Focus on preventing and detecting the criminal conduct or a potential repeat of the event
- Address the most serious (i.e. severity), *and* most likely (i.e. frequency), to occur.



The Eighth Element: Risk Assessment

To meet the requirements of the 8th Element on risk assessment an organization shall…

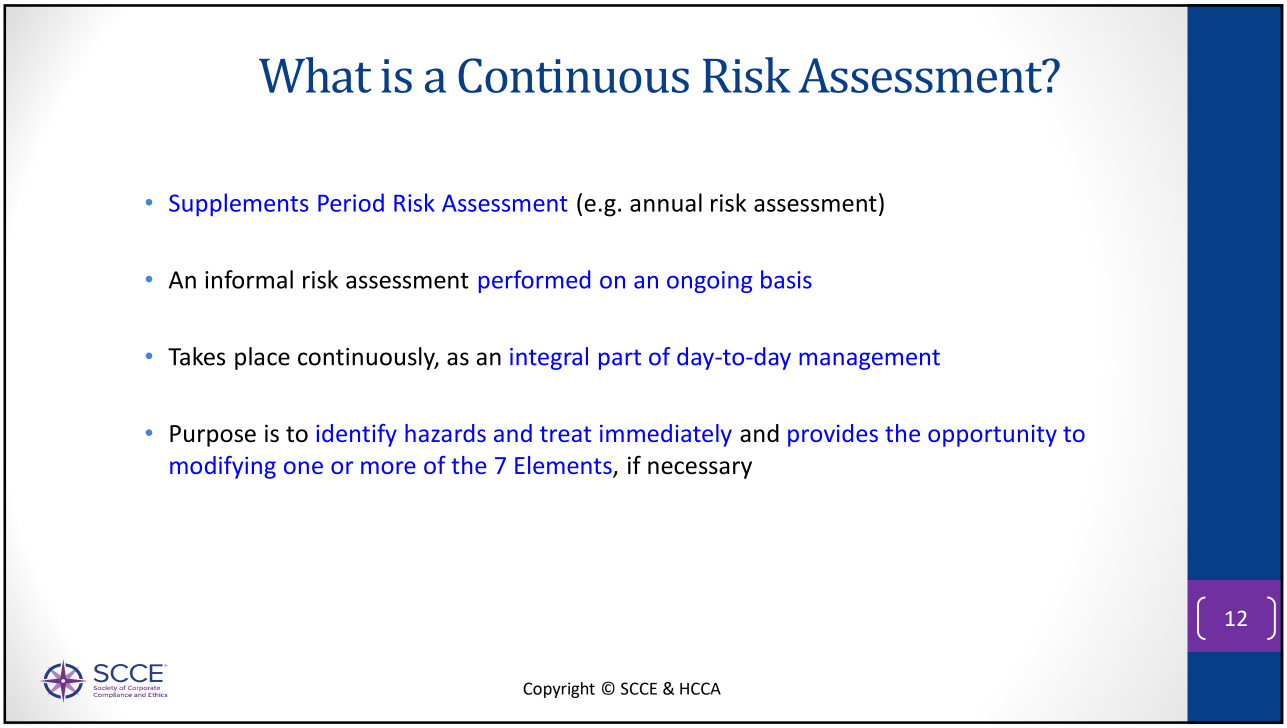
Key Criteria: Assess, Prioritize, Modify

…….modify as appropriate based on:

- Results of continuous and periodic risk assessments to mitigate the risk of future occurrences
- On-going monitoring, auditing, hot-line concerns

11

11



What is a Continuous Risk Assessment?

- Supplements Period Risk Assessment (e.g. annual risk assessment)
- An informal risk assessment performed on an ongoing basis
- Takes place continuously, as an integral part of day-to-day management
- Purpose is to identify hazards and treat immediately and provides the opportunity to modifying one or more of the 7 Elements, if necessary

12

12

Characteristics of a Continuous Risk Assessment

- Should not be complicated but should have some level of formality to differentiate between continuous and periodic risk assessment policies and procedures
- Should create compliance awareness through risk identification (e.g., hot-lines, monitoring, concurrent auditing)
- Should encourage employees and supervisors to observe what is happening in the workplace. This results in first-hand risk observations and provides an opportunity to engage compliance management upfront
- Should assist with identifying and registering possible risks immediately via checklists, documented procedures, or steps

Adopting or Designing A Model for The Periodic Risk Assessment: COSO

COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK

By

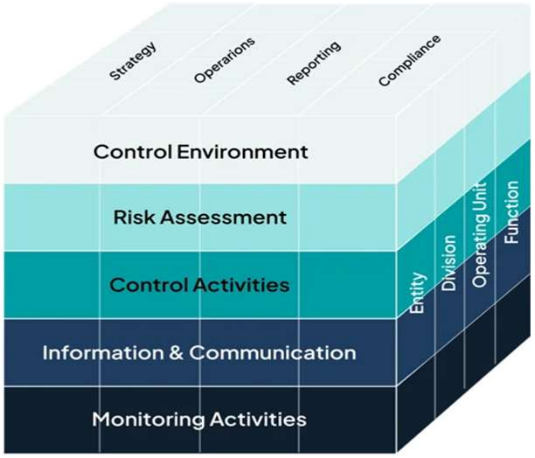
SCCE HCCA

November 11, 2020

COSO releases new guidance, *Compliance Risk Management: Applying the COSO ERM Framework*, detailing the application of the *Enterprise Risk Management—Integrating with Strategy and Performance* (ERM Framework) to the management of compliance risks. The guidance was commissioned by COSO and authored by the Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA).

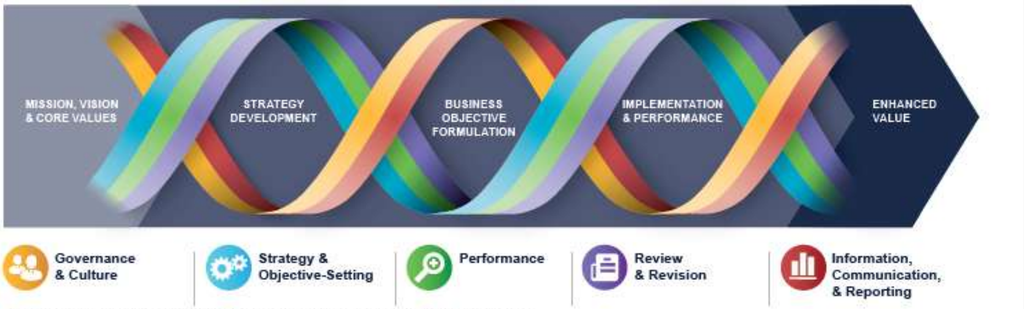
See: https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

Adopting or Designing A Model for The Periodic Risk Assessment: The COSO Internal Control Framework



COSO cube

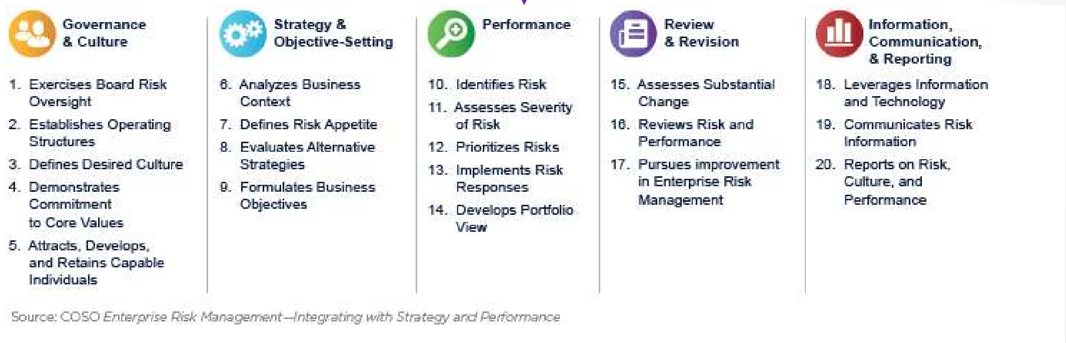
Adopting or Designing A Model for The Periodic Risk Assessment: The Risk Management Components


MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance*

Adopting or Designing A Model for The Periodic Risk Assessment: Principles of Risk Assessment

We will focus on



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance*

Risk Identification Methodology

Key characteristics

- Documented policies and procedures that describe the risk assessment process
- Comprehensive list of Identified risks associated with business strategy and objectives
- Risks identified based on internal and external environments
- Process for identifying new or emerging risks
- Process for identifying risks associated with using third parties
- Includes information gathered through hotlines, other reporting channels, and results of investigations/events

Methods of Risk Identification

Types of Risk	Cognitive Computing	Data Tracking	Interviews	Key Indicators	Process Analysis	Workshops
Existing	●	●	●	●	●	●
New	●	●			●	●
Emerging	●		●	●		●

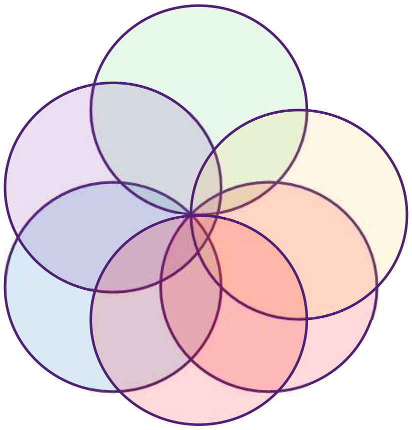
Source: COSO Enterprise Risk Management - Integrating with Strategy and Performance, Volume 1, p. 69

Methods of Risk Identification: Domains of Risk Approach

Legal: Civil and criminal fines and penalties.

Financial: Internal and external costs for investigating and remediation.

Operational: Business disruption, shutdowns, debarments, suspensions, loss of license.

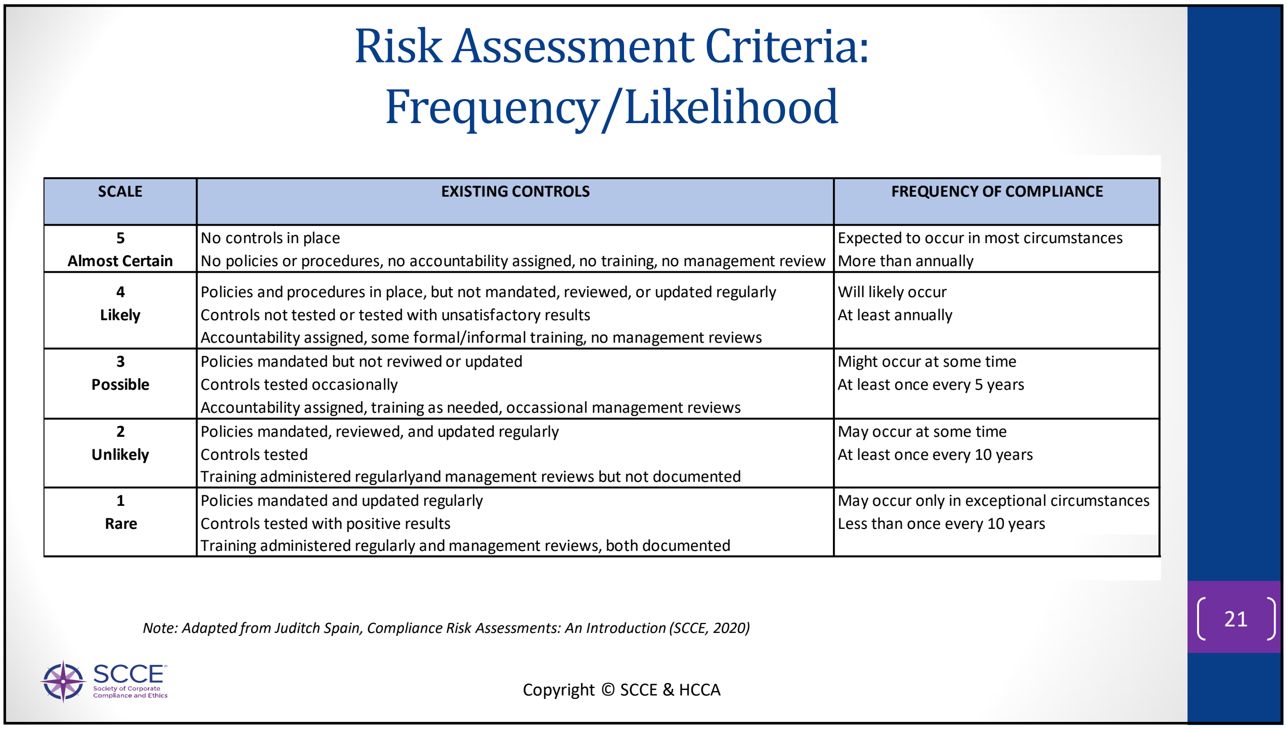


Reputation: Effect of media coverage, damage to image/brand, and reputation, including business partners, vendors, and customers.

Health & Safety: Employees, customers, others.

Strategy: Prohibition to add new customers, loss of license.

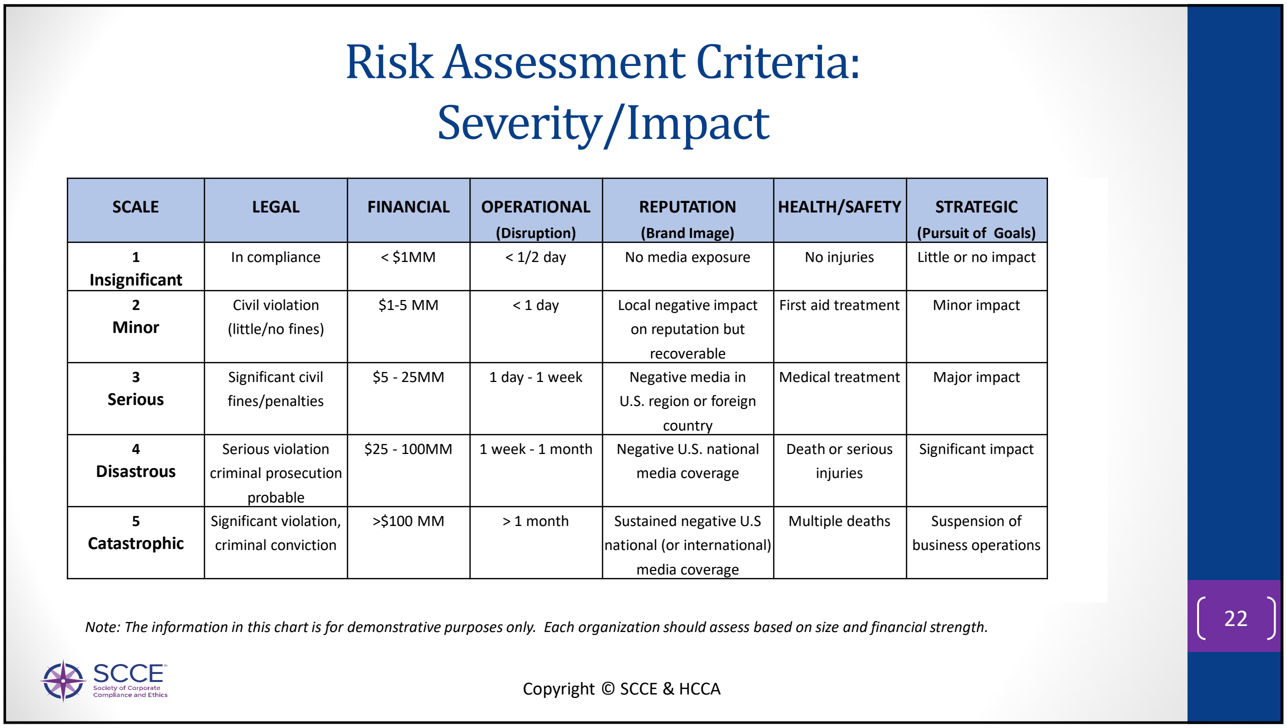
See: https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf



Risk Assessment Criteria: Frequency/Likelihood

SCALE	EXISTING CONTROLS	FREQUENCY OF COMPLIANCE
5 **Almost Certain**	No controls in place No policies or procedures, no accountability assigned, no training, no management review	Expected to occur in most circumstances More than annually
4 **Likely**	Policies and procedures in place, but not mandated, reviewed, or updated regularly Controls not tested or tested with unsatisfactory results Accountability assigned, some formal/informal training, no management reviews	Will likely occur At least annually
3 **Possible**	Policies mandated but not reviwed or updated Controls tested occasionally Accountability assigned, training as needed, occassional management reviews	Might occur at some time At least once every 5 years
2 **Unlikely**	Policies mandated, reviewed, and updated regularly Controls tested Training administered regularlyand management reviews but not documented	May occur at some time At least once every 10 years
1 **Rare**	Policies mandated and updated regularly Controls tested with positive results Training administered regularly and management reviews, both documented	May occur only in exceptional circumstances Less than once every 10 years

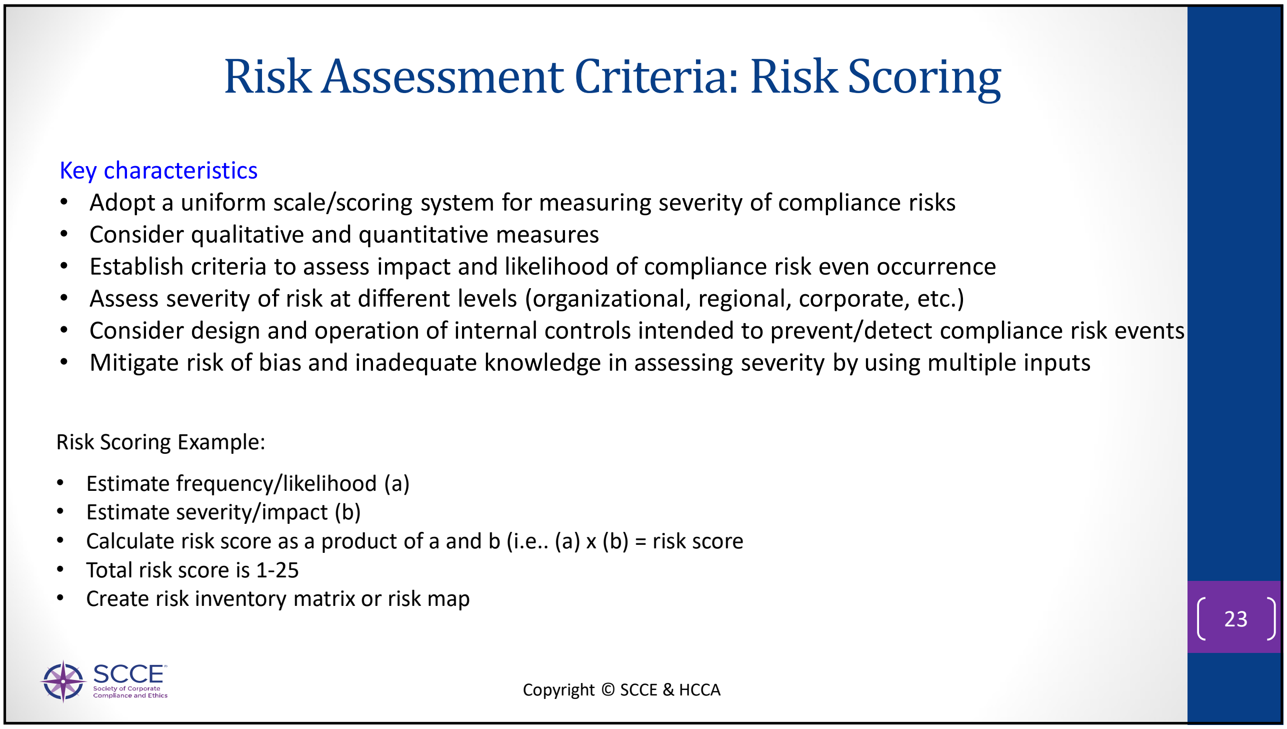
Note: Adapted from Juditch Spain, Compliance Risk Assessments: An Introduction (SCCE, 2020)



Risk Assessment Criteria: Severity/Impact

SCALE	LEGAL	FINANCIAL	OPERATIONAL (Disruption)	REPUTATION (Brand Image)	HEALTH/SAFETY	STRATEGIC (Pursuit of Goals)
1 **Insignificant**	In compliance	< $1MM	< 1/2 day	No media exposure	No injuries	Little or no impact
2 **Minor**	Civil violation (little/no fines)	$1-5 MM	< 1 day	Local negative impact on reputation but recoverable	First aid treatment	Minor impact
3 **Serious**	Significant civil fines/penalties	$5 - 25MM	1 day - 1 week	Negative media in U.S. region or foreign country	Medical treatment	Major impact
4 **Disastrous**	Serious violation criminal prosecution probable	$25 - 100MM	1 week - 1 month	Negative U.S. national media coverage	Death or serious injuries	Significant impact
5 **Catastrophic**	Significant violation, criminal conviction	>$100 MM	> 1 month	Sustained negative U.S national (or international) media coverage	Multiple deaths	Suspension of business operations

Note: The information in this chart is for demonstrative purposes only. Each organization should assess based on size and financial strength.



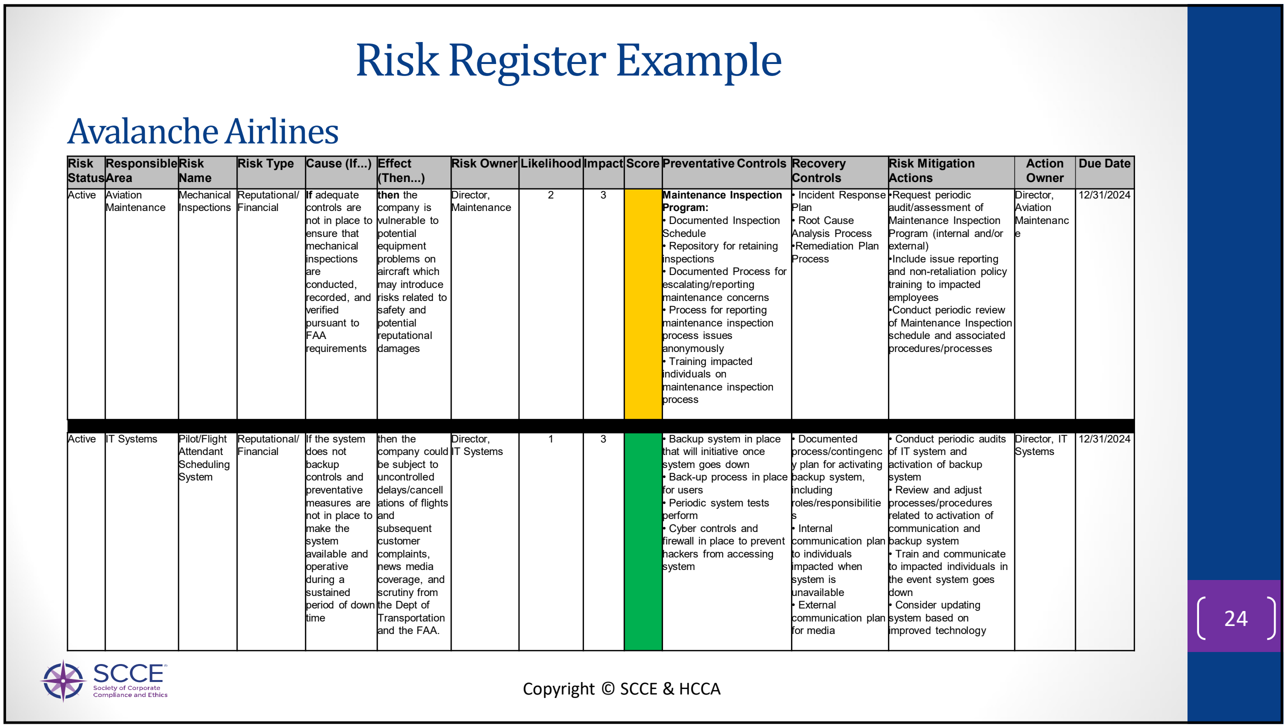
Risk Assessment Criteria: Risk Scoring

Key characteristics

- Adopt a uniform scale/scoring system for measuring severity of compliance risks
- Consider qualitative and quantitative measures
- Establish criteria to assess impact and likelihood of compliance risk even occurrence
- Assess severity of risk at different levels (organizational, regional, corporate, etc.)
- Consider design and operation of internal controls intended to prevent/detect compliance risk events
- Mitigate risk of bias and inadequate knowledge in assessing severity by using multiple inputs

Risk Scoring Example:

- Estimate frequency/likelihood (a)
- Estimate severity/impact (b)
- Calculate risk score as a product of a and b (i.e.. (a) x (b) = risk score
- Total risk score is 1-25
- Create risk inventory matrix or risk map



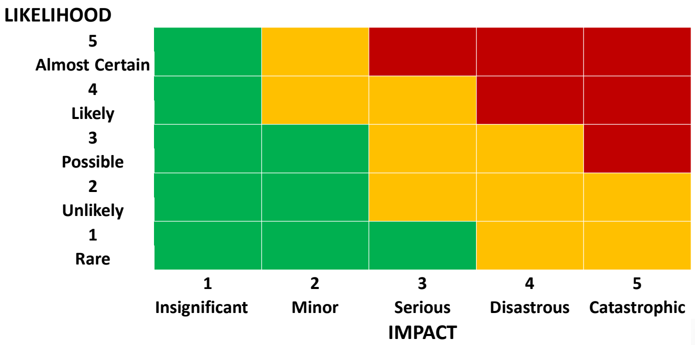
Risk Register Example

Avalanche Airlines

Risk Status	Responsible Area	Risk Name	Risk Type	Cause (If...)	Effect (Then...)	Risk Owner	Likelihood	Impact	Score	Preventative Controls	Recovery Controls	Risk Mitigation Actions	Action Owner	Due Date
Active	Aviation Maintenance	Mechanical Inspections	Reputational/ Financial	**If** adequate controls are not in place to ensure that mechanical inspections are conducted, recorded, and verified pursuant to FAA requirements	**then** the company is vulnerable to potential equipment problems on aircraft which may introduce risks related to safety and potential reputational damages	Director, Maintenance	2	3	🟨	**Maintenance Inspection Program:** • Documented Inspection Schedule • Repository for retaining inspections • Documented Process for escalating/reporting maintenance concerns • Process for reporting maintenance inspection process issues anonymously • Training impacted individuals on maintenance inspection process	• Incident Response Plan • Root Cause Analysis Process •Remediation Plan Process	•Request periodic audit/assessment of Maintenance Inspection Program (internal and/or external) •Include issue reporting and non-retaliation policy training to impacted employees •Conduct periodic review of Maintenance Inspection schedule and associated procedures/processes	Director, Aviation Maintenance	12/31/2024
Active	IT Systems	Pilot/Flight Attendant Scheduling System	Reputational/ Financial	If the system does not backup controls and preventative measures are not in place to make the system available and operative during a sustained period of down time	then the company could be subject to uncontrolled delays/cancellations of flights and subsequent customer complaints, news media coverage, and scrutiny from the Dept of Transportation and the FAA.	Director, IT Systems	1	3	🟩	• Backup system in place that will initiative once system goes down • Back-up process in place for users • Periodic system tests perform • Cyber controls and firewall in place to prevent hackers from accessing system	• Documented process/contingency plan for activating backup system, including roles/responsibilities • Internal communication plan to individuals impacted when system is unavailable • External communication plan for media	• Conduct periodic audits of IT system and activation of backup system • Review and adjust processes/procedures related to activation of communication and backup system • Train and communicate to impacted individuals in the event system goes down • Consider updating system based on improved technology	Director, IT Systems	12/31/2024

Risk Assessment Criteria:
Illustrating Compliance Risk with a Risk Matrix

- Plot each identified risk with their corresponding frequency/likelihood scores and severity/impact scores.
- Utilize the matrix to show intended and/or actual movements prior to risk response, after risk response, or both.



LIKELIHOOD	1 Insignificant	2 Minor	3 Serious	4 Disastrous	5 Catastrophic
5 Almost Certain	🟩	🟨	🟥	🟥	🟥
4 Likely	🟩	🟨	🟨	🟥	🟥
3 Possible	🟩	🟩	🟨	🟨	🟥
2 Unlikely	🟩	🟩	🟨	🟨	🟨
1 Rare	🟩	🟩	🟩	🟨	🟨

IMPACT

Compliance Risk Assessment vs. Enterprise Risk Assessment

Compliance Risk Assessment

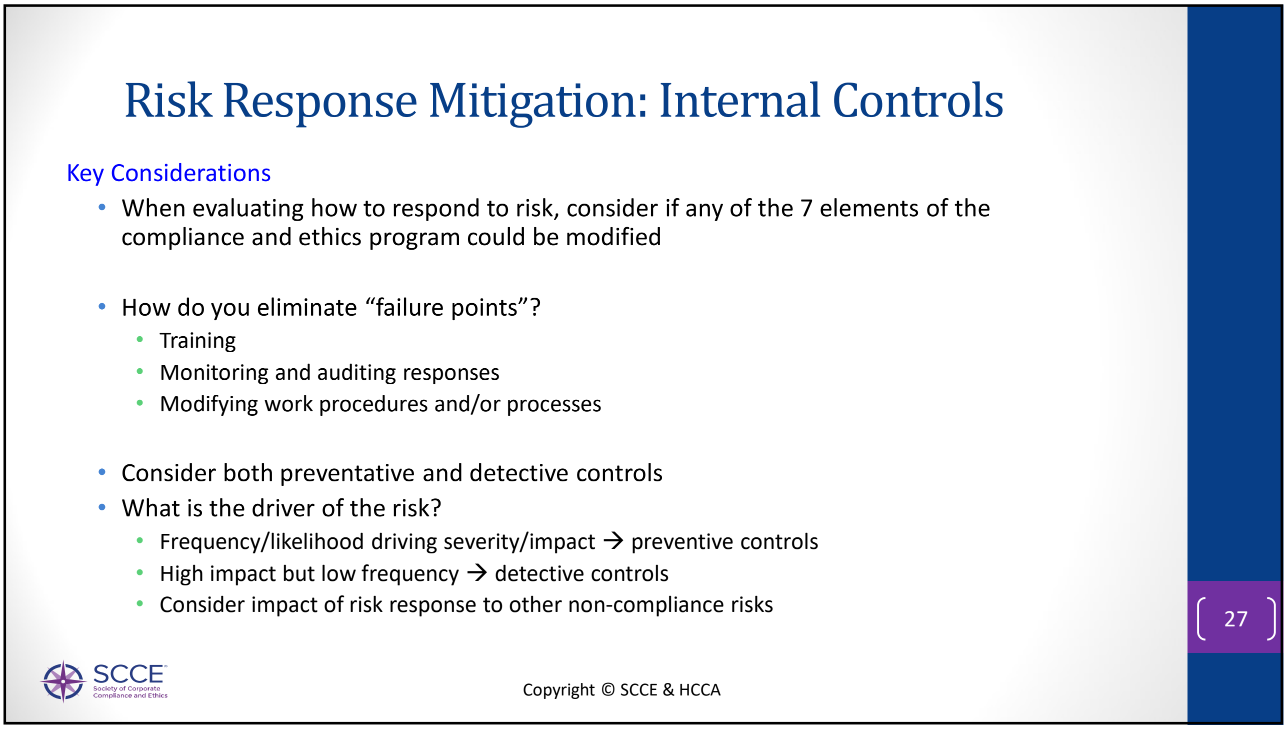
- Conducted on regular cadence
- Incorporates continuous risk assessment
- Evaluated with consistent criteria
- Considered a subset of enterprise risk
- Based on business functions/topics

Enterprise Risk Assessment

- Conducted on regular cadence
- Incorporates continuous risk assessment
- Evaluated with consistent criteria
- Includes all functions/areas of the organization
- Based on risk domains
- High dollar threshold

Key Considerations

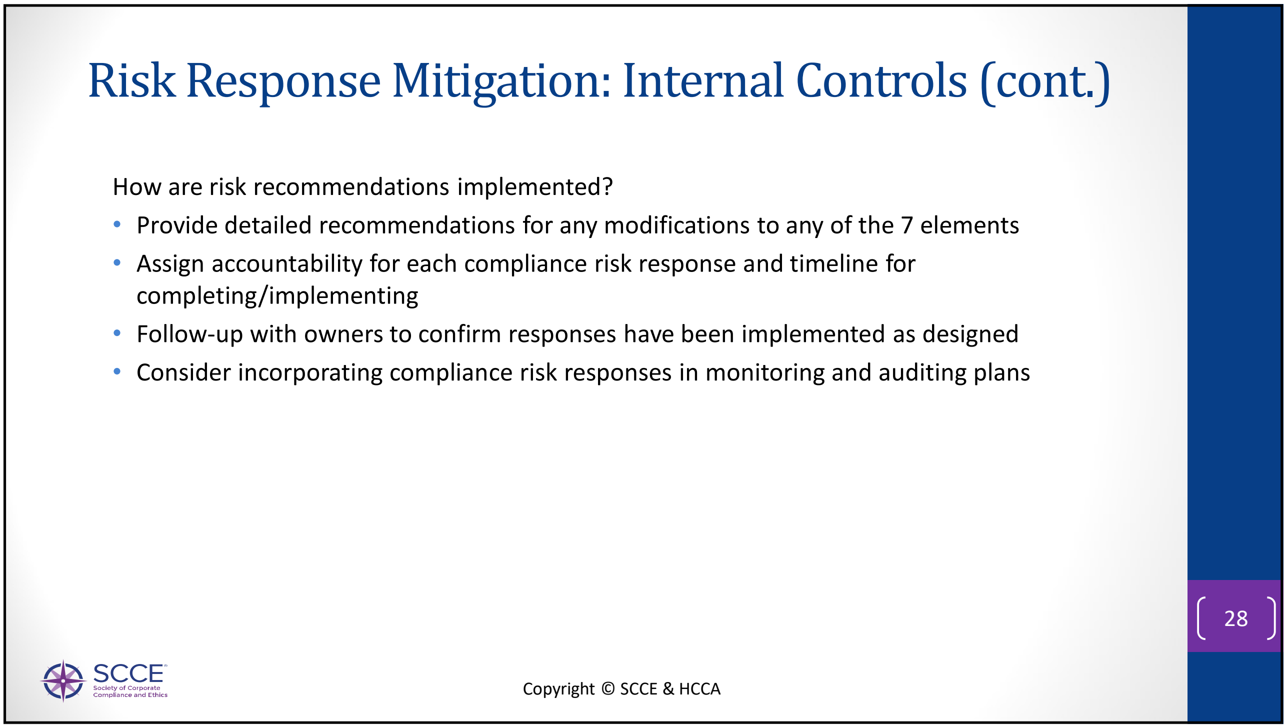
- Understand how mitigating a compliance risk can impact other risks and other risk responses
- Recognize that compliance risk is a component of enterprise risk and integrate accordingly
- Share and communicate both assessments to ensure alignment and prevent overlap
- Ensure that business areas providing input understand the difference between the two
- Clearly distinguish the difference and value of each when communicating with senior leadership



Risk Response Mitigation: Internal Controls

Key Considerations

- When evaluating how to respond to risk, consider if any of the 7 elements of the compliance and ethics program could be modified
- How do you eliminate “failure points”?
  - Training
  - Monitoring and auditing responses
  - Modifying work procedures and/or processes
- Consider both preventative and detective controls
- What is the driver of the risk?
  - Frequency/likelihood driving severity/impact → preventive controls
  - High impact but low frequency → detective controls
  - Consider impact of risk response to other non-compliance risks



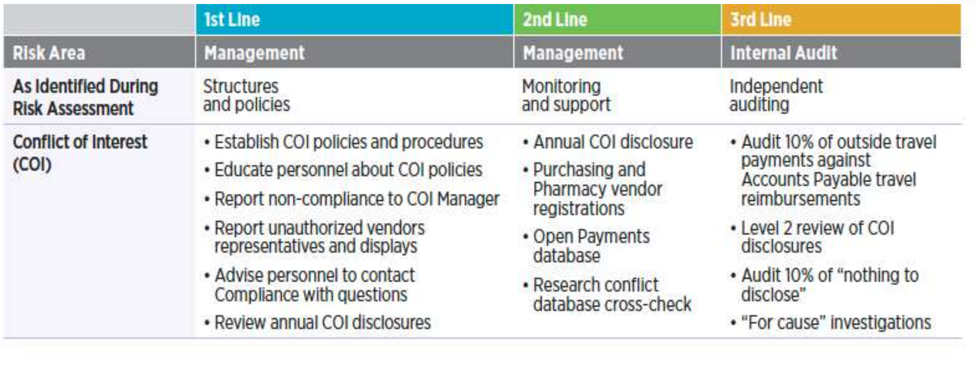
Risk Response Mitigation: Internal Controls (cont.)

How are risk recommendations implemented?

- Provide detailed recommendations for any modifications to any of the 7 elements
- Assign accountability for each compliance risk response and timeline for completing/implementing
- Follow-up with owners to confirm responses have been implemented as designed
- Consider incorporating compliance risk responses in monitoring and auditing plans

Risk Response: Internal Controls

Example



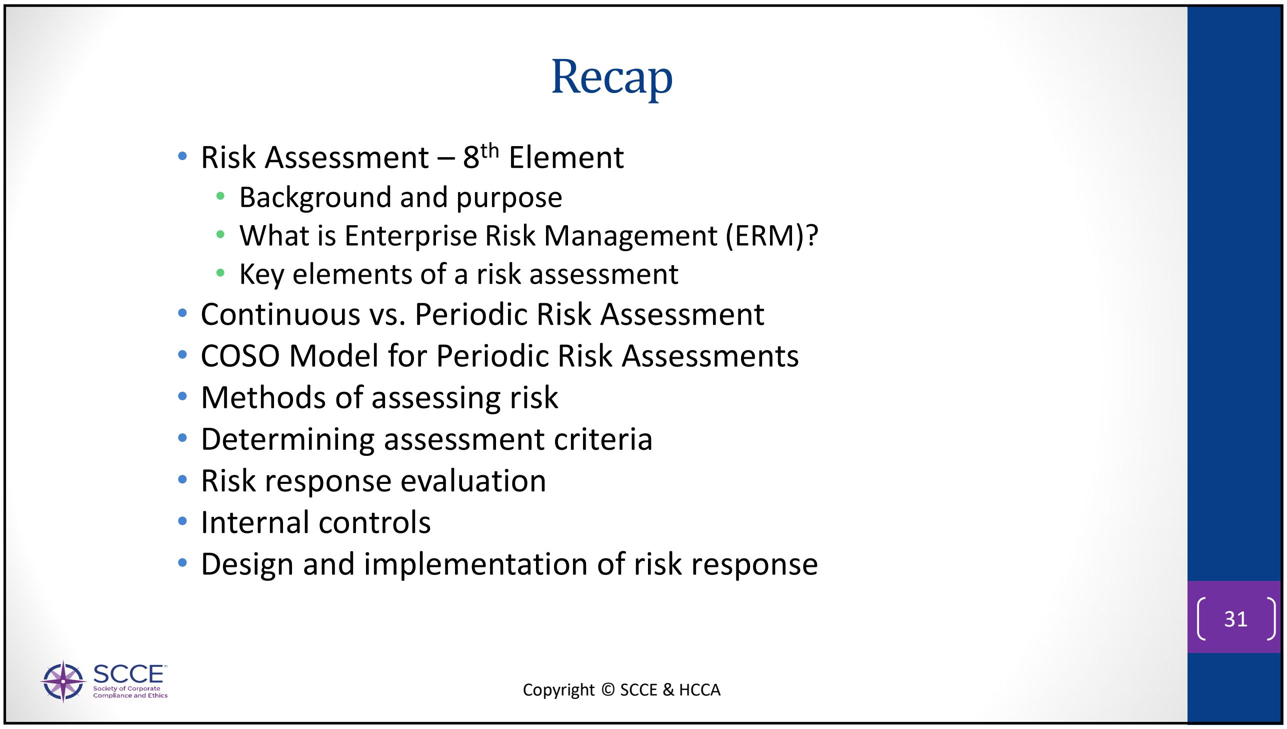
	1st Line	2nd Line	3rd Line
Risk Area	**Management**	**Management**	**Internal Audit**
As Identified During Risk Assessment	Structures and policies	Monitoring and support	Independent auditing
Conflict of Interest (COI)	• Establish COI policies and procedures • Educate personnel about COI policies • Report non-compliance to COI Manager • Report unauthorized vendors representatives and displays • Advise personnel to contact Compliance with questions • Review annual COI disclosures	• Annual COI disclosure • Purchasing and Pharmacy vendor registrations • Open Payments database • Research conflict database cross-check	• Audit 10% of outside travel payments against Accounts Payable travel reimbursements • Level 2 review of COI disclosures • Audit 10% of "nothing to disclose" • "For cause" investigations

See: https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

The Eighth Element: Risk Assessment

Key Elements

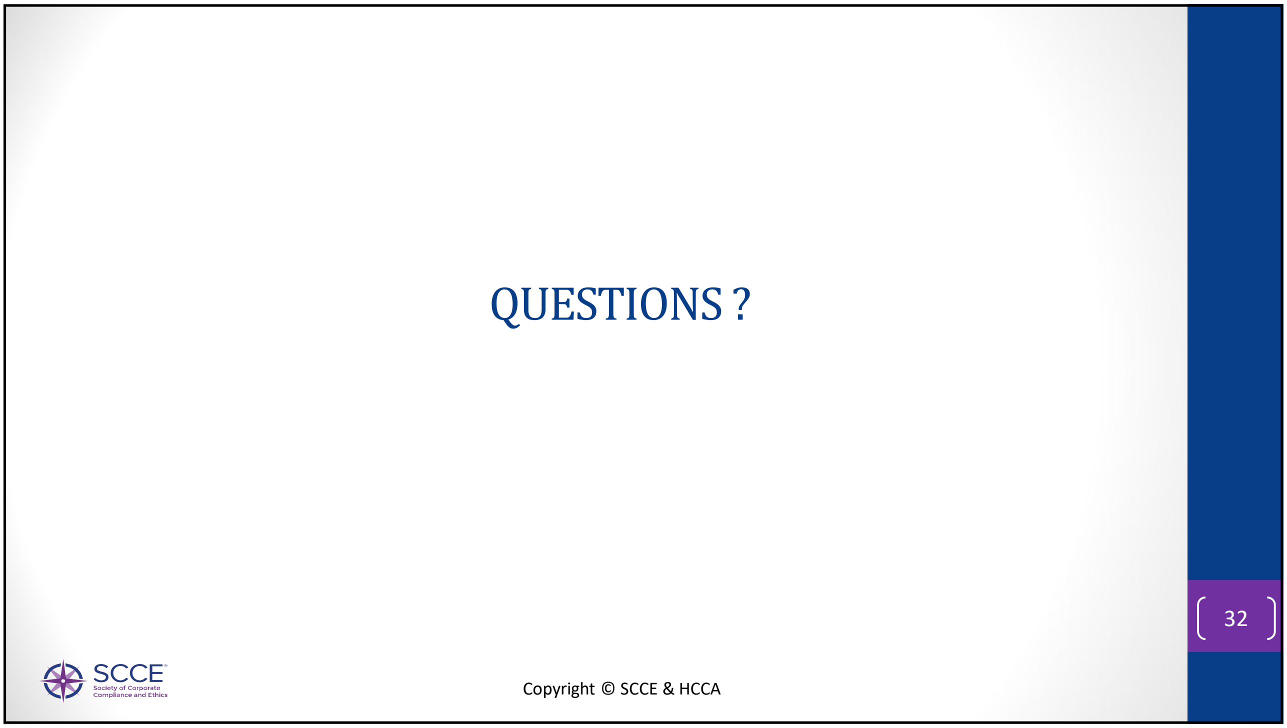
- Concise and easy to follow methodology
- Comprehensive coverage across all functions
- Appropriately defined thresholds
- Established risk domains
- Regular cadence for both continuous and periodic assessments
- Consistent and applicable method for identifying risk
- Includes Risk Criteria/Risk Scoring/Risk Matrix
- Incorporates response to risk assessment that evaluates 7 elements



Recap

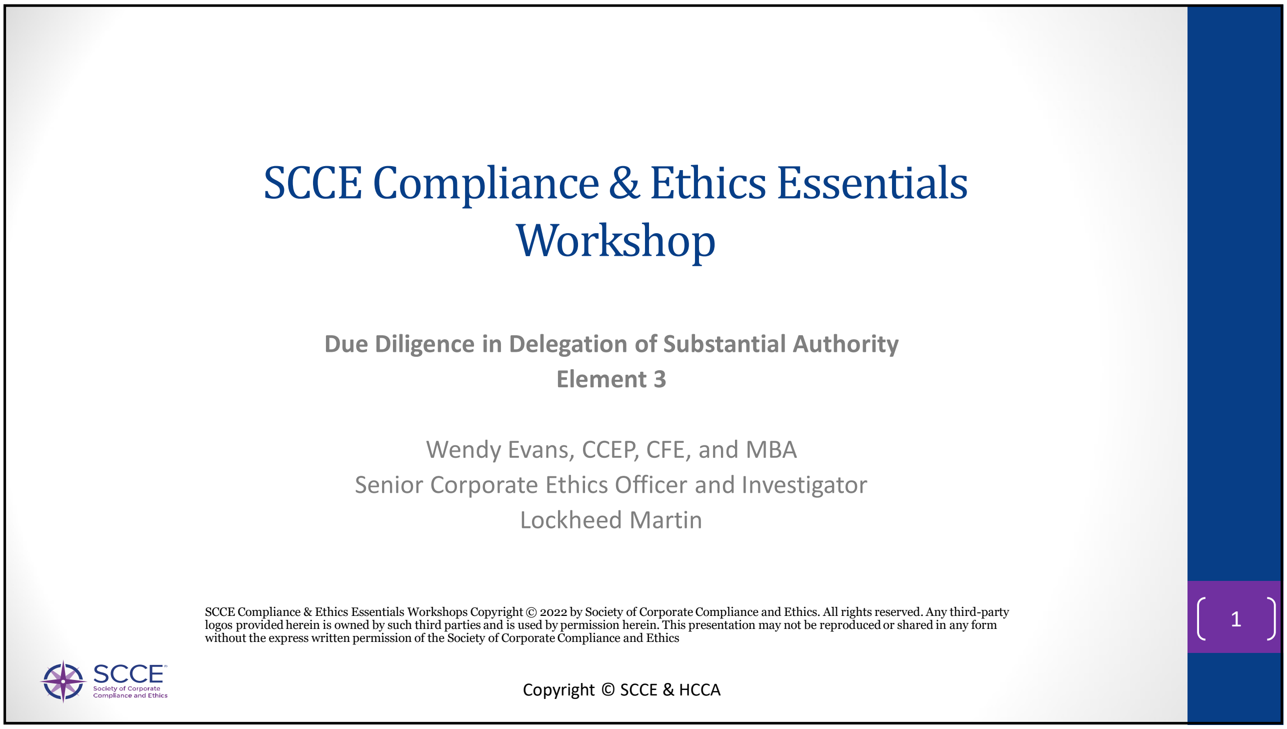
- Risk Assessment – 8th Element
  - Background and purpose
  - What is Enterprise Risk Management (ERM)?
  - Key elements of a risk assessment
- Continuous vs. Periodic Risk Assessment
- COSO Model for Periodic Risk Assessments
- Methods of assessing risk
- Determining assessment criteria
- Risk response evaluation
- Internal controls
- Design and implementation of risk response

31



QUESTIONS ?

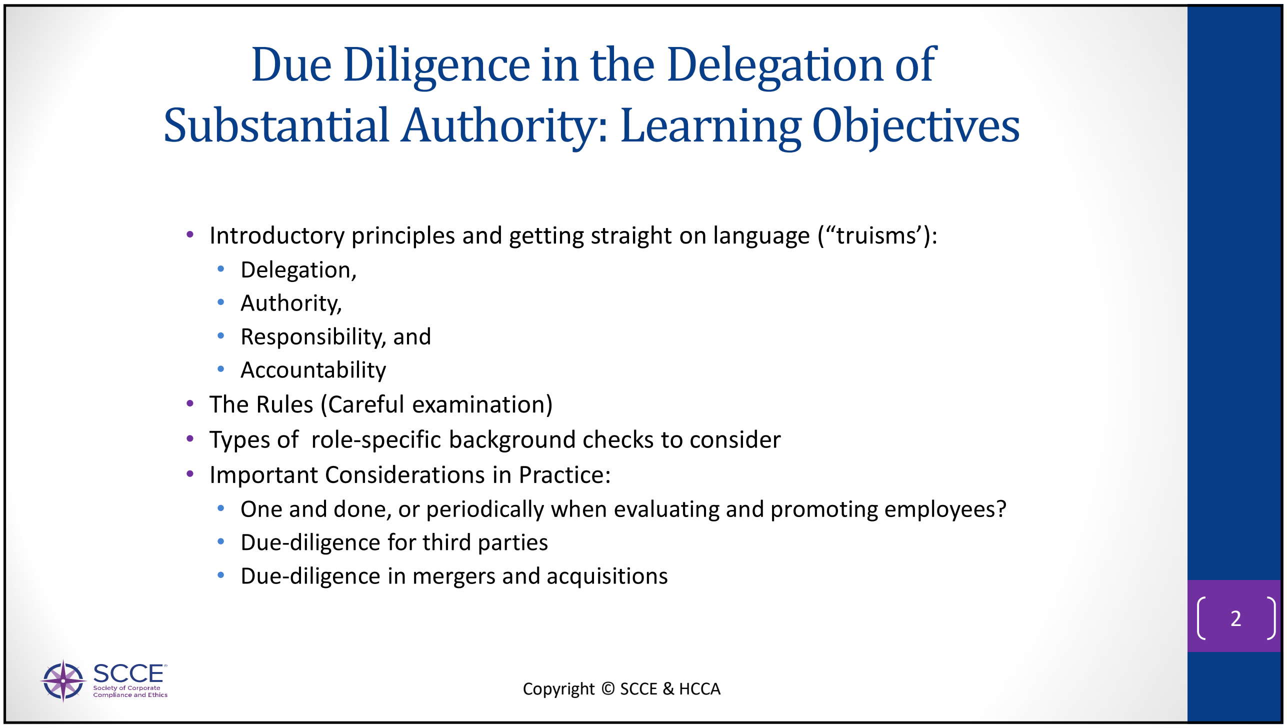
32



SCCE Compliance & Ethics Essentials Workshop

Due Diligence in Delegation of Substantial Authority
Element 3

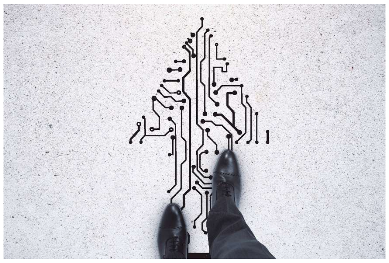
Wendy Evans, CCEP, CFE, and MBA
Senior Corporate Ethics Officer and Investigator
Lockheed Martin



Due Diligence in the Delegation of Substantial Authority: Learning Objectives

- Introductory principles and getting straight on language (“truisms’):
  - Delegation,
  - Authority,
  - Responsibility, and
  - Accountability
- The Rules (Careful examination)
- Types of role-specific background checks to consider
- Important Considerations in Practice:
  - One and done, or periodically when evaluating and promoting employees?
  - Due-diligence for third parties
  - Due-diligence in mergers and acquisitions

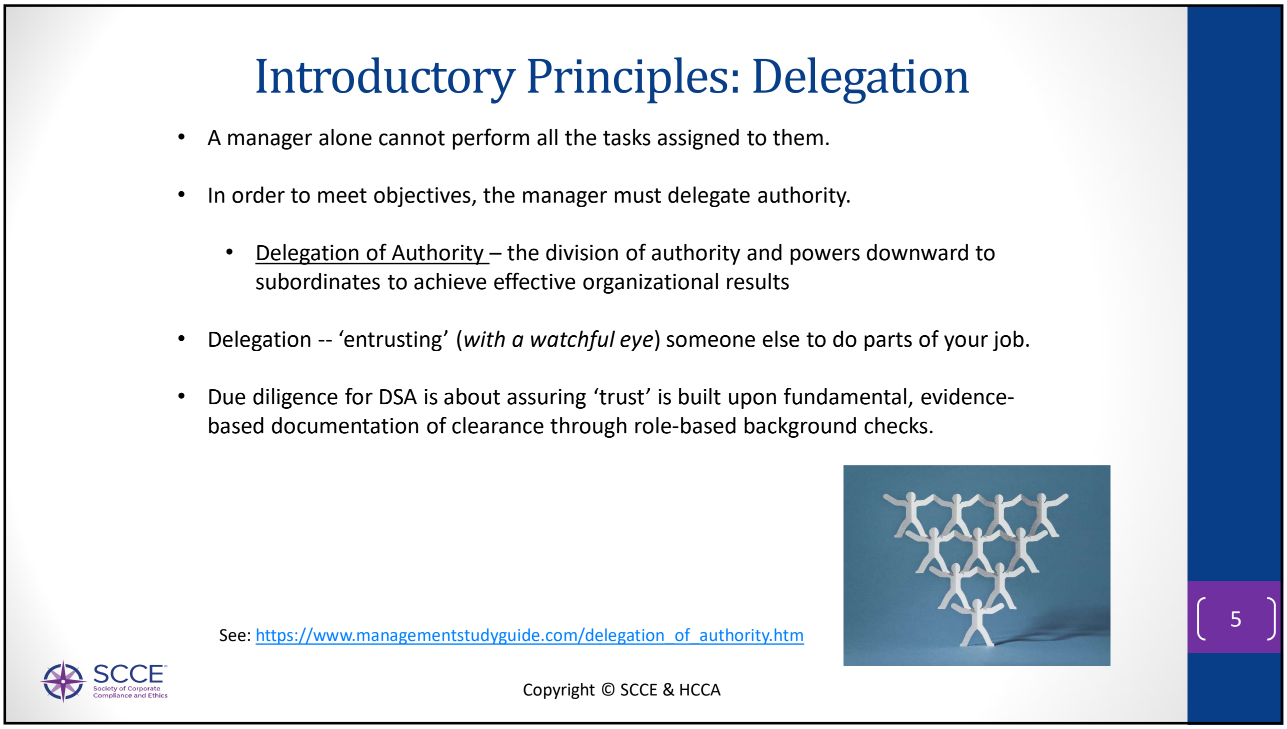
Introductory Principles



Introductory Principles

- **Delegation of authority** – persons with responsibility for binding a company delegate to other company personnel the power to execute actions on behalf of the company
- Organizations should have a **delegation of authority policy and protocol**
  - To assign authority to ensure decisions are made/actions taken by the appropriate staff
  - To assign responsibility to appropriate personnel
  - To ensure a sound control environment
  - To facilitate decision-making and execution
  - To maintain fiscal integrity
  - To ensure transactions executed according to law, regulation and organizational policy
- Delegation of Authority can vary organization to organization
  - Can be determined by Board of Director Resolution
  - Can be communicated through organizational policy
  - Can be demonstrated in organizational charts (reporting structures)
  - Can be dictated by legal/industry requirements applicable to the corporation

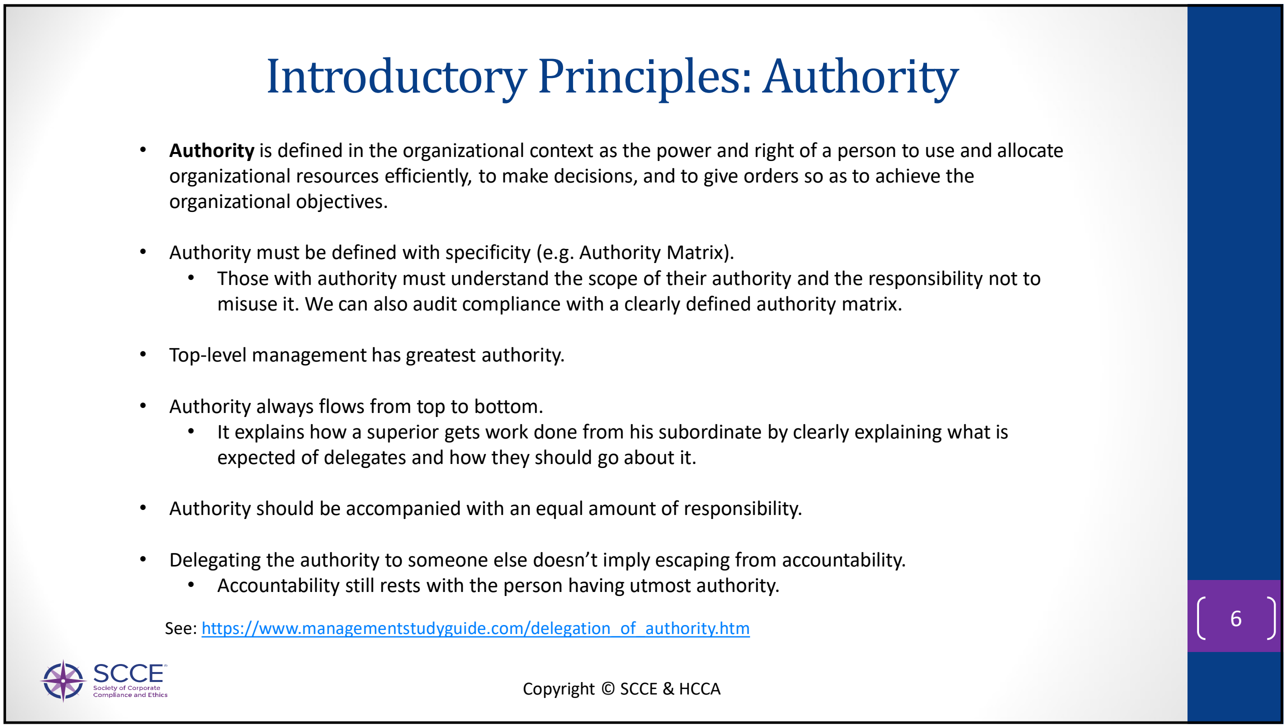
See: Thomson Reuters Practical Law



Introductory Principles: Delegation

- A manager alone cannot perform all the tasks assigned to them.
- In order to meet objectives, the manager must delegate authority.
  - Delegation of Authority – the division of authority and powers downward to subordinates to achieve effective organizational results
- Delegation -- ‘entrusting’ (*with a watchful eye*) someone else to do parts of your job.
- Due diligence for DSA is about assuring ‘trust’ is built upon fundamental, evidence-based documentation of clearance through role-based background checks.

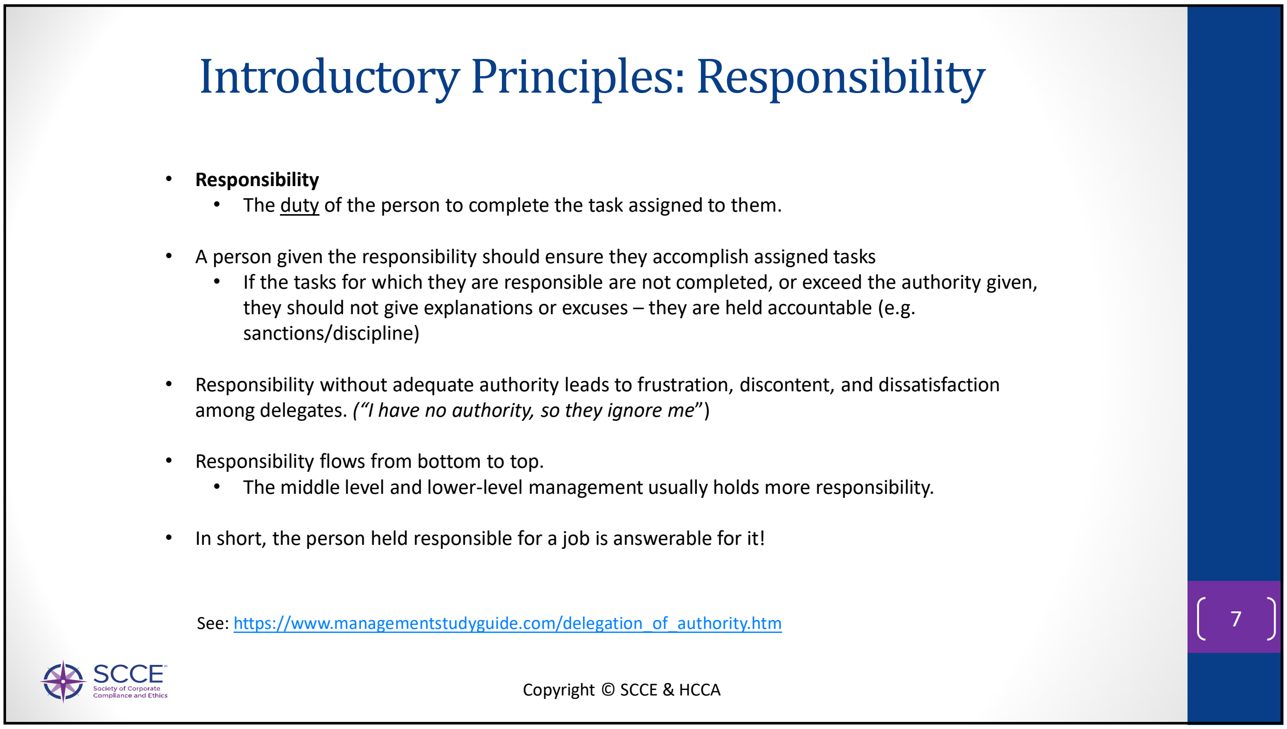
See: https://www.managementstudyguide.com/delegation_of_authority.htm



Introductory Principles: Authority

- **Authority** is defined in the organizational context as the power and right of a person to use and allocate organizational resources efficiently, to make decisions, and to give orders so as to achieve the organizational objectives.
- Authority must be defined with specificity (e.g. Authority Matrix).
  - Those with authority must understand the scope of their authority and the responsibility not to misuse it. We can also audit compliance with a clearly defined authority matrix.
- Top-level management has greatest authority.
- Authority always flows from top to bottom.
  - It explains how a superior gets work done from his subordinate by clearly explaining what is expected of delegates and how they should go about it.
- Authority should be accompanied with an equal amount of responsibility.
- Delegating the authority to someone else doesn’t imply escaping from accountability.
  - Accountability still rests with the person having utmost authority.

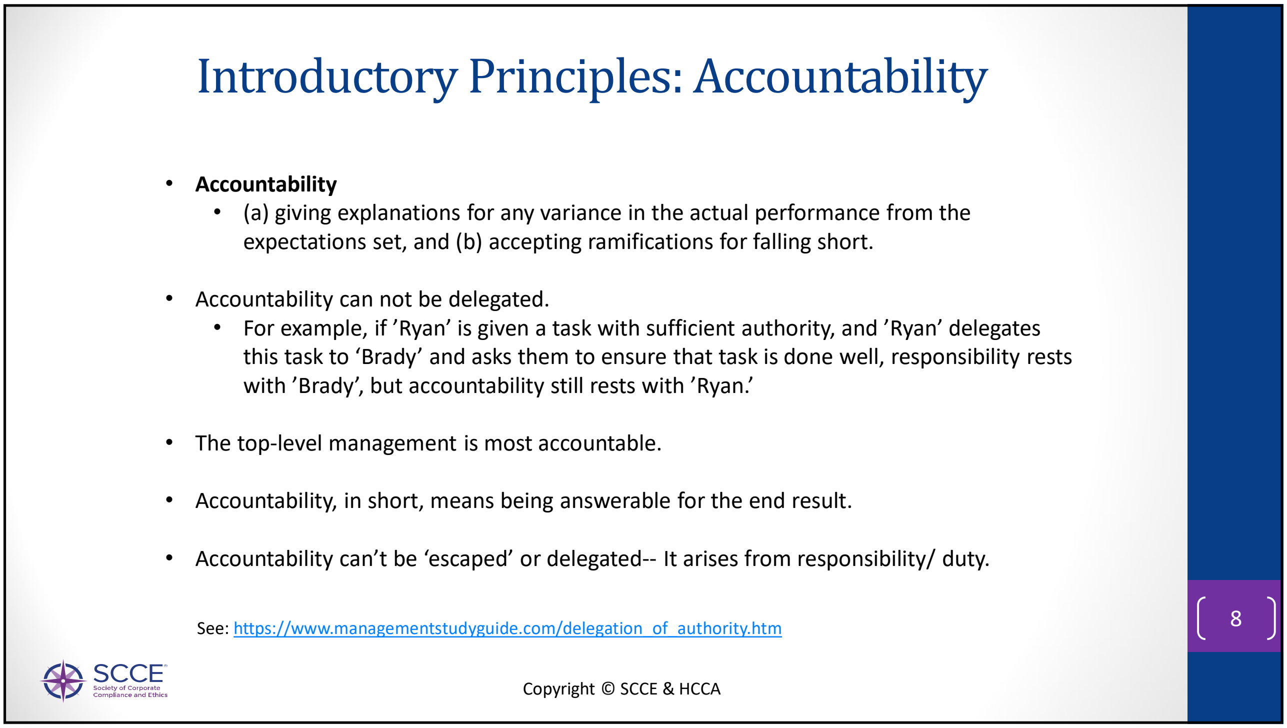
See: https://www.managementstudyguide.com/delegation_of_authority.htm



Introductory Principles: Responsibility

- **Responsibility**
  - The duty of the person to complete the task assigned to them.
- A person given the responsibility should ensure they accomplish assigned tasks
  - If the tasks for which they are responsible are not completed, or exceed the authority given, they should not give explanations or excuses – they are held accountable (e.g. sanctions/discipline)
- Responsibility without adequate authority leads to frustration, discontent, and dissatisfaction among delegates. *(“I have no authority, so they ignore me*”)
- Responsibility flows from bottom to top.
  - The middle level and lower-level management usually holds more responsibility.
- In short, the person held responsible for a job is answerable for it!

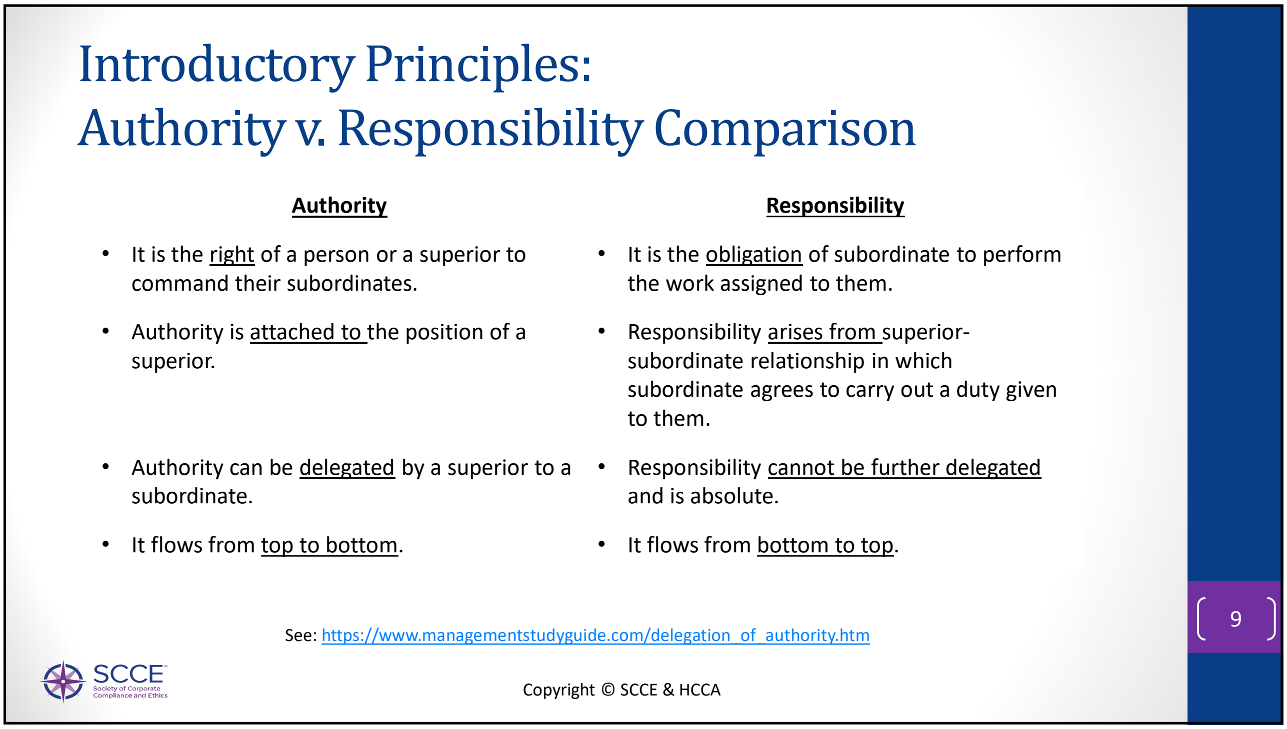
See: https://www.managementstudyguide.com/delegation_of_authority.htm



Introductory Principles: Accountability

- **Accountability**
  - (a) giving explanations for any variance in the actual performance from the expectations set, and (b) accepting ramifications for falling short.
- Accountability can not be delegated.
  - For example, if ’Ryan’ is given a task with sufficient authority, and ’Ryan’ delegates this task to ‘Brady’ and asks them to ensure that task is done well, responsibility rests with ’Brady’, but accountability still rests with ’Ryan.’
- The top-level management is most accountable.
- Accountability, in short, means being answerable for the end result.
- Accountability can’t be ‘escaped’ or delegated-- It arises from responsibility/ duty.

See: https://www.managementstudyguide.com/delegation_of_authority.htm



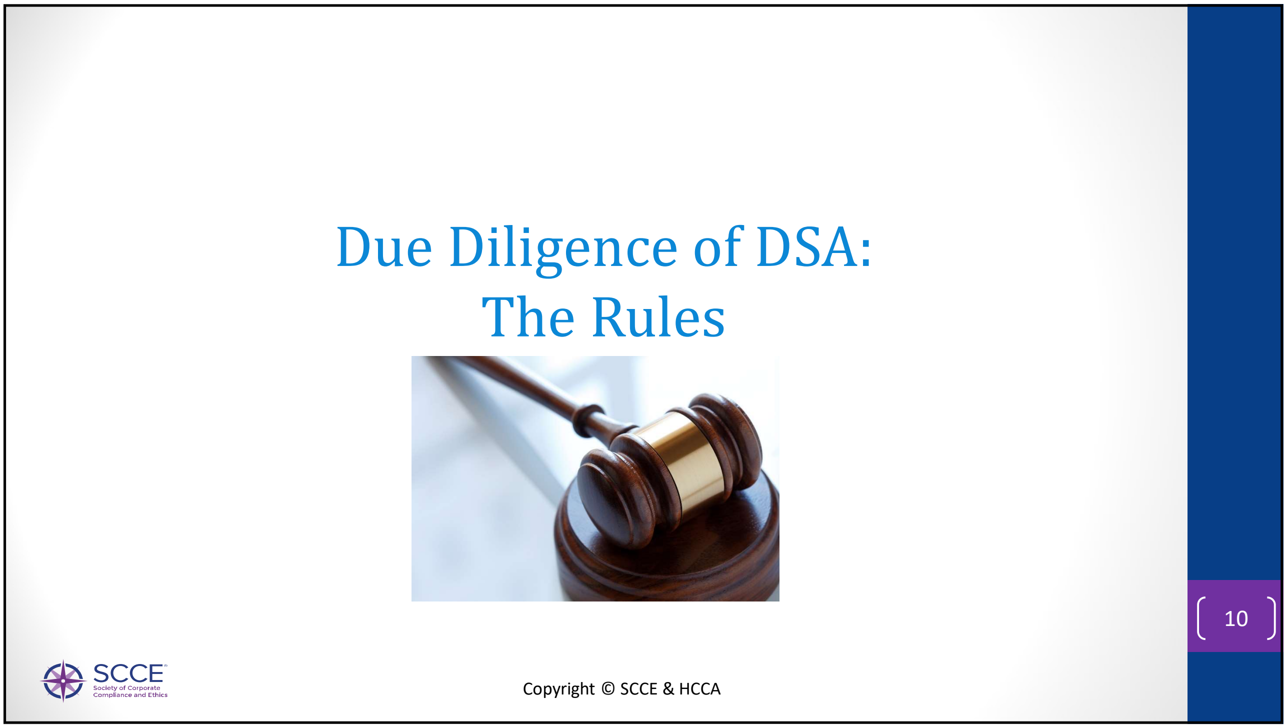
Introductory Principles:
Authority v. Responsibility Comparison

Authority	Responsibility
• It is the right of a person or a superior to command their subordinates.	• It is the obligation of subordinate to perform the work assigned to them.
• Authority is attached to the position of a superior.	• Responsibility arises from superior-subordinate relationship in which subordinate agrees to carry out a duty given to them.
• Authority can be delegated by a superior to a subordinate.	• Responsibility cannot be further delegated and is absolute.
• It flows from top to bottom.	• It flows from bottom to top.

See: https://www.managementstudyguide.com/delegation_of_authority.htm

9

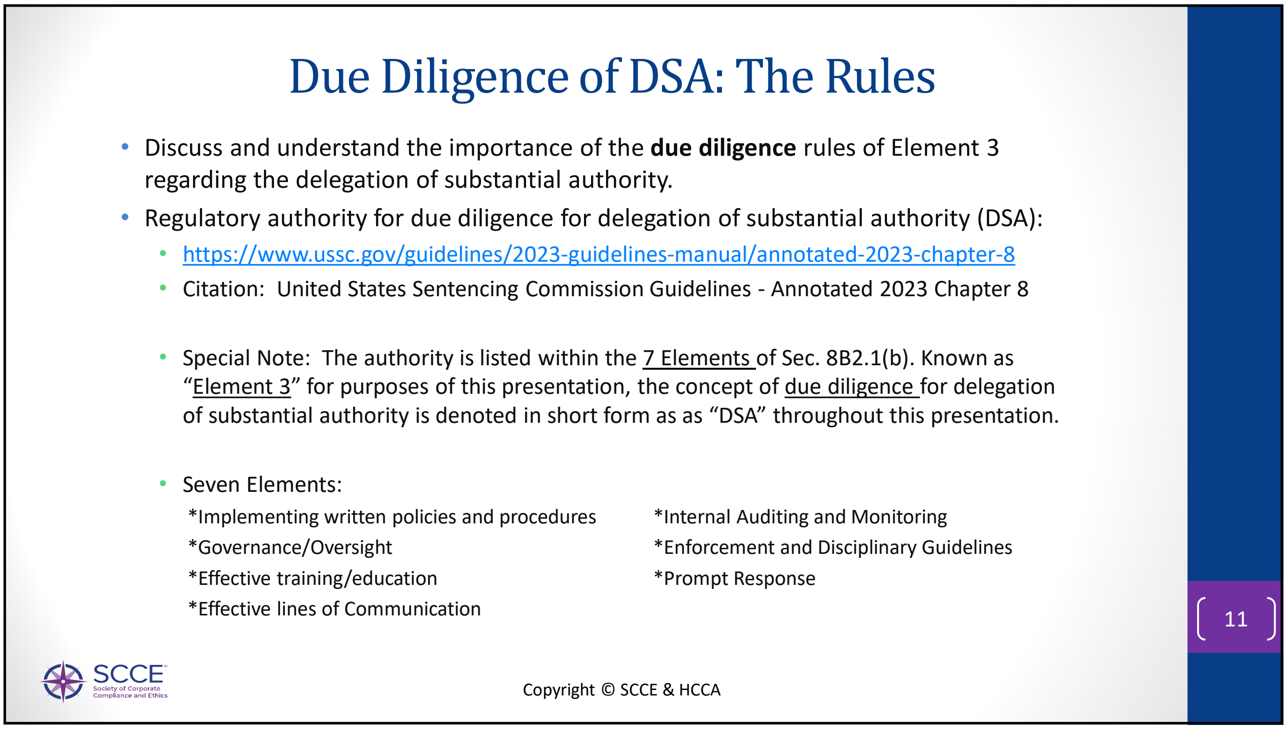
9



Due Diligence of DSA:
The Rules

10

10

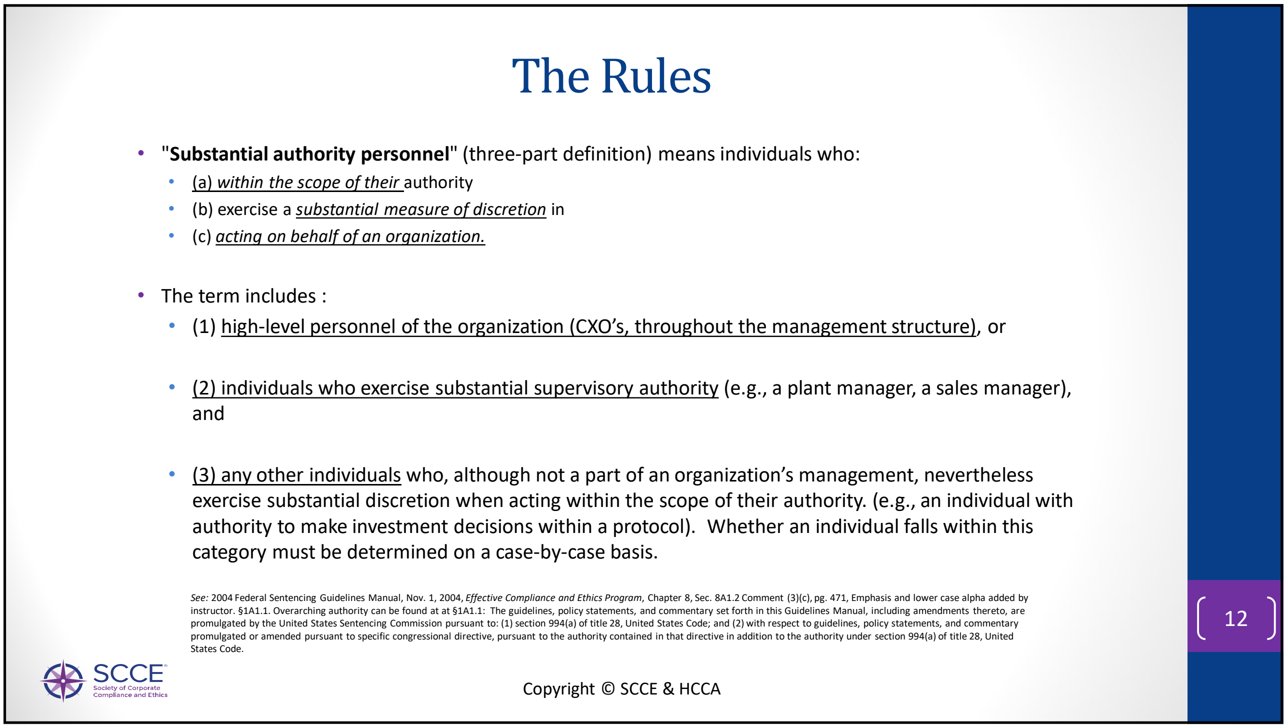


Due Diligence of DSA: The Rules

- Discuss and understand the importance of the **due diligence** rules of Element 3 regarding the delegation of substantial authority.
- Regulatory authority for due diligence for delegation of substantial authority (DSA):
  - https://www.ussc.gov/guidelines/2023-guidelines-manual/annotated-2023-chapter-8
  - Citation: United States Sentencing Commission Guidelines - Annotated 2023 Chapter 8
  - Special Note: The authority is listed within the 7 Elements of Sec. 8B2.1(b). Known as "Element 3" for purposes of this presentation, the concept of due diligence for delegation of substantial authority is denoted in short form as as "DSA" throughout this presentation.
  - Seven Elements:

*Implementing written policies and procedures
*Governance/Oversight
*Effective training/education
*Effective lines of Communication

*Internal Auditing and Monitoring
*Enforcement and Disciplinary Guidelines
*Prompt Response



The Rules

- "**Substantial authority personnel**" (three-part definition) means individuals who:
  - (a) *within the scope of their* authority
  - (b) exercise a *substantial measure of discretion* in
  - (c) *acting on behalf of an organization.*
- The term includes :
  - (1) high-level personnel of the organization (CXO's, throughout the management structure), or
  - (2) individuals who exercise substantial supervisory authority (e.g., a plant manager, a sales manager), and
  - (3) any other individuals who, although not a part of an organization's management, nevertheless exercise substantial discretion when acting within the scope of their authority. (e.g., an individual with authority to make investment decisions within a protocol). Whether an individual falls within this category must be determined on a case-by-case basis.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8A1.2 Comment (3)(c), pg. 471, Emphasis and lower case alpha added by instructor. §1A1.1. Overarching authority can be found at at §1A1.1: The guidelines, policy statements, and commentary set forth in this Guidelines Manual, including amendments thereto, are promulgated by the United States Sentencing Commission pursuant to: (1) section 994(a) of title 28, United States Code; and (2) with respect to guidelines, policy statements, and commentary promulgated or amended pursuant to specific congressional directive, pursuant to the authority contained in that directive in addition to the authority under section 994(a) of title 28, United States Code.

The Rules

- The organization shall use
  - *reasonable efforts*
  - not to include within the substantial authority personnel of the organization
  - any individual
  - whom the organization (a) knew, or (b) should have known through (c) the *exercise of due diligence (generally a background check)*
  - has engaged in (a) illegal activities or (b) other conduct that is (c) *inconsistent with an effective compliance and ethics program. (Note: This is a broad standard and says nothing about being role-based)*

CITATION: *https://guidelines.ussc.gov/apex/r/ussc_apex/guidelinesapp/guidelines?app_gl_id=%C2%A78B2.1*

Implementing Due-Diligence for DSA: The Rules

- Implementation.—In implementing subsection (b)(3), (i.e. Element 3) the organization *shall* hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with:
  - (a) the exercise of due diligence, and
  - (b) the promotion of an organizational culture that encourages ethical conduct, and
  - (c) commitment to compliance with the law under subsection Sec. 8B2.1(a), the rules for an effective compliance and ethics program.

CITATION: *https://guidelines.ussc.gov/apex/r/ussc_apex/guidelinesapp/guidelines?app_gl_id=%C2%A78B2.1*

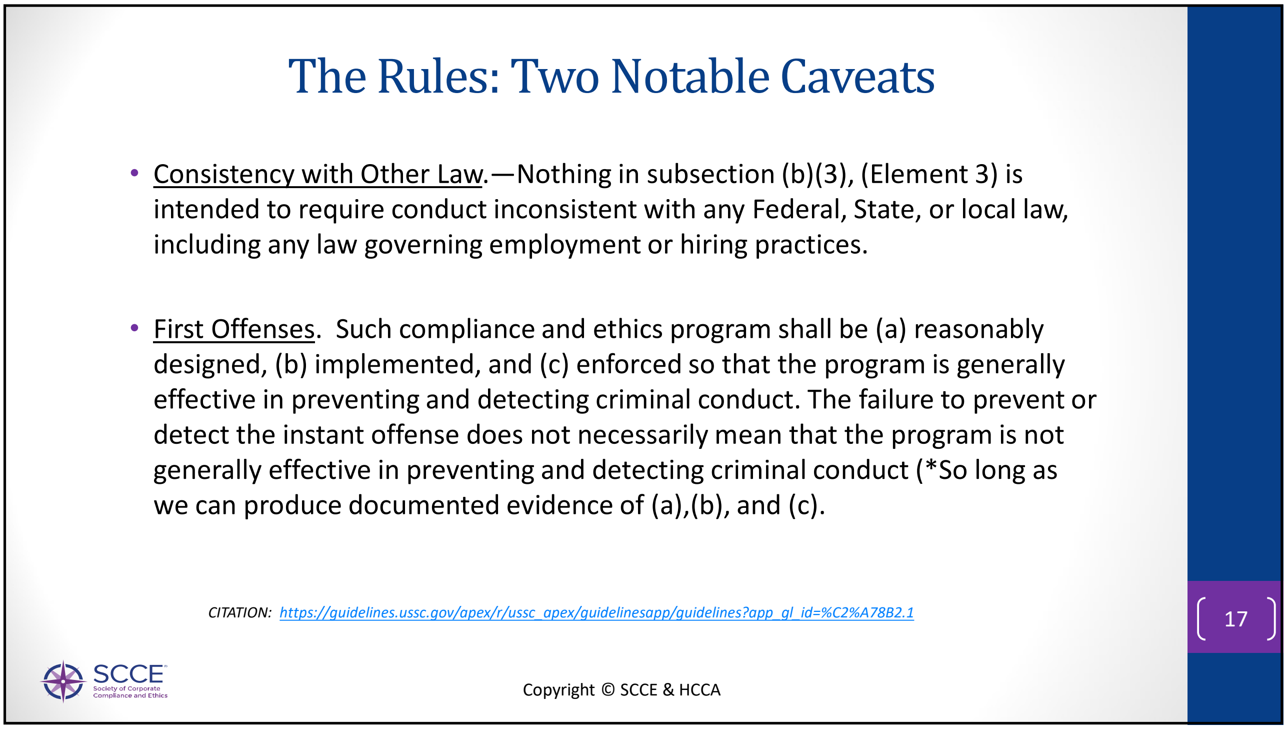
Implementing Due-Diligence for DSA: The Rules

- *Due Diligence w*ith respect to the hiring or promotion of such individuals, an organization shall consider:
  - (a) the relatedness of the individual's illegal activities and/or misconduct
  - (b) other misconduct (i.e., other conduct inconsistent with an effective compliance and ethics program)
  - (c) the specific responsibilities the individual is anticipated to be assigned, and
  - (d) other factors such as:
    - the recency of the individual's illegal activities and other misconduct; and
    - whether the individual has engaged in other such illegal activities *and* other such misconduct.

CITATION: https://guidelines.ussc.gov/apex/r/ussc_apex/guidelinesapp/guidelines?app_gl_id=%C2%A78B2.1

Instructor Commentary/Recommendation:

Looks, feels, and suggests a balancing test. But, be careful to set some 'recommended guidelines' (not rules) to advance equity in documented employment decisions considering the totality of circumstances. Consult with expert jurisdictional employment legal counsel.



The Rules: Two Notable Caveats

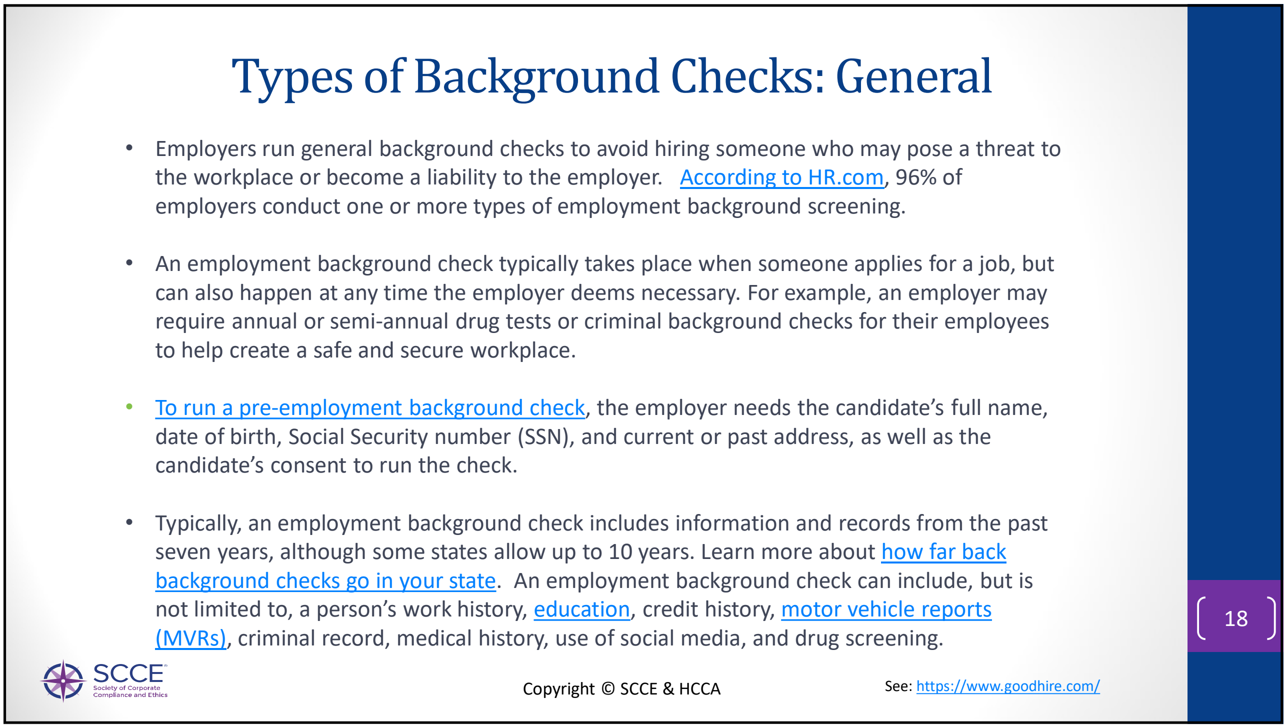
- Consistency with Other Law.—Nothing in subsection (b)(3), (Element 3) is intended to require conduct inconsistent with any Federal, State, or local law, including any law governing employment or hiring practices.

- First Offenses. Such compliance and ethics program shall be (a) reasonably designed, (b) implemented, and (c) enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct (*So long as we can produce documented evidence of (a),(b), and (c).

CITATION: *https://guidelines.ussc.gov/apex/r/ussc_apex/guidelinesapp/guidelines?app_gl_id=%C2%A78B2.1*

17

17



Types of Background Checks: General

- Employers run general background checks to avoid hiring someone who may pose a threat to the workplace or become a liability to the employer. According to HR.com, 96% of employers conduct one or more types of employment background screening.

- An employment background check typically takes place when someone applies for a job, but can also happen at any time the employer deems necessary. For example, an employer may require annual or semi-annual drug tests or criminal background checks for their employees to help create a safe and secure workplace.

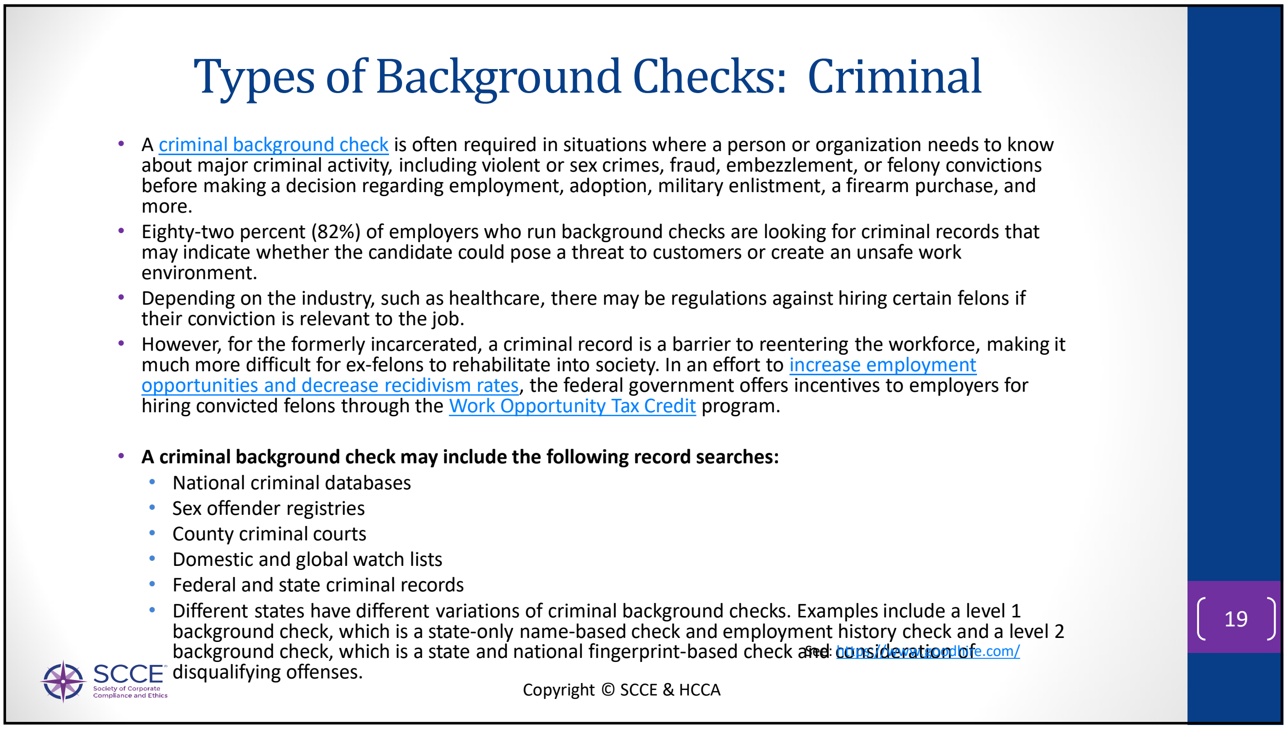
- To run a pre-employment background check, the employer needs the candidate's full name, date of birth, Social Security number (SSN), and current or past address, as well as the candidate's consent to run the check.

- Typically, an employment background check includes information and records from the past seven years, although some states allow up to 10 years. Learn more about how far back background checks go in your state. An employment background check can include, but is not limited to, a person's work history, education, credit history, motor vehicle reports (MVRs), criminal record, medical history, use of social media, and drug screening.

18

See: https://www.goodhire.com/

18



Types of Background Checks: Criminal

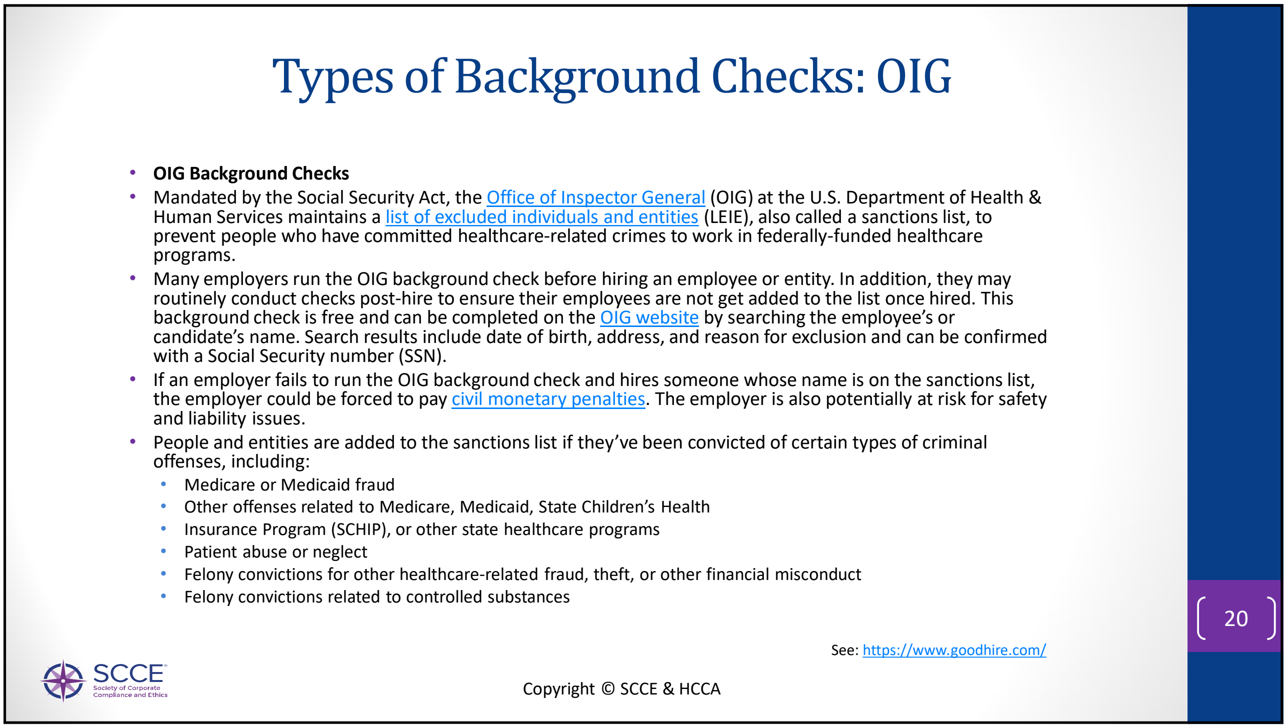
- A criminal background check is often required in situations where a person or organization needs to know about major criminal activity, including violent or sex crimes, fraud, embezzlement, or felony convictions before making a decision regarding employment, adoption, military enlistment, a firearm purchase, and more.
- Eighty-two percent (82%) of employers who run background checks are looking for criminal records that may indicate whether the candidate could pose a threat to customers or create an unsafe work environment.
- Depending on the industry, such as healthcare, there may be regulations against hiring certain felons if their conviction is relevant to the job.
- However, for the formerly incarcerated, a criminal record is a barrier to reentering the workforce, making it much more difficult for ex-felons to rehabilitate into society. In an effort to increase employment opportunities and decrease recidivism rates, the federal government offers incentives to employers for hiring convicted felons through the Work Opportunity Tax Credit program.

- **A criminal background check may include the following record searches:**
  - National criminal databases
  - Sex offender registries
  - County criminal courts
  - Domestic and global watch lists
  - Federal and state criminal records
  - Different states have different variations of criminal background checks. Examples include a level 1 background check, which is a state-only name-based check and employment history check and a level 2 background check, which is a state and national fingerprint-based check and consideration of disqualifying offenses.

See: https://www.goodhire.com/

19

19



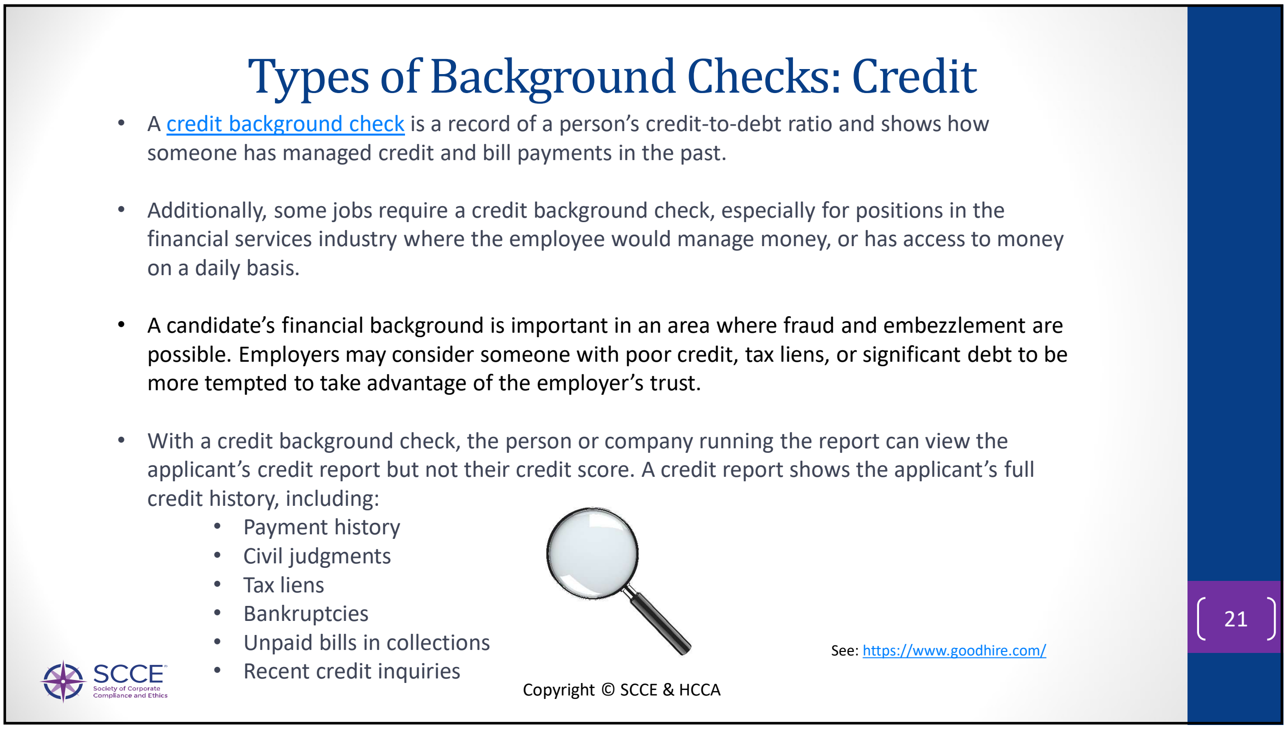
Types of Background Checks: OIG

- **OIG Background Checks**
- Mandated by the Social Security Act, the Office of Inspector General (OIG) at the U.S. Department of Health & Human Services maintains a list of excluded individuals and entities (LEIE), also called a sanctions list, to prevent people who have committed healthcare-related crimes to work in federally-funded healthcare programs.
- Many employers run the OIG background check before hiring an employee or entity. In addition, they may routinely conduct checks post-hire to ensure their employees are not get added to the list once hired. This background check is free and can be completed on the OIG website by searching the employee's or candidate's name. Search results include date of birth, address, and reason for exclusion and can be confirmed with a Social Security number (SSN).
- If an employer fails to run the OIG background check and hires someone whose name is on the sanctions list, the employer could be forced to pay civil monetary penalties. The employer is also potentially at risk for safety and liability issues.
- People and entities are added to the sanctions list if they've been convicted of certain types of criminal offenses, including:
  - Medicare or Medicaid fraud
  - Other offenses related to Medicare, Medicaid, State Children's Health
  - Insurance Program (SCHIP), or other state healthcare programs
  - Patient abuse or neglect
  - Felony convictions for other healthcare-related fraud, theft, or other financial misconduct
  - Felony convictions related to controlled substances

See: https://www.goodhire.com/

20

20



Types of Background Checks: Credit

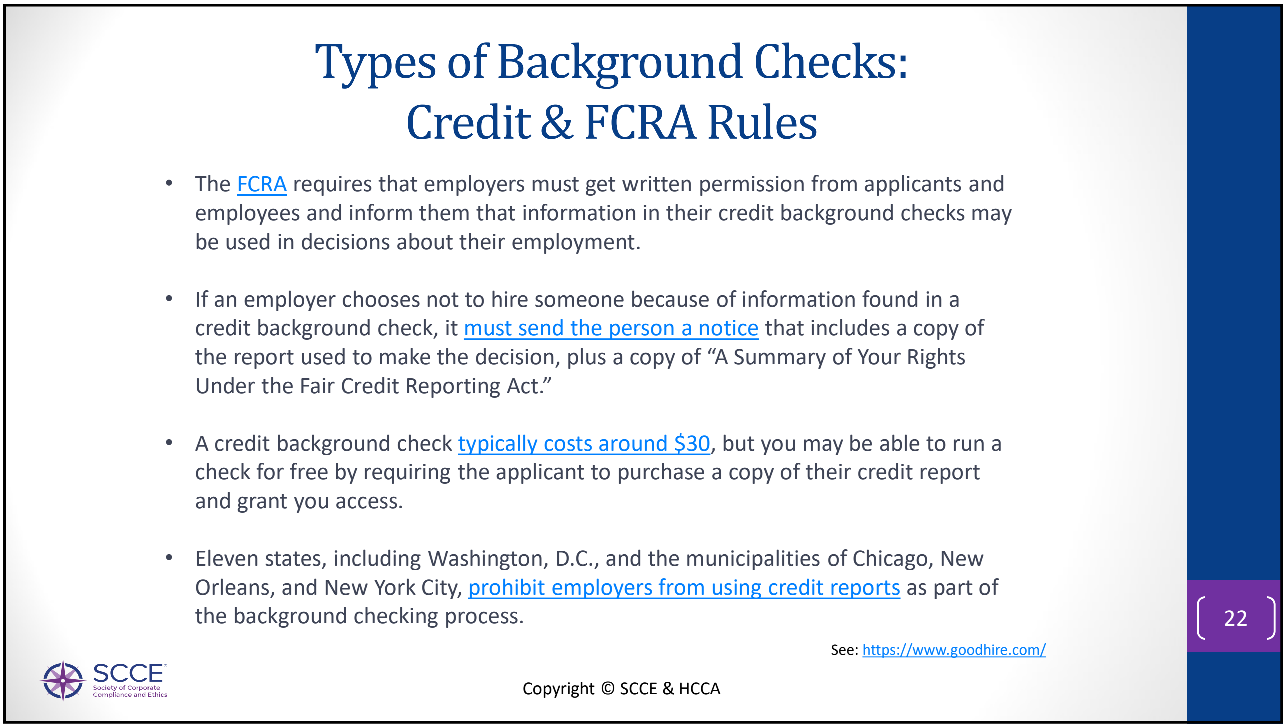
- A credit background check is a record of a person's credit-to-debt ratio and shows how someone has managed credit and bill payments in the past.

- Additionally, some jobs require a credit background check, especially for positions in the financial services industry where the employee would manage money, or has access to money on a daily basis.

- A candidate's financial background is important in an area where fraud and embezzlement are possible. Employers may consider someone with poor credit, tax liens, or significant debt to be more tempted to take advantage of the employer's trust.

- With a credit background check, the person or company running the report can view the applicant's credit report but not their credit score. A credit report shows the applicant's full credit history, including:
  - Payment history
  - Civil judgments
  - Tax liens
  - Bankruptcies
  - Unpaid bills in collections
  - Recent credit inquiries

See: https://www.goodhire.com/



Types of Background Checks: Credit & FCRA Rules

- The FCRA requires that employers must get written permission from applicants and employees and inform them that information in their credit background checks may be used in decisions about their employment.

- If an employer chooses not to hire someone because of information found in a credit background check, it must send the person a notice that includes a copy of the report used to make the decision, plus a copy of "A Summary of Your Rights Under the Fair Credit Reporting Act."

- A credit background check typically costs around $30, but you may be able to run a check for free by requiring the applicant to purchase a copy of their credit report and grant you access.

- Eleven states, including Washington, D.C., and the municipalities of Chicago, New Orleans, and New York City, prohibit employers from using credit reports as part of the background checking process.

See: https://www.goodhire.com/

Types of Background Checks: Professional License

- A professional license background check, or an education verification check, verifies that the applicant does indeed possess a valid license as claimed. This is an important step in helping to protect the employer from negligent hiring claims.
- Certain industries rely on professional licenses to ensure that people working in that industry have the experience, knowledge, and credentials required to perform the job.
- For professional license background checks, background screening companies typically contact the applicable industry or state licensing board to verify that the license is held and hasn't lapsed or expired, that the license is in good standing and that there are no restrictions or violations associated with the license.
- Industries that require a professional license background check include:
  - The financial services industry, including financial planning, real estate, accounting, banking, and insurance
  - Home contractors, including plumbers, builders, and electricians
  - Education, including teachers, professors, and administrators

23

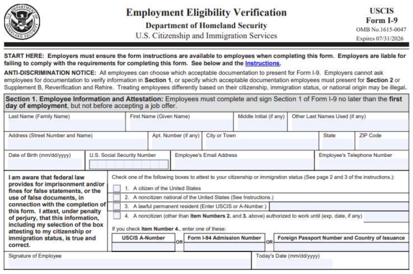
See: https://www.goodhire.com/

SCCE Society of Corporate Compliance and Ethics

23

Types of Background Checks: E-Verify

- E-Verify is used by employers to verify the identity and employment eligibility of newly hired employees.
- The online check compares information from the US Citizenship and Immigration Services (USCIS) I-9 form that new employees are required to complete with government records to confirm that the employee is authorized to work in the U.S. This I-9 form is valid through 7/31/2026.



Employment Eligibility Verification
Department of Homeland Security
U.S. Citizenship and Immigration Services

USCIS
Form I-9
OMB No.1615-0047
Expires 07/31/2026

START HERE: Employers must ensure the form instructions are available to employees when completing this form. Employers are liable for failing to comply with the requirements for completing this form. See below and the Instructions.

ANTI-DISCRIMINATION NOTICE: All employees can choose which acceptable documentation to present for Form I-9. Employers cannot ask employees for documentation to verify information in **Section 1**, or specify which acceptable documentation employees must present for **Section 2** or Supplement B, Reverification and Rehire. Treating employees differently based on their citizenship, immigration status, or national origin may be illegal.

Section 1. Employee Information and Attestation: Employees must complete and sign Section 1 of Form I-9 no later than the **first day of employment**, but not before accepting a job offer.

Last Name (Family Name) | First Name (Given Name) | Middle Initial (if any) | Other Last Names Used (if any)

Address (Street Number and Name) | Apt. Number (if any) | City or Town | State | ZIP Code

Date of Birth (mm/dd/yyyy) | U.S. Social Security Number | Employee's Email Address | Employee's Telephone Number

I am aware that federal law provides for imprisonment and/or fines for false statements, or the use of false documents, in connection with the completion of this form. I attest, under penalty of perjury, that this information, including my selection of the box attesting to my citizenship or immigration status, is true and correct.

Check one of the following boxes to attest to your citizenship or immigration status (See page 2 and 3 of the instructions.):

□ 1. A citizen of the United States
□ 2. A noncitizen national of the United States (See Instructions.)
□ 3. A lawful permanent resident (Enter USCIS or A-Number.)
□ 4. A noncitizen (other than **Item Numbers 2.** and **3.** above) authorized to work until (exp. date, if any)

If you check **Item Number 4.**, enter one of these:

USCIS A-Number OR **Form I-94 Admission Number** OR **Foreign Passport Number and Country of Issuance**

Signature of Employee | Today's Date (mm/dd/yyyy)

See: https://www.uscis.gov/i-9

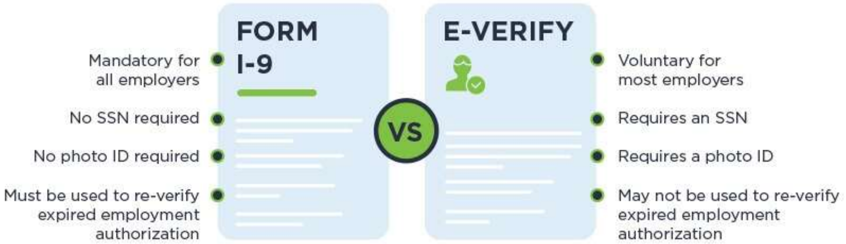
24

SCCE Society of Corporate Compliance and Ethics

24

Types of Background Checks: I-9 v. E-Verify

Form I-9 and E-Verify are similar in their purpose, but E-Verify takes the process one step further to make sure new employees are authorized to work in the country. Here are some key differences between the two:


FORM I-9
E-VERIFY
VS
Mandatory for all employers
No SSN required
No photo ID required
Must be used to re-verify expired employment authorization
Voluntary for most employers
Requires an SSN
Requires a photo ID
May not be used to re-verify expired employment authorization

See: https://www.goodhire.com/

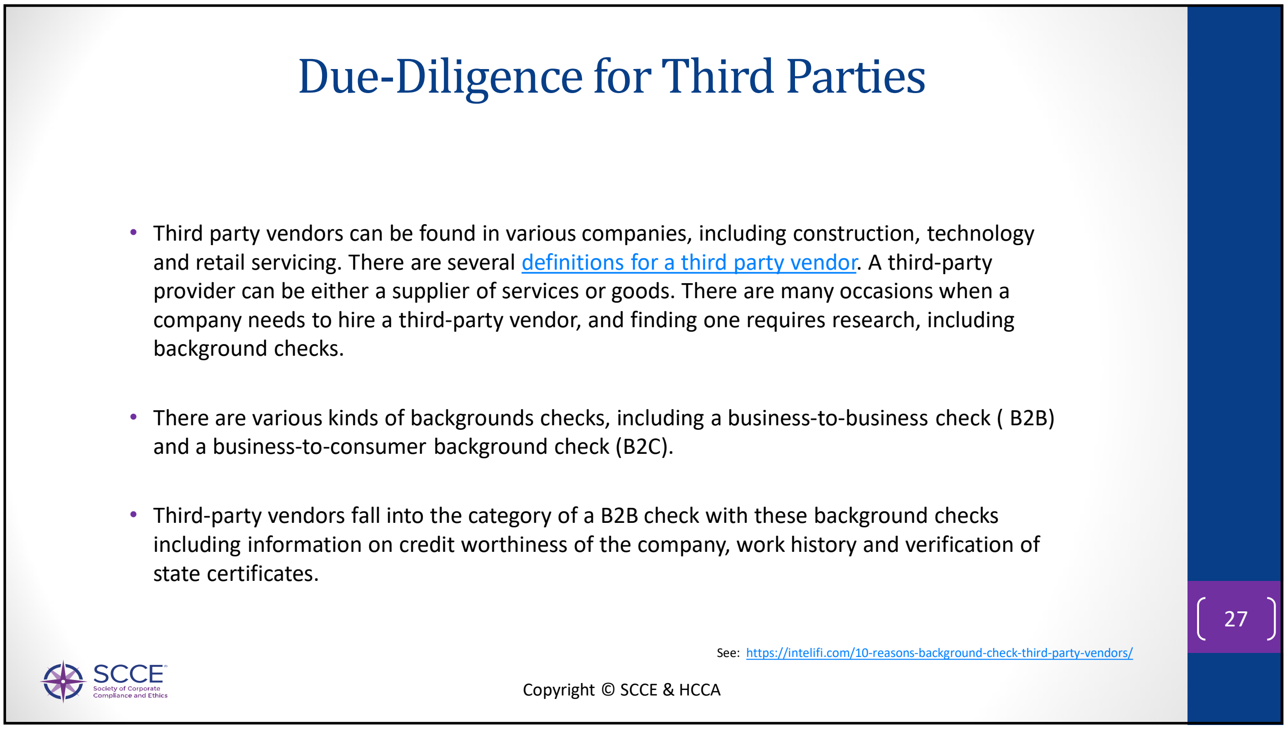
Considerations when Evaluating & Promoting Employees

- **Background Checks Work to Improve Trust and Safety.** The purpose of background checks is to provide helpful information about a person's history to assess whether they may pose a threat to the organization or to others and whether they are generally trustworthy—or not.

- **While a person's past actions do not necessarily predict their future actions, background checks are increasingly common** and are meant to help create more trust and safety in society and the workplace.

- **When might an organization complete a background check (*subject to applicable laws or *employee union rules):**
  - Preplacement/Preemployment
  - Promotion
  - Job change within the same company
  - Interdepartmental transfer
  - Inter-company transfer
  - For cause and/or investigations

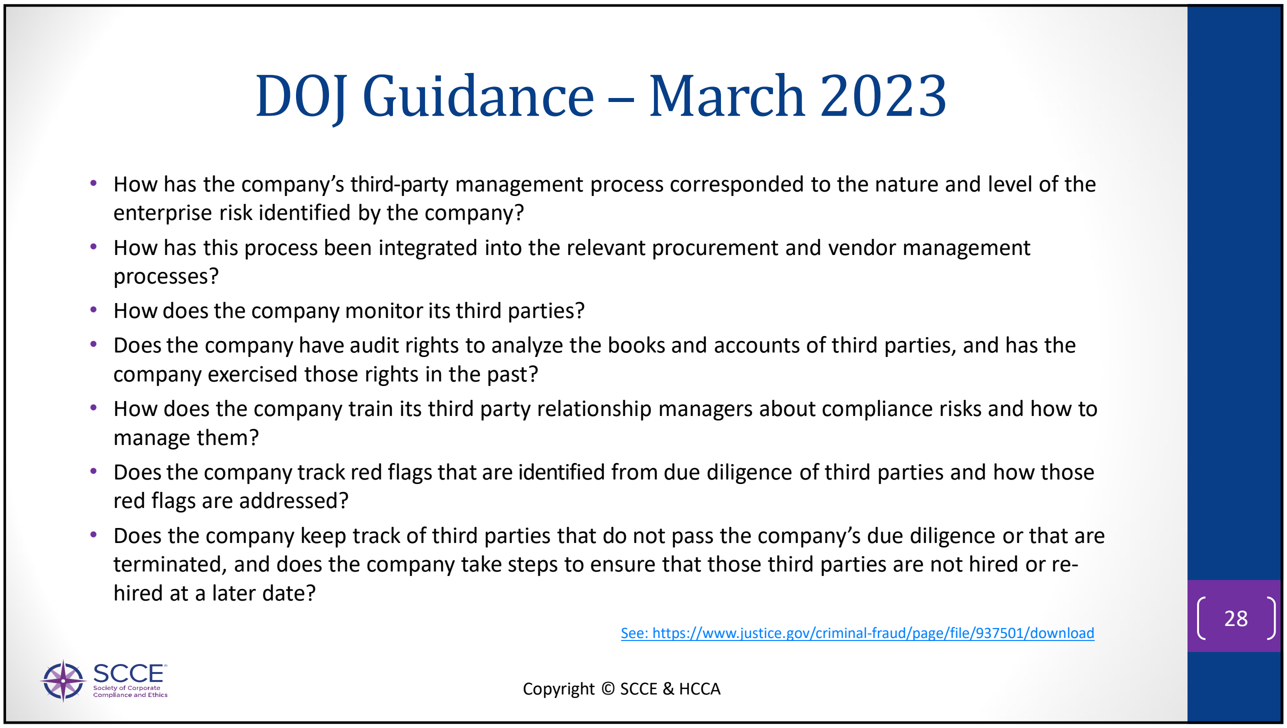
See: https://www.goodhire.com/



Due-Diligence for Third Parties

- Third party vendors can be found in various companies, including construction, technology and retail servicing. There are several definitions for a third party vendor. A third-party provider can be either a supplier of services or goods. There are many occasions when a company needs to hire a third-party vendor, and finding one requires research, including background checks.
- There are various kinds of backgrounds checks, including a business-to-business check (B2B) and a business-to-consumer background check (B2C).
- Third-party vendors fall into the category of a B2B check with these background checks including information on credit worthiness of the company, work history and verification of state certificates.

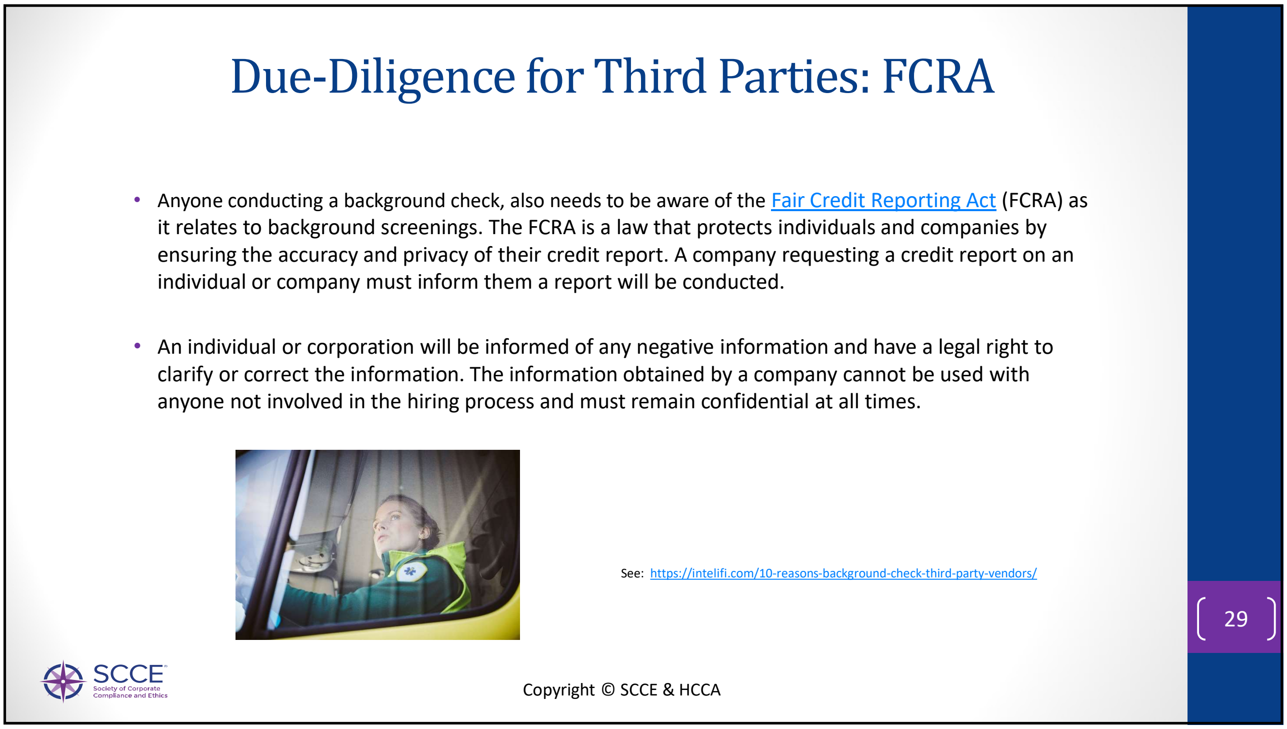
See: https://intelifi.com/10-reasons-background-check-third-party-vendors/



DOJ Guidance – March 2023

- How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company?
- How has this process been integrated into the relevant procurement and vendor management processes?
- How does the company monitor its third parties?
- Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past?
- How does the company train its third party relationship managers about compliance risks and how to manage them?
- Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed?
- Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date?

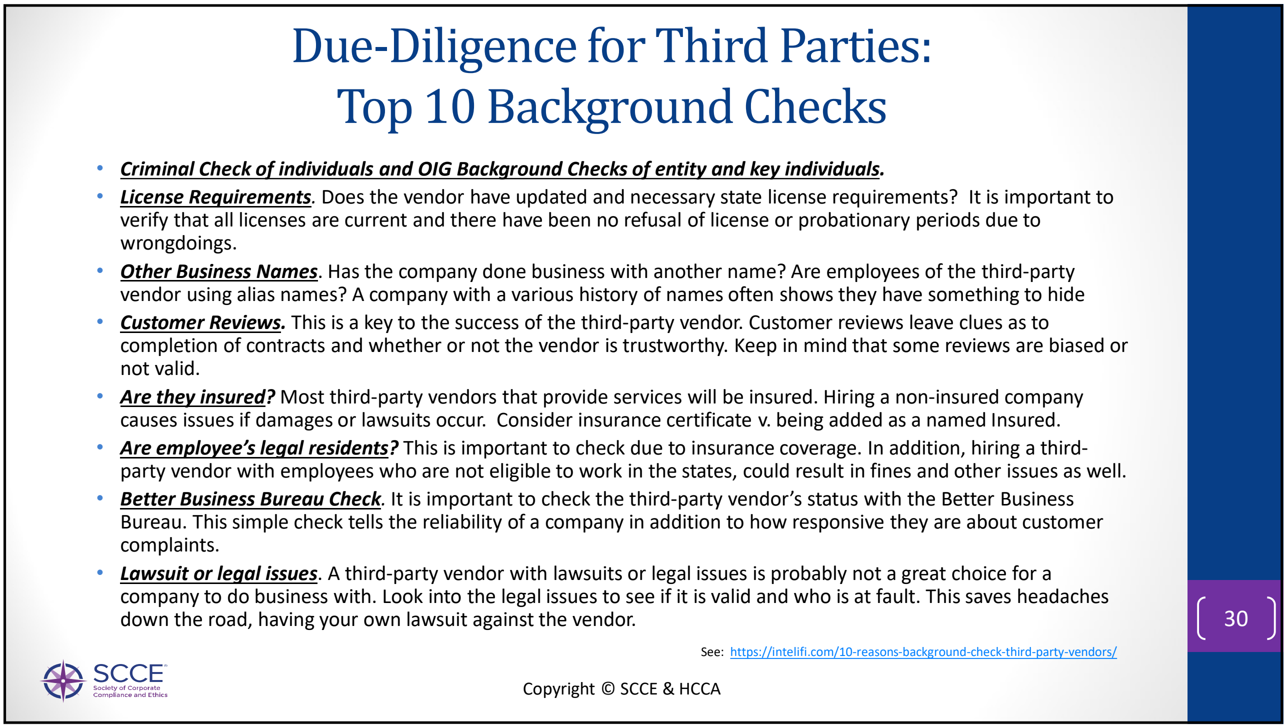
See: https://www.justice.gov/criminal-fraud/page/file/937501/download



Due-Diligence for Third Parties: FCRA

- Anyone conducting a background check, also needs to be aware of the Fair Credit Reporting Act (FCRA) as it relates to background screenings. The FCRA is a law that protects individuals and companies by ensuring the accuracy and privacy of their credit report. A company requesting a credit report on an individual or company must inform them a report will be conducted.
- An individual or corporation will be informed of any negative information and have a legal right to clarify or correct the information. The information obtained by a company cannot be used with anyone not involved in the hiring process and must remain confidential at all times.

See: https://intelifi.com/10-reasons-background-check-third-party-vendors/



Due-Diligence for Third Parties: Top 10 Background Checks

- ***Criminal Check of individuals and OIG Background Checks of entity and key individuals.***
- ***License Requirements***. Does the vendor have updated and necessary state license requirements? It is important to verify that all licenses are current and there have been no refusal of license or probationary periods due to wrongdoings.
- ***Other Business Names***. Has the company done business with another name? Are employees of the third-party vendor using alias names? A company with a various history of names often shows they have something to hide
- ***Customer Reviews.*** This is a key to the success of the third-party vendor. Customer reviews leave clues as to completion of contracts and whether or not the vendor is trustworthy. Keep in mind that some reviews are biased or not valid.
- ***Are they insured?*** Most third-party vendors that provide services will be insured. Hiring a non-insured company causes issues if damages or lawsuits occur. Consider insurance certificate v. being added as a named Insured.
- ***Are employee's legal residents?*** This is important to check due to insurance coverage. In addition, hiring a third-party vendor with employees who are not eligible to work in the states, could result in fines and other issues as well.
- ***Better Business Bureau Check***. It is important to check the third-party vendor's status with the Better Business Bureau. This simple check tells the reliability of a company in addition to how responsive they are about customer complaints.
- ***Lawsuit or legal issues***. A third-party vendor with lawsuits or legal issues is probably not a great choice for a company to do business with. Look into the legal issues to see if it is valid and who is at fault. This saves headaches down the road, having your own lawsuit against the vendor.

See: https://intelifi.com/10-reasons-background-check-third-party-vendors/

DoJ Guidance – March 2023

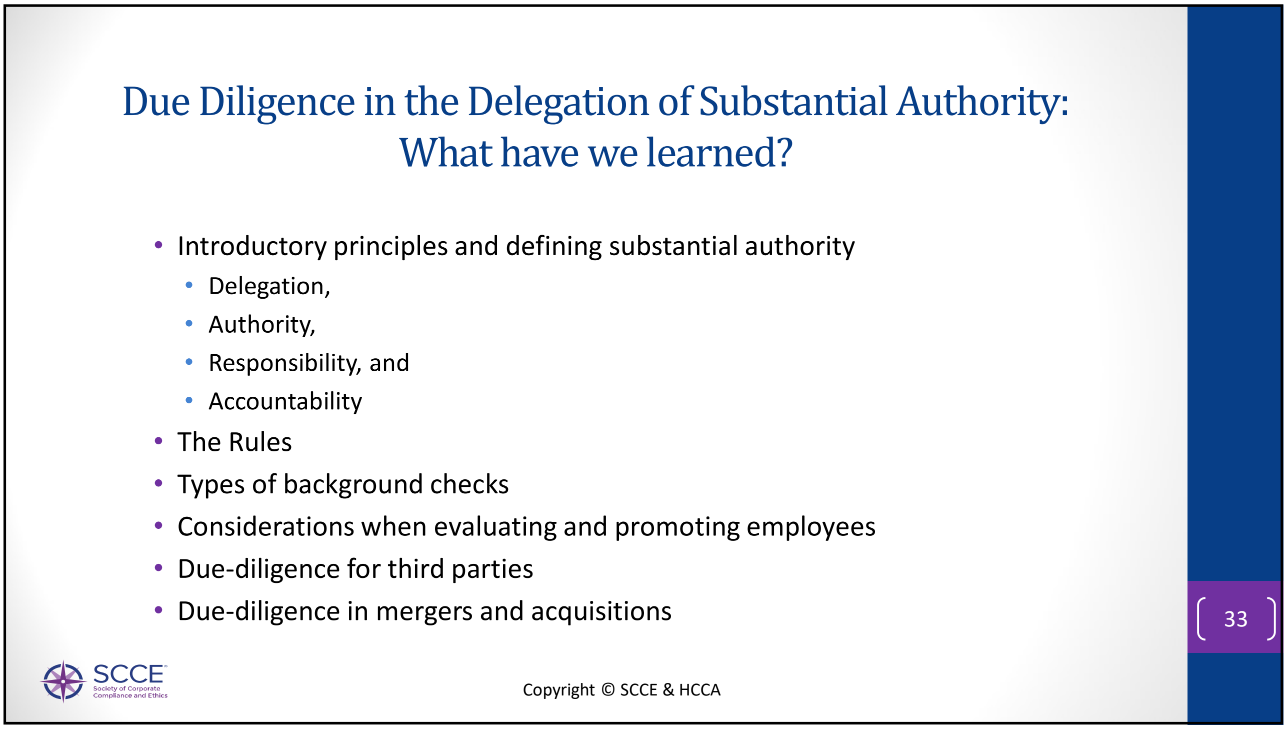
- What is the M&A due diligence process generally?
- Was the company able to complete pre-acquisition due diligence and, if not, why not?
- How has the compliance function been integrated into the merger, acquisition, and integration process?
- What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process?
- What has been the company's process for implementing compliance policies and procedures, and conducting post- acquisition audits, at newly acquired entities?

See: https://www.justice.gov/criminal-fraud/page/file/937501/download

Due-Diligence: Rescreening Employees in Mergers & Acquisitions

- **Rescreening of employees** is always a good idea, especially when undergoing a merger or acquisition. Unfortunately, many companies adopt background check policies that only examine new hires.
- **This fails to consider illegal behaviors during the course of employment.** An employee's ability to get caught breaking the law does not end once hired by his or her original employer.
- **A new employee gained through a merger or acquisition can become a risk when the employee comes with a criminal record, drug use, or falsified education credentials.** What if you're acquiring an employee through the merger or acquisition who committed fraud? You might be bringing the human equivalent of a computer virus inside your organization.
- **Rescreening of employees during M&A protects your company's image as well as profitability.** Reduce the risk of employee turnover and associated costs of replacement with comprehensive employee rescreening that includes all elements of the background checks policy of parent/purchasing organization.

See: https://baradainc.com/background-checks-in-mergers-and-acquisitions/

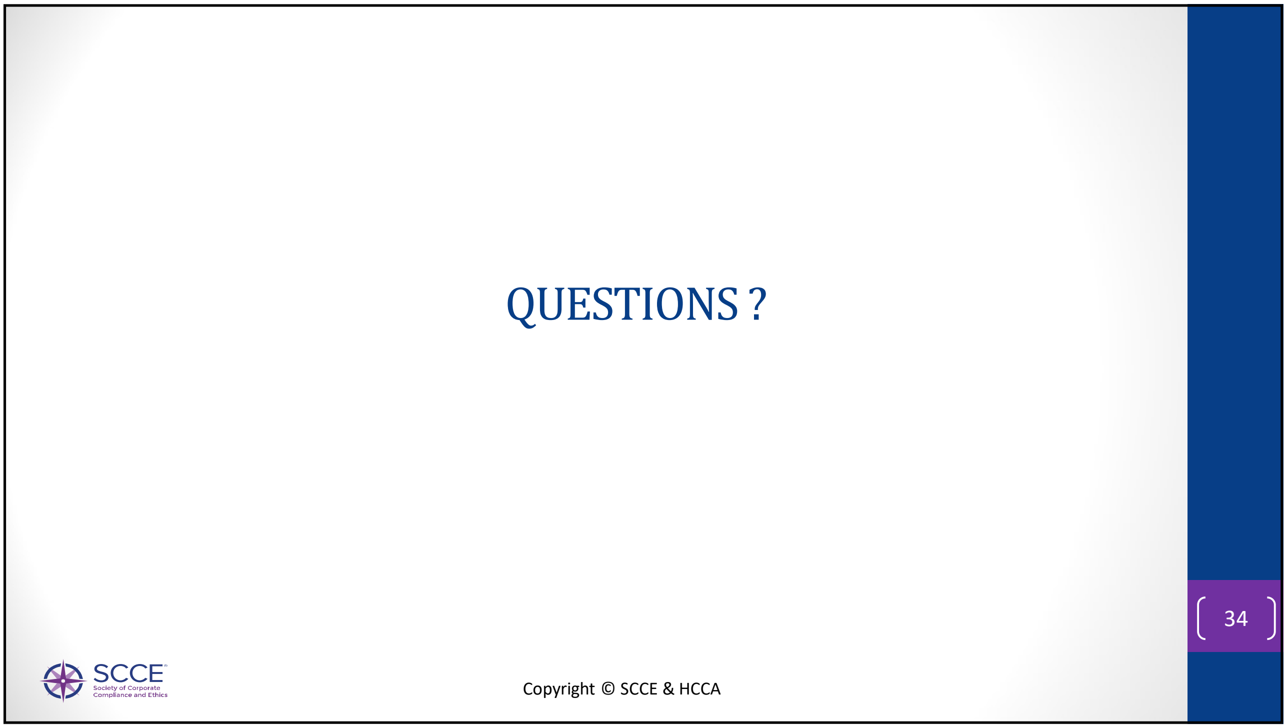


Due Diligence in the Delegation of Substantial Authority: What have we learned?

- Introductory principles and defining substantial authority
  - Delegation,
  - Authority,
  - Responsibility, and
  - Accountability
- The Rules
- Types of background checks
- Considerations when evaluating and promoting employees
- Due-diligence for third parties
- Due-diligence in mergers and acquisitions

33

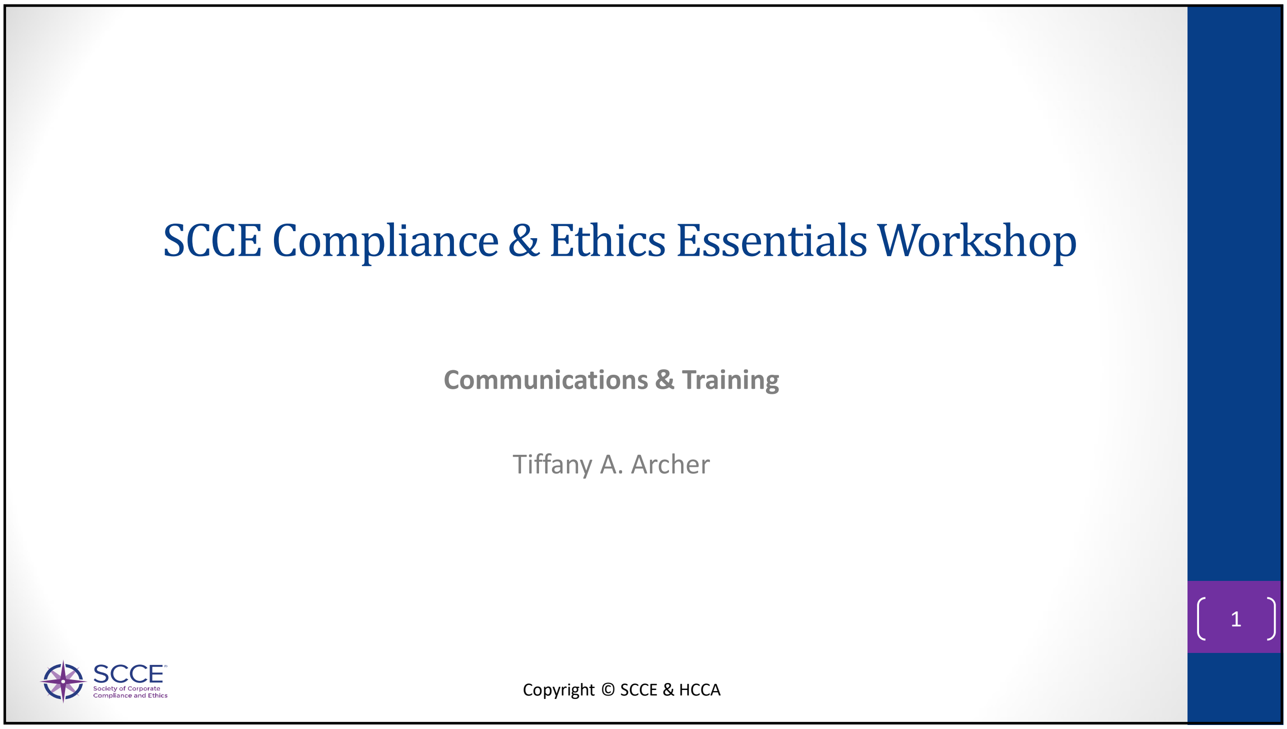
33



QUESTIONS ?

34

34



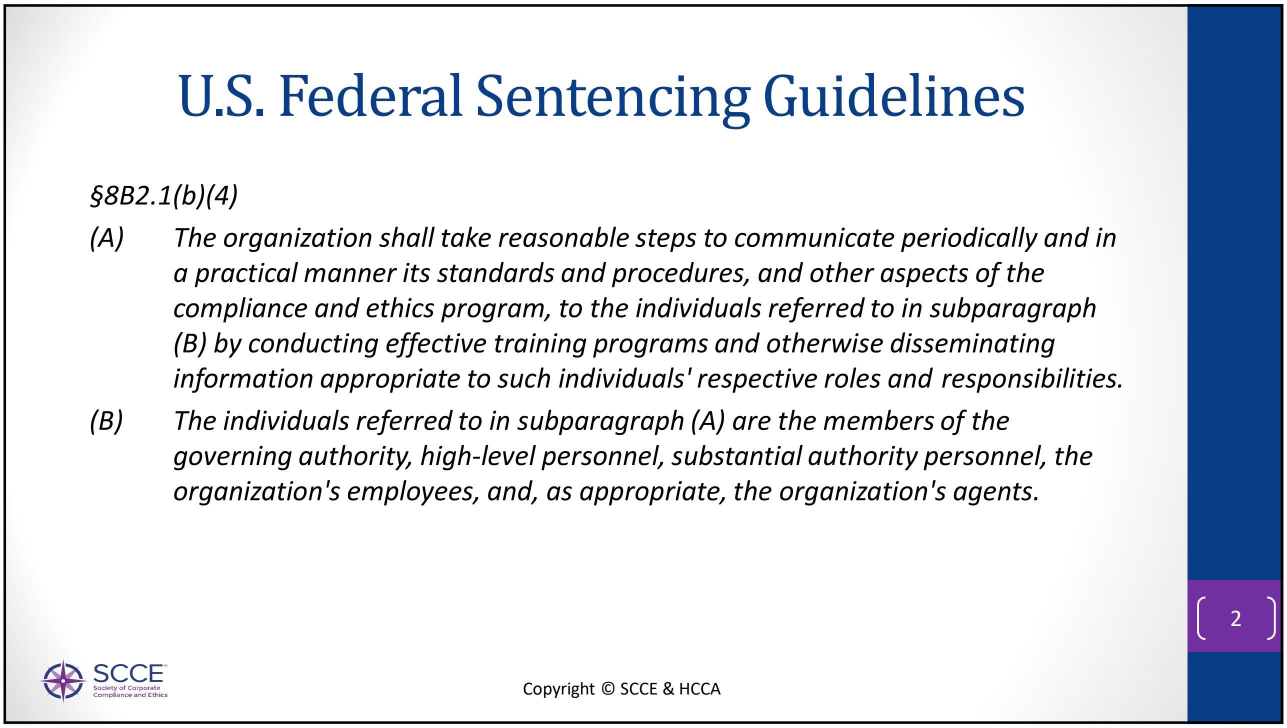
SCCE Compliance & Ethics Essentials Workshop

Communications & Training

Tiffany A. Archer

1

1



U.S. Federal Sentencing Guidelines

§8B2.1(b)(4)

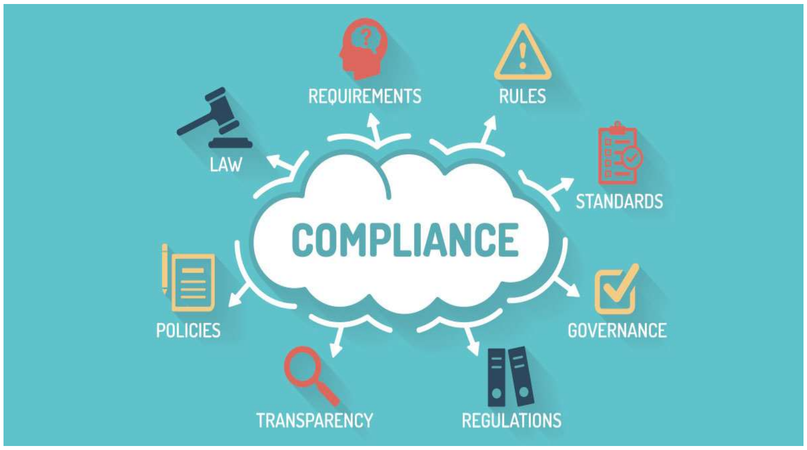
(A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

2

2

What does a "Compliance Officer" really do?



SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

3

3

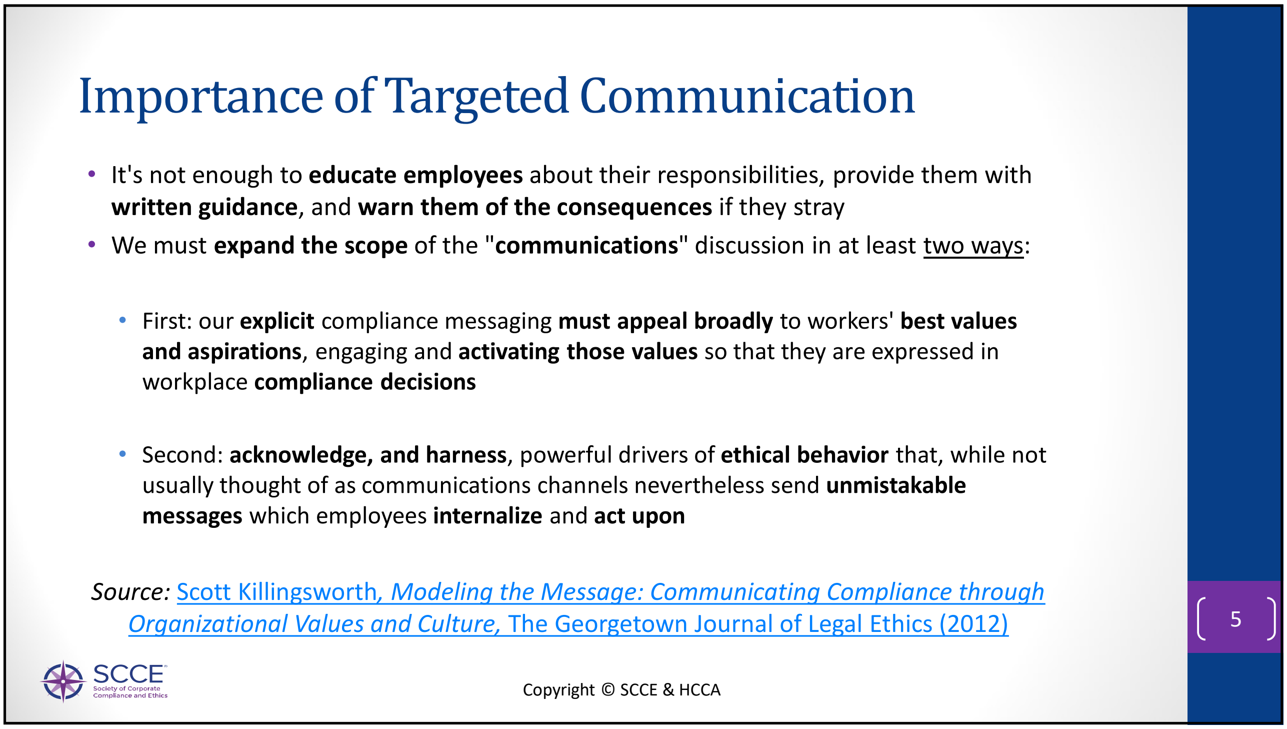
The Problem: A Not So Unfamiliar Training Scenario

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

4

4



Importance of Targeted Communication

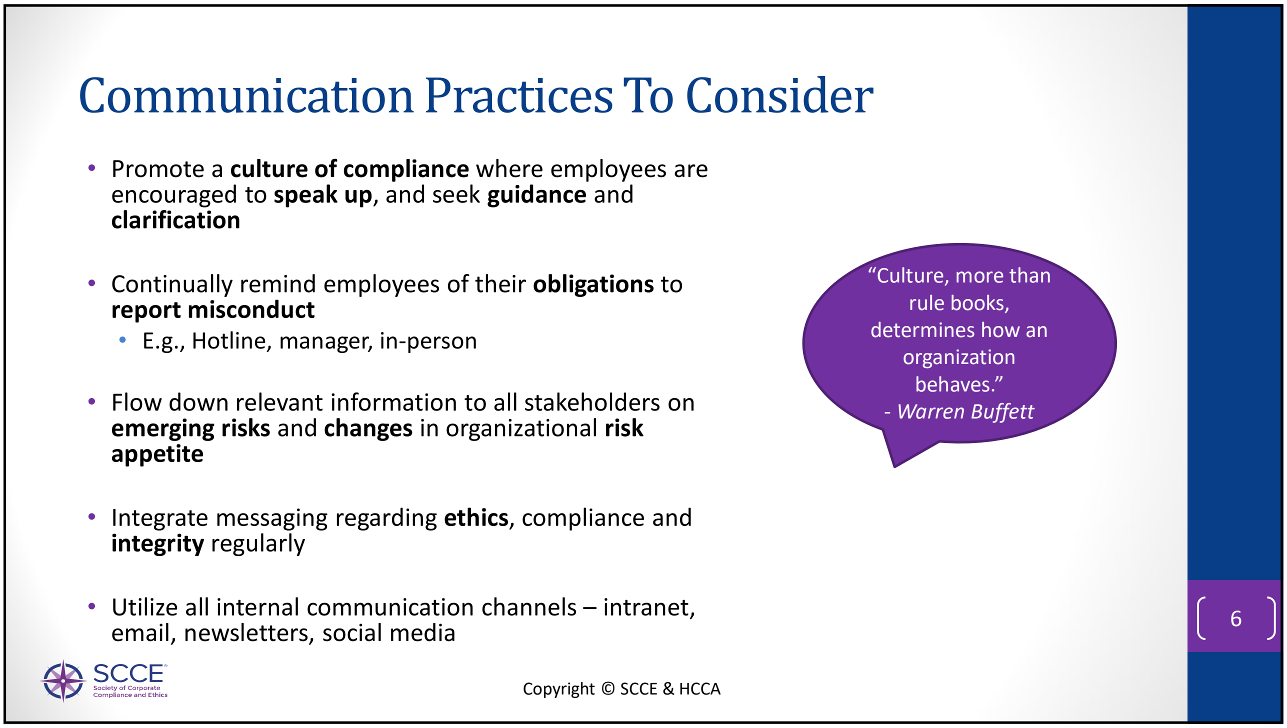
- It's not enough to **educate employees** about their responsibilities, provide them with **written guidance**, and **warn them of the consequences** if they stray
- We must **expand the scope** of the "**communications**" discussion in at least <u>two ways</u>:
  - First: our **explicit** compliance messaging **must appeal broadly** to workers' **best values and aspirations**, engaging and **activating those values** so that they are expressed in workplace **compliance decisions**
  - Second: **acknowledge, and harness**, powerful drivers of **ethical behavior** that, while not usually thought of as communications channels nevertheless send **unmistakable messages** which employees **internalize** and **act upon**

Source: Scott Killingsworth, *Modeling the Message: Communicating Compliance through Organizational Values and Culture,* The Georgetown Journal of Legal Ethics (2012)

SCCE Society of Corporate Compliance and Ethics

5

5



Communication Practices To Consider

- Promote a **culture of compliance** where employees are encouraged to **speak up**, and seek **guidance** and **clarification**
- Continually remind employees of their **obligations** to **report misconduct**
  - E.g., Hotline, manager, in-person
- Flow down relevant information to all stakeholders on **emerging risks** and **changes** in organizational **risk appetite**
- Integrate messaging regarding **ethics**, compliance and **integrity** regularly
- Utilize all internal communication channels – intranet, email, newsletters, social media

"Culture, more than rule books, determines how an organization behaves."
- *Warren Buffett*

SCCE Society of Corporate Compliance and Ethics

6

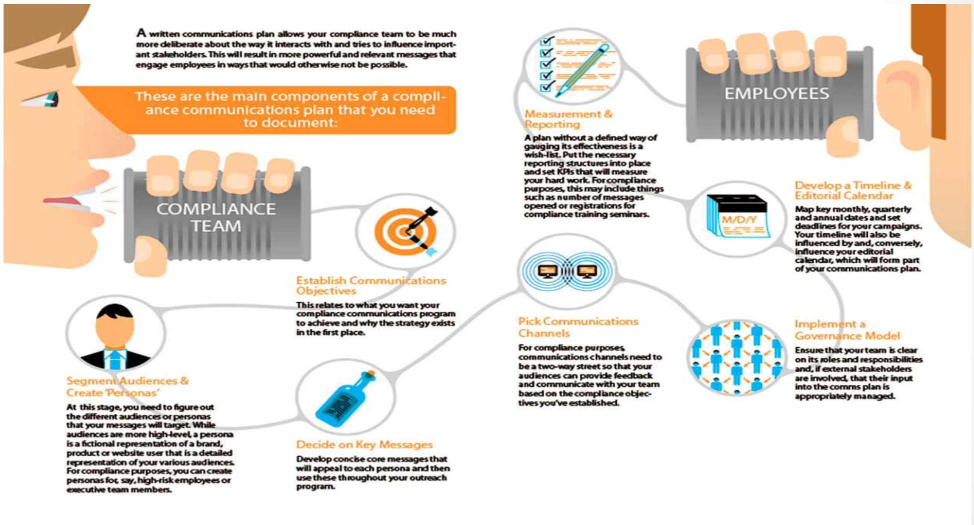
6

Communication Practices To Consider

- **Tone From the Top & Middle**: Messaging and involvement from **Senior Leaders** and **Management** is paramount
- Employ a **"cascade"** approach to ensure messaging is **flowing down** to employees at all levels
- Multinational organizations should consider **cultural nuances** and **practices** to ensure appropriateness
- Critical that employees have **ready access** to guidance around **policies**, **procedures** and **controls**

> "The more consistent and pervasive the messaging within an organization – explicit messaging and, crucially, messaging through behavior –the more likely employees will internalize the corresponding values, principles, will frame decisions in terms of those values, and will put them in action."
>
> *- Scott Killingsworth*

Developing A Communication Plan & Strategy



A written communications plan allows your compliance team to be much more deliberate about the way it interacts with and tries to influence important stakeholders. This will result in more powerful and relevant messages that engage employees in ways that would otherwise not be possible.

These are the main components of a compliance communications plan that you need to document:

Establish Communications Objectives

This relates to what you want your compliance communications program to achieve and why the strategy exists in the first place.

Segment Audiences & Create 'Personas'

At this stage, you need to figure out the different audiences or personas that your messages will target. While audiences are more high-level, a persona is a fictional representation of a brand, product or website user that is a detailed representation of your various audiences. For compliance purposes, you can create personas for, say, high-risk employees or executive team members.

Decide on Key Messages

Develop concise core messages that will appeal to each persona and then use these throughout your outreach program.

Pick Communications Channels

For compliance purposes, communications channels need to be a two-way street so that your audiences can provide feedback and communicate with your team based on the compliance objectives you've established.

Implement a Governance Model

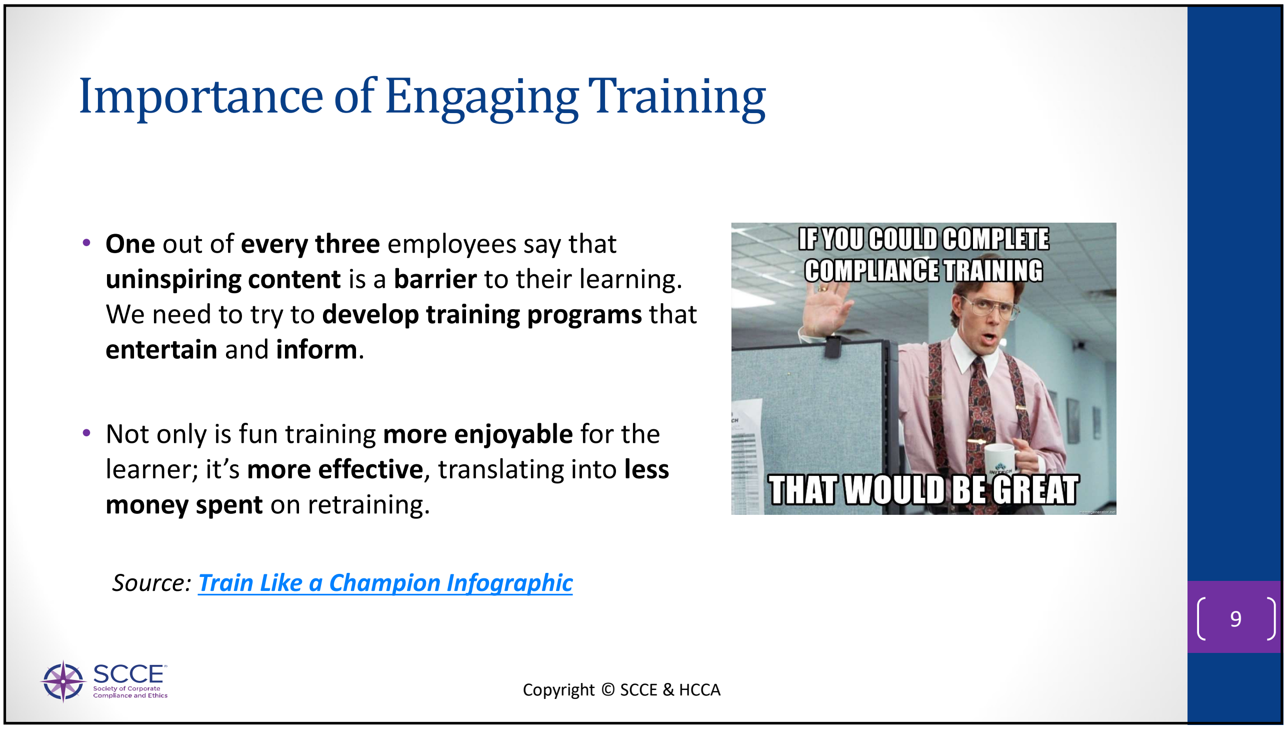
Ensure that your team is clear on its roles and responsibilities and, if external stakeholders are involved, that their input into the comms plan is appropriately managed.

Develop a Timeline & Editorial Calendar

Map key monthly, quarterly and annual dates and set deadlines for your campaigns. Your timeline will also be influenced by and, conversely, influence your editorial calendar, which will form part of your communications plan.

Measurement & Reporting

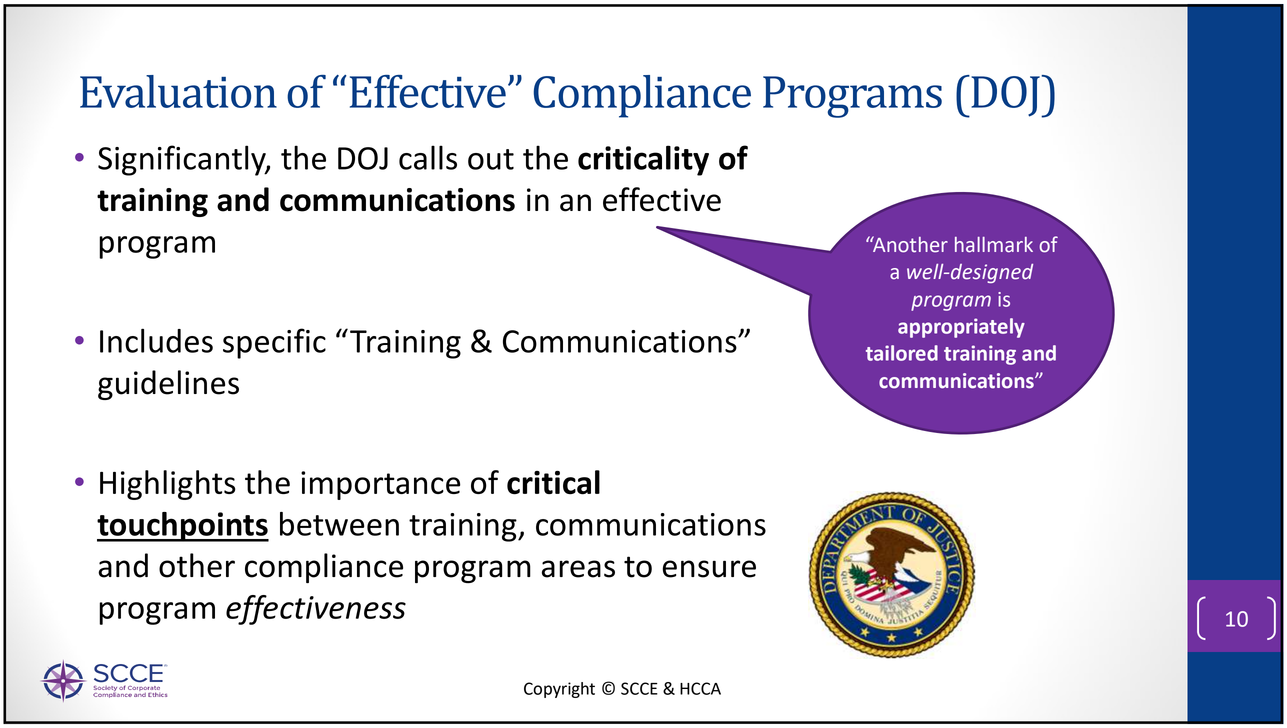
A plan without a defined way of gauging its effectiveness is a wish-list. Put the necessary reporting structures into place and set KPIs that will measure your hard work. For compliance purposes, this may include things such as number of messages opened or registrations for compliance training seminars.



Importance of Engaging Training

- **One** out of **every three** employees say that **uninspiring content** is a **barrier** to their learning. We need to try to **develop training programs** that **entertain** and **inform**.
- Not only is fun training **more enjoyable** for the learner; it's **more effective**, translating into **less money spent** on retraining.

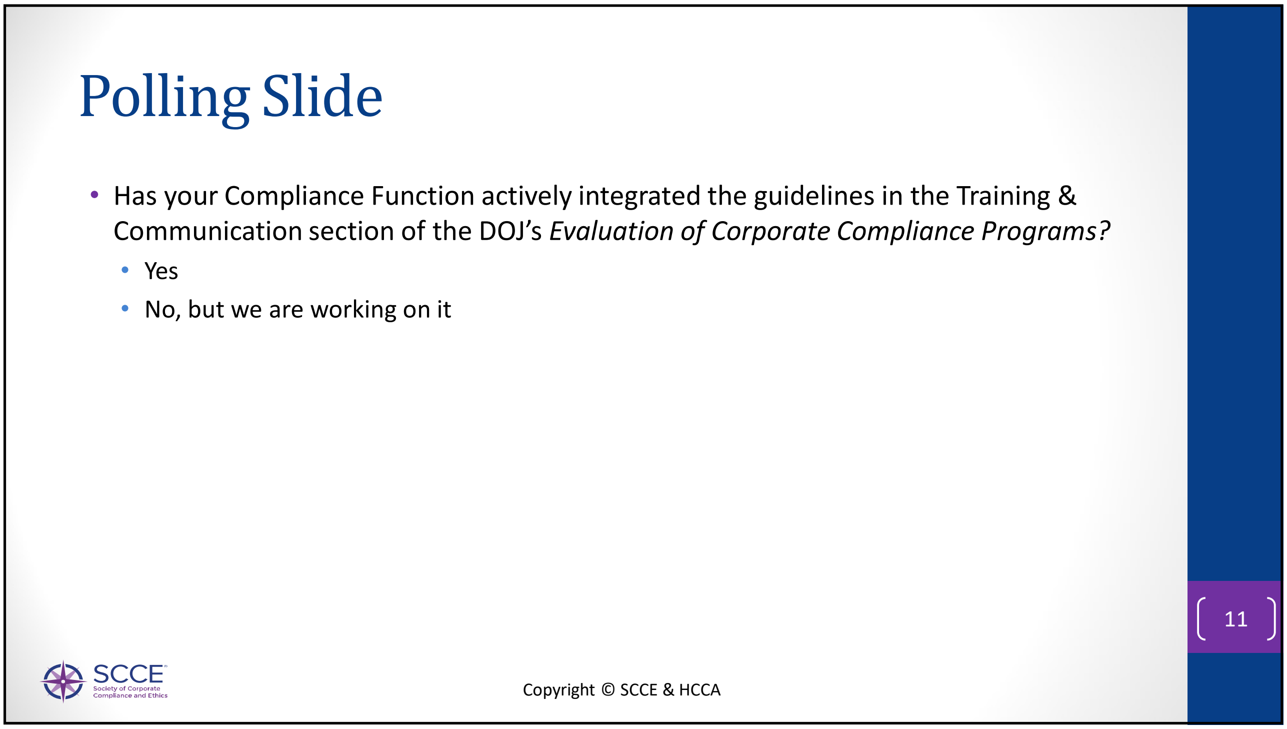
Source: ***Train Like a Champion Infographic***



Evaluation of "Effective" Compliance Programs (DOJ)

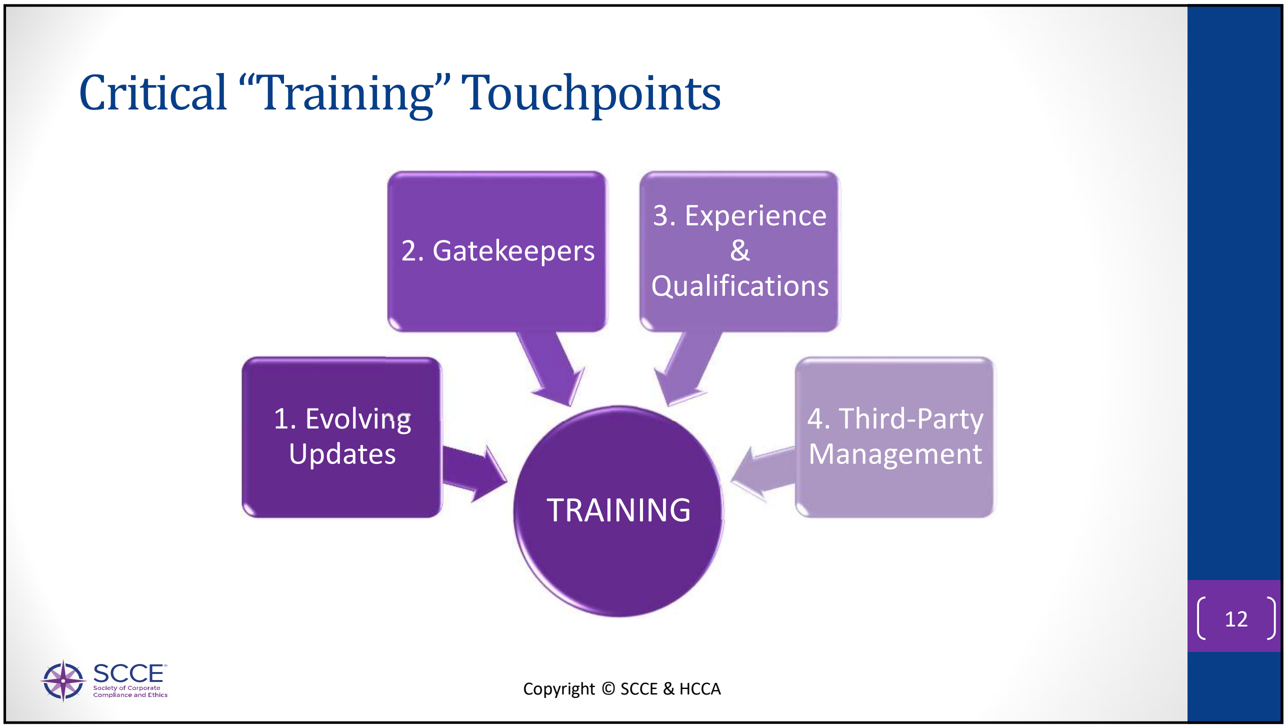
- Significantly, the DOJ calls out the **criticality of training and communications** in an effective program
- Includes specific "Training & Communications" guidelines
- Highlights the importance of **critical <u>touchpoints</u>** between training, communications and other compliance program areas to ensure program *effectiveness*

"Another hallmark of a *well-designed program* is **appropriately tailored training and communications**"



Polling Slide

- Has your Compliance Function actively integrated the guidelines in the Training & Communication section of the DOJ's *Evaluation of Corporate Compliance Programs?*
  - Yes
  - No, but we are working on it



Critical "Training" Touchpoints

2. Gatekeepers

3. Experience & Qualifications

1. Evolving Updates

TRAINING

4. Third-Party Management

"Training Touchpoint": Evolving Updates

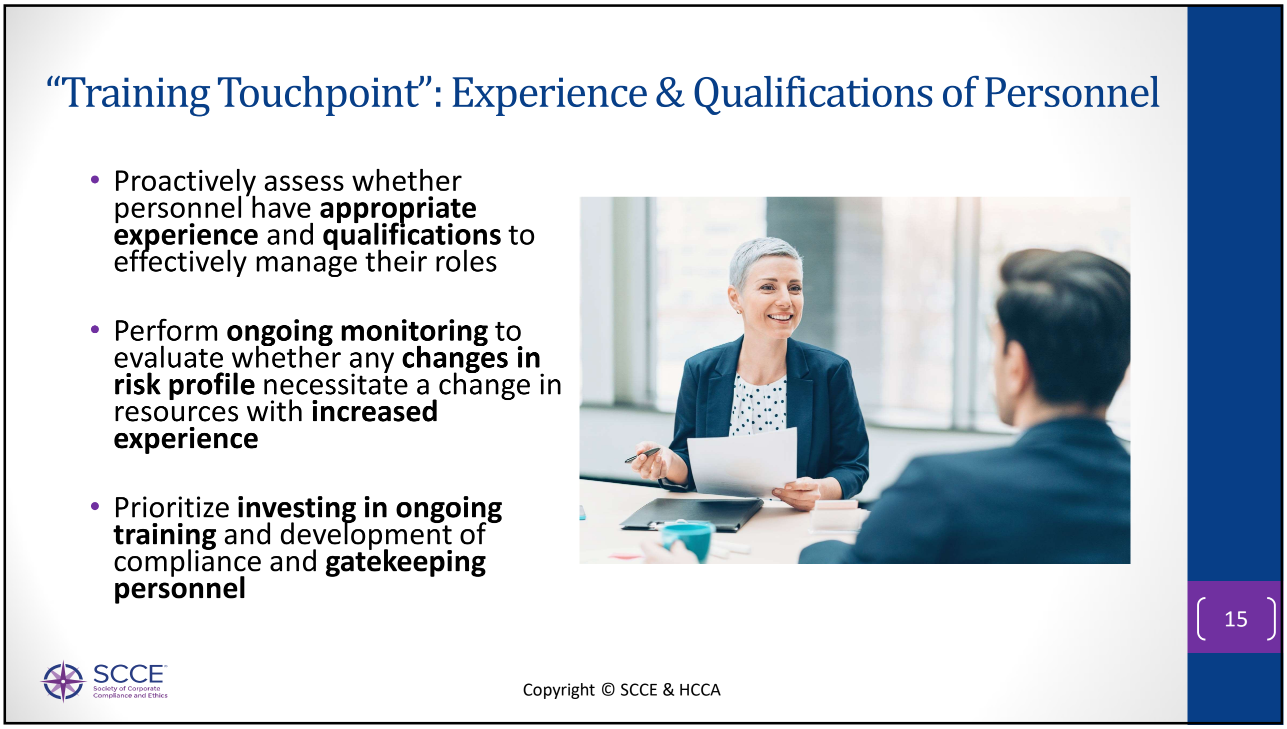
- Expectation of **continuous improvement** through awareness of company changes
- **Risk assessments** and **gap analyses** help inform which areas of risk may need to updated in policies/procedures or practices
- **Include findings** in training to keep employees apprised of **changes and expectations**

SCCE Society of Corporate Compliance and Ethics

"Training Touchpoint": Gatekeepers

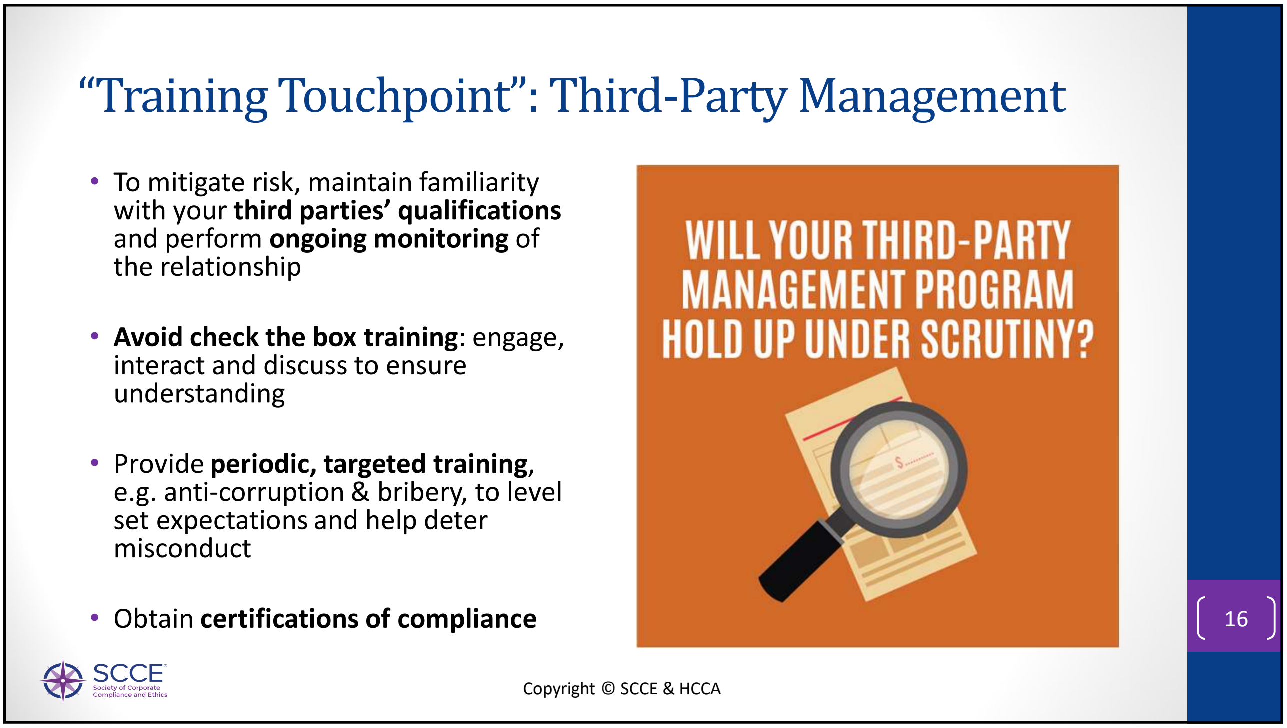
- Employees with **approval authority** or **certification responsibilitie**s should be well informed through targeted training
- Training geared towards **identifying misconduct** and procedures around **escalating concerns**
- Tailored training for **supervisory employees covering** areas where misconduct occurred

SCCE Society of Corporate Compliance and Ethics



“Training Touchpoint”: Experience & Qualifications of Personnel

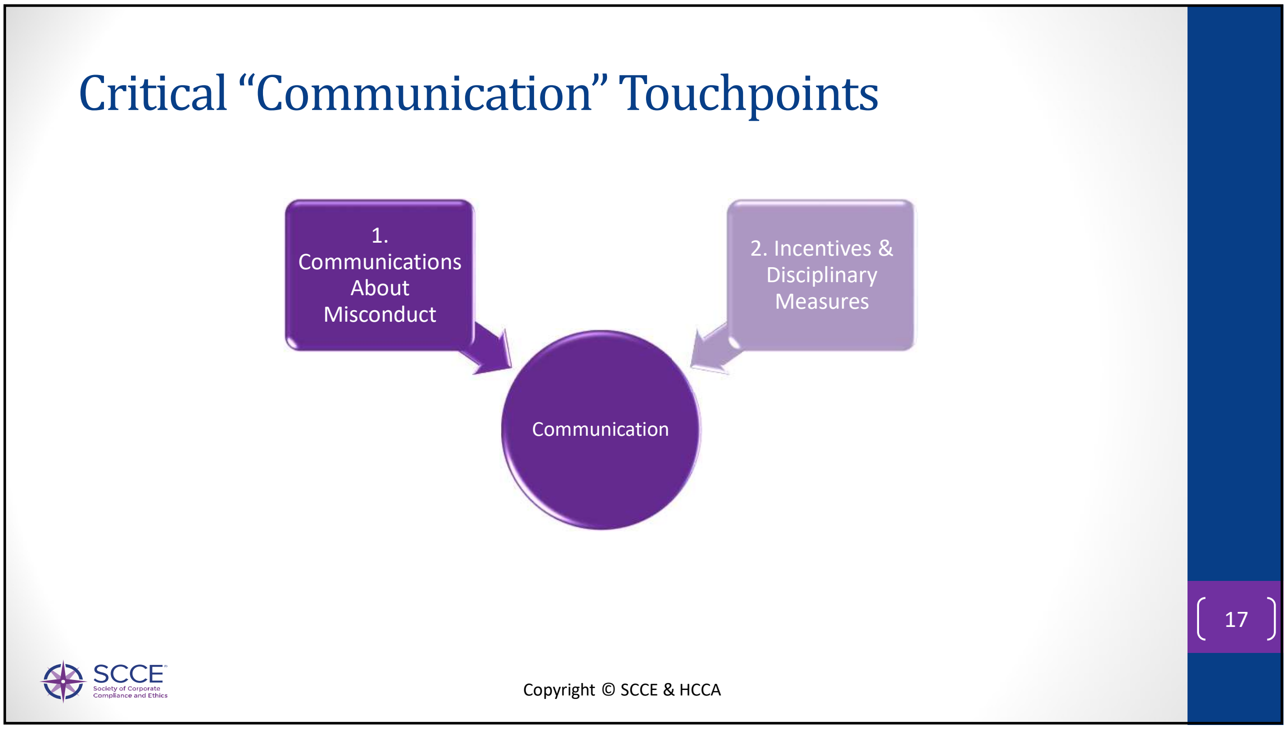
- Proactively assess whether personnel have **appropriate experience** and **qualifications** to effectively manage their roles
- Perform **ongoing monitoring** to evaluate whether any **changes in risk profile** necessitate a change in resources with **increased experience**
- Prioritize **investing in ongoing training** and development of compliance and **gatekeeping personnel**



“Training Touchpoint”: Third-Party Management

- To mitigate risk, maintain familiarity with your **third parties’ qualifications** and perform **ongoing monitoring** of the relationship
- **Avoid check the box training**: engage, interact and discuss to ensure understanding
- Provide **periodic, targeted training**, e.g. anti-corruption & bribery, to level set expectations and help deter misconduct
- Obtain **certifications of compliance**

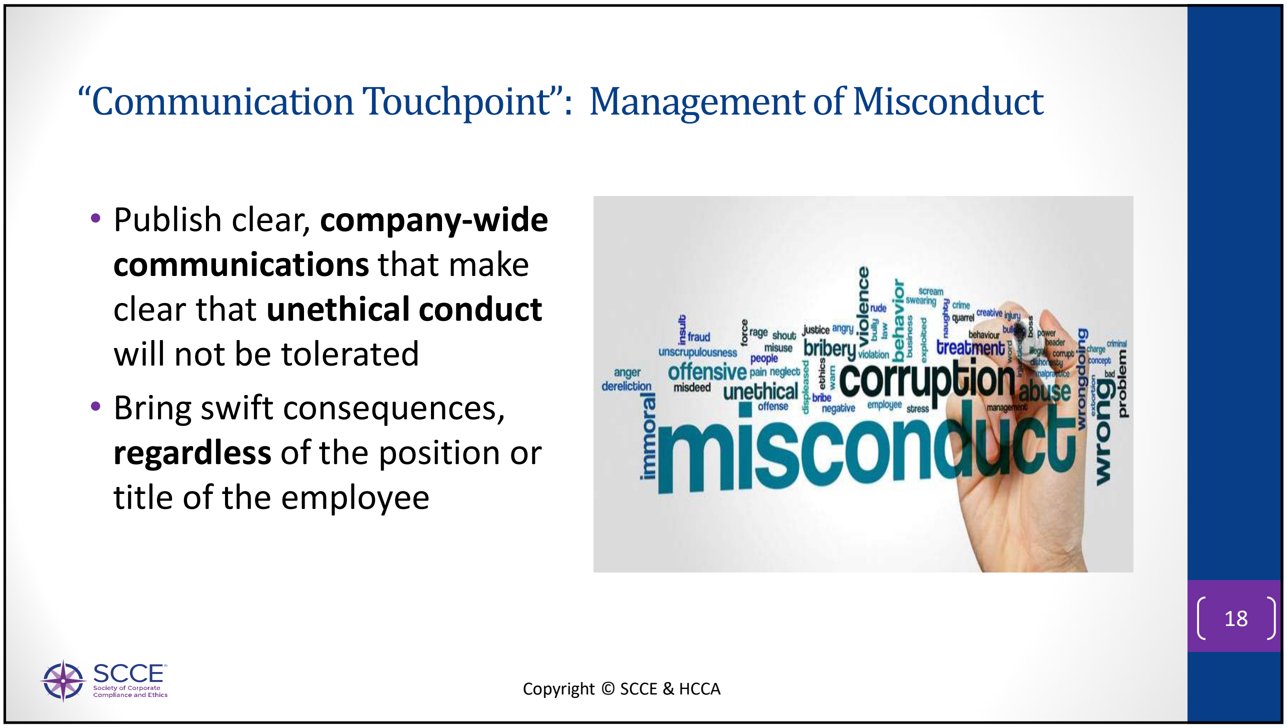
WILL YOUR THIRD-PARTY MANAGEMENT PROGRAM HOLD UP UNDER SCRUTINY?
SCCE
Society of Corporate Compliance and Ethics



Critical "Communication" Touchpoints

1. Communications About Misconduct
2. Incentives & Disciplinary Measures
Communication

SCCE Society of Corporate Compliance and Ethics

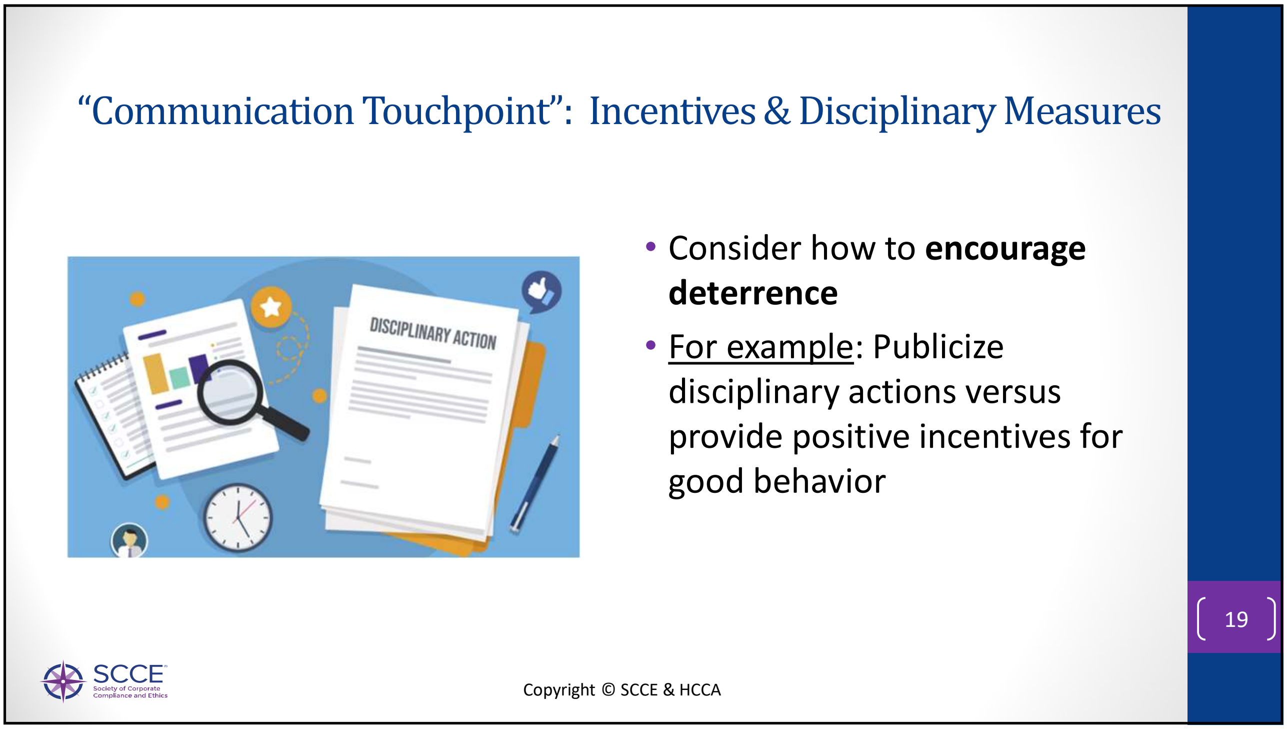


"Communication Touchpoint": Management of Misconduct

- Publish clear, **company-wide communications** that make clear that **unethical conduct** will not be tolerated
- Bring swift consequences, **regardless** of the position or title of the employee

misconduct
corruption
abuse
unethical
offensive
bribery
treatment
violence
behavior
immoral
wrong
wrongdoing
problem
fraud
anger
dereliction

SCCE Society of Corporate Compliance and Ethics



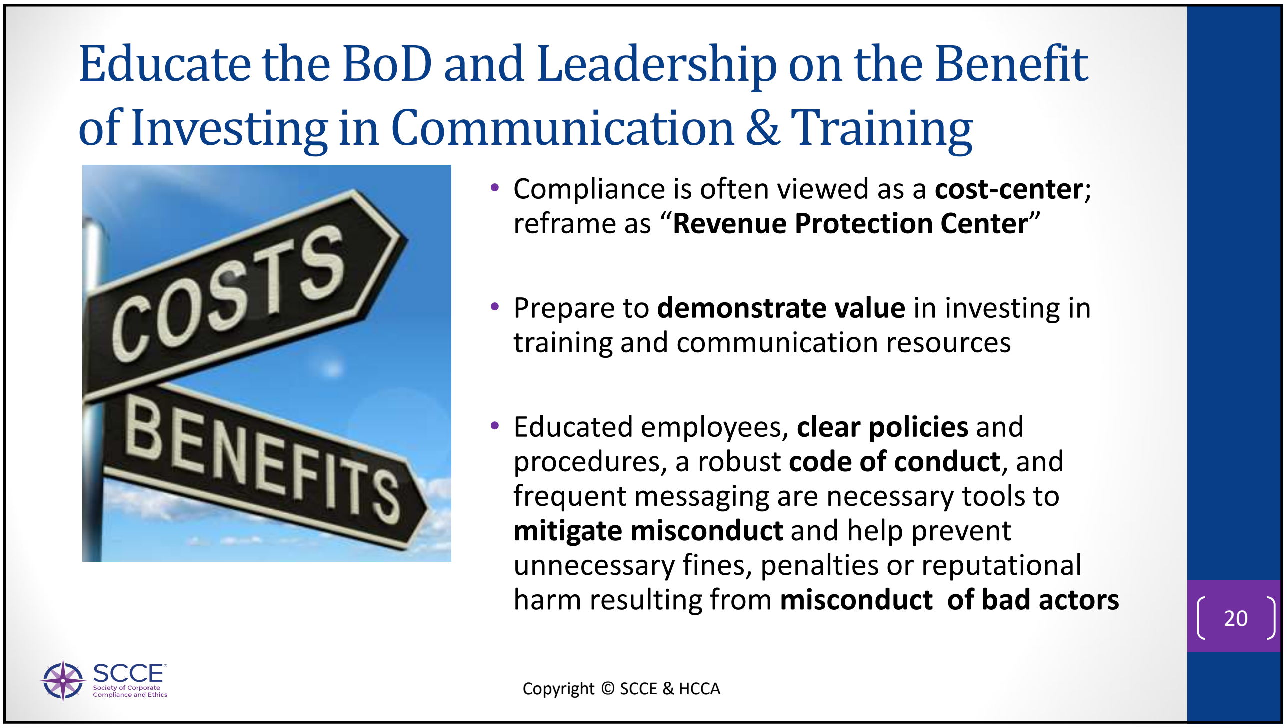
"Communication Touchpoint": Incentives & Disciplinary Measures

- Consider how to **encourage deterrence**
- For example: Publicize disciplinary actions versus provide positive incentives for good behavior

SCCE Society of Corporate Compliance and Ethics

19

19



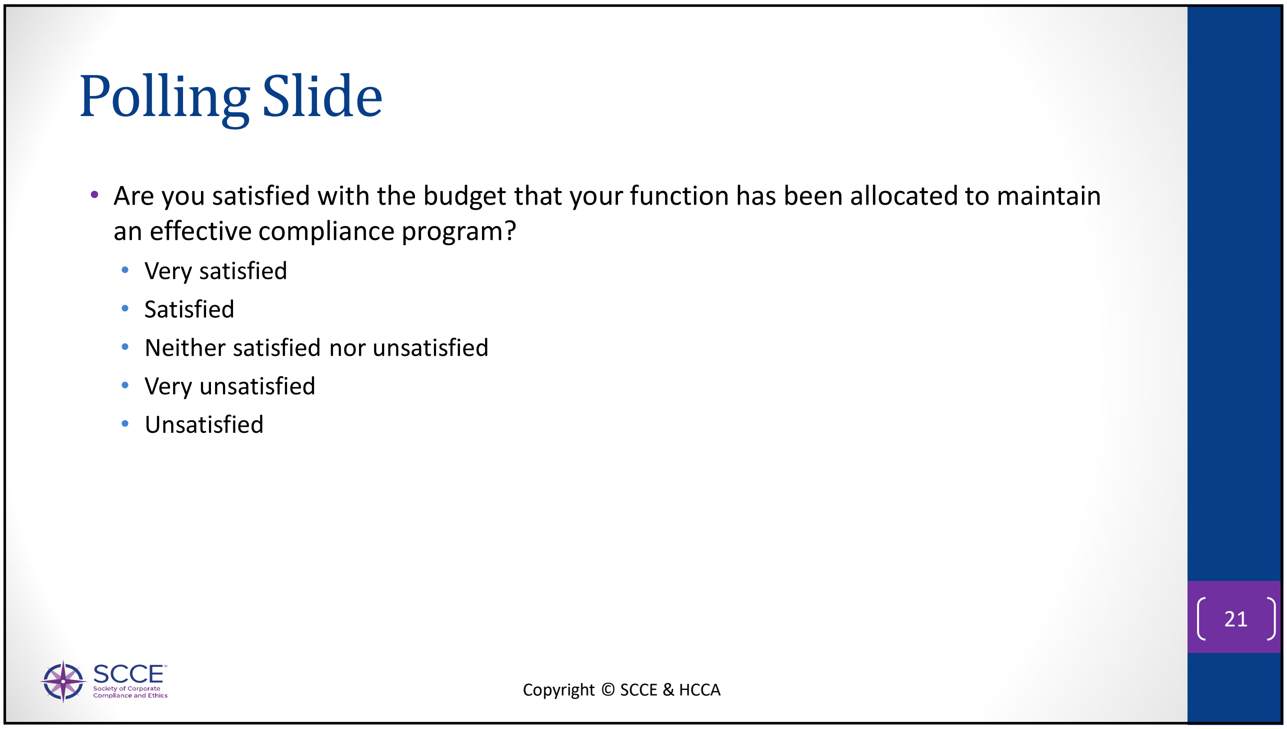
Educate the BoD and Leadership on the Benefit of Investing in Communication & Training

- Compliance is often viewed as a **cost-center**; reframe as "**Revenue Protection Center**"
- Prepare to **demonstrate value** in investing in training and communication resources
- Educated employees, **clear policies** and procedures, a robust **code of conduct**, and frequent messaging are necessary tools to **mitigate misconduct** and help prevent unnecessary fines, penalties or reputational harm resulting from **misconduct of bad actors**

SCCE Society of Corporate Compliance and Ethics

20

20



Polling Slide

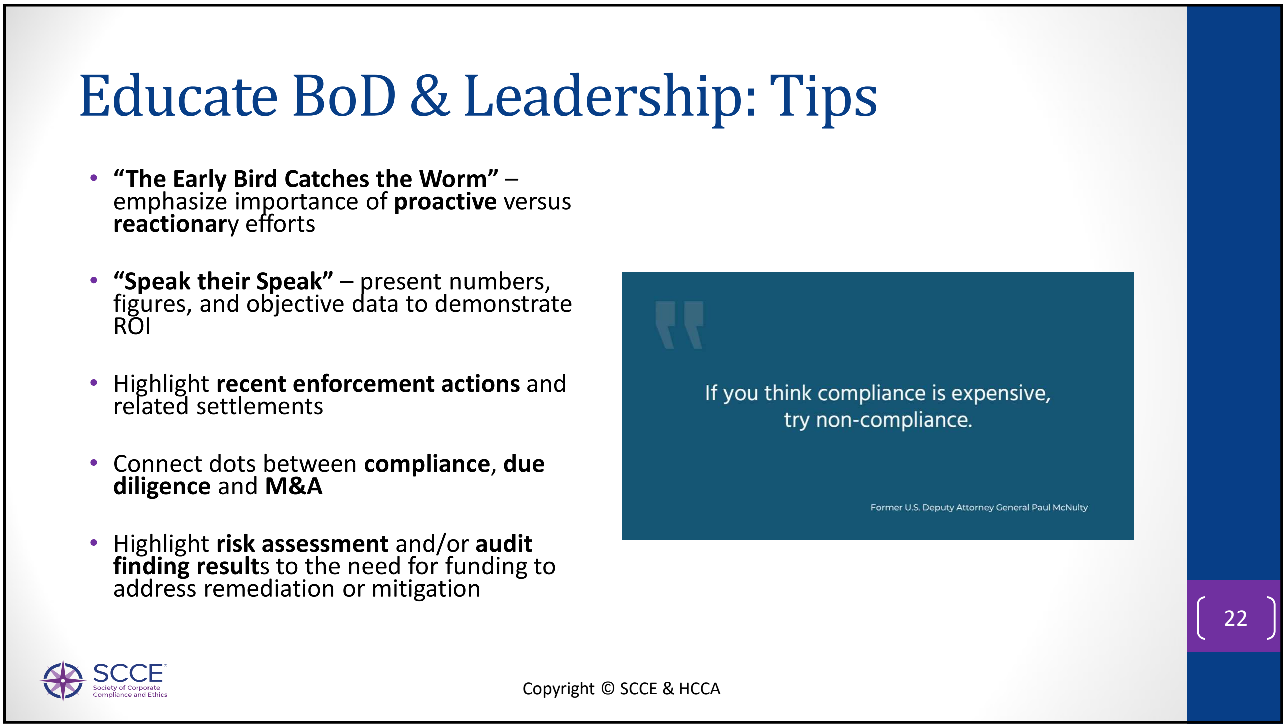
- Are you satisfied with the budget that your function has been allocated to maintain an effective compliance program?
  - Very satisfied
  - Satisfied
  - Neither satisfied nor unsatisfied
  - Very unsatisfied
  - Unsatisfied

21

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

21



Educate BoD & Leadership: Tips

- **"The Early Bird Catches the Worm"** – emphasize importance of **proactive** versus **reactionar**y efforts
- **"Speak their Speak"** – present numbers, figures, and objective data to demonstrate ROI
- Highlight **recent enforcement actions** and related settlements
- Connect dots between **compliance**, **due diligence** and **M&A**
- Highlight **risk assessment** and/or **audit finding result**s to the need for funding to address remediation or mitigation

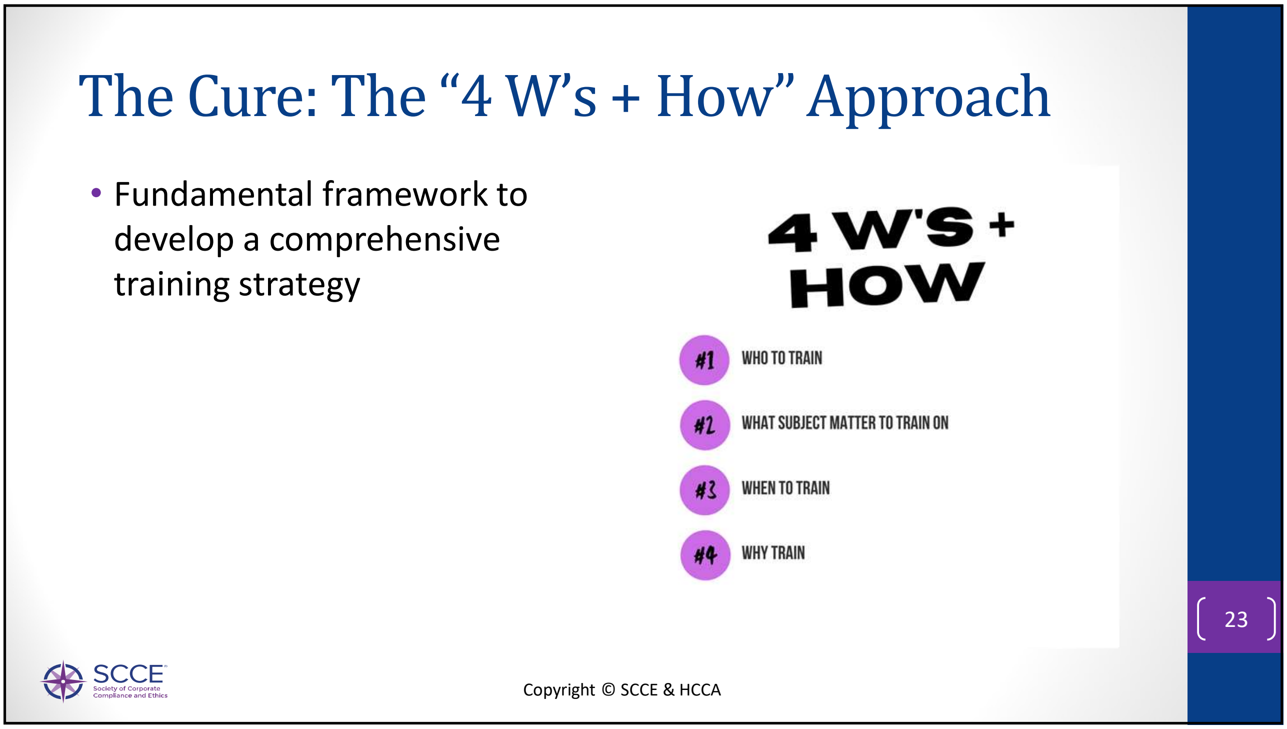
> If you think compliance is expensive, try non-compliance.
>
> Former U.S. Deputy Attorney General Paul McNulty

22

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

22



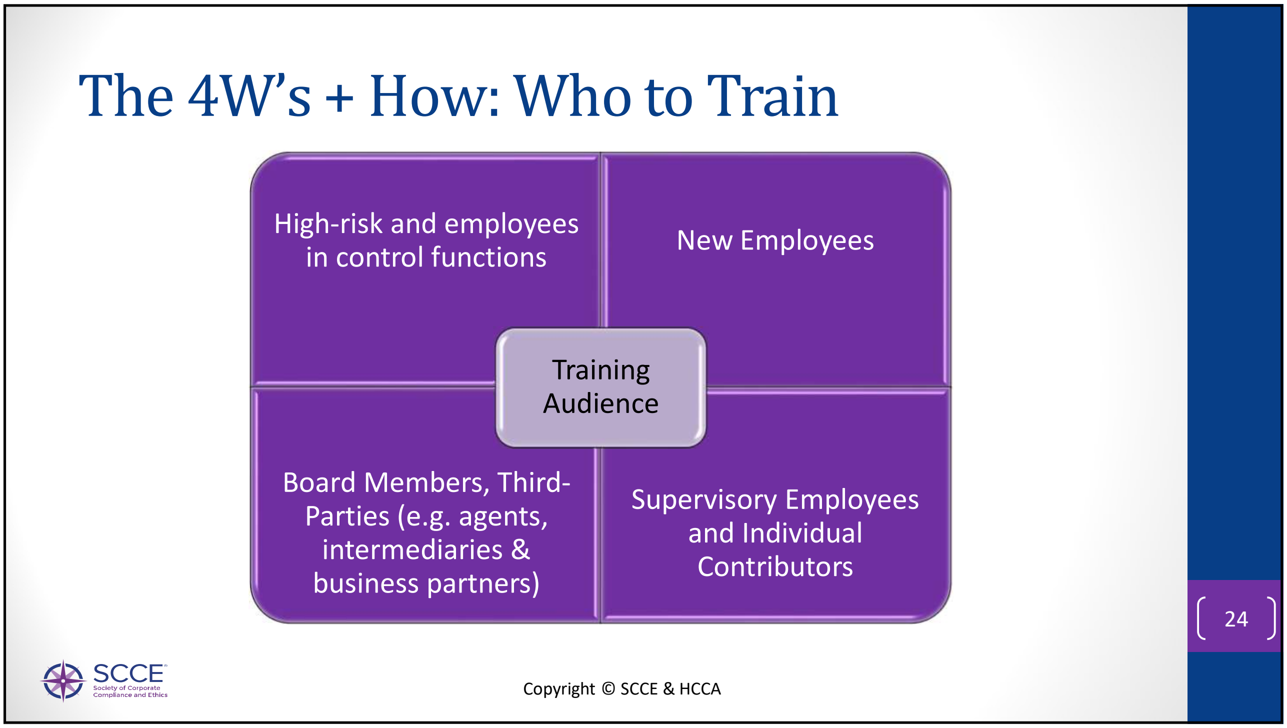
The Cure: The “4 W’s + How” Approach

- Fundamental framework to develop a comprehensive training strategy

4 W'S + HOW

- #1 WHO TO TRAIN
- #2 WHAT SUBJECT MATTER TO TRAIN ON
- #3 WHEN TO TRAIN
- #4 WHY TRAIN

23

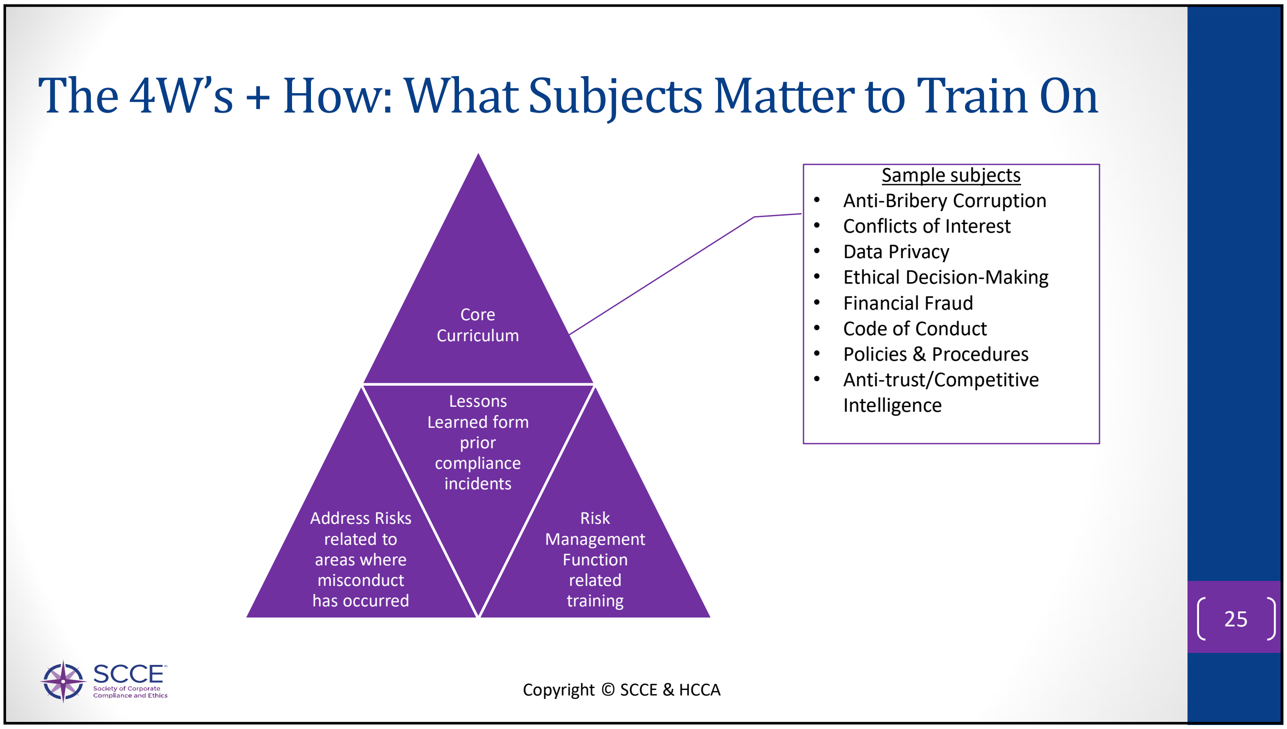


The 4W’s + How: Who to Train

Training Audience

- High-risk and employees in control functions
- New Employees
- Board Members, Third-Parties (e.g. agents, intermediaries & business partners)
- Supervisory Employees and Individual Contributors

24



The 4W's + How: What Subjects Matter to Train On

Core Curriculum

Lessons Learned form prior compliance incidents

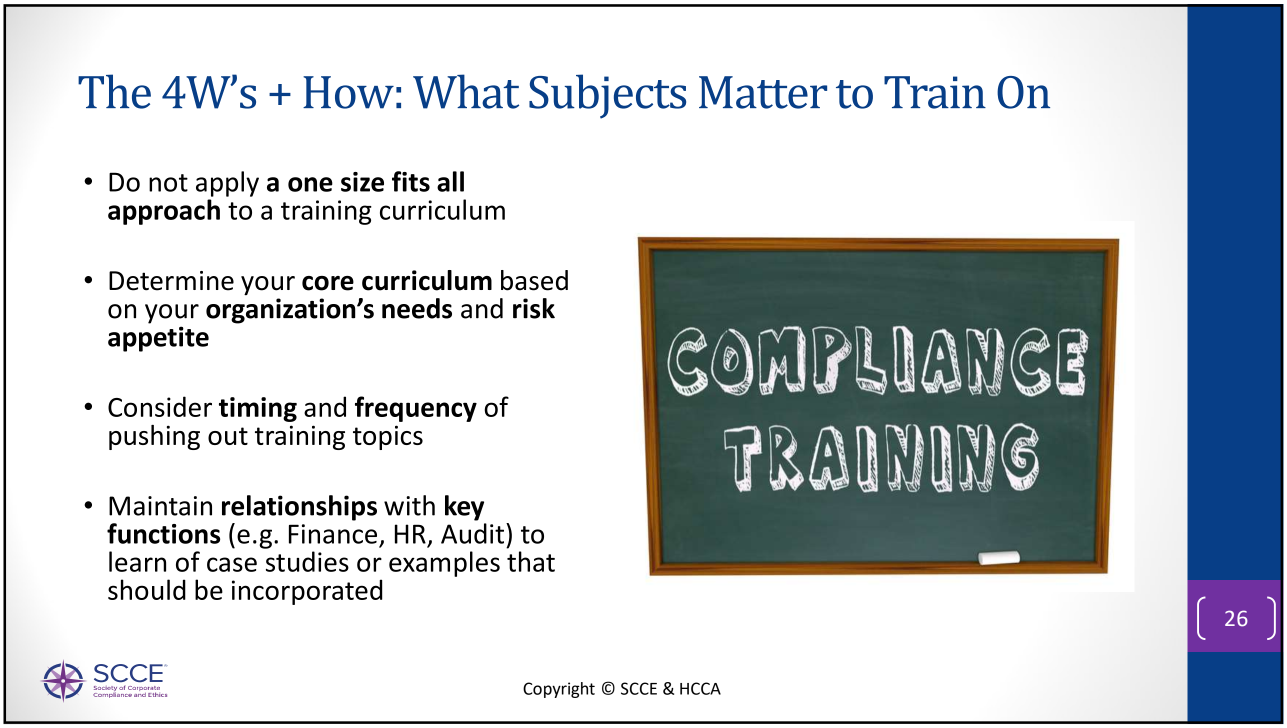
Address Risks related to areas where misconduct has occurred

Risk Management Function related training

Sample subjects

- Anti-Bribery Corruption
- Conflicts of Interest
- Data Privacy
- Ethical Decision-Making
- Financial Fraud
- Code of Conduct
- Policies & Procedures
- Anti-trust/Competitive Intelligence

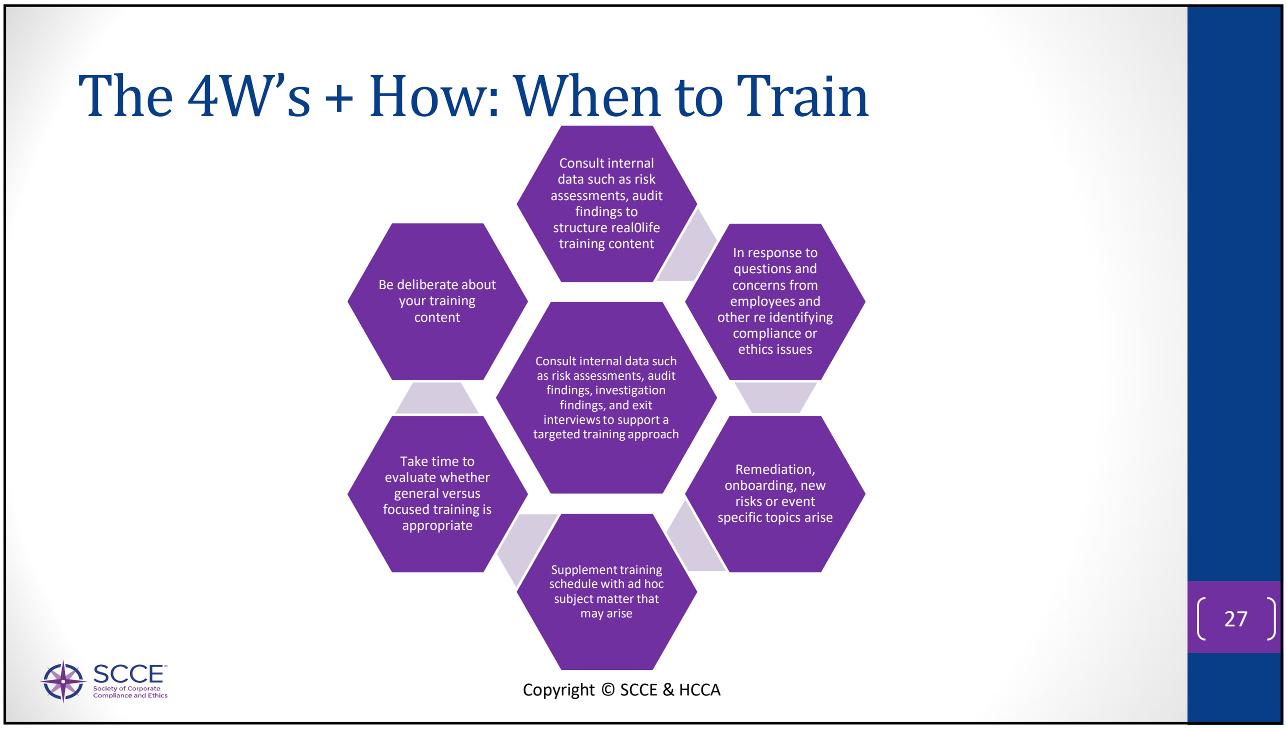
SCCE Society of Corporate Compliance and Ethics



The 4W's + How: What Subjects Matter to Train On

- Do not apply **a one size fits all approach** to a training curriculum
- Determine your **core curriculum** based on your **organization's needs** and **risk appetite**
- Consider **timing** and **frequency** of pushing out training topics
- Maintain **relationships** with **key functions** (e.g. Finance, HR, Audit) to learn of case studies or examples that should be incorporated

SCCE Society of Corporate Compliance and Ethics



The 4W’s + How: When to Train

Consult internal data such as risk assessments, audit findings to structure real0life training content

In response to questions and concerns from employees and other re identifying compliance or ethics issues

Remediation, onboarding, new risks or event specific topics arise

Supplement training schedule with ad hoc subject matter that may arise

Take time to evaluate whether general versus focused training is appropriate

Be deliberate about your training content

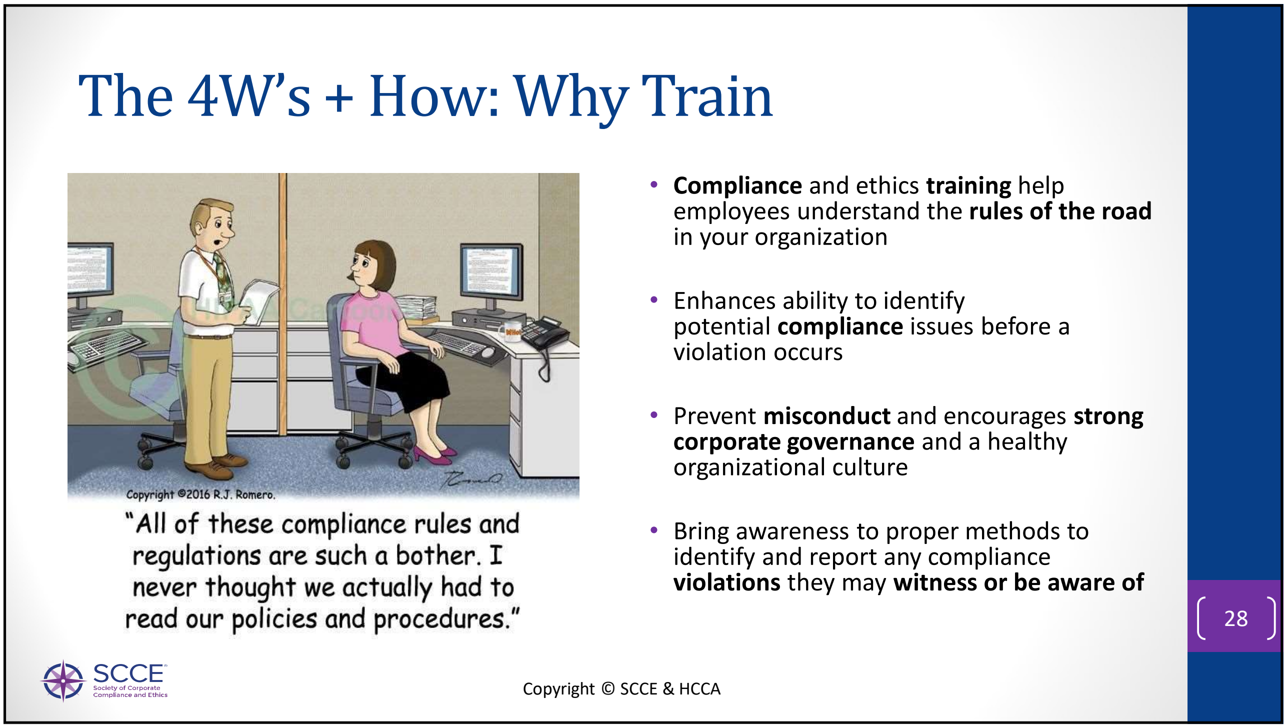
Consult internal data such as risk assessments, audit findings, investigation findings, and exit interviews to support a targeted training approach

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

27

27



The 4W’s + How: Why Train

Copyright ©2016 R.J. Romero.

“All of these compliance rules and regulations are such a bother. I never thought we actually had to read our policies and procedures.”

- **Compliance** and ethics **training** help employees understand the **rules of the road** in your organization
- Enhances ability to identify potential **compliance** issues before a violation occurs
- Prevent **misconduct** and encourages **strong corporate governance** and a healthy organizational culture
- Bring awareness to proper methods to identify and report any compliance **violations** they may **witness or be aware of**

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

28

28

The 4W’s + How: How to Train

- The most successful compliance programs use a **hybrid approach** to their training and communication methodology; engagement using **different mediums** is **critical**

Microlearning

Gamification and Incentivization

Case Studies

Blended Learning

- Impactful, yet **fun, unexpected methodologies** allow for **effective connection** with stakeholders
- Importantly, in light of COVID-19, **innovative approaches** will help to maintain **attention** and **increase retention**

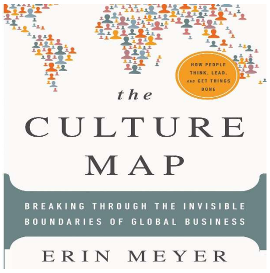
29

SCCE Society of Corporate Compliance and Ethics

29

The 4W’s + How: How to Train

- Be mindful of **audience size**, level of sophistication and **subject matter expertise**
- Multinational organizations should consider **cultural nuances** and **native language** in message preparation

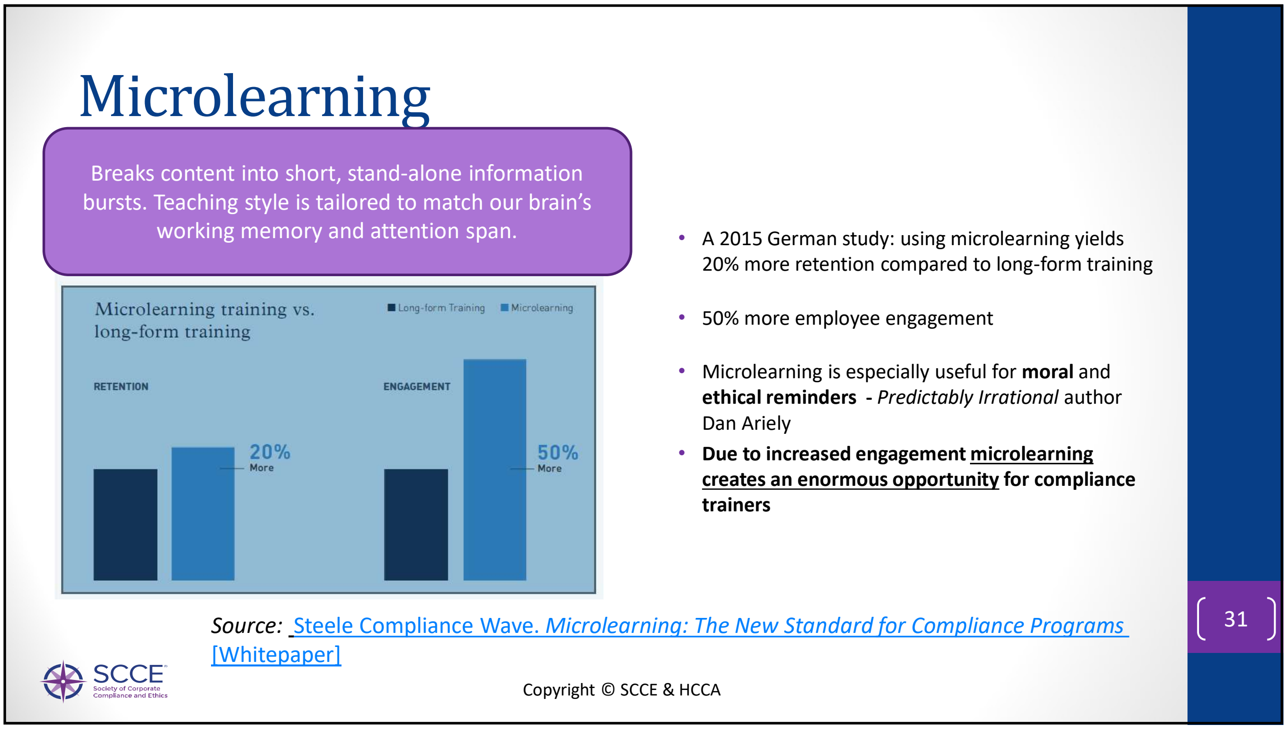

HOW PEOPLE THINK, LEAD, AND GET THINGS DONE
the CULTURE MAP
BREAKING THROUGH THE INVISIBLE BOUNDARIES OF GLOBAL BUSINESS
ERIN MEYER

- Ensure employees are **tested** on what they have learned, obtain **certifications of completion**

30

SCCE Society of Corporate Compliance and Ethics

30



Microlearning

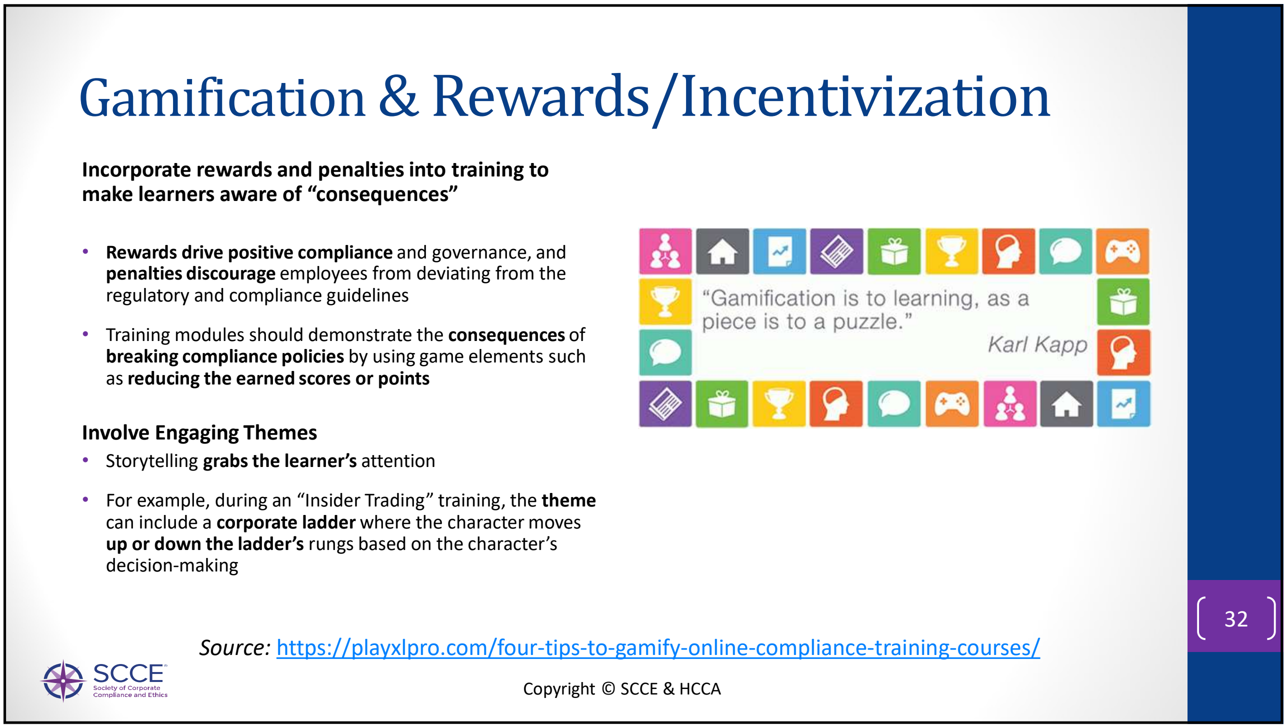
Breaks content into short, stand-alone information bursts. Teaching style is tailored to match our brain's working memory and attention span.

Microlearning training vs. long-form training
Long-form Training
Microlearning
RETENTION
20%
More
ENGAGEMENT
50%
More

- A 2015 German study: using microlearning yields 20% more retention compared to long-form training
- 50% more employee engagement
- Microlearning is especially useful for **moral** and **ethical reminders** - *Predictably Irrational* author Dan Ariely
- **Due to increased engagement microlearning creates an enormous opportunity for compliance trainers**

Source: Steele Compliance Wave. *Microlearning: The New Standard for Compliance Programs* [Whitepaper]

31



Gamification & Rewards/Incentivization

Incorporate rewards and penalties into training to make learners aware of "consequences"

- **Rewards drive positive compliance** and governance, and **penalties discourage** employees from deviating from the regulatory and compliance guidelines
- Training modules should demonstrate the **consequences** of **breaking compliance policies** by using game elements such as **reducing the earned scores or points**

Involve Engaging Themes

- Storytelling **grabs the learner's** attention
- For example, during an "Insider Trading" training, the **theme** can include a **corporate ladder** where the character moves **up or down the ladder's** rungs based on the character's decision-making

"Gamification is to learning, as a piece is to a puzzle."
Karl Kapp

Source: https://playxlpro.com/four-tips-to-gamify-online-compliance-training-courses/

32

Using Case Studies

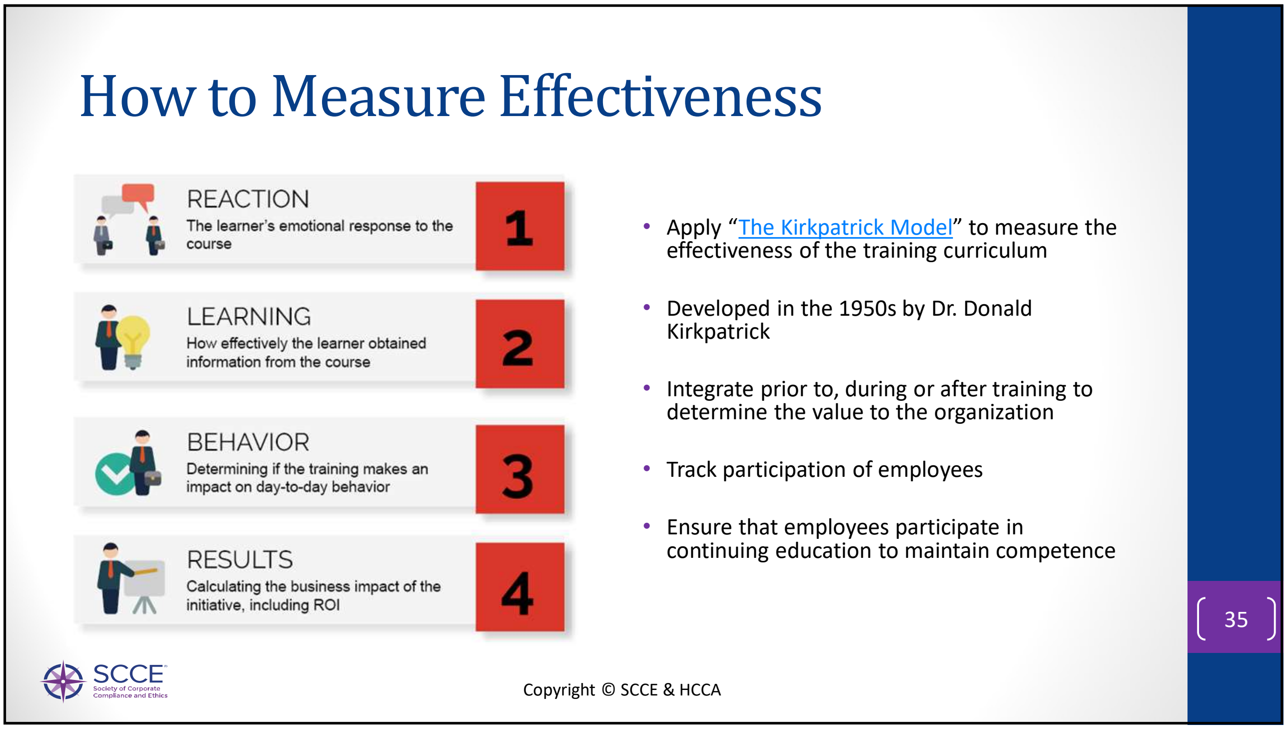
- Case studies are a **practical** and **effective** way to train employees by using **real-life situations or scenarios** as examples, and delivering guidance that promotes **adherence** to an organization's policies and procedures
- Employees are forced to **think through a set of facts** and make determinations to address the **dilemmas** and solve for the **correct outcome**. Through this analysis an employee can learn **what is "right" and "wrong"**
- Effective way to deliver messaging around **prior misconduct** or disciplinary actions for **failure to comply** with company policy, procedure or controls. For example, provide **anonymized descriptions** of real-life scenarios that lead to discipline
- An appropriate methodology to **pose ethical dilemmas.** Present case studies where there are **different paths** to the preferred outcome to **challenge their understanding** and reinforce appropriate decision-making

33

Blended Learning

- Simply a combination of **e-learning** and **in-person learning**
- Evidence shows that the **human interaction** component of **in-person training** still has tangible benefits: "Where human interaction was present, it was reported to be linked with **more active behavioral engagement, higher cognitive engagement** and **stronger and more positive emotional engagement** than where human interaction was absent." Hewett, Becker, & Bish (2019)
- Use your **best judgment** to achieve the appropriate **blended balance** for your stakeholders
- **Online training** may be more **cost-effective however in-person training** allows for social interaction **and live instructor feedback**

34



How to Measure Effectiveness

REACTION
The learner's emotional response to the course
1

LEARNING
How effectively the learner obtained information from the course
2

BEHAVIOR
Determining if the training makes an impact on day-to-day behavior
3

RESULTS
Calculating the business impact of the initiative, including ROI
4

- Apply "The Kirkpatrick Model" to measure the effectiveness of the training curriculum
- Developed in the 1950s by Dr. Donald Kirkpatrick
- Integrate prior to, during or after training to determine the value to the organization
- Track participation of employees
- Ensure that employees participate in continuing education to maintain competence

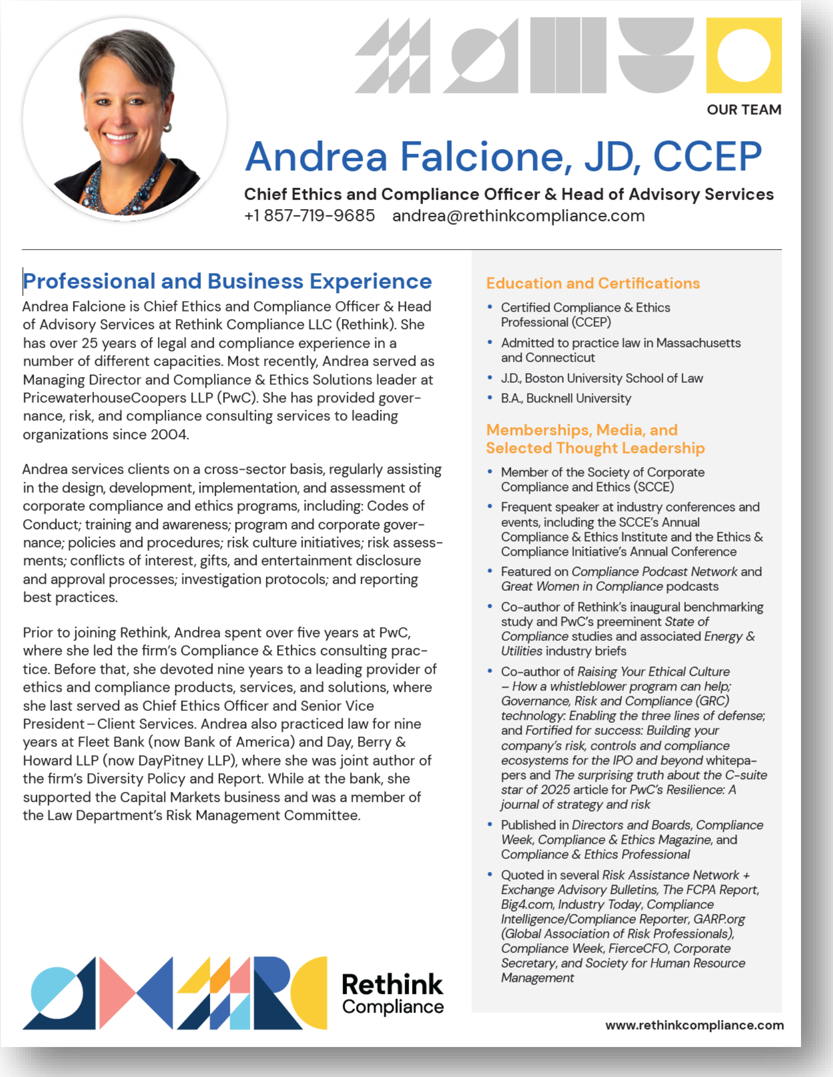
SCCE Compliance & Ethics Essentials Workshop

Incentives and Enforcement (Element no. 4)

Andrea Falcione

SCCE Society of Corporate Compliance and Ethics

Introductions



OUR TEAM

Andrea Falcione, JD, CCEP

Chief Ethics and Compliance Officer & Head of Advisory Services
+1 857-719-9685 andrea@rethinkcompliance.com

Professional and Business Experience

Andrea Falcione is Chief Ethics and Compliance Officer & Head of Advisory Services at Rethink Compliance LLC (Rethink). She has over 25 years of legal and compliance experience in a number of different capacities. Most recently, Andrea served as Managing Director and Compliance & Ethics Solutions leader at PricewaterhouseCoopers LLP (PwC). She has provided governance, risk, and compliance consulting services to leading organizations since 2004.

Andrea services clients on a cross-sector basis, regularly assisting in the design, development, implementation, and assessment of corporate compliance and ethics programs, including: Codes of Conduct; training and awareness; program and corporate governance; policies and procedures; risk culture initiatives; risk assessments; conflicts of interest, gifts, and entertainment disclosure and approval processes; investigation protocols; and reporting best practices.

Prior to joining Rethink, Andrea spent over five years at PwC, where she led the firm's Compliance & Ethics consulting practice. Before that, she devoted nine years to a leading provider of ethics and compliance products, services, and solutions, where she last served as Chief Ethics Officer and Senior Vice President – Client Services. Andrea also practiced law for nine years at Fleet Bank (now Bank of America) and Day, Berry & Howard LLP (now DayPitney LLP), where she was joint author of the firm's Diversity Policy and Report. While at the bank, she supported the Capital Markets business and was a member of the Law Department's Risk Management Committee.

Education and Certifications

- Certified Compliance & Ethics Professional (CCEP)
- Admitted to practice law in Massachusetts and Connecticut
- J.D., Boston University School of Law
- B.A., Bucknell University

Memberships, Media, and Selected Thought Leadership

- Member of the Society of Corporate Compliance and Ethics (SCCE)
- Frequent speaker at industry conferences and events, including the SCCE's Annual Compliance & Ethics Institute and the Ethics & Compliance Initiative's Annual Conference
- Featured on *Compliance Podcast Network* and *Great Women in Compliance* podcasts
- Co-author of Rethink's inaugural benchmarking study and PwC's preeminent *State of Compliance* studies and associated *Energy & Utilities* industry briefs
- Co-author of *Raising Your Ethical Culture – How a whistleblower program can help; Governance, Risk and Compliance (GRC) technology: Enabling the three lines of defense*; and *Fortified for success: Building your company's risk, controls and compliance ecosystems for the IPO and beyond* whitepapers and *The surprising truth about the C-suite star of 2025* article for *PwC's Resilience: A journal of strategy and risk*
- Published in *Directors and Boards, Compliance Week, Compliance & Ethics Magazine*, and *Compliance & Ethics Professional*
- Quoted in several *Risk Assistance Network + Exchange Advisory Bulletins, The FCPA Report, Big4.com, Industry Today, Compliance Intelligence/Compliance Reporter, GARP.org (Global Association of Risk Professionals), Compliance Week, FierceCFO, Corporate Secretary, and Society for Human Resource Management*

Rethink Compliance

www.rethinkcompliance.com

What we will cover today

- Incentives and enforcement (Element No. 4): 5 min.
- Incorporating compliance / ethics into performance evaluations: 15 min.
- Active promotion of the CEP: 15 min.
- Incentives: 15 min.
- Consistency in discipline for wrongdoing: 15 min.
- Considerations with vendors and other third parties: 10 min.
- TOTAL SESSION TIME: 75 minutes

____

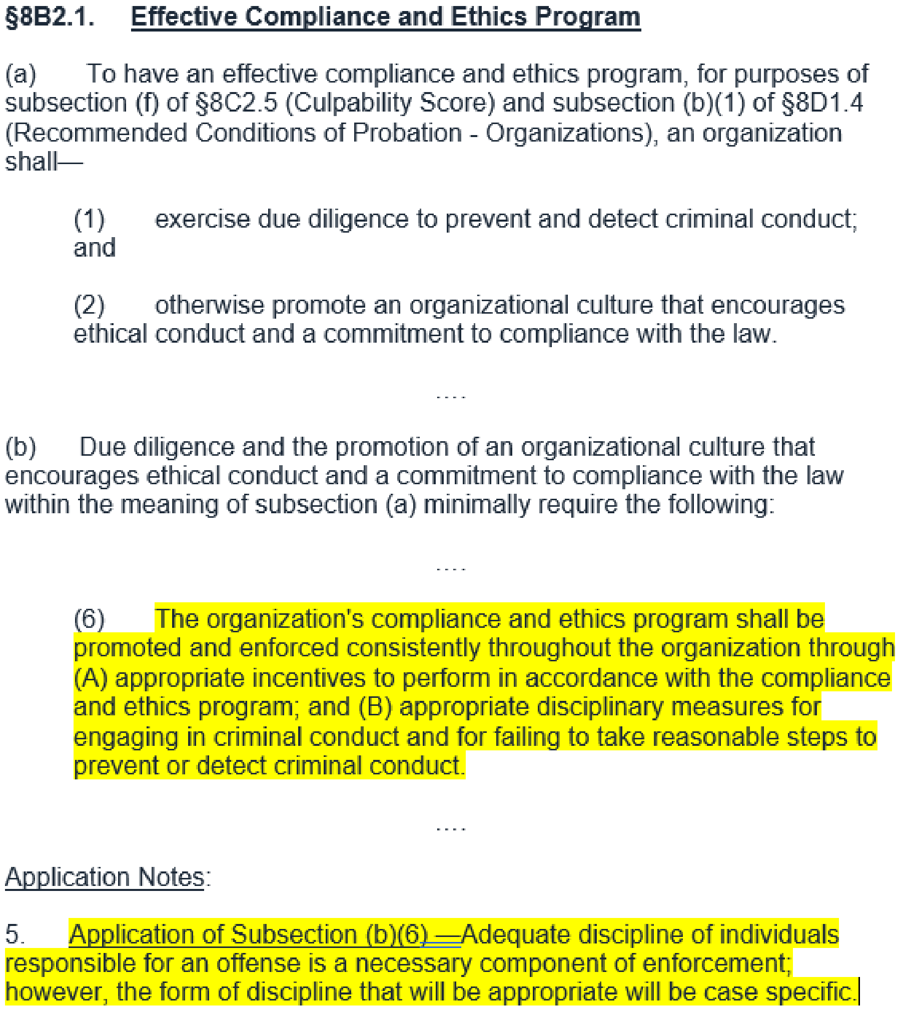
- Reference material

5 minutes

INCENTIVES AND ENFORCEMENT (ELEMENT NO. 4)

SCCE® Society of Corporate Compliance and Ethics

Sentencing Guidelines



§8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (b)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

. . . .

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

. . . .

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

. . . .

Application Notes:

5. Application of Subsection (b)(6).—Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

Source: U.S. Federal Sentencing Guidelines for Organizations

15 minutes

INCORPORATING COMPLIANCE / ETHICS INTO PERFORMANCE EVALS

SCCE® Society of Corporate Compliance and Ethics

A few things to consider

You’ll meet … **RESISTANCE!**

You’ll hear … **“It’s too subjective.”**

“Rewarding people for doing the right thing?!?”

“Stay in your lane!”

SCCE®
Society of Corporate
Compliance and Ethics

So, what can you do?

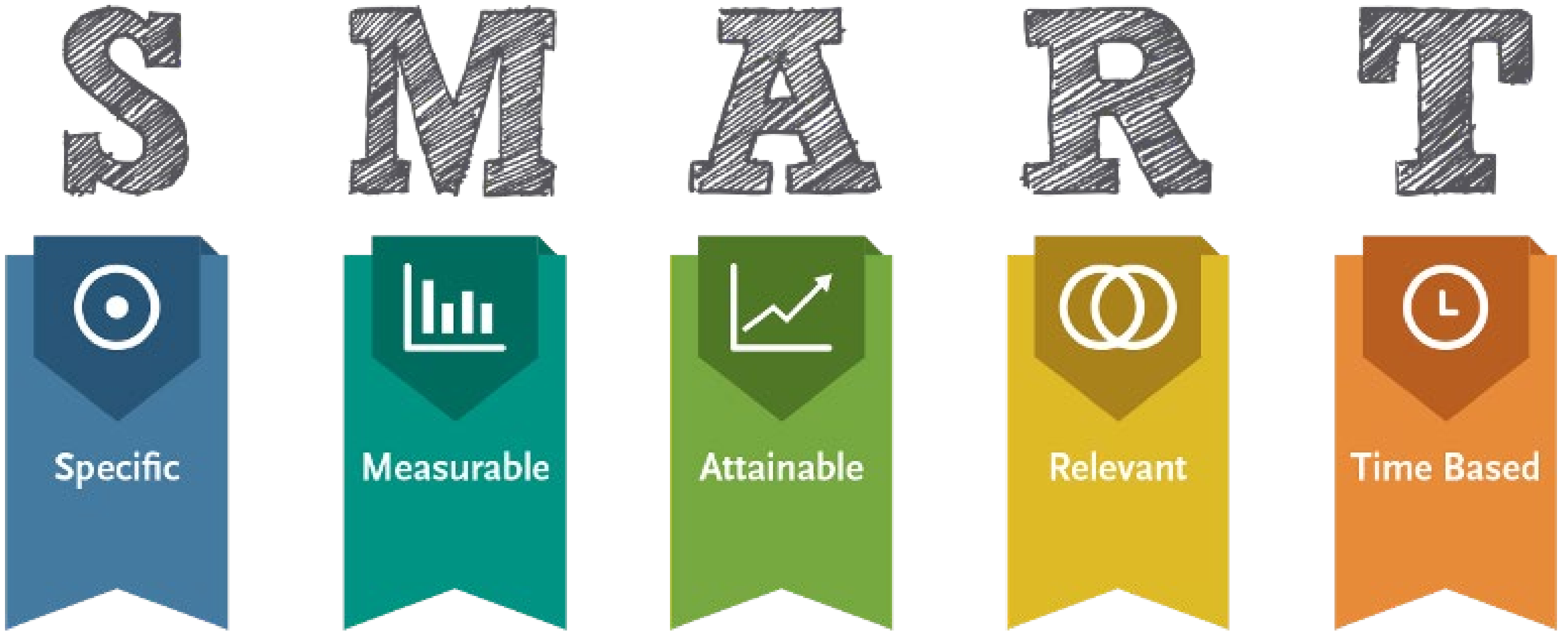
What did Peter Drucker say?

"People in organizations, we have known for a century, tend to act in response to being recognized and rewarded — everything else is preaching. . . . The moment they realize that the organization rewards for the right behavior they will accept it."

- Peter Drucker

SCCE
Society of Corporate
Compliance and Ethics

The best goals are …



"SMART-goals" by Dungdm93 is licensed under CC BY-SA 4.0.

Smart C&E goals might include

- Timely completion by the employee – *and* by the folks who report to the employee – of C&E tasks / participation in the CEP:
  - ✓ Training
  - ✓ Policy certifications
  - ✓ Regulatory risk management processes
- Delivery of compliance and ethics messaging to teammates
- Behavior demonstrating commitment to the Code
- Behavior demonstrating the support of team members in *their* commitment to the Code

Other considerations

- Benefits of 360^o reviews
- Benefits of self evaluation
- Specific examples of how to meet C&E metrics
- Look backs prior to promotion
- Departmental / BU metrics

15 minutes

ACTIVE PROMOTION OF THE CEP

SCCE®
Society of Corporate
Compliance and Ethics

What is “active promotion?”

- Top of mind
- Once is never enough
- Make it a reflex

- Standards and procedures
- Culture of compliance
- Risk culture and response
- Red flags and warning signs
- Speaking up

What can we impact?

Who should promote the CEP?

EVERYONE!

15 minutes

INCENTIVES

"Good-Bad-Ugly" by b.frahm is licensed under CC BY 2.0.

Creative ways to use incentives

- Competitions, with rewards on an individual or team level:
  - Highest scores on assessments
  - Quickest to complete training, certifications, etc.
  - Content competitions – *e.g.,* selfie or other video contests

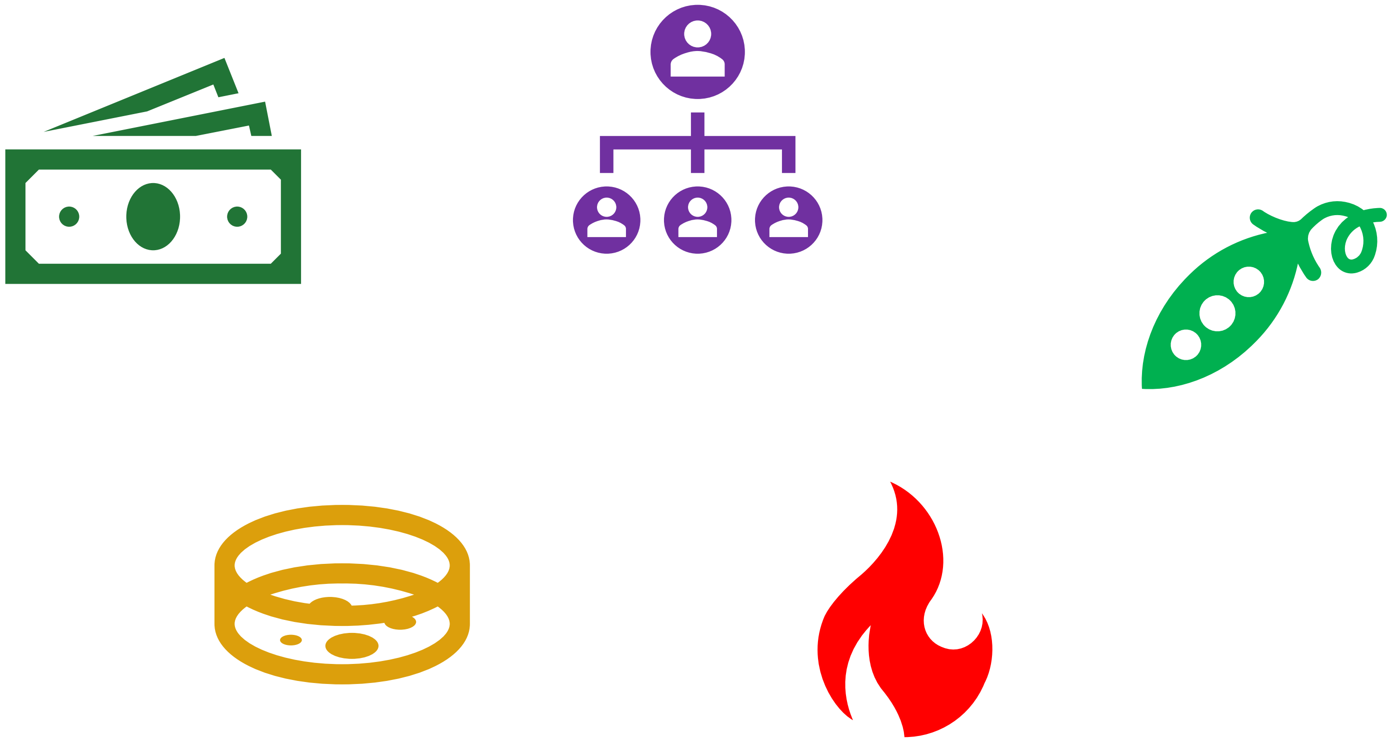
- Celebrations of compliance and ethics successes

- Examples:
  - Awards dinners
  - Team lunches
  - Recognition at All Hands meetings
  - Letters of commendation
  - Invitations to leadership events

"Wells Fargo 5/2014" by JeepersMedia is licensed under CC BY 2.0.

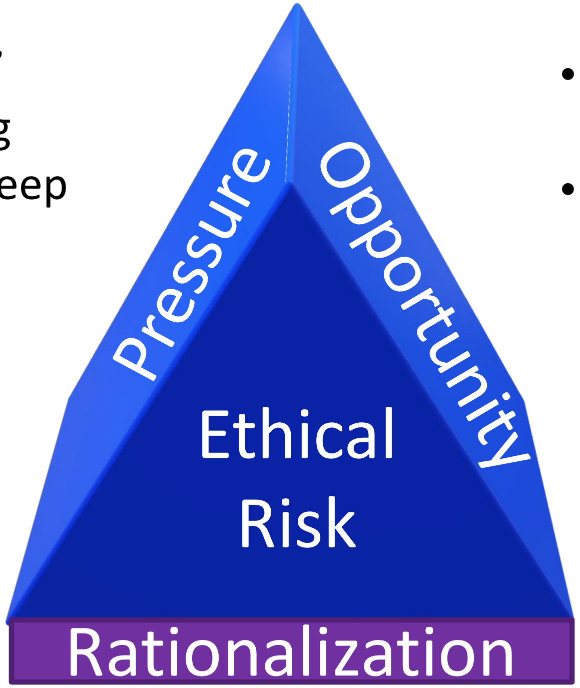
A cautionary tale….

What can we learn?



What can we learn? (cont.)

- "I need the money."
- "If I don't meet these goals, I'll lose my job."
- "Companies are laying people off. I have to keep my job."



- Weak or circumventable internal controls
- Management's tacit approval / corrupt culture
- Poor oversight and lack of monitoring

- "Everybody's doing it."
- "Nobody will get hurt."
- "I don't make enough money – they owe me."

What else do we know?

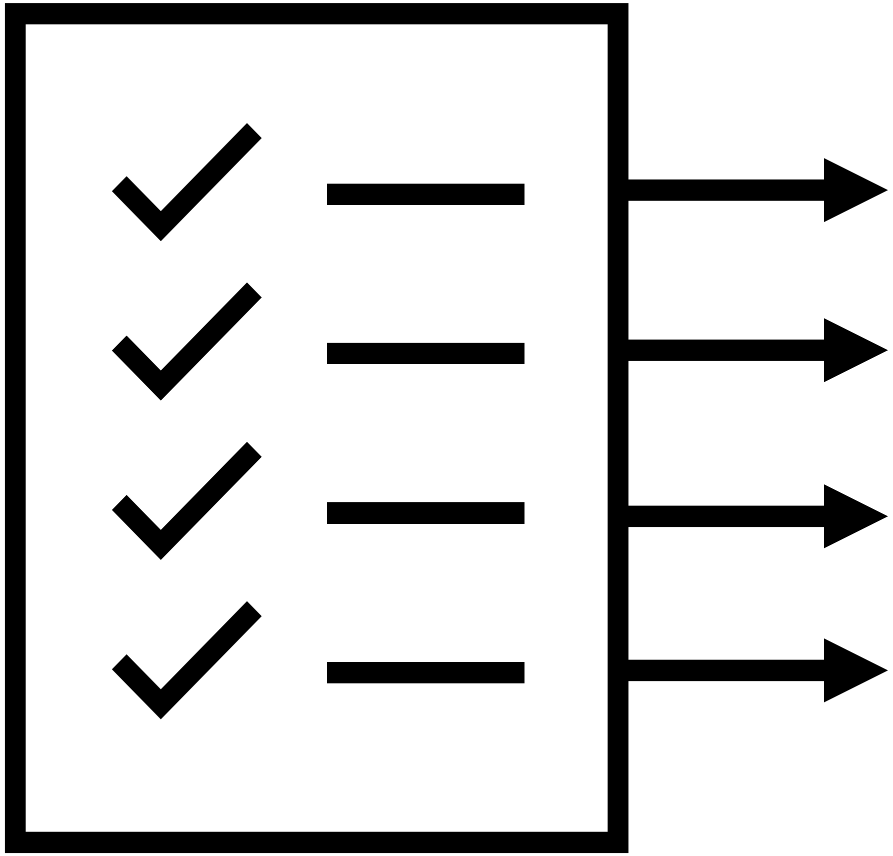
- Incentives programs are prevalent
- The Compliance & Ethics team is typically involved in neither the development nor the review of incentive plans
- Regulators began to focus on incentive plan risk in the aftermath of Wells Fargo
- Now, regulators will also consider whether incentive plans include clawback provisions that are both communicated to employees *and* enforced

2023 Enforcement Action

"DOJ seal" by Mike Licht, NotionsCapital.com is licensed under CC BY 2.0.

To review the Ablemarle press release, click the graphic above.

What should we do?



Add incentive plan risk to risk assessment and appropriately assess inherent and residual risk

Review new and existing plans with HR and the business

Partner with the business to develop a risk monitoring plan

Partner with internal audit to develop an audit plan

15 minutes

CONSISTENCY IN DISCIPLINE FOR WRONGDOING

Interestingly …

“[A]ppropriate disciplinary measures”

- “for engaging in criminal conduct”

AND

- “for failing to take reasonable steps to prevent or detect criminal conduct”

SCCE Society of Corporate Compliance and Ethics

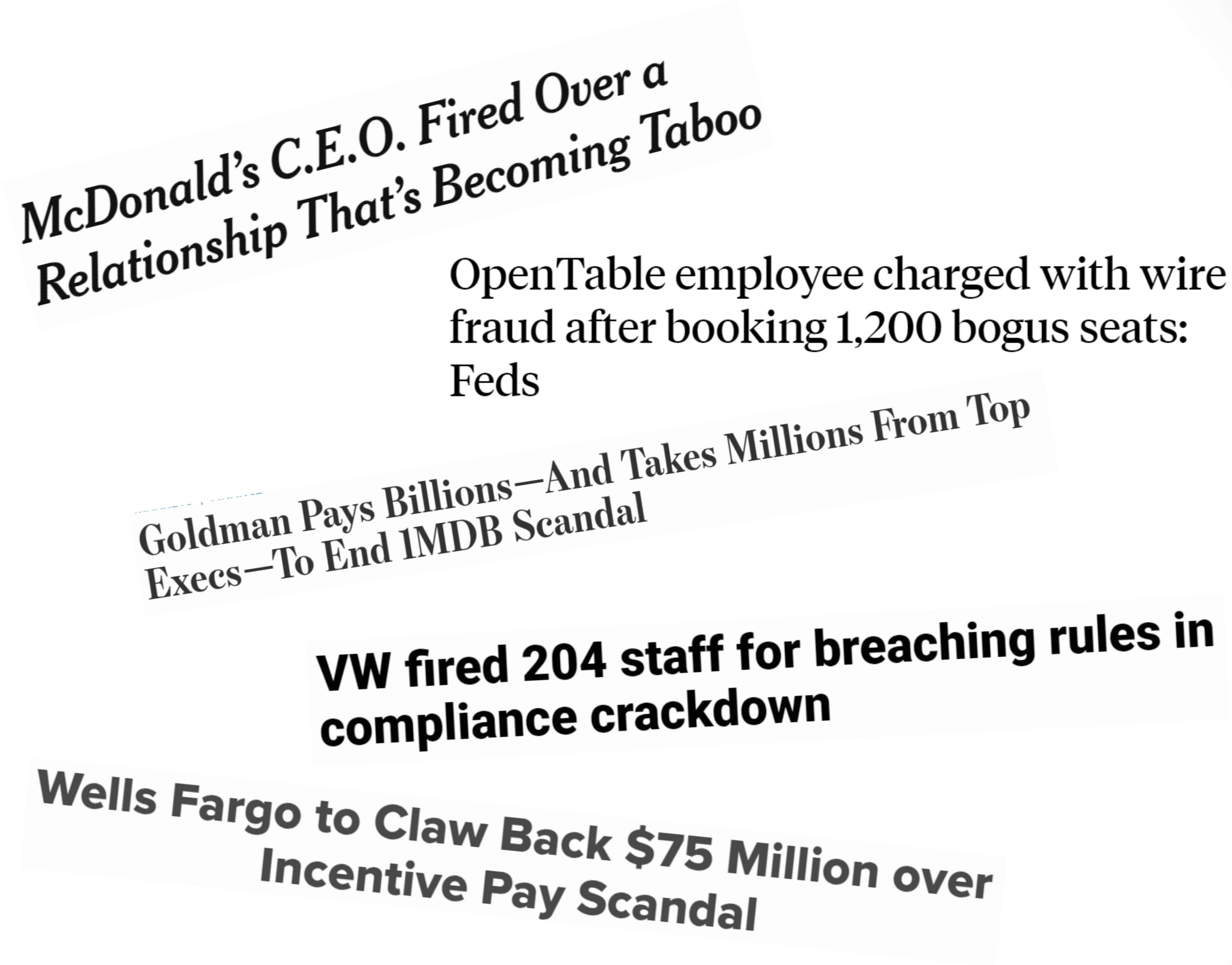
At a minimum

Appropriate program or policy

Fairly applied

Policy by Nick Youngson CC BY-SA 3.0 Alpha Stock Images

"Scales of Justice" by North Charleston is licensed under CC BY-SA 2.0.



McDonald's C.E.O. Fired Over a Relationship That's Becoming Taboo

OpenTable employee charged with wire fraud after booking 1,200 bogus seats: Feds

Goldman Pays Billions—And Takes Millions From Top Execs—To End 1MDB Scandal

VW fired 204 staff for breaching rules in compliance crackdown

Wells Fargo to Claw Back $75 Million over Incentive Pay Scandal

SCCE® Society of Corporate Compliance and Ethics

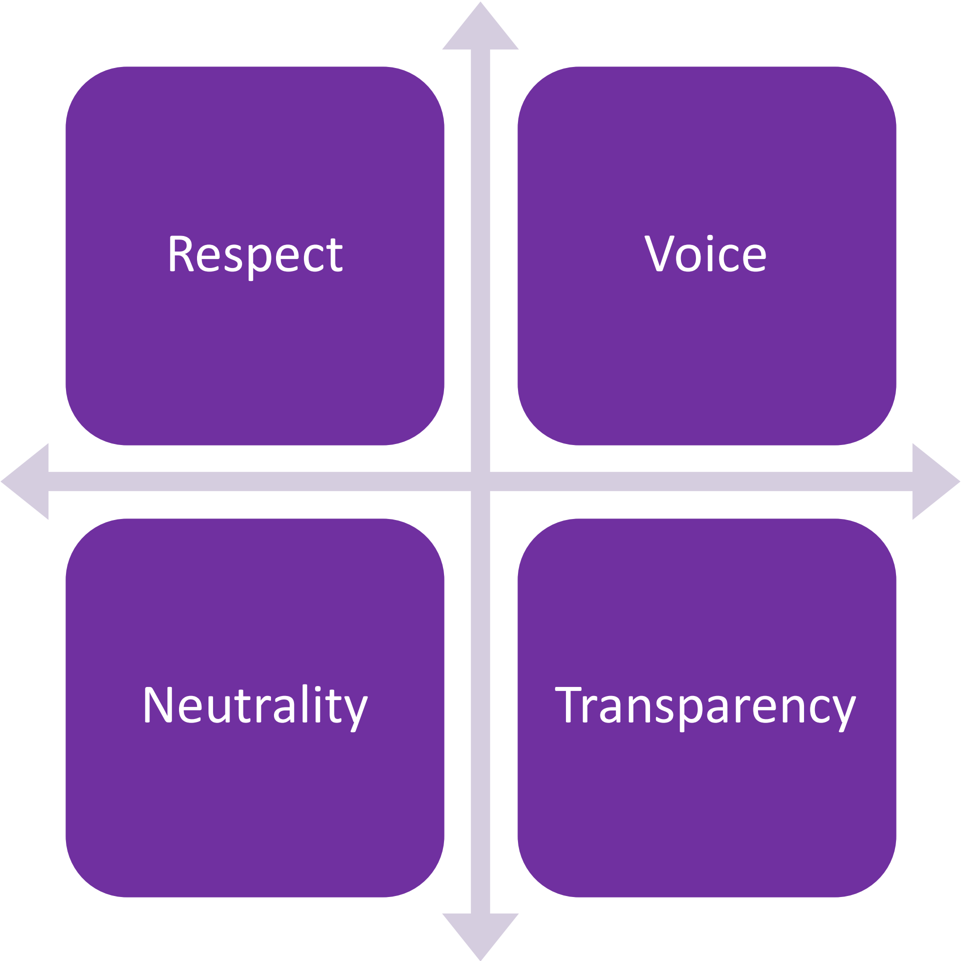
Let’s start with the easy part …

Microsoft Word
7 - 2003 Documer

To access the policy, double click the graphic above.

Now the hard part …

Procedural Justice



Respect

Voice

Neutrality

Transparency

Copyright © SCCE & HCCA

Track your progress

- Consistency in discipline is another area that should be subject to ongoing monitoring and auditing
- It’s an area that will be tested when you undergo a program assessment
- Document, document, document – so you can prove your commitment and identify areas for improvement

10 minutes

CONSIDERATIONS WITH VENDORS AND OTHER THIRD PARTIES

Third-party business partners

- Guess what? They matter, too!

- Certain third parties are treated like an extension of our companies, particularly agents, contract employees, and even subcontractors.

- In fact, the majority of FCPA enforcement actions relate to – or at least include – third-party misconduct (*e.g.,* intermediaries engaging in bribery and corruption on behalf of another organization, whether that organization has condoned the behavior or not).

- Under U.S. law, companies may also be held responsible for third-party harassment or discrimination.

Supplier Codes of Conduct

ATC Supplier Code of Conduct

To view this Supplier Code, click the link above.

Regular, old Codes of Conduct

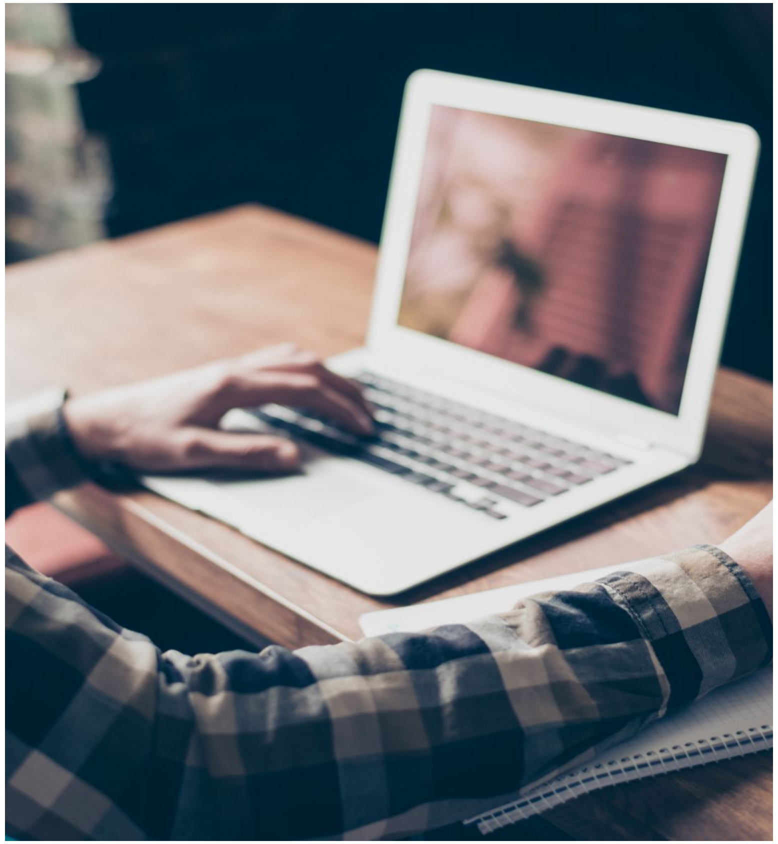
“Anyone who works on the Company’s behalf (including suppliers, consultants and other business partners) must share our commitment to integrity by following the principles of our Code when providing goods and services to the Company or acting on our behalf.”

“The UnitedHealth Group Board of Directors has adopted this global Code of Conduct, which applies to all employees, directors, and contractors, to provide guidelines for our decision-making and behavior.”

Accountability, continued

Contractual provisions

Training



How can we know?

Monitor

Audit

"Check mark 23x20 02" by Quasar is licensed under CC BY-SA 3.0.

SCCE Society of Corporate Compliance and Ethics

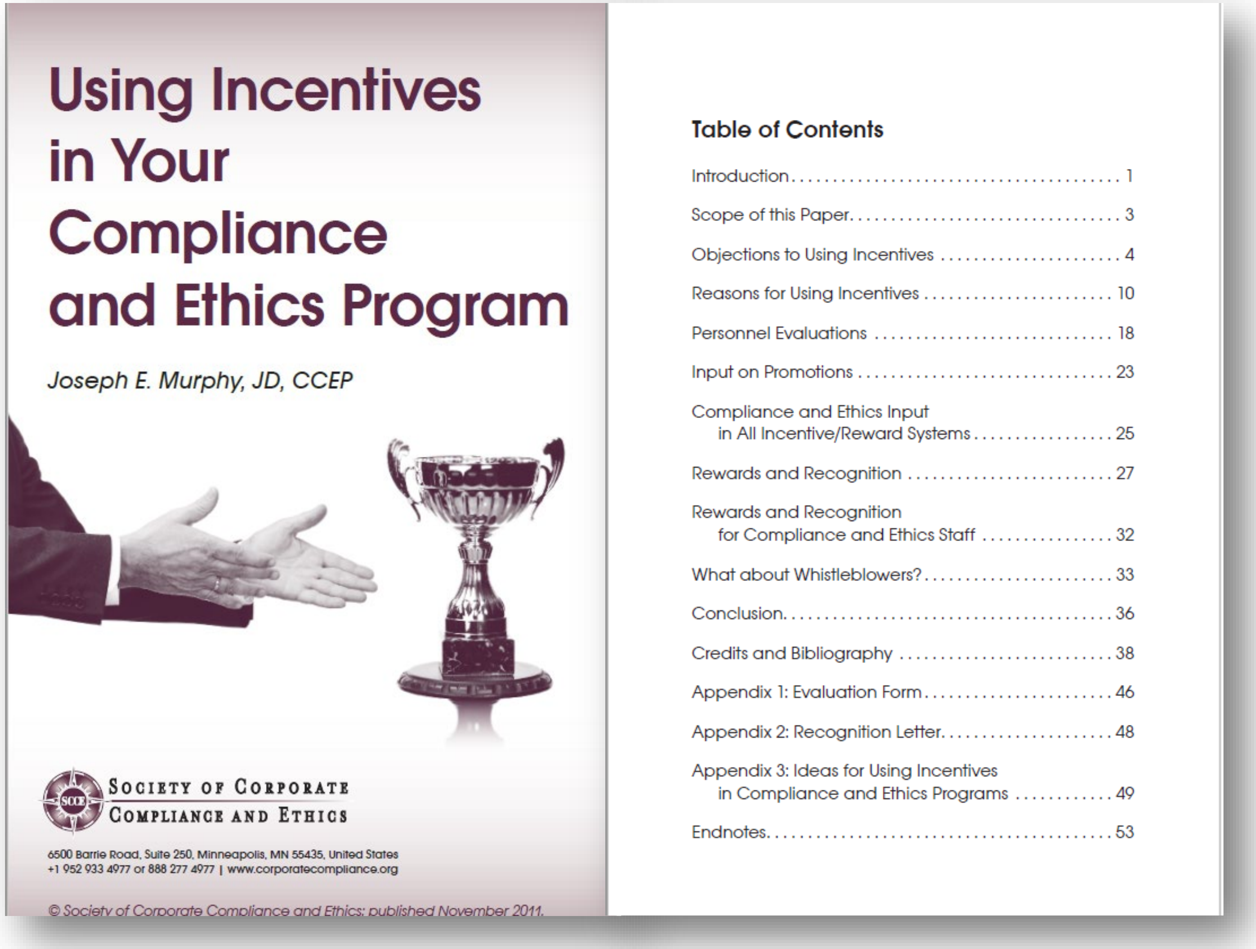
"Warning unintended consequences ahead" by RealDealDUILawyer is licensed under CC BY-SA 2.0.

In the face of third-party non-compliance ….

THANK YOU!

SCCE®
Society of Corporate
Compliance and Ethics

Reference material



Using Incentives in Your Compliance and Ethics Program

Joseph E. Murphy, JD, CCEP

Society of Corporate Compliance and Ethics

6500 Barrie Road, Suite 250, Minneapolis, MN 55435, United States
+1 952 933 4977 or 888 277 4977 | www.corporatecompliance.org

Table of Contents

Introduction 1

Scope of this Paper. 3

Objections to Using Incentives 4

Reasons for Using Incentives 10

Personnel Evaluations 18

Input on Promotions 23

Compliance and Ethics Input
in All Incentive/Reward Systems 25

Rewards and Recognition 27

Rewards and Recognition
for Compliance and Ethics Staff 32

What about Whistleblowers? 33

Conclusion. 36

Credits and Bibliography 38

Appendix 1: Evaluation Form 46

Appendix 2: Recognition Letter. 48

Appendix 3: Ideas for Using Incentives
in Compliance and Ethics Programs 49

Endnotes. 53

SCCE Compliance & Ethics Essentials Workshop

Monitoring, Auditing, and Reporting Systems

SCCE™
Society of Corporate Compliance and Ethics

Greg Triguba, JD, CCEP, CCEP-I
Caroline McMichen, CCEP

1

Agenda

1	**Monitoring & Auditing *Overview***	✓ Value Proposition ✓ Benefits of Effective Practice ✓ Global Guidelines/Frameworks
2	**Core Practice Considerations**	✓ Fundamentals ✓ Practice Planning/Scoping ✓ Monitoring/Auditing – *Overview* ✓ Use of Data Analytics
3	**Periodic Evaluation of C&E Programs**	✓ Effectiveness ✓ Continuous Improvement
4	**C&E Reporting Systems**	✓ Infrastructure ✓ Best Practices

2

1 Monitoring & Auditing - *Overview*

SCCE™
Society of Corporate
Compliance and Ethics

3

Value Proposition

- ✓ Heartbeat of effective C&E programs; essential to understanding how you are doing!
- ✓ Prevents and detects wrongdoing; reduces risks and liabilities from government inquires, enforcement challenges, and reputational damage
- ✓ Supports and enhances legal/regulatory compliance and risk responses; assures top compliance and ethics risks are being effectively managed and addressed
- ✓ Helps assure internal controls and approaches to mitigate risk are working and meaningful through testing and ongoing monitoring
- ✓ Serves to identify gaps and areas of potential non-compliance
- ✓ Supports continuous improvement efforts; provides opportunities to improve and enhance compliance infrastructures

More…

4

Value Proposition – ***Benefits of Effective Practice***

Primary objectives and outcomes of an effective compliance and ethics program from the U.S. Sentencing Guidelines (USSG):

(1) Prevent and detect wrongdoing

(2) Organizational culture that encourages ethical conduct and commitment to compliance with the law

(USSG §8B2.1. Effective Compliance and Ethics Program)

✓ ***Meaningful auditing and monitoring infrastructures are essential to achieving these outcomes and support all C&E Program Effectiveness Elements!***

Value Proposition – ***Benefits of Effective Practice***

C&E Program Effectiveness: *Monitoring/Auditing*

USSG § 8B2.1(b)(5)

"(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct; …"

. . .

Value Proposition – Global Guidelines/Frameworks

Example Global Standards, Guidelines, & Frameworks

- COSO Internal Control – *Integrated Framework*
- NIST Cybersecurity Framework – *Risk Management*
- International Organization for Standardization (ISO) (*e.g., 19011, 37301*)
- Federation of European Risk Management Associations (FERMA)
- French Anticorruption Agency (AFA) – *French Sapin II Law*
- Singapore Investigations Bureau – *The Prevention of Corruption Act*
- Brazil Clean Companies Act
- UK Bribery Act and U.S. Foreign Corrupt Practices Act
- OECD Good Practice Guidance
- Competition Bureau Canada – *Corporate Compliance Programs*
- U.S. Sarbanes-Oxley Act of 2002
- World Bank Group Integrity Compliance Guidelines
- Stock Exchange Listing Standards (*e.g., NYSE*)
- Regulatory and legal standards unique to the business

More…

Value Proposition – Global Guidelines/Frameworks

Example

U.S. Department of Justice – "*Evaluation of Corp Compliance Programs*", (*Sept 2024)*

- **Key Monitoring Considerations:**
  - ✓ Methodologies used to identify, analyze, and address particular risks?
  - ✓ What monitoring infrastructures are in place? Rationale?
  - ✓ What information and metrics are used to help prevent and detect wrongdoing?
  - ✓ Is periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions?
  - ✓ Are findings actively leveraged to improve/enhance the compliance program?
  - ✓ Does the company engage in ongoing monitoring of third-party relationships? How does the company monitor its third parties?

Value Proposition – *Global Guidelines/Frameworks*

Example

DOJ Evaluation Guidance (*Sept 2024*) – *(Cont.)*

- **Internal Audit Considerations:**
  - ✓ Is there a process in place? What is the rationale for that process?
  - ✓ Are audits actually taking place? Adequate frequency?
  - ✓ Are auditing efforts focused on the right risks and issues?
  - ✓ What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings?
  - ✓ Is management and the board kept informed of audit activities and findings? How does leadership and board engage and follow-up?
  - ✓ Are audit findings leveraged for continuous improvement and mitigation efforts?

Value Proposition – *Global Guidelines/Frameworks*

Example

DOJ Evaluation Guidance (*Sept 2024*) – *(Cont.)*

- **Data Resources and Access:**
  - ✓ Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions?
  - ✓ Do any impediments exist that limit or delay access to relevant sources of data and, if so, what is the company doing to address the impediments?
- **Funding and Resources:**
  - ✓ Is there sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has sufficient funds been allocated? Have requests for resources by compliance and control functions been denied? If so, on what grounds?

Value Proposition – *Global Guidelines/Frameworks*

Example

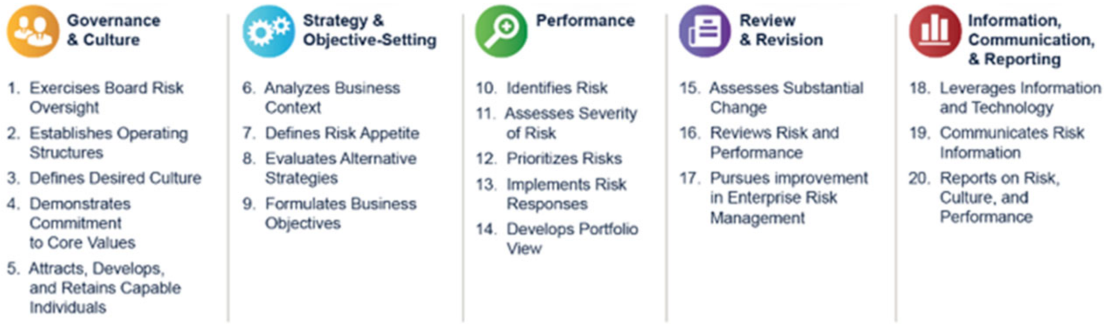
COSO - Committee of Sponsoring Organizations of the Treadway Commission

- *Established in 1985, a professional association that helps organizations improve performance through thought leadership and development of frameworks/guidance on internal control, ERM, governance and fraud deterrence*
- *Known for establishing globally recognized frameworks and guidance on Internal Control and Enterprise Risk Management (ERM); widely used by risk, audit, compliance, and other professionals to manage and mitigate risk*
- *In a joint 2020 collaboration, SCCE/HCCA and COSO introduced a global resource and framework that helps organizations effectively apply the COSO ERM Framework to compliance risk management practice (See, Compliance Risk Management: Applying the COSO ERM Framework)*

Value Proposition – *Global Guidelines/Frameworks*

Example

COSO Enterprise Risk Management (ERM) Framework



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

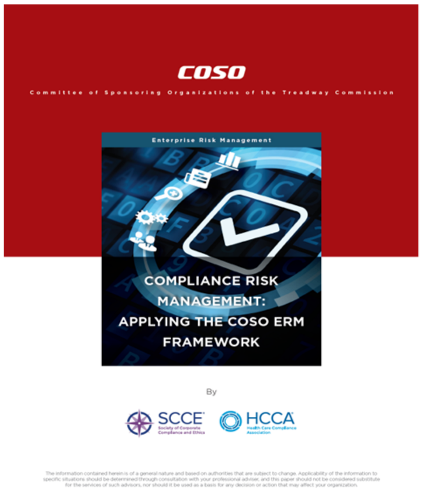
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

***See, COSO Enterprise Risk Management – Integrating with Strategy and Performance (*June 2017*)**

Value Proposition – *Global Guidelines/Frameworks*



COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK

By

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your professional adviser, and this paper should not be considered substitute for the services of such advisors, nor should it be used as a basis for any decision or action that may affect your organization.

https://www.coso.org

Value Proposition – *Global Guidelines/Frameworks*

Example

COSO Internal Control – Integrated Framework

- As defined by COSO: "*Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance*."
- Under the COSO Internal Control Framework, "monitoring" is defined as the process that assesses the quality of the internal control system's performance over time.
- Compliance with laws, regulations, and mitigation of compliance-related risks is a fundamental objective of an organization's internal control system, and is supported throughout the organization by five key components of internal control support, efforts, and activities.

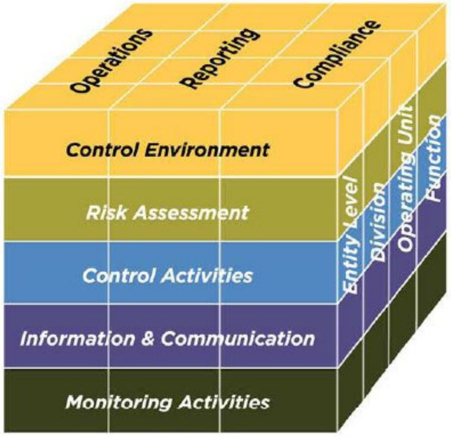
***See**, **COSO Internal Control – Integrated Framework (©2013) (www.coso.org)**

Value Proposition – *Global Guidelines/Frameworks*

Three Objectives

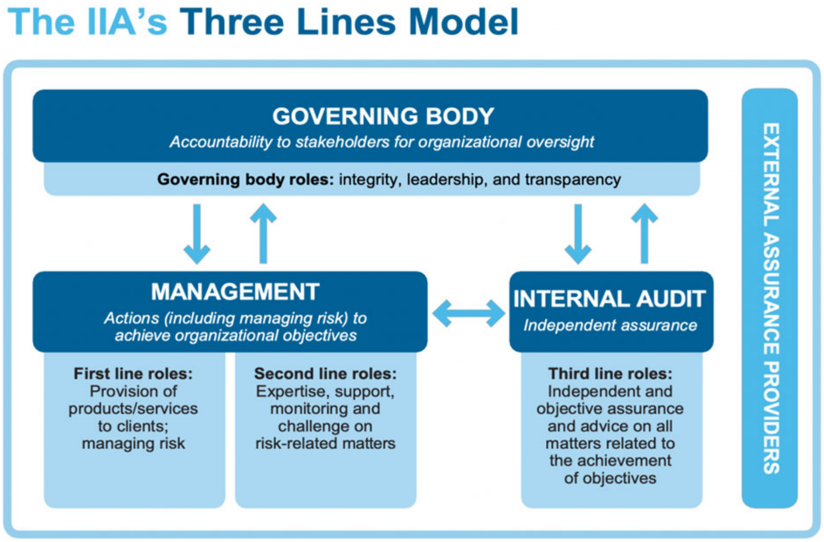
Five Components

At Various Org. Levels



***See, COSO Internal Control – Integrated Framework (©2013) (www.coso.org)**

Value Proposition – *Global Guidelines/Frameworks*



The IIA's Three Lines Model

GOVERNING BODY
Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT
Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT
Independent assurance

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

Source: The IIA's Three Line Model

Value Proposition – *Global Guidelines/Frameworks*

IIA's Three Lines Model (2020) - *Overview*

- Assists organizations in identifying structures and processes that enable the achievement of objectives and facilitate strong governance and risk management

- Enables organizations to better structure interactions and responsibilities of management, internal audit, and the governing body to more effectively and efficiently create and protect value
  - Roles are better aligned with each other on risk management priorities and stakeholder interests
  - Alignment is achieved through collaboration, communication, cooperation to ensure reliability and transparency that improves risk-based decision making

- Identifies responsibilities at:
  - **Governing body** – *Oversight Responsibilities*
  - **Management, including Operational Leaders like Risk and Compliance** – *First- and Second-Line Roles*
  - **Internal Audit** – *Third-Line Role (Independent Assurance)*
  - **External Assurance** – *Additional Assurance*

- First-Line management roles are responsible for managing risk, whereas Second-Line management roles serve to provide complementary expertise, support, monitoring, etc., to First-Line roles (e.g., C&E, ERM, HR)

17

2 Core Practice Considerations

SCCE™
Society of Corporate
Compliance and Ethics

18

Core Practice - ***Fundamentals***

What Monitoring & Auditing has in Common:

- Both Monitoring and Auditing Goals serve to:
  - ✓ *Prevent* or *Detect* non-compliance and wrongdoing
  - ✓ Test and evaluate effectiveness of compliance-related internal controls: *Design & Operating Effectiveness*
- Findings and outcomes of both activities:
  - ✓ Support continuous improvement efforts
  - ✓ May result in investigations, potential disclosures, etc.

Core Practice - ***Fundamentals***

How Monitoring & Auditing is Distinguished:

- **Auditing**
  - ✓ Independent (*Internal Audit, independent third party, etc.*)
  - ✓ Structured; uses a formalized approach
  - ✓ Usually periodic in nature; focuses on a specific period of time in the past or a snapshot view
- **Monitoring**
  - ✓ Less formal; not necessarily independent; integrated and built into the routine operations of a function
  - ✓ More likely to be ongoing/continuous in nature rather than periodic
  - ✓ More timely than auditing; identifies issues in real-time

Core Practice - *Fundamentals*

Challenges/Considerations:

- Resource Allocation and Management Accountability
- Data and Metrics – Access, Quality, Analysis, Interpretation
- Design/Implementation – Establishing scalable monitoring and auditing programs across the organization
- Effectiveness of Internal Controls – Are mitigation controls and strategies working?
- Proactive Risk Management - Without auditing and monitoring infrastructures, it is difficult to proactively identify and manage risk

Core Practice - *Fundamentals*

What about Culture?!

Effective Monitoring & Auditing Practice and related outcomes rely heavily on the existence of a strong Culture

Core elements of a good ethical culture include:

- ✓ Board engagement and oversight
- ✓ Leadership tone and commitment; Tone in Middle; Buzz at the Bottom
- ✓ Aligned core values; *accountability at all levels*
- ✓ Positive perceptions of leadership, organizational justice, core values, integrity, and ethics
- ✓ Periodic culture assessments, surveys, and related touch-points
- ✓ Speak-up culture; employees feel safe seeking help and reporting concerns
- ✓ Strong risk awareness *integrated into the DNA;* ongoing training and communication
- ✓ Continuous improvement

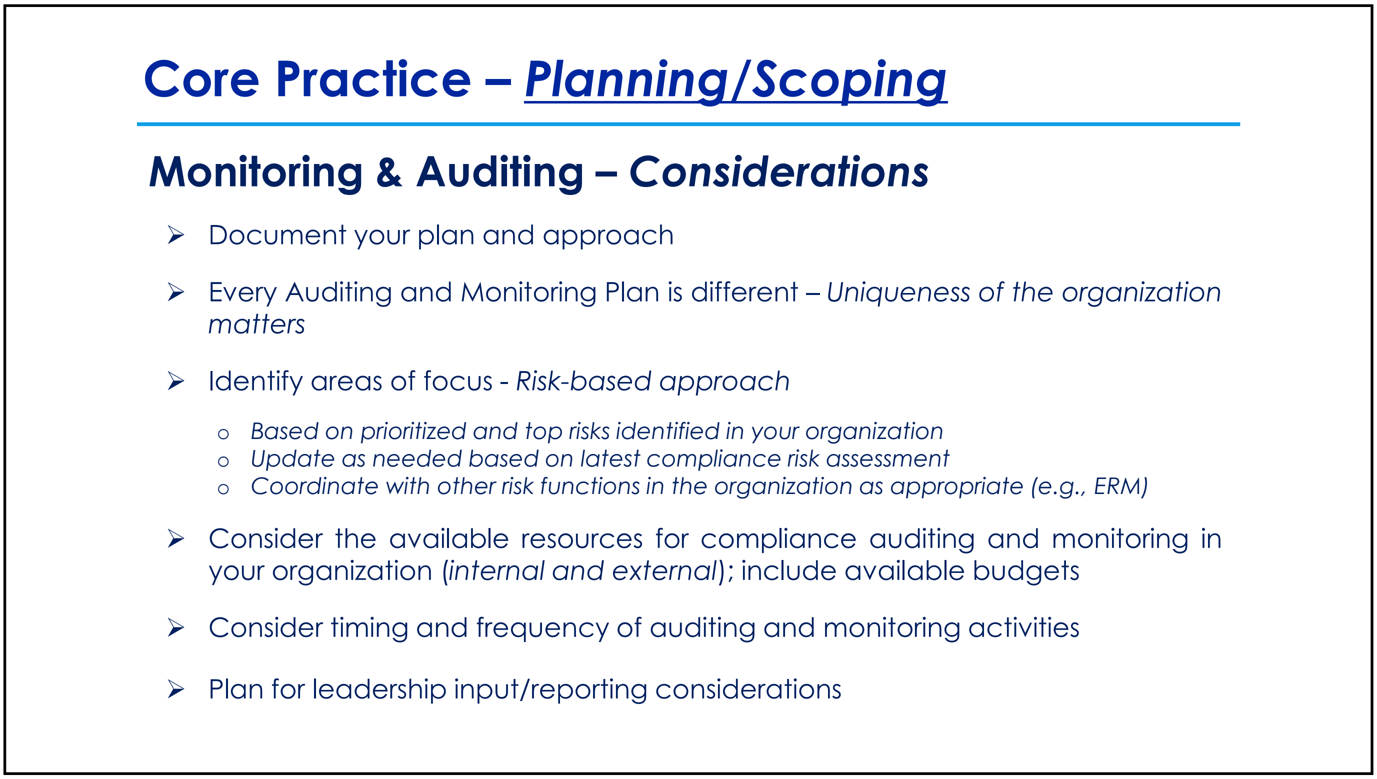
More…

Practice Planning/Scoping

Core Practice – *Planning/Scoping*

Monitoring & Auditing - *Lifecycle*

- ➢ Identify key areas of risks and focus for auditing and monitoring
- ➢ Determine type and scope of auditing and monitoring activities
- ➢ Consider specific techniques and methods to be used
  - ✓ *Include methods for capturing information, data, and findings*
- ➢ Implement and conduct auditing and monitoring activities
- ➢ Document and assess findings and output
- ➢ Reporting activities (*e.g., Board, Leadership, business*)
- ➢ Leverage auditing/monitoring findings for continuous improvement

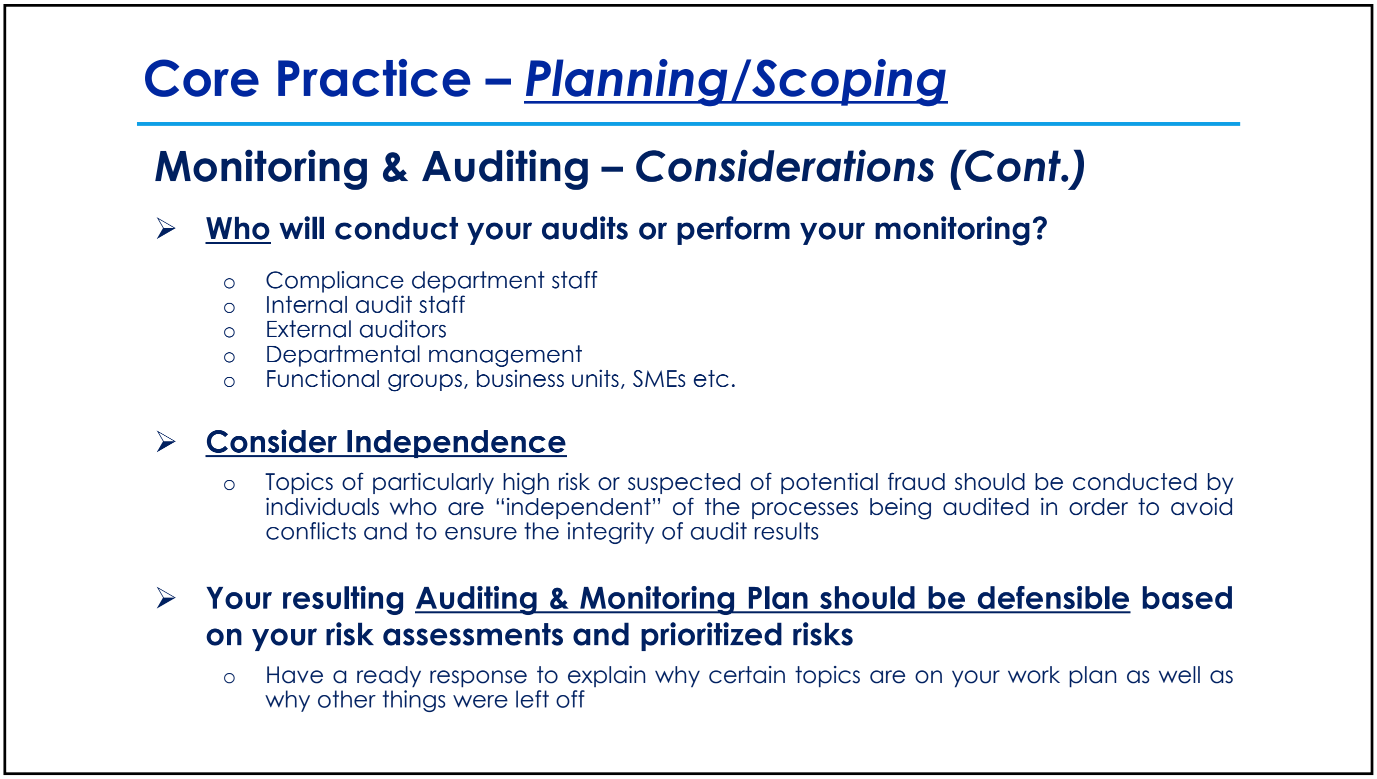


Core Practice – *Planning/Scoping*

Monitoring & Auditing – *Considerations*

- Document your plan and approach
- Every Auditing and Monitoring Plan is different – *Uniqueness of the organization matters*
- Identify areas of focus - *Risk-based approach*
  - *Based on prioritized and top risks identified in your organization*
  - *Update as needed based on latest compliance risk assessment*
  - *Coordinate with other risk functions in the organization as appropriate (e.g., ERM)*
- Consider the available resources for compliance auditing and monitoring in your organization (*internal and external*); include available budgets
- Consider timing and frequency of auditing and monitoring activities
- Plan for leadership input/reporting considerations

25



Core Practice – *Planning/Scoping*

Monitoring & Auditing – *Considerations (Cont.)*

- **Who will conduct your audits or perform your monitoring?**
  - Compliance department staff
  - Internal audit staff
  - External auditors
  - Departmental management
  - Functional groups, business units, SMEs etc.
- **Consider Independence**
  - Topics of particularly high risk or suspected of potential fraud should be conducted by individuals who are "independent" of the processes being audited in order to avoid conflicts and to ensure the integrity of audit results
- **Your resulting Auditing & Monitoring Plan should be defensible based on your risk assessments and prioritized risks**
  - Have a ready response to explain why certain topics are on your work plan as well as why other things were left off

Core Practice – *Planning/Scoping*

Common Techniques used in Monitoring & Auditing

- Verbal inquiries/Interviews (*e.g., One-on-one and Focus Groups*)
- Surveys
- Observation
- Statistical Review/Analysis
- Review of policies and procedures
- Checklists
- Vouching/testing
- Reperforming/recalculating
- Analytics; review of metrics (*e.g., KPIs & KRIs*)

27

Monitoring Overview

28

Core Practice – *Monitoring*

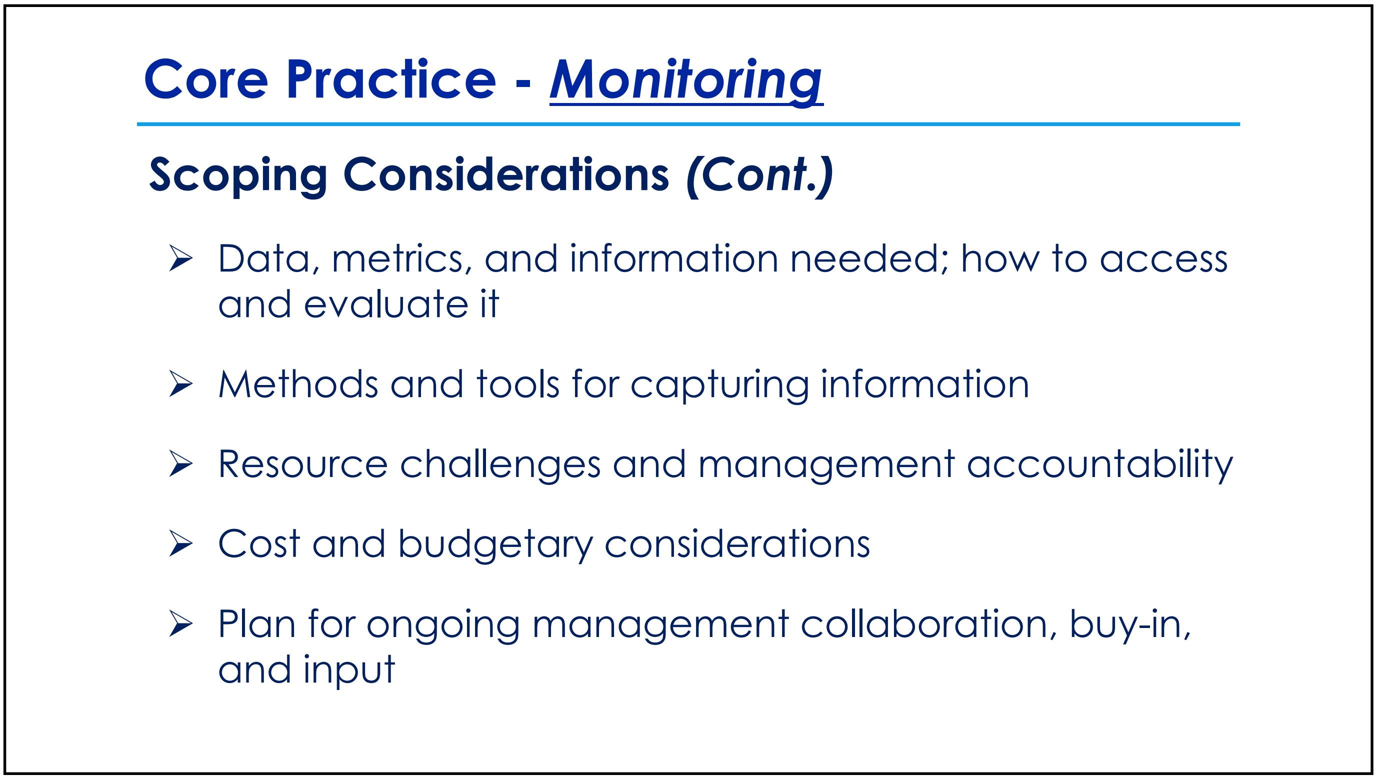
Overview

- ➢ Effective monitoring leverages consistent tools to evaluate ongoing performance; tracked over time and measured for improvement and trending
  - ❖ Consistent measuring tools evaluate the same factors, metrics, attributes each time they are used
  - ❖ Routine monitoring over time generally includes a consistent interval (*e.g., weekly, monthly, quarterly*). Intervals may also be event driven (*e.g., each time an event occurs*)
  - ❖ Allows for effective tracking and trending of performance to confirm ongoing compliance or flag variances that may indicate noncompliance, adverse outcomes or need for follow-up
  - ❖ Automate wherever possible to save time and effort; Leverage technology

Core Practice - *Monitoring*

Scoping Considerations

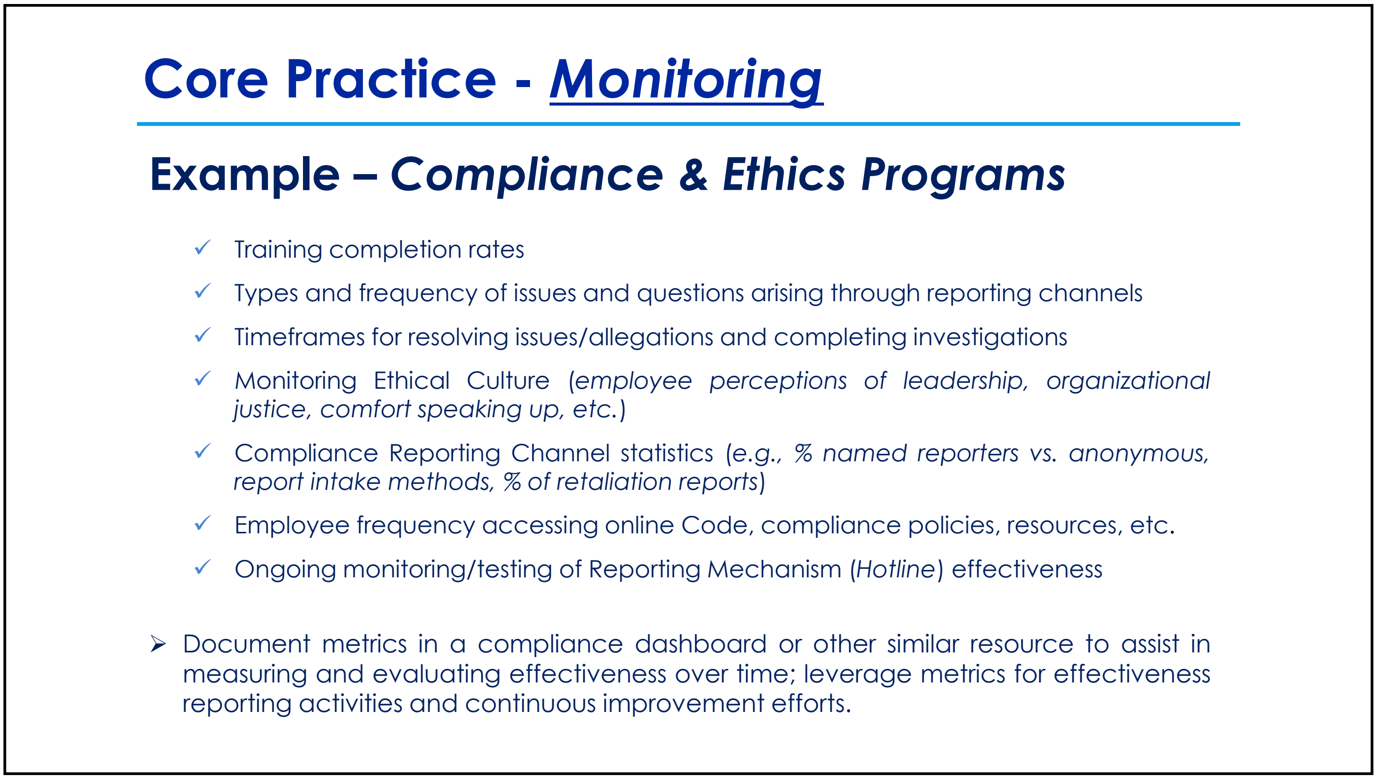
- ➢ Coverage across operations and business
  - ❖ *Risk based approach*
  - ❖ *Identify specific risk areas, metrics, and related business operations that will be monitored*
    - ✓ Include areas with potential for risk of non-compliance; people, processes, and technology
- ➢ Volume of transactions, activities, and metrics to be monitored



Core Practice - *Monitoring*

Scoping Considerations *(Cont.)*

- Data, metrics, and information needed; how to access and evaluate it
- Methods and tools for capturing information
- Resource challenges and management accountability
- Cost and budgetary considerations
- Plan for ongoing management collaboration, buy-in, and input



Core Practice - *Monitoring*

Example – *Compliance & Ethics Programs*

- ✓ Training completion rates
- ✓ Types and frequency of issues and questions arising through reporting channels
- ✓ Timeframes for resolving issues/allegations and completing investigations
- ✓ Monitoring Ethical Culture (*employee perceptions of leadership, organizational justice, comfort speaking up, etc.*)
- ✓ Compliance Reporting Channel statistics (*e.g., % named reporters vs. anonymous, report intake methods, % of retaliation reports*)
- ✓ Employee frequency accessing online Code, compliance policies, resources, etc.
- ✓ Ongoing monitoring/testing of Reporting Mechanism (*Hotline*) effectiveness

- Document metrics in a compliance dashboard or other similar resource to assist in measuring and evaluating effectiveness over time; leverage metrics for effectiveness reporting activities and continuous improvement efforts.

Auditing Overview

Core Practice - ***Auditing***

Overview

➢ Audits typically ***look back*** at activity ***over a specific period of time*** and enable you to determine whether controls have been operating effectively and detect potential incidences of non-compliance. Consider compliance areas of highest risk

- ❖ Identify business processes and internal controls related to the risk areas chosen
- ❖ Review results of any existing monitoring efforts, control assessments or audit activities already in place for each risk area, identify gaps
- ❖ Identify the auditing tools and techniques that will be required
- ❖ Consider internal resources available with the necessary language, skill, expertise and independence or cost of obtaining external resources
- ❖ Establish process for legal oversight if necessary

Core Practice - ***Auditing***

Scoping Considerations

- Objectives (*financial, operational, compliance, fraud*)
- Entities under review (*business units/locations/functions, third parties*)
- Time period under review
- Specific areas under review (*compliance risks, business processes, internal controls*)
- Volume of transactions, activities to be audited
- Approach (*techniques/methodologies used, announced/scheduled v. surprise*)
- Who will conduct (*internal and/or external resources*)
- What will be excluded

Core Practice - ***Auditing***

Audit Sampling - ***Defined***

"Audit sampling is the application of an audit procedure to less than 100 percent of the items within an account balance or class of transactions for the purpose of evaluating some characteristic of the balance or class."

Source: PCAOB - https://pcaobus.org/oversight/standards/auditing-standards/details/AS2315

Approaches to Sampling

Method of pulling a random sample from the population to be tested:

- **Retrospective** – going backwards in time
  - ✓ Identify a milestone to go back to (*new guideline, system, new product, people, timeframe, etc.*)
- **Concurrent** – real time (*while the activity is occurring*)
  - ✓ Best way to change behavior

Core Practice - ***Auditing***

Audit Sampling Methodology - *Statistical*

- Statistical sampling is a technique where a representative sample size is defined, and ***conclusions can be drawn about the population from testing that sample***
  - Every member of the population must have an ***equal positive probability of being selected***
  - To be statistically valid, the sample ***must be selected at random*** with no bias or other distortions that could make it non-representative
  - The results of a statistical sample ***can be extrapolated*** to make assumptions about the population universe
  - Precision and confidence levels indicate an acceptable level of sampling error

Core Practice - ***Auditing***

Audit Sampling Methodology – *Non-Statistical or Judgmental*

- Generally, refers to a sampling technique based on an auditor's judgment rather than a formal statistical approach (*e.g., discretion on how results are evaluated*)
  - May be selected based on pre-determined red flags or key indicators of a particular risk
  - Is *NOT* random
    - **Can't assure equal positive probability** of every member of the population being selected
    - Sample **CANNOT be extrapolated** to make assumptions about the population universe
    - May require expansion of sample or scope based on findings

Core Practice - *Auditing*

Audit Findings/Results - *Reporting*

- Description of the original audit scope, including any scope limitations/modifications made and the reasons for them
- The approach to the audit (*sampling, nature of tests, techniques applied, etc.*)
- Background/context for the area under review
- Opinion on results of the audit *(satisfactory, needs improvement, unsatisfactory)*
- Detailed listing of findings *(control weaknesses/failures, incidences of noncompliance)* made *(typically ranked by significance)*
- Recommendations for action to address findings in the audit
- Final report should include management's action plans and commitment to complete within an agreed timeframe

Core Practice - *Auditing*

Audit Results – *Management Action Plans*

- **Obtain Management Action Plans (MAPs) from Business Owners**
  - Format and content of MAPs
    - Audit finding and recommendation made by auditors
    - Management stated action plan agreed with auditors
    - Person/Role responsible for completing the MAP
    - Target completion date

- **Reporting to appropriate leaders/stakeholders**
  - Status of MAPs should be routinely reported in your leadership meetings (*Compliance Committee, Board Audit Committee*) until they are completed
  - MAPs will need to be tracked and followed-up on over time, so the MAP format provides a convenient tracking mechanism; consider a MAP tracking tool

Monitoring & Auditing

Use of Data Analytics

Use of Data Analytics - *Overview*

Data analytics is a **multidisciplinary field that employs a wide range of analysis techniques, including math, statistics, and computer science, to draw insights from data sets.**

It is the process of **collecting, cleaning, sorting, and processing raw data to extract relevant and valuable information to help businesses.**

Data analysis is the process of **evaluating data using analytical or statistical tools to discover useful information.**

Tools such as Microsoft Excel and programming languages like R or Python are popular in the world of data analytics.

Use of Data Analytics – *Application*

- ***Data Analytics*** tools are used to analyze large data sets to identify trends and anomalies, make monitoring and/or audit processes more efficient and improve accuracy. Enables the user to analyze 100% of a population.
- Compliance & Ethics program applications include:
  - ***Risk Assessment*** - Assessing the risk of noncompliance
  - ***Monitoring & Auditing*** – identify possible incidences of noncompliance or internal control breakdowns; assess the effectiveness of compliance & ethics programs
  - ***Investigations*** – to help identify extent of potential noncompliance

Use of Data Analytics – *Advanced Practice*

More sophisticated Data Analytics or Artificial Intelligence may also be used in Monitoring & Auditing efforts

- **Artificial Intelligence (AI)** -"Artificial intelligence (AI) applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions."(Gartner IT Glossary 2019)
- **Machine Learning (ML) -** allows machines to scan large volumes of data to learn and make recommendations, provide insights or take actions.
- **Predictive Analytics -** A data analytics category that uses statistical techniques, machine learning, and other tools to analyze data and predict outcomes. Predictive analytics can help companies anticipate trends and behaviors.

Use of Data Analytics - *Example*

- **Corruption Risk Control –** Gift and Entertainment approval process, policy and limits

- **Previous way of monitoring/auditing:** Manually review random sample of gift and entertainment expenditures to look for exceptions, failures to follow process or policy, instances of exceeding limits – perhaps use Excel to assist with data sorting

- **AI/ML method:** AI tool automatically "trawls" your system on a continuous basis for data from Concur, your GL, your gift registry, etc. Automatically reviews ALL data for exceptions and provides you with a short risk-ranked list of exceptions; tracks master data to enable targeted interventions and revisions to controls

Monitoring & Auditing

Takeaways

Monitoring & Auditing – *Takeaways*

Identified Compliance Concerns

What to do when monitoring or audit results indicate a possible compliance concern

- ➢ Consult with Legal immediately upon identification to determine whether legal supervision and privilege are warranted
- ➢ Open a new investigation, staffed by appropriate expert resources
- ➢ Prepare a separate report of investigation findings and recommendations for limited distribution to appropriate leadership and Board Audit/Compliance Committee

Monitoring & Auditing – *Takeaways*

Effective Monitoring and Auditing practice supports the following:

- ➢ Identification of risk to the business that may have otherwise been undetected
- ➢ Provides assurance to management regarding risk mitigation efforts, including the effectiveness of internal controls
- ➢ Prevention of risk events from escalating through early detection which helps avoid additional harm to the company's business
- ➢ Demonstrates a commitment to effective management and mitigation of risk across the business and continuous improvement

Monitoring and Auditing is a critical element for an effective compliance program and helps to drive compliance and behavior!

3 Periodic Evaluation of C&E Programs

SCCE™
Society of Corporate
Compliance and Ethics

49

Periodic Evaluation of C&E Programs

C&E Program Effectiveness: *Periodic Evaluation*

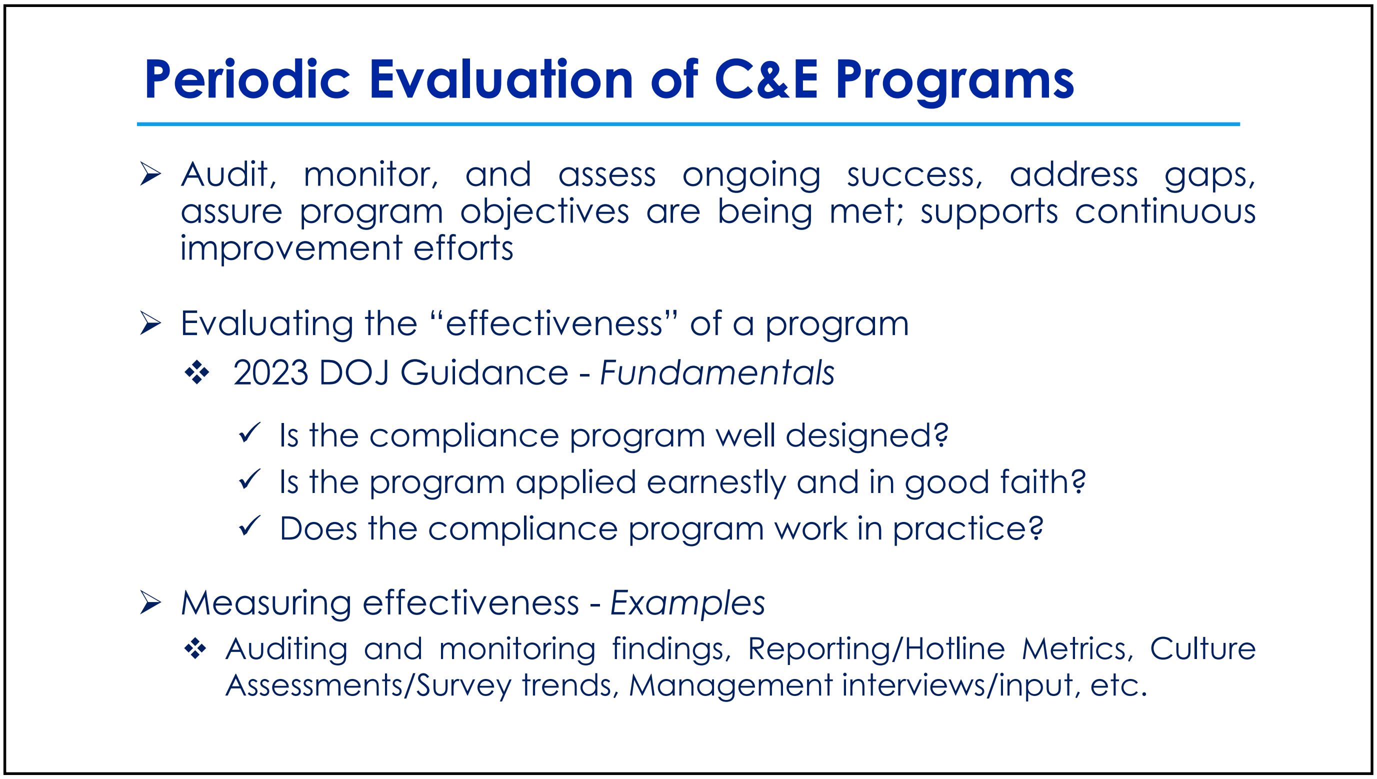
USSG § 8B2.1(b)(5)

“(5) The organization shall take reasonable steps—

> …
>
> *(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program;…”*

SCCE™
Society of Corporate
Compliance and Ethics

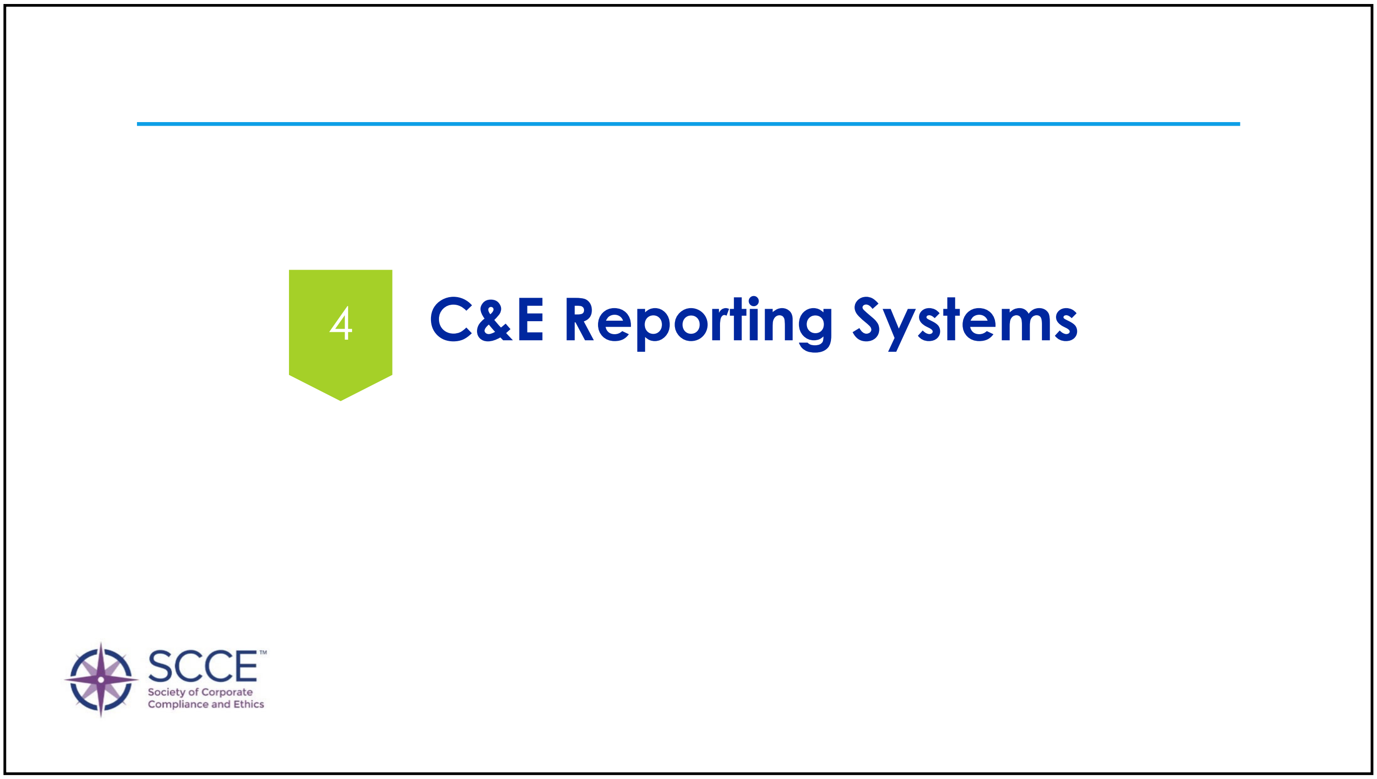
50



Periodic Evaluation of C&E Programs

- Audit, monitor, and assess ongoing success, address gaps, assure program objectives are being met; supports continuous improvement efforts
- Evaluating the “effectiveness” of a program
  - 2023 DOJ Guidance - *Fundamentals*
    - ✓ Is the compliance program well designed?
    - ✓ Is the program applied earnestly and in good faith?
    - ✓ Does the compliance program work in practice?
- Measuring effectiveness - *Examples*
  - Auditing and monitoring findings, Reporting/Hotline Metrics, Culture Assessments/Survey trends, Management interviews/input, etc.

51



4 C&E Reporting Systems

SCCE™
Society of Corporate
Compliance and Ethics

52

Compliance & Ethics Reporting Systems

C&E Program Effectiveness: *Reporting Systems*

USSG § 8B2.1(b)(5)

"(5) The organization shall take reasonable steps—

…

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."

Compliance & Ethics Reporting Systems

- **Purpose:**
  - ❖ Reporting allegations or suspicions of wrongdoing
  - ❖ Asking questions and/or seeking guidance on C&E matters
- **Value Proposition**
  - ✓ Prevents and detects wrongdoing
  - ✓ Enables effective issue/incident management and response
  - ✓ Provides timely support for C&E inquiries and questions
  - ✓ Supports risk mitigation and remedial measures
  - ✓ C&E continuous improvement (*Use of Hotline metrics, Lessons learned, etc.*)

Compliance & Ethics Reporting Systems

- **Reporting Infrastructures** - ***Keys to success***
  - Speak Up Culture
  - Zero-tolerance Non-Retaliation Policy in place; consistently enforced
  - Multiple Reporting Channels Provided
    - ✓ Management
    - ✓ E&C Office, Legal, Other
    - ✓ Hotline/Helpline

55

Compliance & Ethics Reporting Systems

- **Reporting Infrastructures** - ***Keys to success (Cont.)***
  - Confidential/Anonymous Reporting Options
    - ✓ Includes options for anonymous reporting if preferred
  - Global Considerations
    - ✓ Culture
    - ✓ Reporting Limitations
  - Ongoing Awareness efforts and Hotline Mechanism effectiveness
    - ✓ *Includes Monitoring/Testing activities*

56

Compliance & Ethics Reporting Systems

- **Reporting Infrastructures** - ***Keys to success (Cont.)***
  - Timely and effective issue-handling and management protocols
    - ✓ All reports and/or inquiries logged and reviewed to determine next steps, as appropriate
    - ✓ Written policies and procedures for follow-up and investigations, consistently followed
    - ✓ Reporting back to reporter, as appropriate, with status and outcomes

57

Compliance & Ethics Reporting Systems

- **Reporting Infrastructures** - ***Keys to success (Cont.)***
  - Hotline/Helpline Considerations
    - ✓ Independent Third-Party Vender; 24/7/365 capabilities
    - ✓ Multi-lingual operators/translation services
    - ✓ Offers confidential/anonymous reporting options – *Telephonic/Online*
    - ✓ Detailed/consistent intake methods and reports; timely escalations when appropriate
      - Includes protocol for re-routing if company contact is named
  - System Security!

58

Questions?

Compliance Essentials Workshop

Compliance Investigations

SCCE & HCCA

Wendy Evans
Senior Investigator & Senior Manager, Ethics Core Programs
Lockheed Martin

1

1

Key Topics for Today

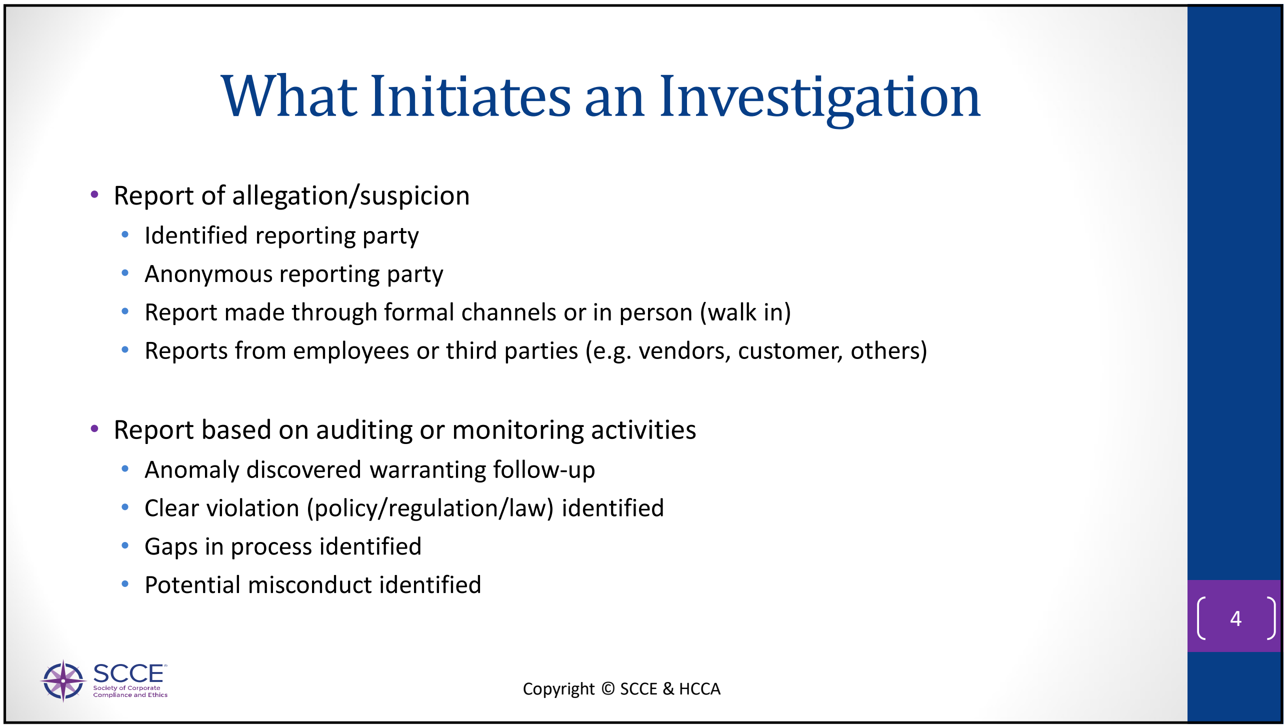
- Initiating an investigation
- Gathering and analyzing evidence
- Conducting interviews
- Managing investigator bias
- Following investigative procedures
- Documenting investigative efforts
- Using third parties to assist with investigations
- Reporting investigative results

2

2

Initiating an investigation

SCCE Society of Corporate Compliance and Ethics



What Initiates an Investigation

- Report of allegation/suspicion
  - Identified reporting party
  - Anonymous reporting party
  - Report made through formal channels or in person (walk in)
  - Reports from employees or third parties (e.g. vendors, customer, others)

- Report based on auditing or monitoring activities
  - Anomaly discovered warranting follow-up
  - Clear violation (policy/regulation/law) identified
  - Gaps in process identified
  - Potential misconduct identified

SCCE Society of Corporate Compliance and Ethics

Purposes of an Investigation

- Determining whether an act of misconduct or non-compliance occurred
- Determining who was involved
- Determining how long the issue has been occurring
- Determining how the act(s) occurred
  - Incidental or Systemic Issue?
  - Remediation to prevent future risks
- Determining extent of damages
  - Are disclosures necessary to government? Notifications to stakeholders?

SCCE Society of Corporate Compliance and Ethics

Common Areas of Focus

- Billing-related matters (False Claims Act)
- Bribery and corruption issues (FCPA, UK Bribery Act)
- Privacy or data protection (HIPAA, GDPR, State Laws)
- Other federal, state or local laws and regulations
- Contract violations
- Noncompliance with professional standards
- Conflicts of interest
- Violations of code of conduct or other policies

SCCE Society of Corporate Compliance and Ethics

Assessing Allegations

- Guidance/advice versus Investigation
  - Who, what, when, where, how (and how long has conduct or issue been going on?)
  - What processes are involved in this matter (expense reporting? Behavioral issue?)
  - What needs to have happened in order for the allegation to be true?
  - What motivated the Reporting Party to come forward?
  - What policy may be impacted?
  - Were internal controls circumvented?
  - Does RP have all the facts/information? (Probably not)
  - What digital, documentary or other evidence is there?

7

SCCE Society of Corporate Compliance and Ethics

Notifications

- Misconduct, non-compliance event or policy/code violation must be investigated
- Enter into your case management system ASAP
- Notifications
  - Subject’s manager and Human Resources Business Partner
- Subject Matter Experts
  - IT
  - Security
  - EEO
  - Legal (internal/external)
- Regular updates to Reporting Party

8

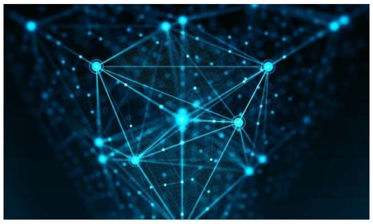
SCCE Society of Corporate Compliance and Ethics

Doing your Homework
Gathering Data and Documents

9

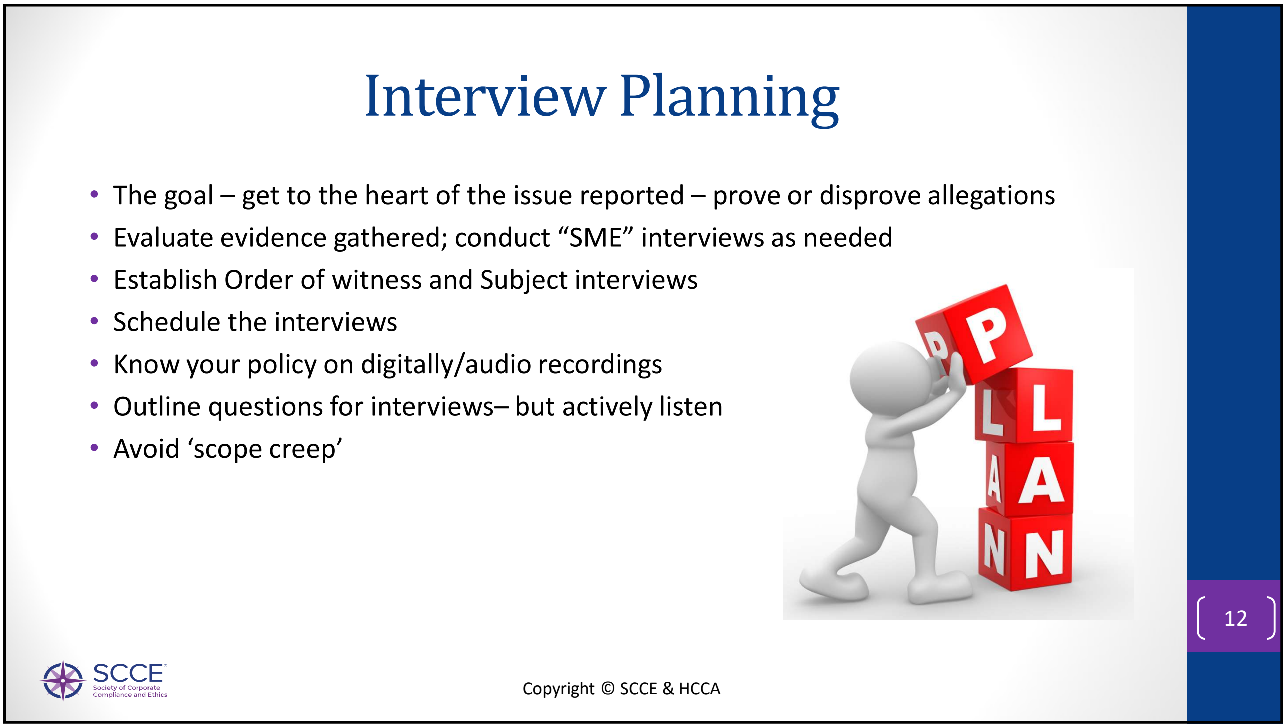
Identifying Records & Data Needed

- Background
  - Research the organization; leadership, direct reports, what the team does for the org
  - Check case management database for previous issues/involvements of the RP, Subjects
- Process Maps
  - MUST understand processes involved, and/or how the transaction cycle operates in order to identify relevant records needed
- Identify:
  - Leaders/stakeholders
  - Witnesses
  - SMEs
  - Internal controls
  - Documents and records



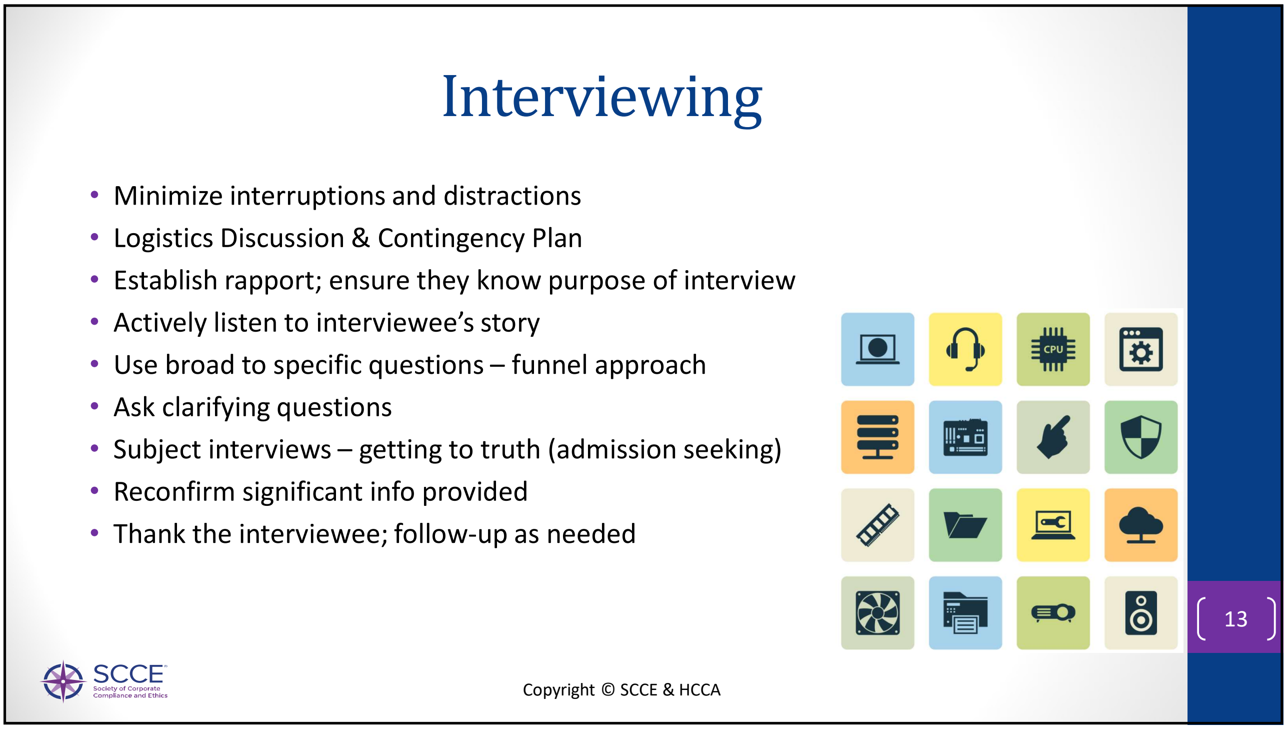
10

Conducting Interviews



Interview Planning

- The goal – get to the heart of the issue reported – prove or disprove allegations
- Evaluate evidence gathered; conduct “SME” interviews as needed
- Establish Order of witness and Subject interviews
- Schedule the interviews
- Know your policy on digitally/audio recordings
- Outline questions for interviews– but actively listen
- Avoid ‘scope creep’

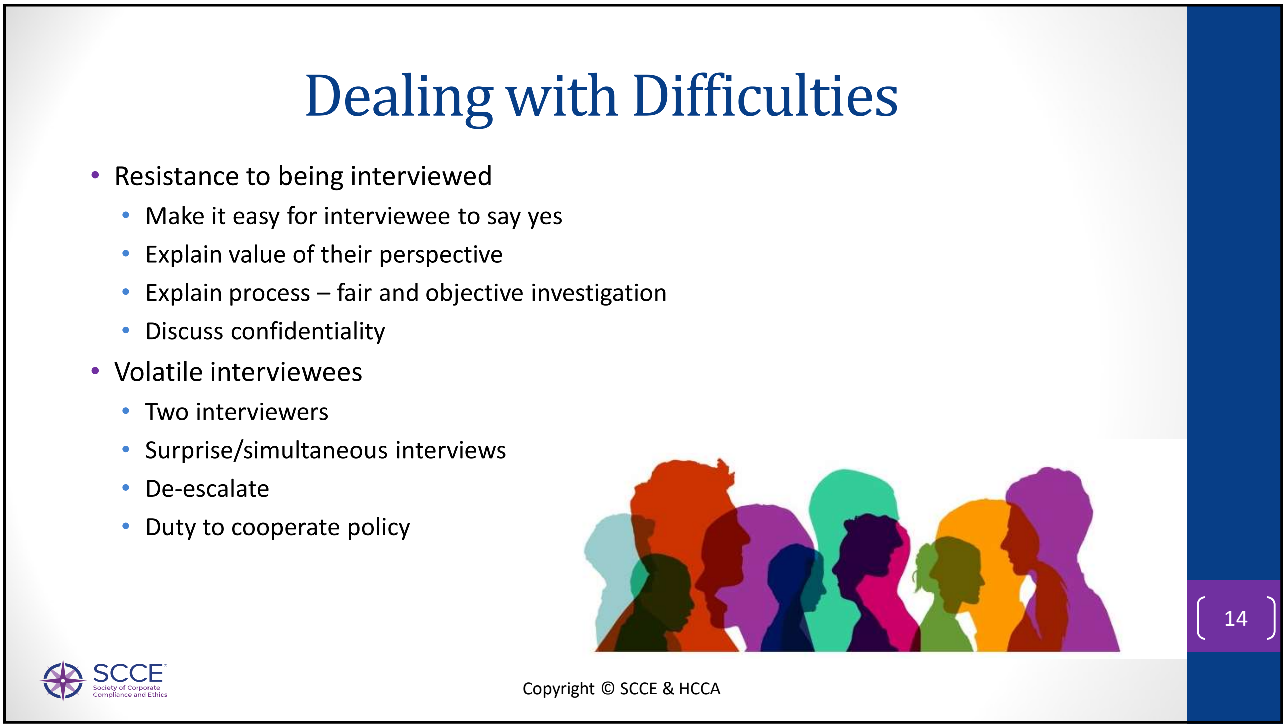


Interviewing

- Minimize interruptions and distractions
- Logistics Discussion & Contingency Plan
- Establish rapport; ensure they know purpose of interview
- Actively listen to interviewee’s story
- Use broad to specific questions – funnel approach
- Ask clarifying questions
- Subject interviews – getting to truth (admission seeking)
- Reconfirm significant info provided
- Thank the interviewee; follow-up as needed

13

13



Dealing with Difficulties

- Resistance to being interviewed
  - Make it easy for interviewee to say yes
  - Explain value of their perspective
  - Explain process – fair and objective investigation
  - Discuss confidentiality
- Volatile interviewees
  - Two interviewers
  - Surprise/simultaneous interviews
  - De-escalate
  - Duty to cooperate policy

14

14

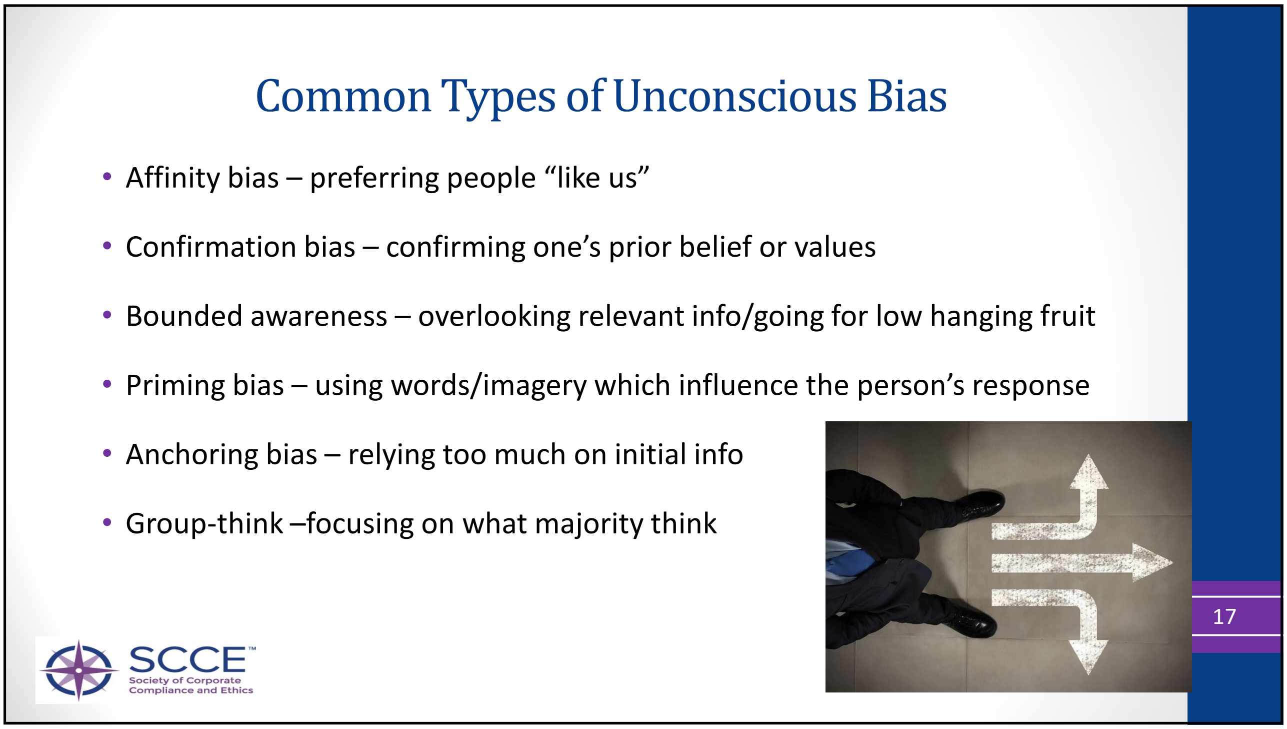
Admission-Seeking Interviews

- Don’t go fishing; don’t mislead (purport to have more information than you do)
- Allow sufficient time for interview
- **Ask the tough, direct questions (use funnel approach – broad to specific)**
- Avoid using emotive words like “fraud” “crime”
- Ask for and offer understanding for why the subject did what they did
- Dealing with denial

SCCE Society of Corporate Compliance and Ethics

How Bias Impacts Investigations

SCCE Society of Corporate Compliance and Ethics



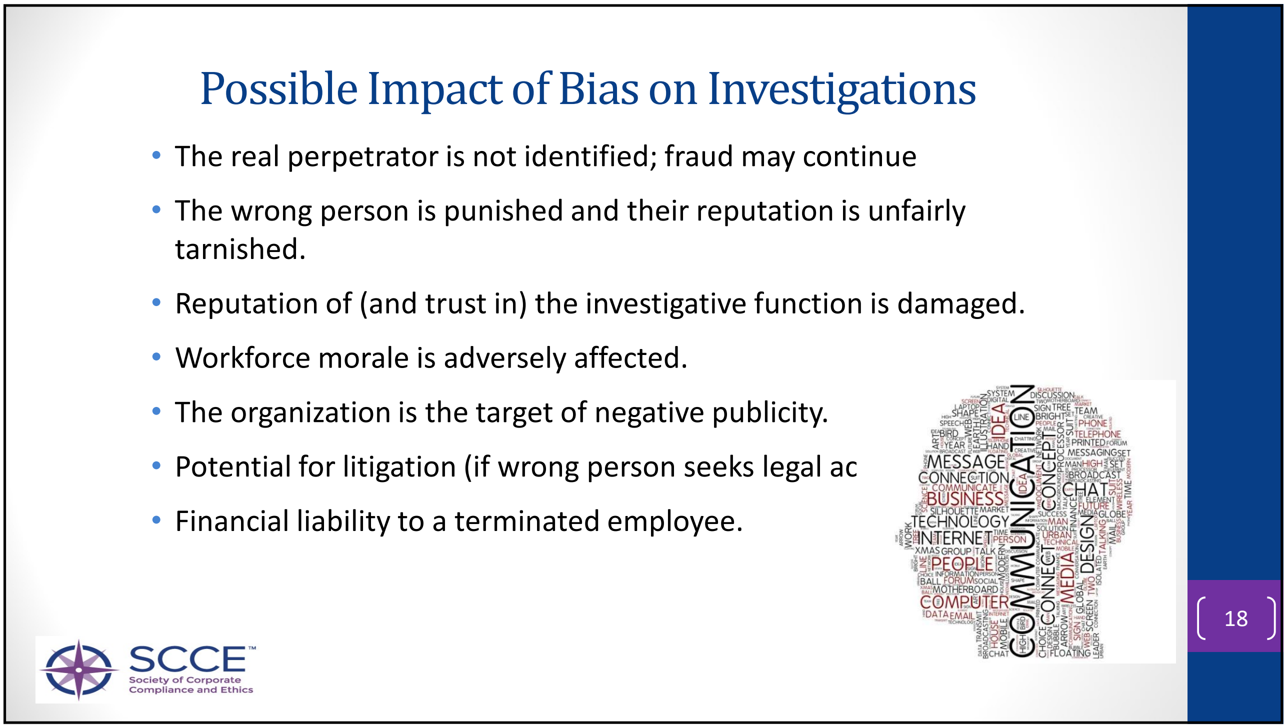
Common Types of Unconscious Bias

- Affinity bias – preferring people "like us"
- Confirmation bias – confirming one's prior belief or values
- Bounded awareness – overlooking relevant info/going for low hanging fruit
- Priming bias – using words/imagery which influence the person's response
- Anchoring bias – relying too much on initial info
- Group-think –focusing on what majority think

SCCE™ Society of Corporate Compliance and Ethics

17

17



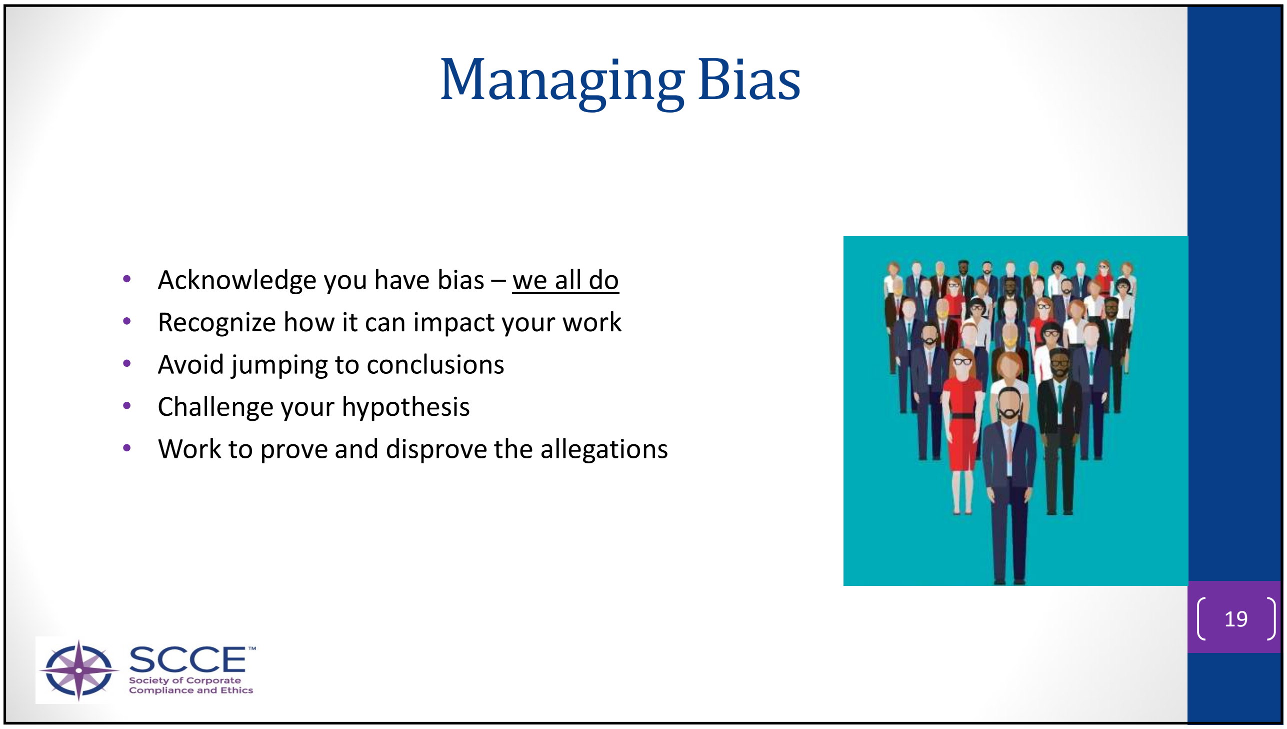
Possible Impact of Bias on Investigations

- The real perpetrator is not identified; fraud may continue
- The wrong person is punished and their reputation is unfairly tarnished.
- Reputation of (and trust in) the investigative function is damaged.
- Workforce morale is adversely affected.
- The organization is the target of negative publicity.
- Potential for litigation (if wrong person seeks legal ac
- Financial liability to a terminated employee.

SCCE™ Society of Corporate Compliance and Ethics

18

18



Managing Bias

- Acknowledge you have bias – we all do
- Recognize how it can impact your work
- Avoid jumping to conclusions
- Challenge your hypothesis
- Work to prove and disprove the allegations

Investigative Policies & Procedures

Best Practices

- In-house policy on investigations
- Expectations of employee participation
- Process for initial intake
- Checklists and Investigative Plans
- Case management system
- Escalation and notification guidelines
- Documentation requirements
- Toolkit – templates and forms
- Review (quality control) processes
- Training for investigators

SCCE
Society of Corporate Compliance and Ethics

Using Third Parties to Assist in Performing Investigations

SCCE
Society of Corporate Compliance and Ethics

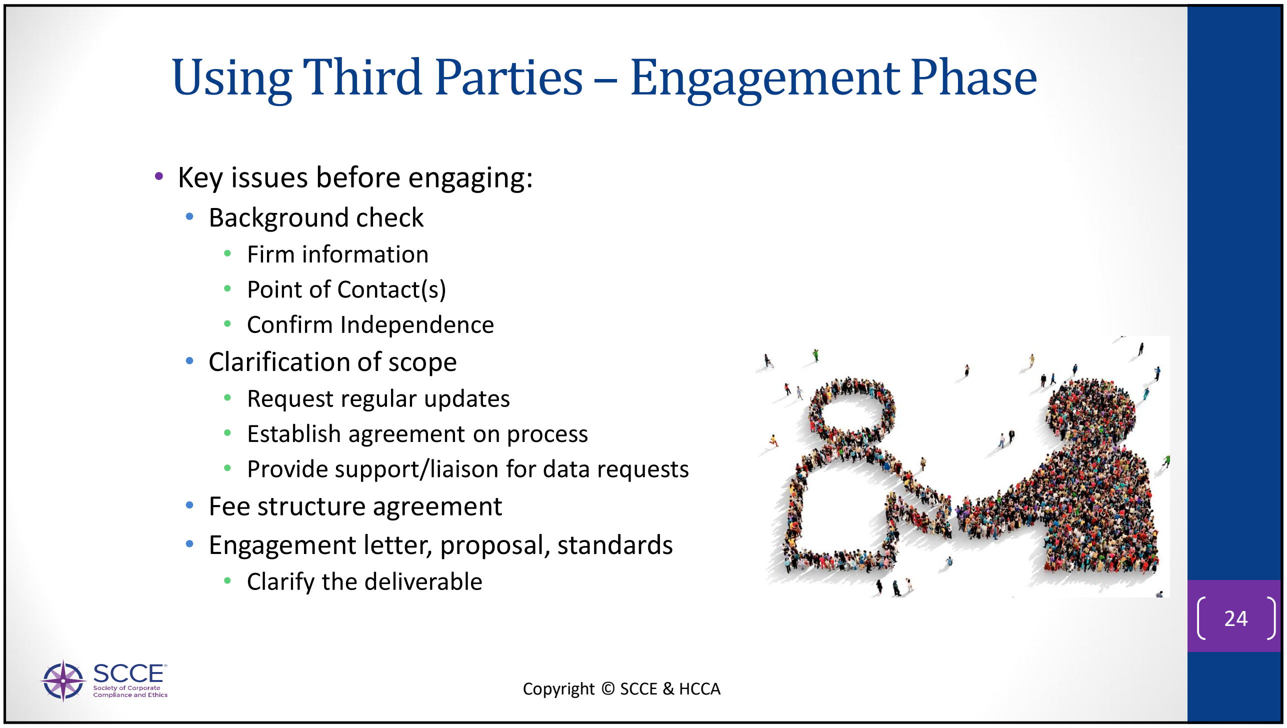
When/Why Use Third Parties?

- Independence
- Specialized expertise
- Localized expertise/geographic location
- Time constraints for business
- High risk matters

23

SCCE Society of Corporate Compliance and Ethics

23



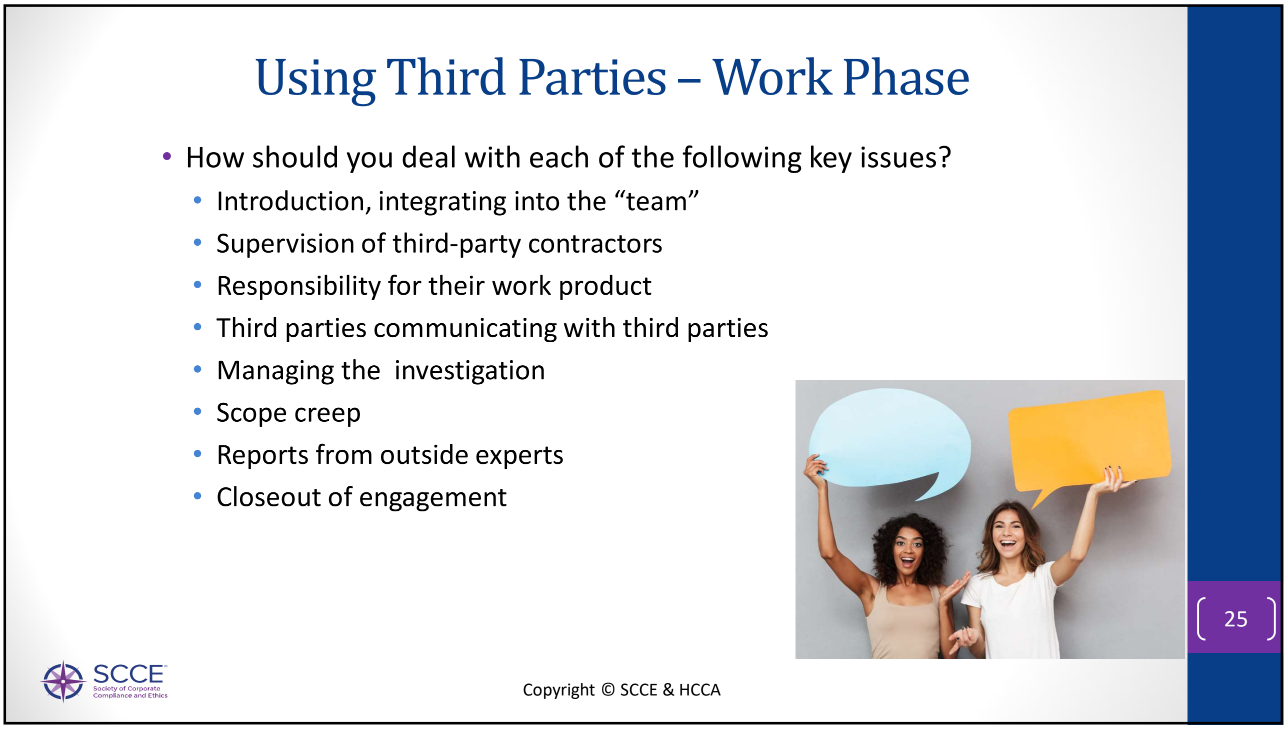
Using Third Parties – Engagement Phase

- Key issues before engaging:
  - Background check
    - Firm information
    - Point of Contact(s)
    - Confirm Independence
  - Clarification of scope
    - Request regular updates
    - Establish agreement on process
    - Provide support/liaison for data requests
  - Fee structure agreement
  - Engagement letter, proposal, standards
    - Clarify the deliverable

24

SCCE Society of Corporate Compliance and Ethics

24



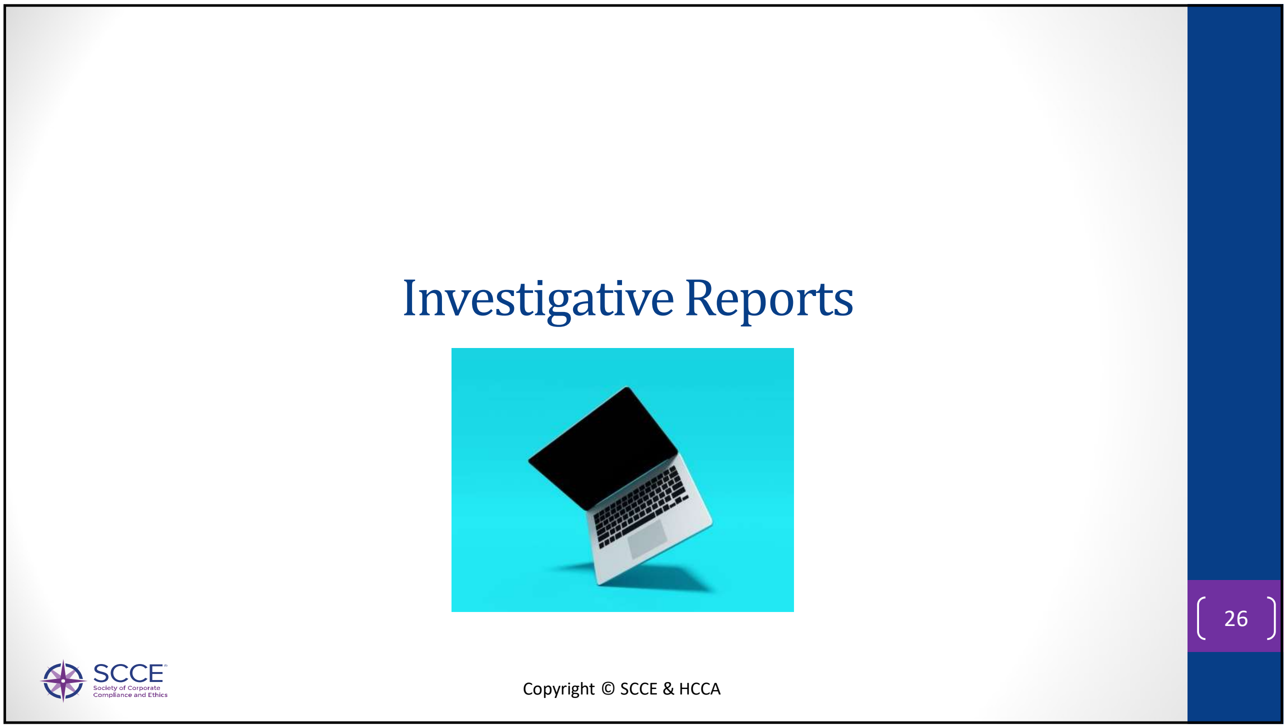
Using Third Parties – Work Phase

- How should you deal with each of the following key issues?
  - Introduction, integrating into the "team"
  - Supervision of third-party contractors
  - Responsibility for their work product
  - Third parties communicating with third parties
  - Managing the investigation
  - Scope creep
  - Reports from outside experts
  - Closeout of engagement

25

SCCE
Society of Corporate Compliance and Ethics

25



Investigative Reports

26

SCCE
Society of Corporate Compliance and Ethics

26

Investigative Reports

- Document investigation – substantiated or not
- Include direct quotes where impactful
- Avoid opinion – remain objective
- Ensure fact-gathering remained in scope
- Articulate fact-based investigative conclusion
    - More likely than not standard
- Distribute report on “need to know” basis

SCCE Society of Corporate Compliance and Ethics

Key Take-Aways

- Plan your investigation
- Avoid confirmation and other bias
- Evaluate relevant data
- Seek SME assistance as needed
- Prepare for interviews – maintain scope
- Document investigative process
- Prepare report of investigation
- Present investigative results
- Note any post-investigative corrective action

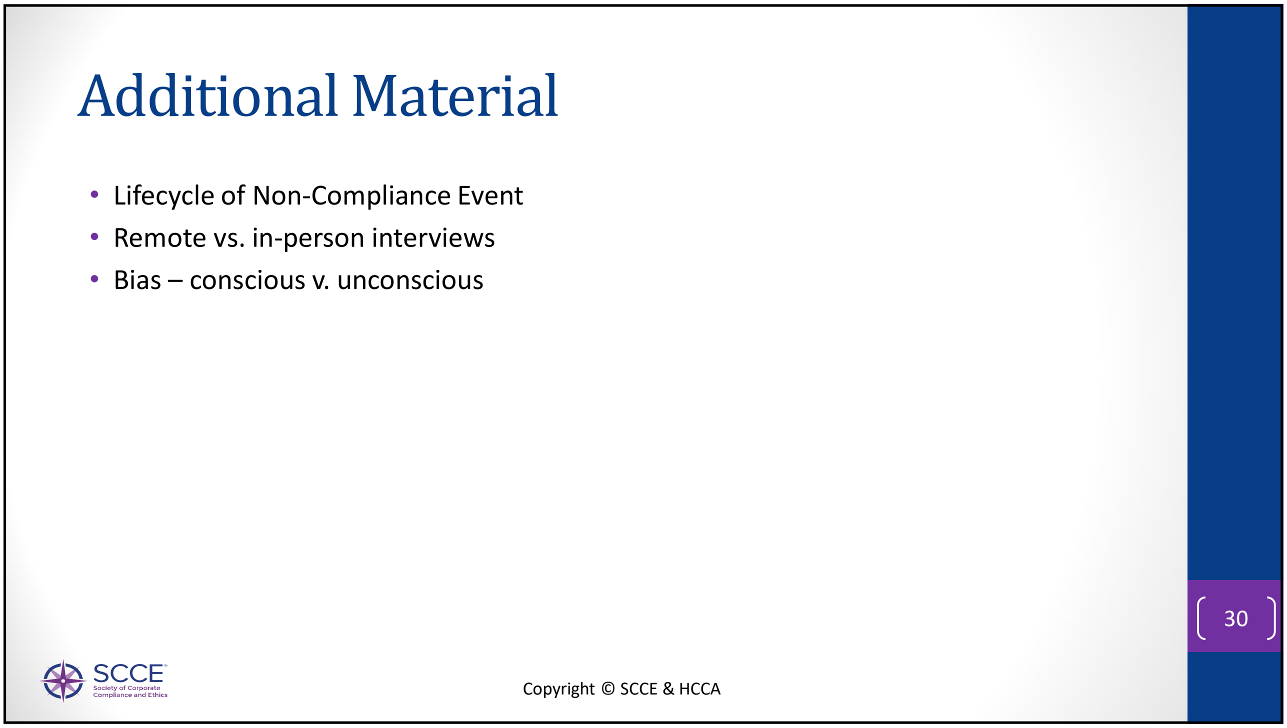
SCCE Society of Corporate Compliance and Ethics

Questions ?

wendy.w.evans@lmco.com

29

29

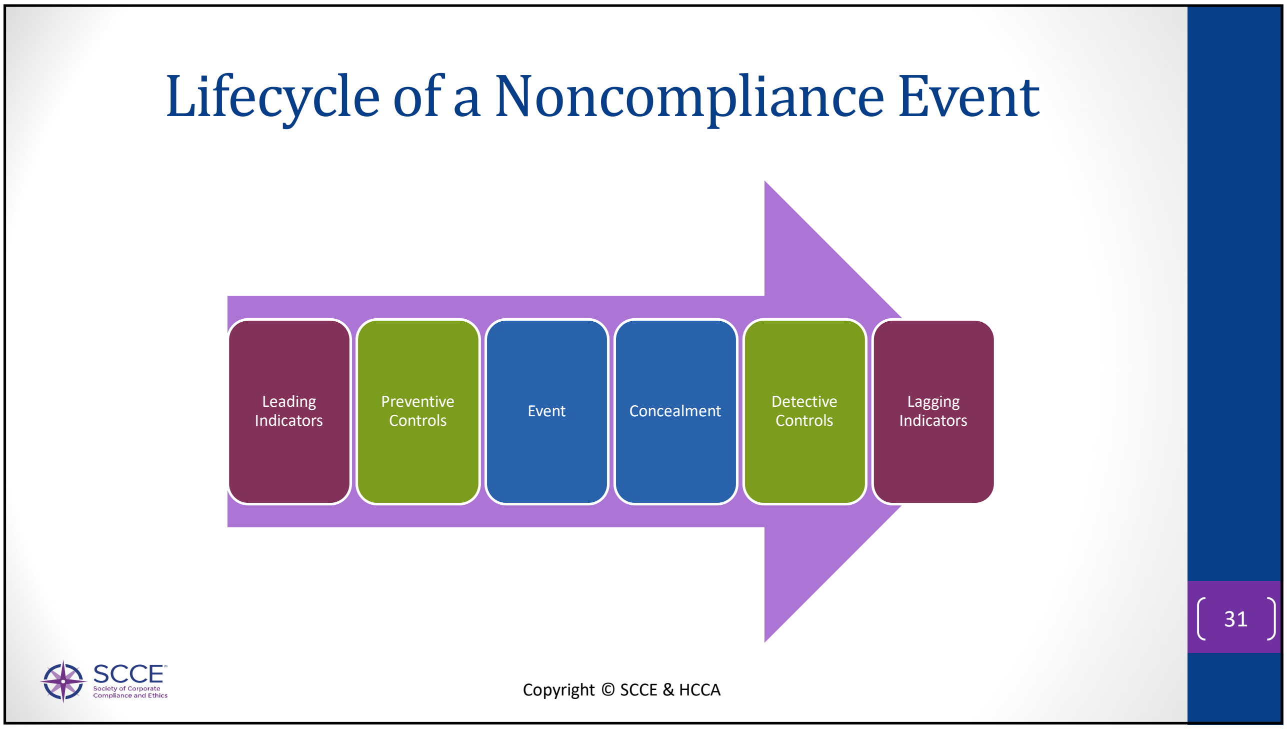


Additional Material

- Lifecycle of Non-Compliance Event
- Remote vs. in-person interviews
- Bias – conscious v. unconscious

30

30



Lifecycle of a Noncompliance Event

Leading Indicators

Preventive Controls

Event

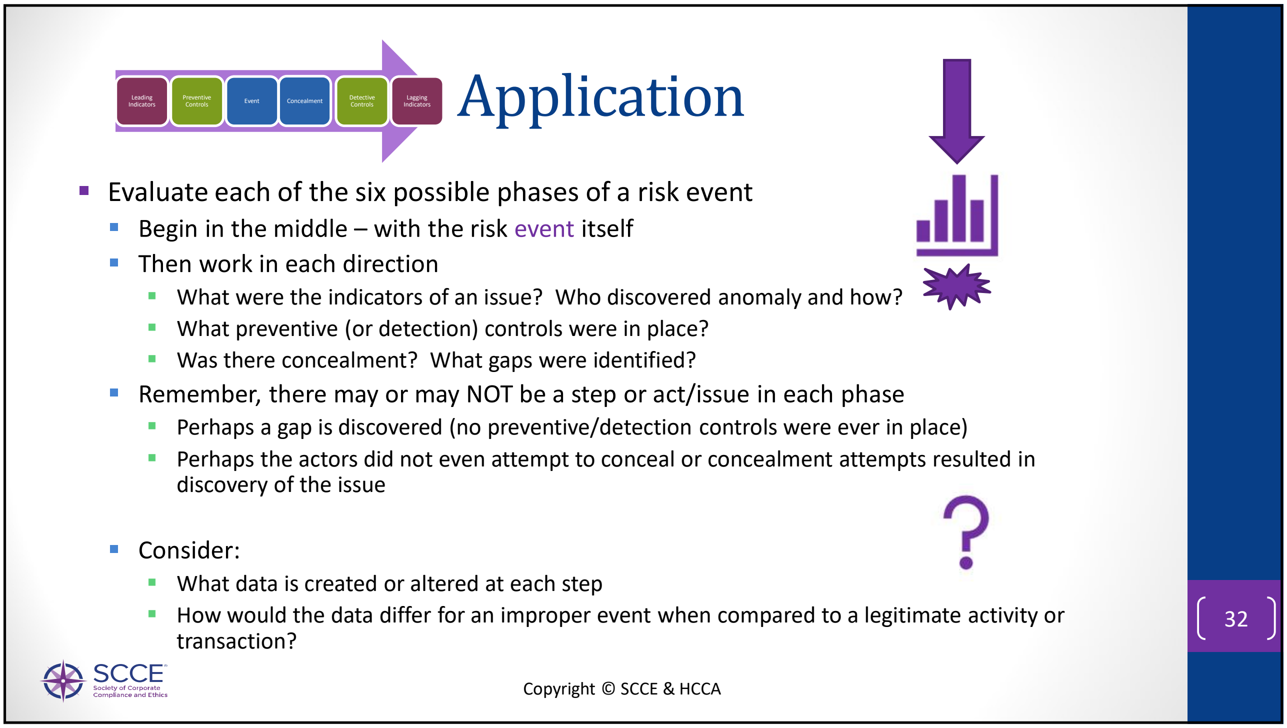
Concealment

Detective Controls

Lagging Indicators

31

31

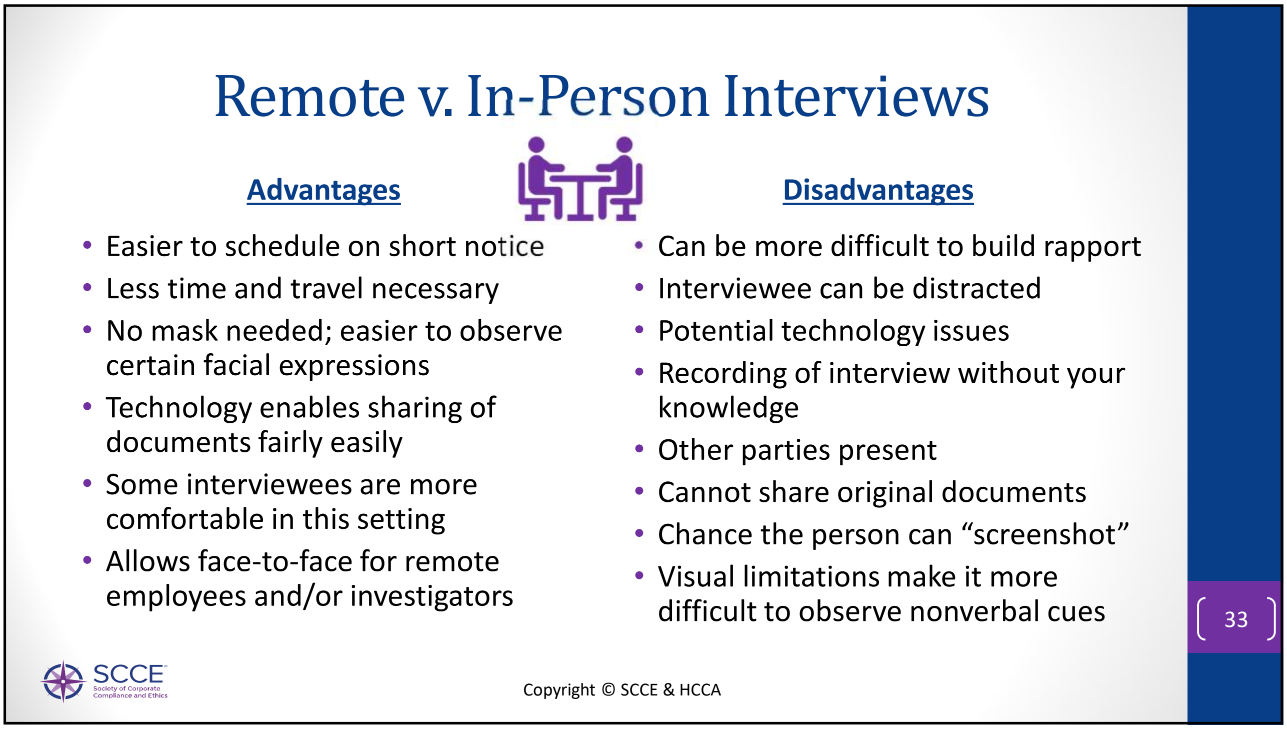


Application

- Evaluate each of the six possible phases of a risk event
  - Begin in the middle – with the risk event itself
  - Then work in each direction
    - What were the indicators of an issue? Who discovered anomaly and how?
    - What preventive (or detection) controls were in place?
    - Was there concealment? What gaps were identified?
  - Remember, there may or may NOT be a step or act/issue in each phase
    - Perhaps a gap is discovered (no preventive/detection controls were ever in place)
    - Perhaps the actors did not even attempt to conceal or concealment attempts resulted in discovery of the issue
  - Consider:
    - What data is created or altered at each step
    - How would the data differ for an improper event when compared to a legitimate activity or transaction?

32

32



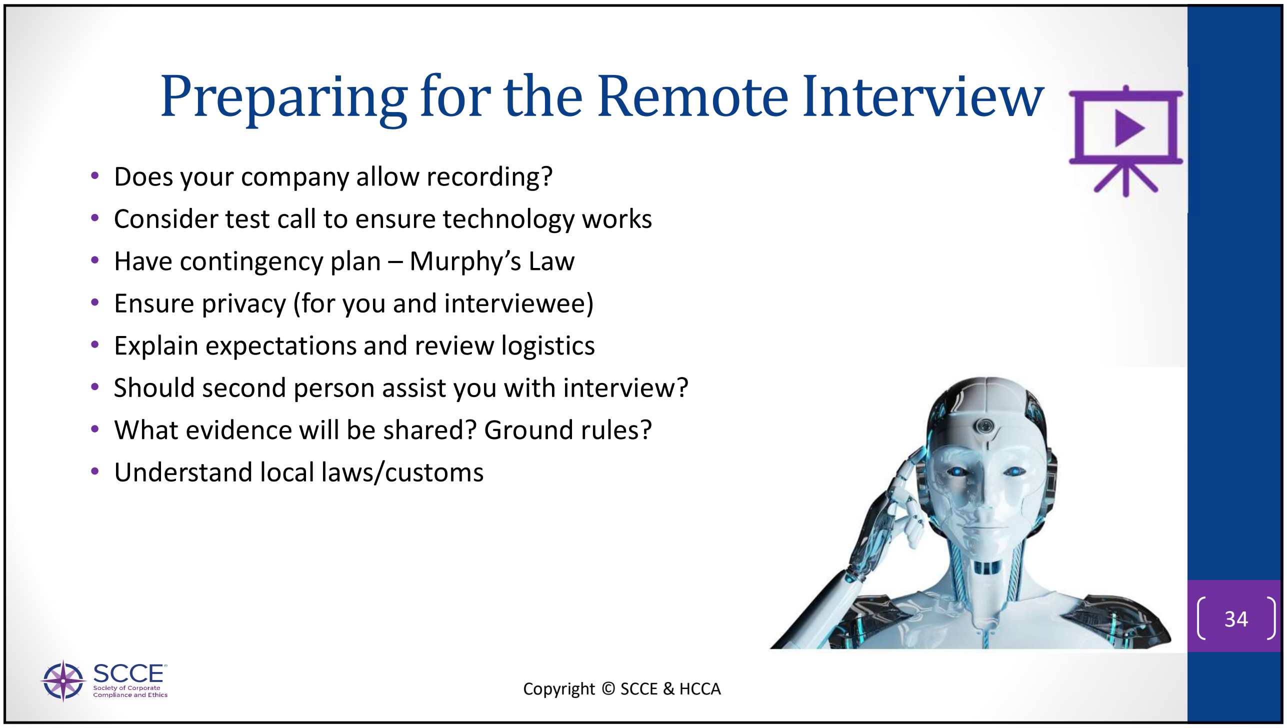
Remote v. In-Person Interviews

Advantages

- Easier to schedule on short notice
- Less time and travel necessary
- No mask needed; easier to observe certain facial expressions
- Technology enables sharing of documents fairly easily
- Some interviewees are more comfortable in this setting
- Allows face-to-face for remote employees and/or investigators

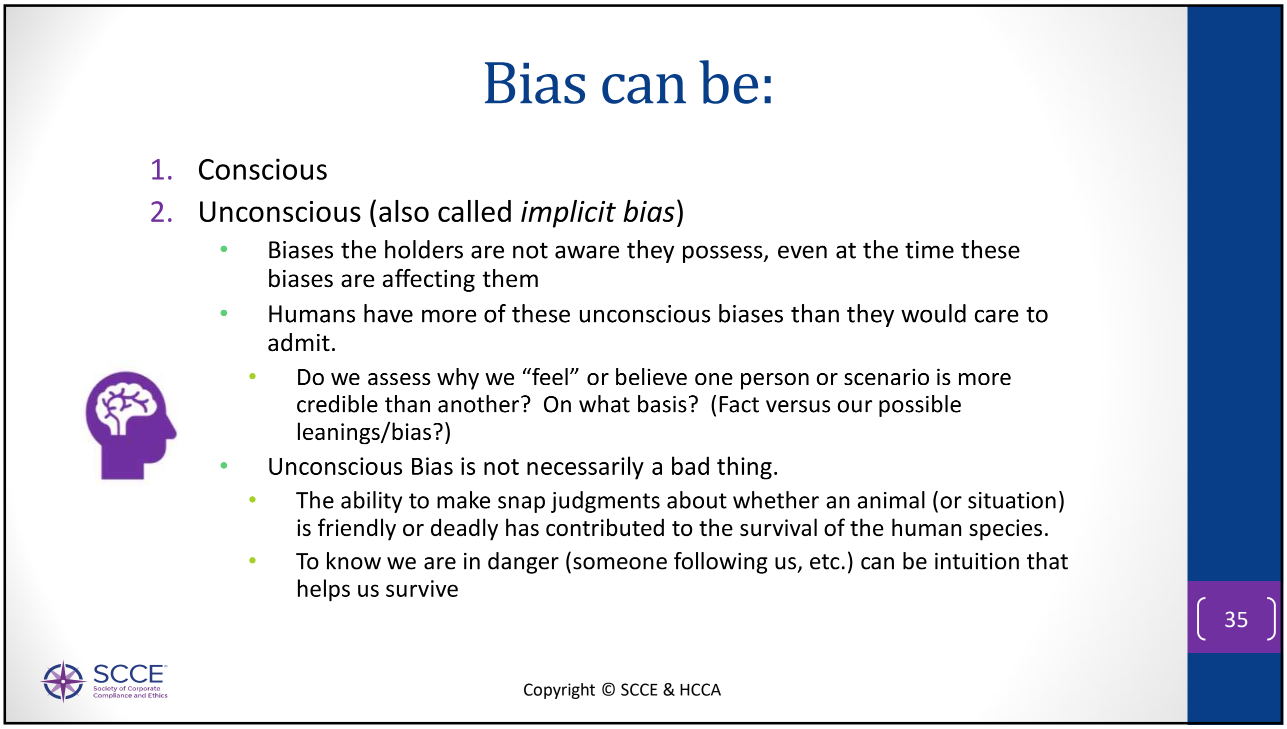
Disadvantages

- Can be more difficult to build rapport
- Interviewee can be distracted
- Potential technology issues
- Recording of interview without your knowledge
- Other parties present
- Cannot share original documents
- Chance the person can "screenshot"
- Visual limitations make it more difficult to observe nonverbal cues



Preparing for the Remote Interview

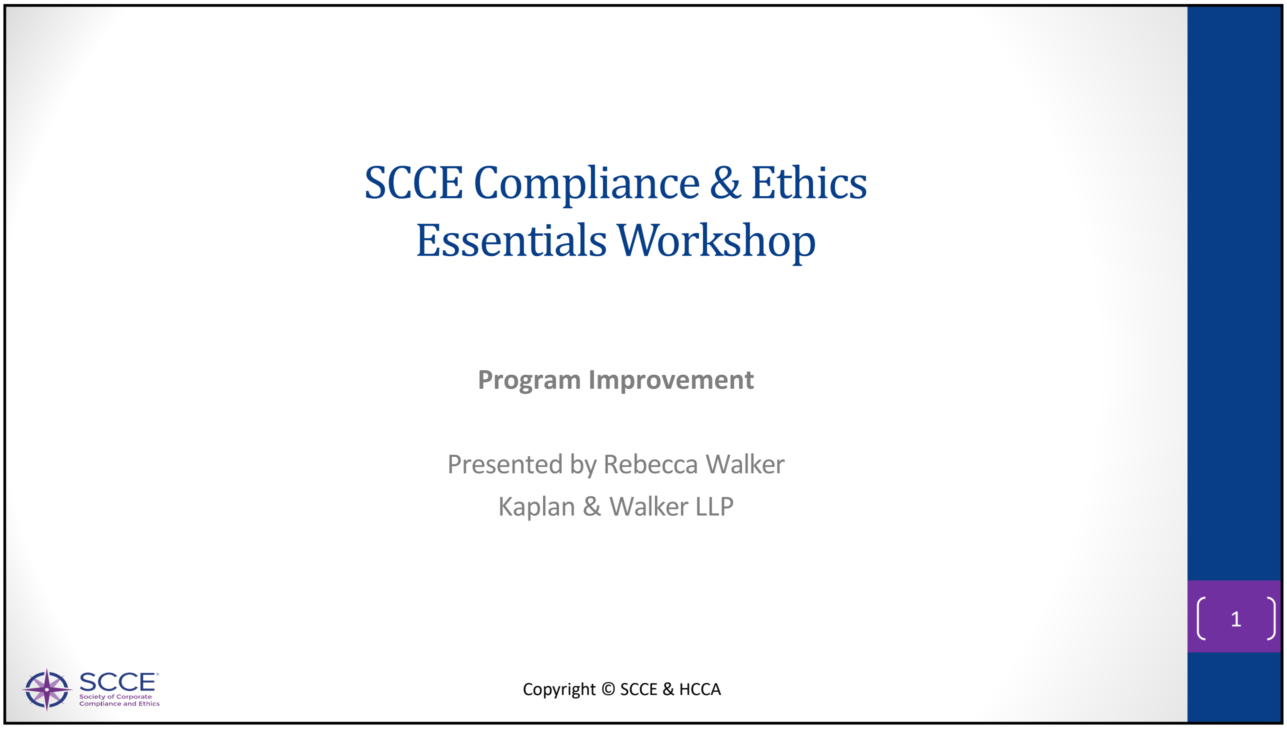
- Does your company allow recording?
- Consider test call to ensure technology works
- Have contingency plan – Murphy's Law
- Ensure privacy (for you and interviewee)
- Explain expectations and review logistics
- Should second person assist you with interview?
- What evidence will be shared? Ground rules?
- Understand local laws/customs



Bias can be:

1. Conscious
2. Unconscious (also called *implicit bias*)
   - Biases the holders are not aware they possess, even at the time these biases are affecting them
   - Humans have more of these unconscious biases than they would care to admit.
     - Do we assess why we “feel” or believe one person or scenario is more credible than another? On what basis? (Fact versus our possible leanings/bias?)
   - Unconscious Bias is not necessarily a bad thing.
     - The ability to make snap judgments about whether an animal (or situation) is friendly or deadly has contributed to the survival of the human species.
     - To know we are in danger (someone following us, etc.) can be intuition that helps us survive

SCCE Society of Corporate Compliance and Ethics



SCCE Compliance & Ethics Essentials Workshop

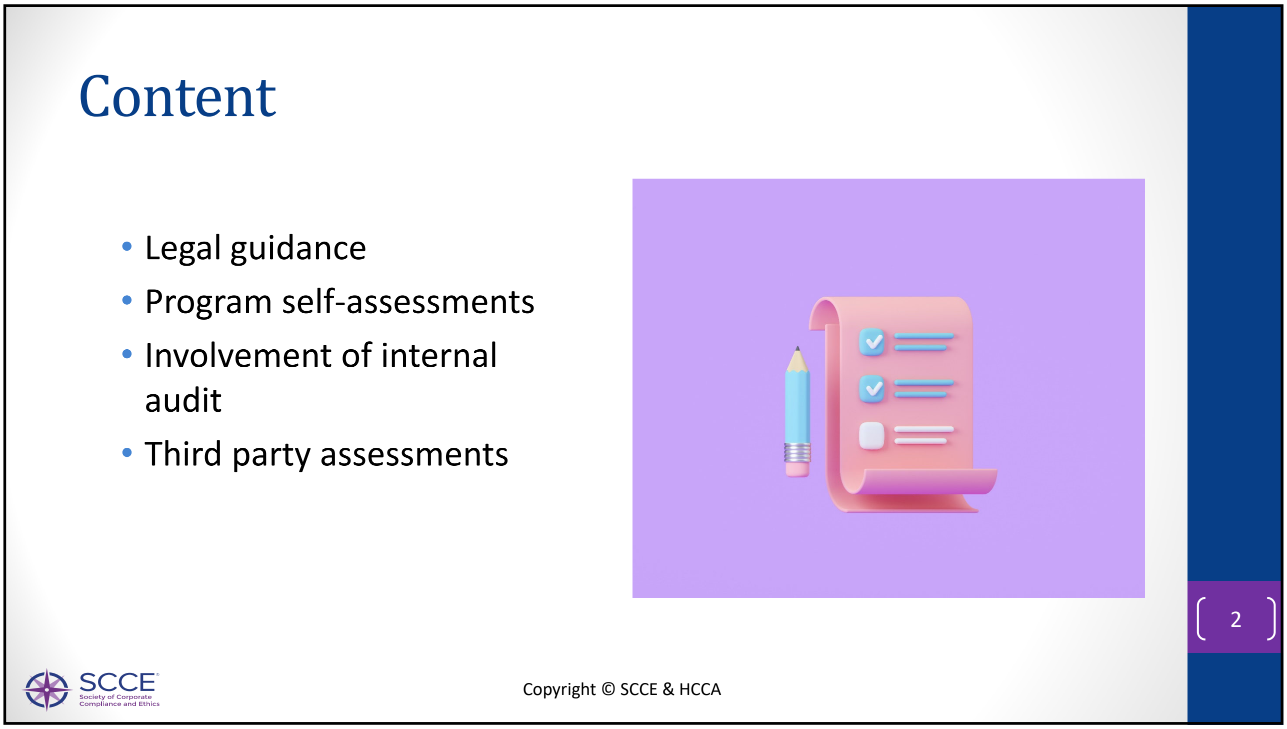
Program Improvement

Presented by Rebecca Walker

Kaplan & Walker LLP

1

1



Content

- Legal guidance
- Program self-assessments
- Involvement of internal audit
- Third party assessments

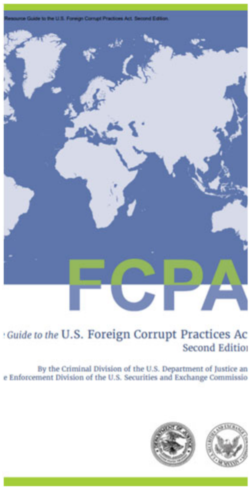
2

2

Legal Guidance

DOJ and SEC Resource Guide to the FCPA

Finally, a good compliance program should constantly evolve. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the standards of its industry. In addition, compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements. Consequently, DOJ and SEC evaluate whether companies regularly review and improve their compliance programs and do not allow them to become stale.



Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition.

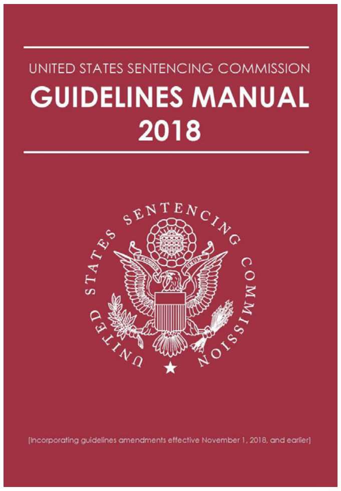
FCPA

Guide to the U.S. Foreign Corrupt Practices Ac
Second Editio

By the Criminal Division of the U.S. Department of Justice an
e Enforcement Division of the U.S. Securities and Exchange Commissio

Legal Guidance

- Sentencing Guidelines
  - The organization shall take reasonable steps (A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct; (B) to evaluate periodically the effectiveness of the organization’s compliance and ethics program. . . .   U.S.S.G. 8B2.1(b)(5).
- DOJ and SEC Resource Guide to the FCPA
  - Although the nature and the frequency of proactive evaluations may vary depending on the size and complexity of an organization, the idea behind such efforts is the same: continuous improvement and sustainability.


UNITED STATES SENTENCING COMMISSION
GUIDELINES MANUAL
2018
UNITED STATES SENTENCING COMMISSION
(incorporating guidelines amendments effective November 1, 2018, and earlier)

DOJ Evaluation of Corporate Compliance Programs

- Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training?
- What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?
- Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?
- How often and how does the company measure its culture of compliance?
- What steps has the company taken in response to its measurement of the compliance culture?

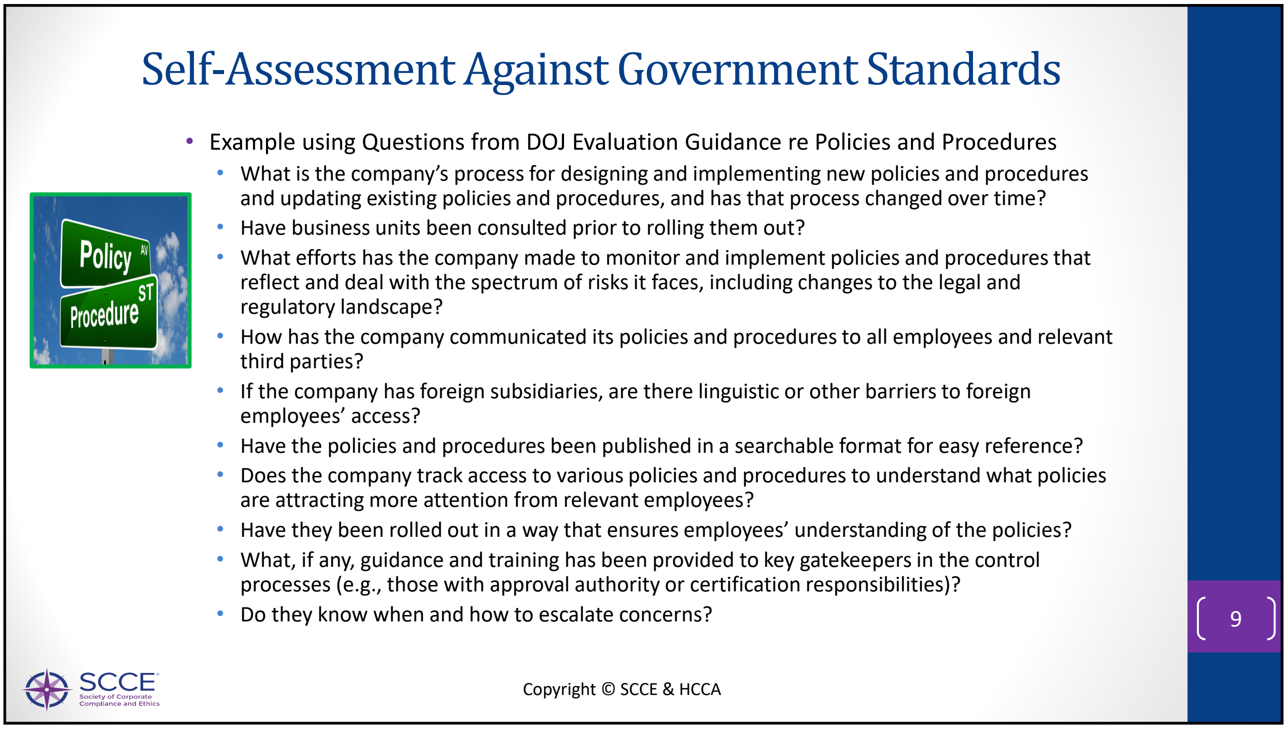
Program Self Assessment

SCCE Society of Corporate Compliance and Ethics

Self-Assessment Tools

- Self-assessment against government standards
  - Sentencing Guidelines
  - DOJ Evaluation Guidance
  - Other agency guidance
- Benchmarking
- Maturity models
- Surveys
- Data analytics
- Focus groups
- Exit interviews

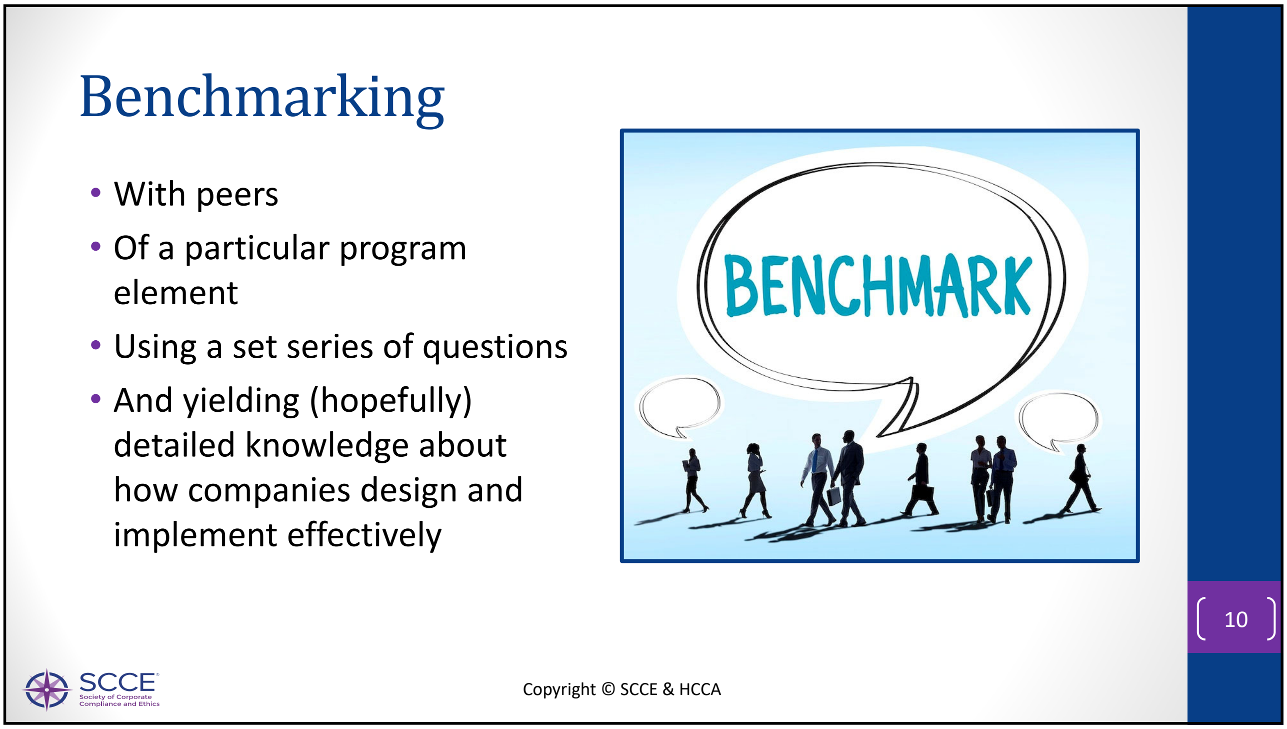
SCCE Society of Corporate Compliance and Ethics


Policy
AV
ST
Procedure

Self-Assessment Against Government Standards

- Example using Questions from DOJ Evaluation Guidance re Policies and Procedures
  - What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time?
  - Have business units been consulted prior to rolling them out?
  - What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?
  - How has the company communicated its policies and procedures to all employees and relevant third parties?
  - If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access?
  - Have the policies and procedures been published in a searchable format for easy reference?
  - Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?
  - Have they been rolled out in a way that ensures employees' understanding of the policies?
  - What, if any, guidance and training has been provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)?
  - Do they know when and how to escalate concerns?

9



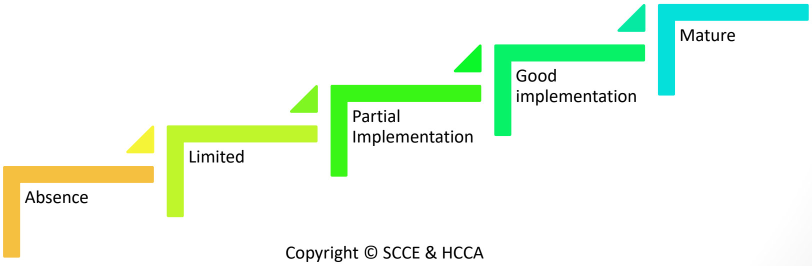
Benchmarking

- With peers
- Of a particular program element
- Using a set series of questions
- And yielding (hopefully) detailed knowledge about how companies design and implement effectively

10

Maturity Models: One Example

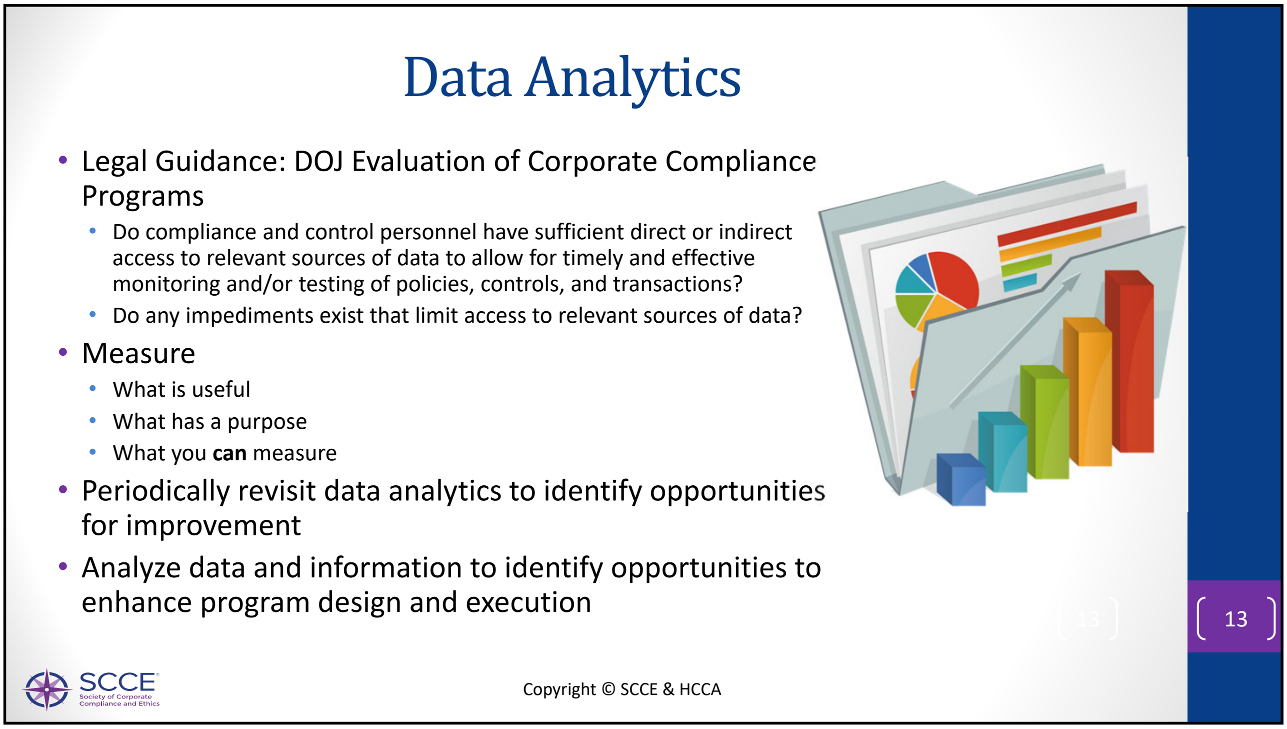
- Each element of a program is assessed by each operating company, business unit or function.
- Examples of maturity levels
  1. Absence – nothing in place
  2. Limited – limited awareness and ad hoc process
  3. Partial implementation – broader awareness, some policies and procedures in place
  4. Good implementation – Broad awareness with policies and procedures in place
  5. Mature – Enterprise-wide awareness; policies and procedures in place and embedded in operations
- So one might conclude, e.g., that:
  - Investigations procedures in the Europe sector are at level 4.
  - Third-party due diligence procedures in APAC are at level 3.
  - Company would then formulate remedial measures to move the program elements toward level 5.



?

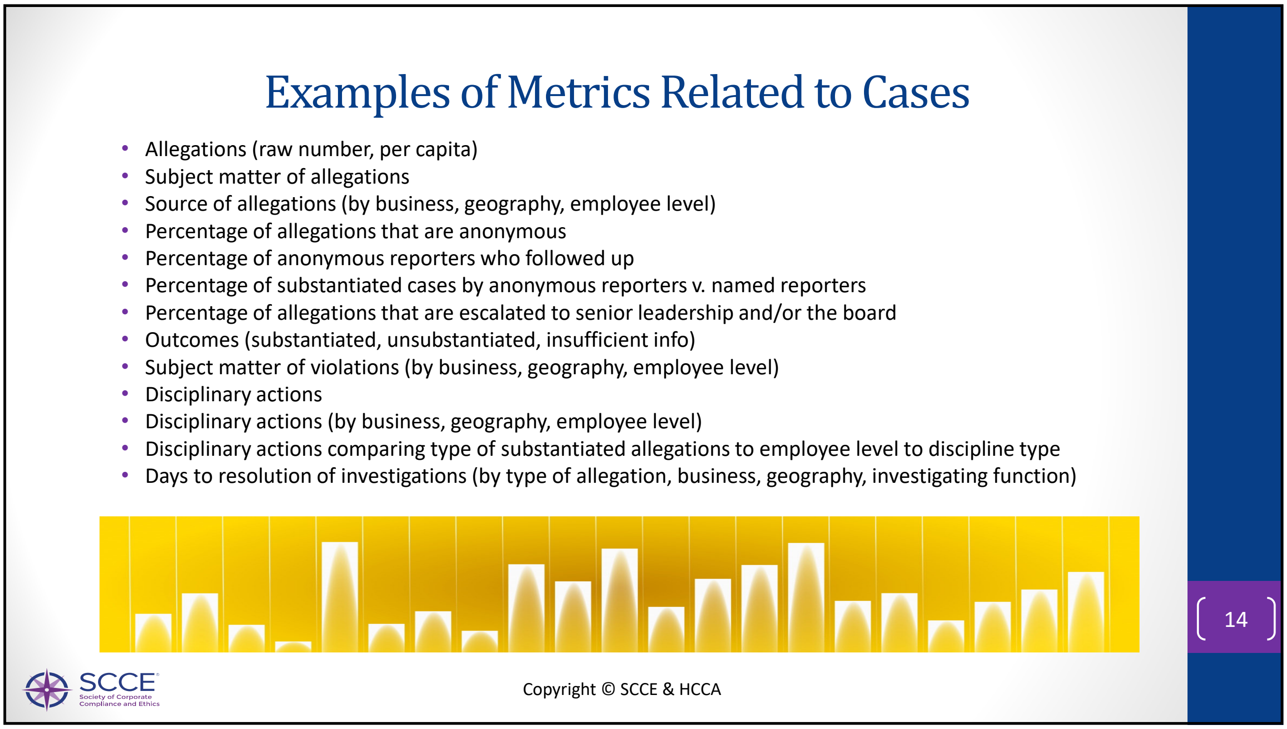
Surveys

- Surveys can provide important data regarding employee knowledge of and perceptions regarding the program.
- Surveys can be repeated over time.
- Opportunities for both internal benchmarking and external benchmarking.
- Sample question areas:
  - Awareness of code of business conduct and C&E policies and procedures
  - Awareness of how to report suspected misconduct
  - Comfort level reporting suspected misconduct
  - Manager's and management's support of ethical conduct and of the program
  - Perception of company's commitment to C&E



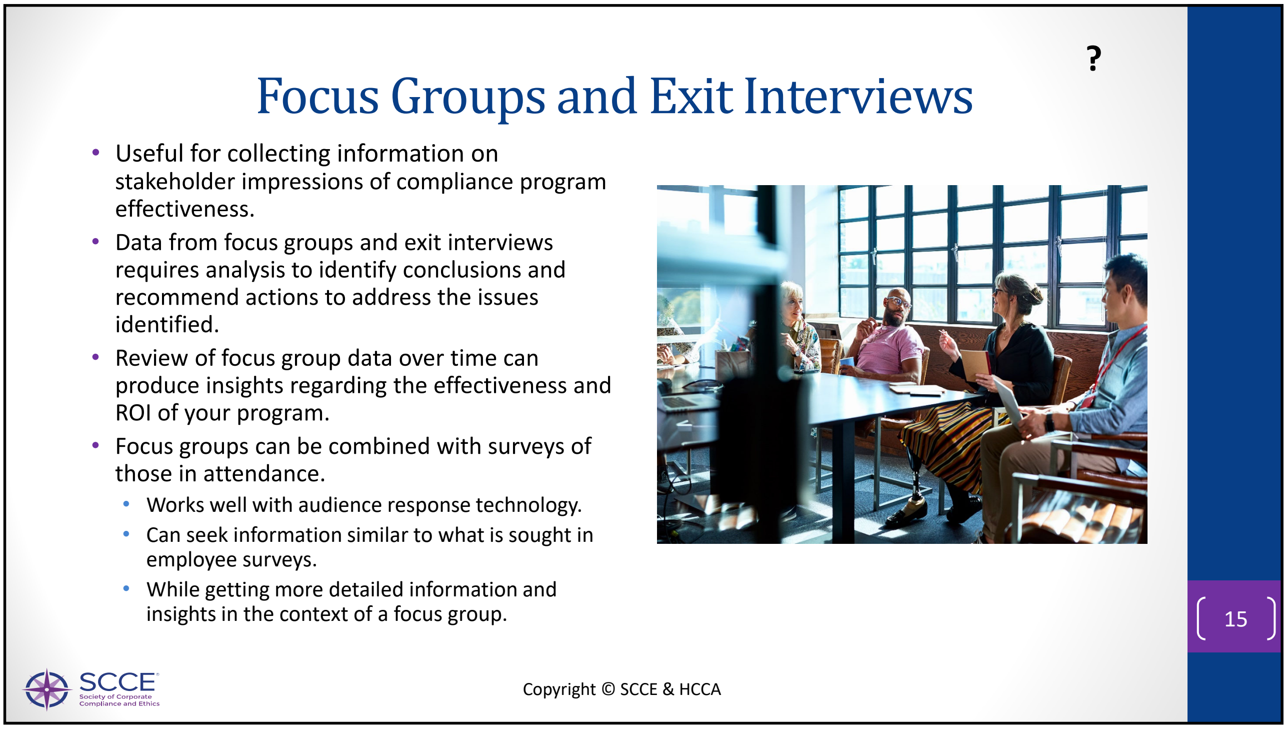
Data Analytics

- Legal Guidance: DOJ Evaluation of Corporate Compliance Programs
  - Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions?
  - Do any impediments exist that limit access to relevant sources of data?
- Measure
  - What is useful
  - What has a purpose
  - What you **can** measure
- Periodically revisit data analytics to identify opportunities for improvement
- Analyze data and information to identify opportunities to enhance program design and execution



Examples of Metrics Related to Cases

- Allegations (raw number, per capita)
- Subject matter of allegations
- Source of allegations (by business, geography, employee level)
- Percentage of allegations that are anonymous
- Percentage of anonymous reporters who followed up
- Percentage of substantiated cases by anonymous reporters v. named reporters
- Percentage of allegations that are escalated to senior leadership and/or the board
- Outcomes (substantiated, unsubstantiated, insufficient info)
- Subject matter of violations (by business, geography, employee level)
- Disciplinary actions
- Disciplinary actions (by business, geography, employee level)
- Disciplinary actions comparing type of substantiated allegations to employee level to discipline type
- Days to resolution of investigations (by type of allegation, business, geography, investigating function)



?

Focus Groups and Exit Interviews

- Useful for collecting information on stakeholder impressions of compliance program effectiveness.
- Data from focus groups and exit interviews requires analysis to identify conclusions and recommend actions to address the issues identified.
- Review of focus group data over time can produce insights regarding the effectiveness and ROI of your program.
- Focus groups can be combined with surveys of those in attendance.
  - Works well with audience response technology.
  - Can seek information similar to what is sought in employee surveys.
  - While getting more detailed information and insights in the context of a focus group.

15

Copyright © SCCE & HCCA

15

Involvement of Internal Audit

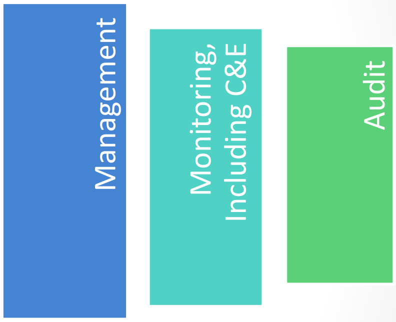
16

Copyright © SCCE & HCCA

16

Auditing

- The “third line”
  - Tests to ensure controls are operating as designed
  - Retrospective in nature
  - Independence is critical
- C&E audits are
  - Sometimes stand-alone
  - More often part of broader audits
- Utilize formal planning, process and reports



Management

Monitoring, Including C&E

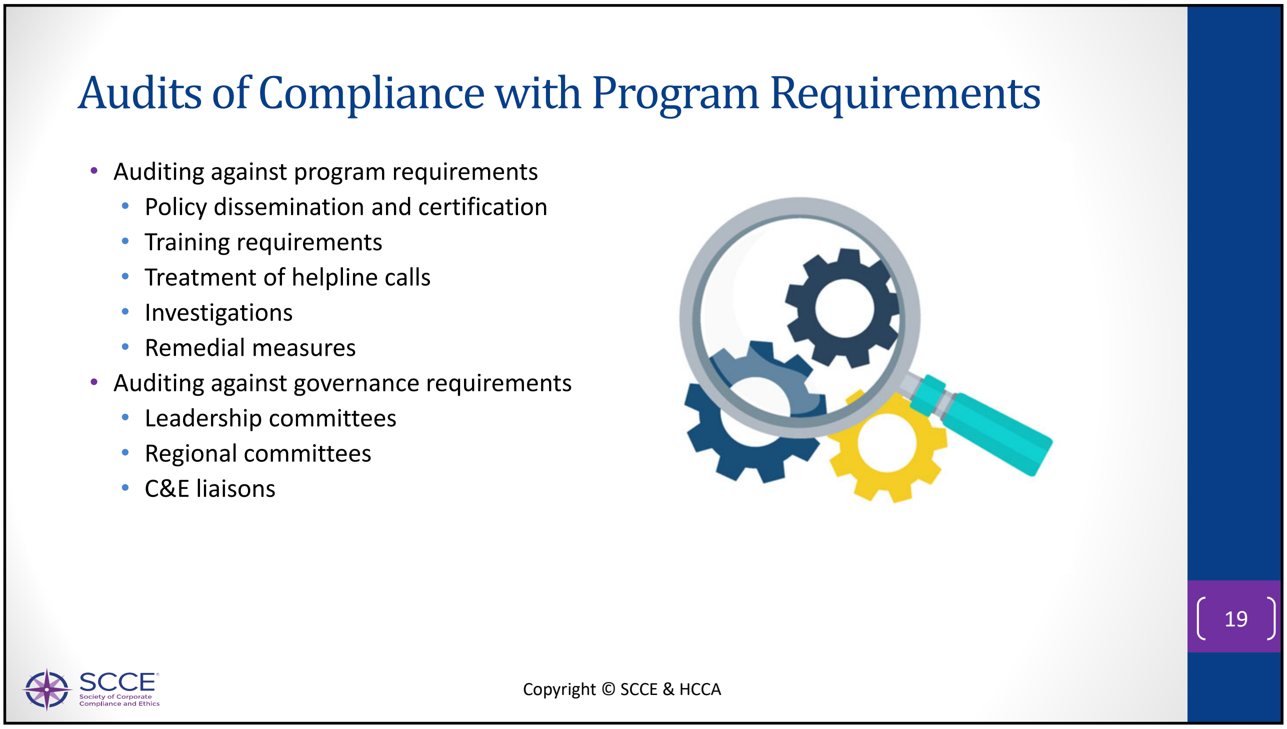
Audit

SCCE Society of Corporate Compliance and Ethics

Audits of Legal Risk Areas

- Risk areas commonly audited
  - FCPA (anti-bribery)
  - Conflicts of interest
  - Fraud
  - Privacy
  - IP/confidential information
  - IT compliance
  - Trade controls
  - Industry-specific regulated areas
- Many others

SCCE Society of Corporate Compliance and Ethics

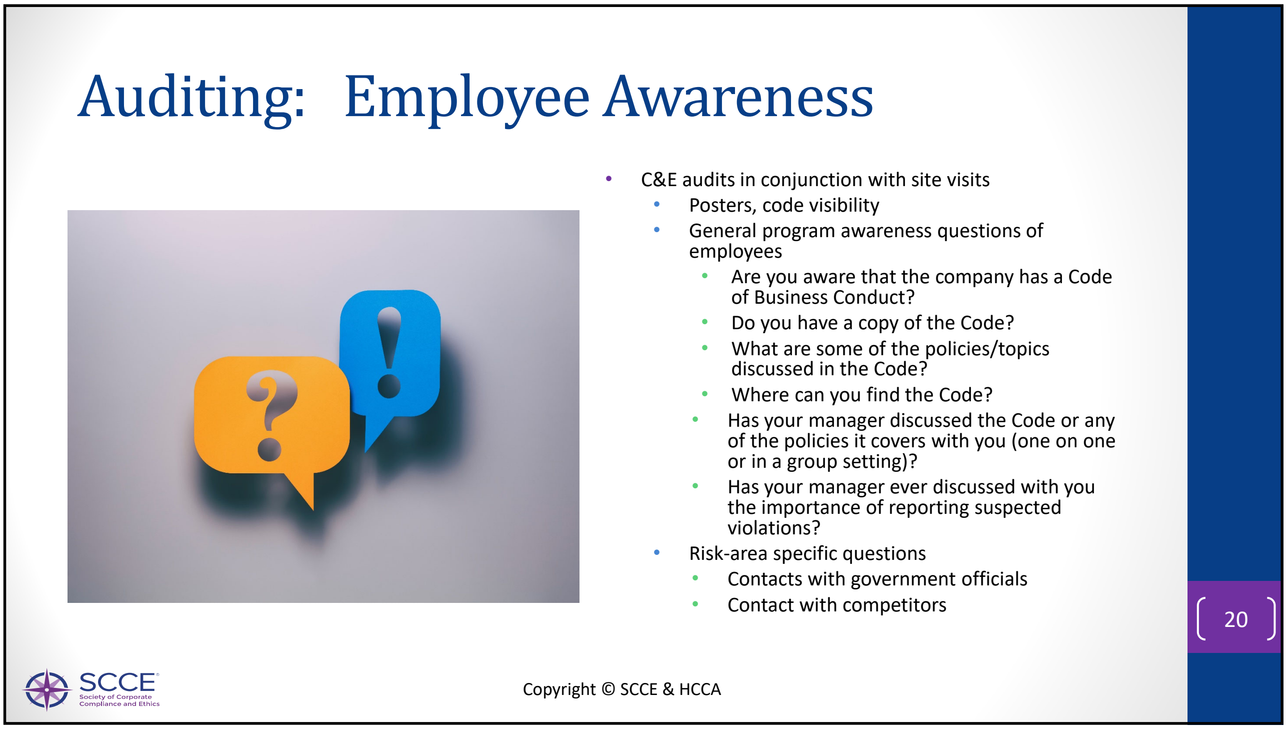


Audits of Compliance with Program Requirements

- Auditing against program requirements
  - Policy dissemination and certification
  - Training requirements
  - Treatment of helpline calls
  - Investigations
  - Remedial measures
- Auditing against governance requirements
  - Leadership committees
  - Regional committees
  - C&E liaisons

19

19



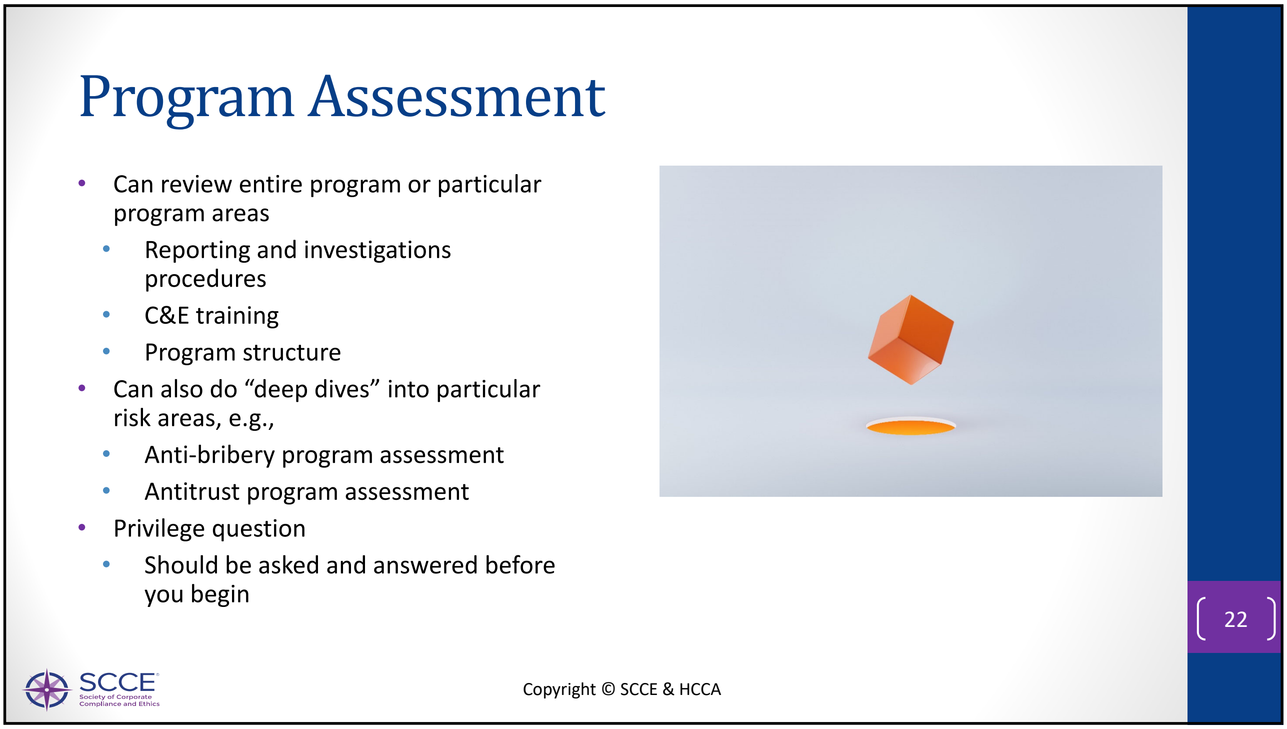
Auditing: Employee Awareness

- C&E audits in conjunction with site visits
  - Posters, code visibility
  - General program awareness questions of employees
    - Are you aware that the company has a Code of Business Conduct?
    - Do you have a copy of the Code?
    - What are some of the policies/topics discussed in the Code?
    - Where can you find the Code?
    - Has your manager discussed the Code or any of the policies it covers with you (one on one or in a group setting)?
    - Has your manager ever discussed with you the importance of reporting suspected violations?
  - Risk-area specific questions
    - Contacts with government officials
    - Contact with competitors

20

20

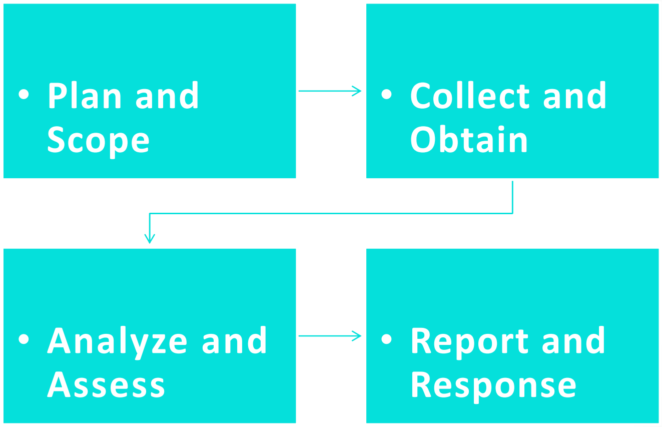
Third Party Assessments



Program Assessment

- Can review entire program or particular program areas
  - Reporting and investigations procedures
  - C&E training
  - Program structure
- Can also do “deep dives” into particular risk areas, e.g.,
  - Anti-bribery program assessment
  - Antitrust program assessment
- Privilege question
  - Should be asked and answered before you begin

Process Overview



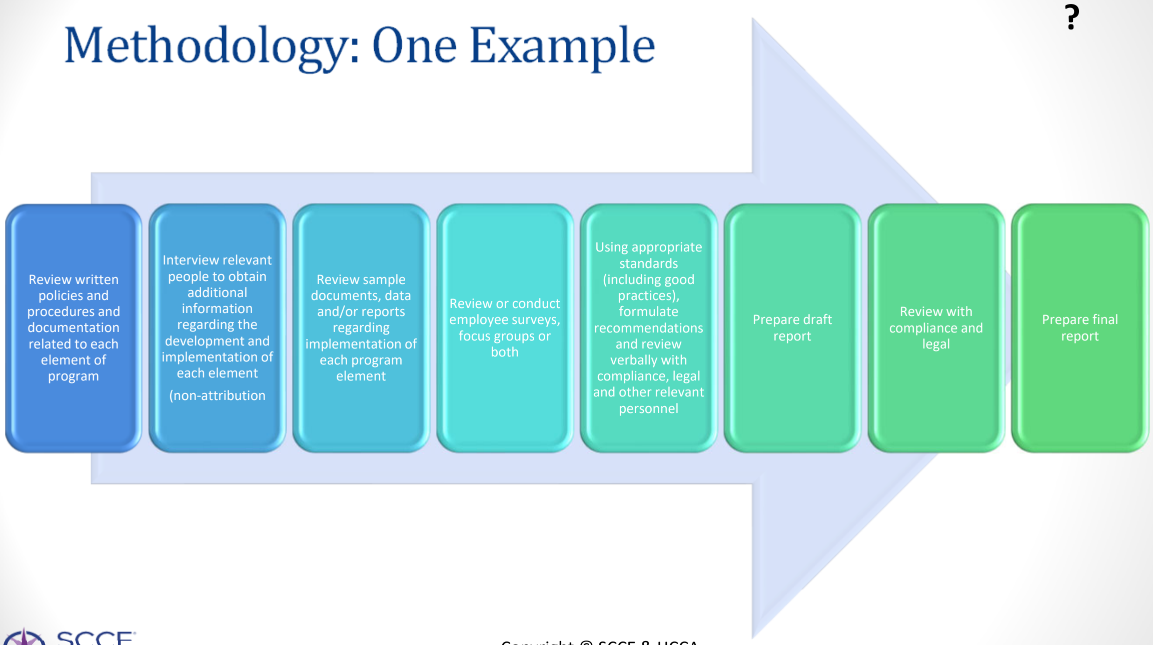
- Plan and Scope
- Collect and Obtain
- Analyze and Assess
- Report and Response

23

23

Methodology: One Example

?



- Review written policies and procedures and documentation related to each element of program
- Interview relevant people to obtain additional information regarding the development and implementation of each element (non-attribution
- Review sample documents, data and/or reports regarding implementation of each program element
- Review or conduct employee surveys, focus groups or both
- Using appropriate standards (including good practices), formulate recommendations and review verbally with compliance, legal and other relevant personnel
- Prepare draft report
- Review with compliance and legal
- Prepare final report

24

24

Program Elements For Review

- Program Structure
  - CCO and implementation personnel
  - Independence, authority, reach and resources of the function
- Board Oversight
- Management Oversight (including committees)
- Compliance Risk Assessment
- Standards, Policies and Procedures
  - Code of Conduct & compliance policies
- Effective Training & Communication
  - Compliance training
  - Compliance communications
- Monitoring, Auditing & Assessment
- Reporting Procedures
  - Non-retaliation
- Investigations
- Disciplinary Action
- Remediation
- Incentives
- Diligence in Hiring & Promotions
- Culture of compliance and ethics
  - Tone at the top
  - Tone at the middle
  - Speak up culture
  - Pressure to commit misconduct

Attorney-Client Privilege

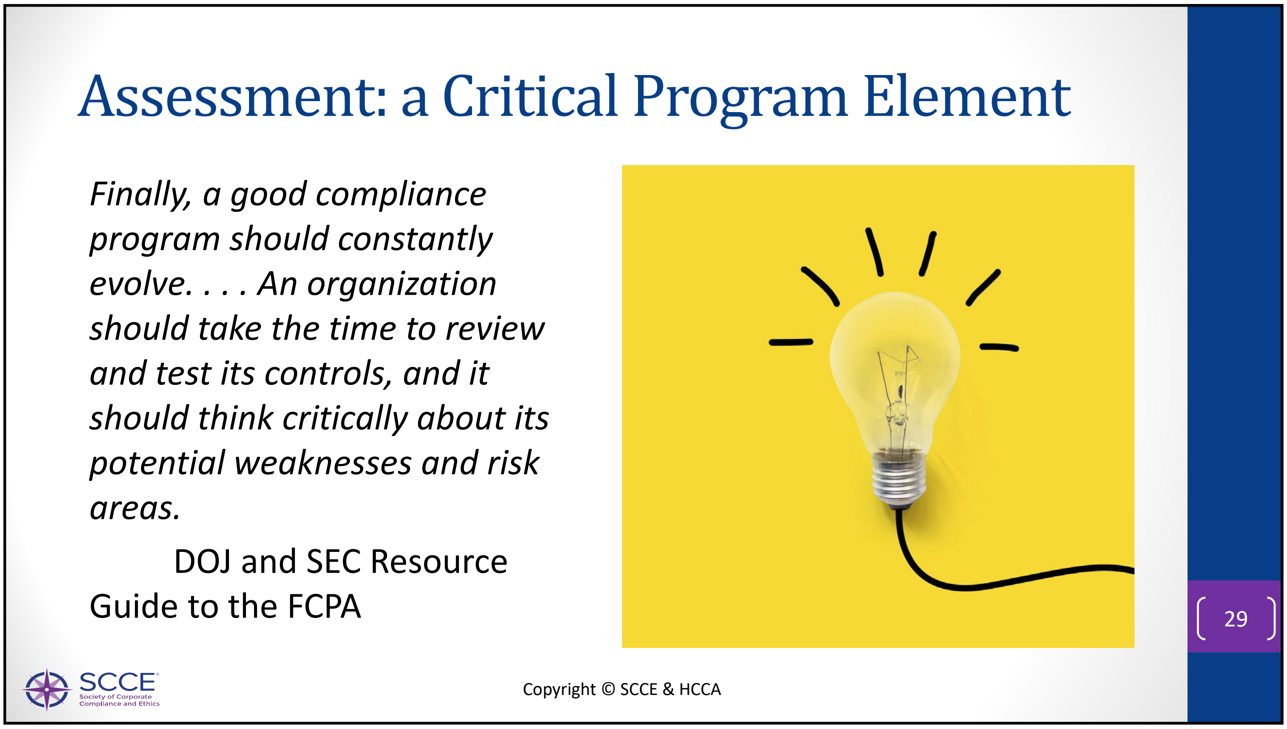
- In order for communications to be protected by attorney-client privilege, the following requirements must be satisfied:
  - existence of the a/c relationship (or prospective relationship)
  - a communication
  - that takes place for the purpose of obtaining or providing legal advice
  - in confidence
  - where there has been no waiver.
    - See U.S. v. Schwimmer, 892 F.2d 237, 243 (2d Cir. 1989).
- Since *Upjohn v. United States,* 449 U.S. 383 (1981), it has been generally settled that a corporation can claim the attorney-client privilege.

Attorney-Client Privilege

- *Legal* – not business – advice or assistance must be sought.
- In C&E, legal advice is often sought, and rendered, to facilitate compliance with the law or simply to guide a client's course of conduct, rather than in traditional law-related contexts.
- Relevant case law is limited.
- Risks can be mitigated by commitment to addressing non-compliance.
  - AND CAUTIOUS DOCUMENTATION!

Closing the Loop

- Final report should include or generate an action plan.
- Company may wish to prepare a formal response to the report (if, e.g., company determines not to implement one or more significant recommendations).
- Periodically revisit the action plan (e.g., at the time of formulation of the next program plan or the next program assessment) to ensure that recommendations are being implemented or to generate a response as to why not.



Assessment: a Critical Program Element

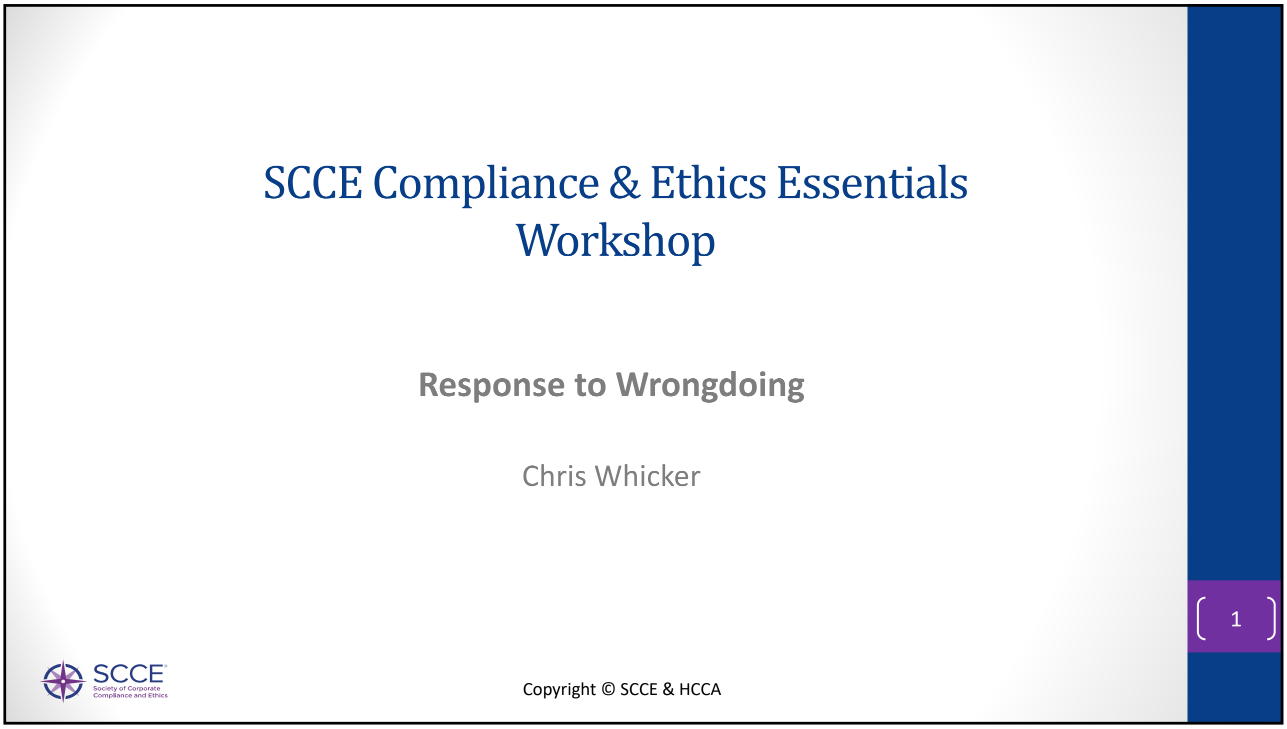
Finally, a good compliance program should constantly evolve. . . . An organization should take the time to review and test its controls, and it should think critically about its potential weaknesses and risk areas.

DOJ and SEC Resource Guide to the FCPA

29

Questions?

30



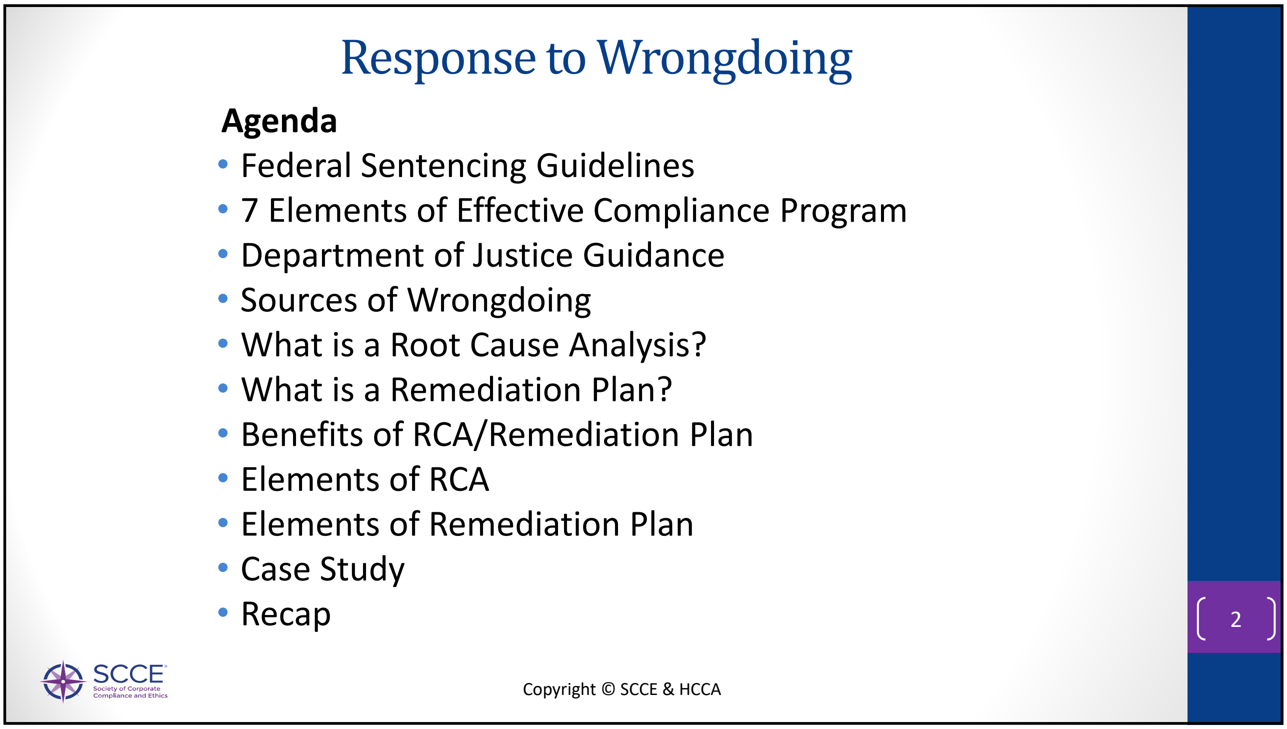
SCCE Compliance & Ethics Essentials Workshop

Response to Wrongdoing

Chris Whicker

1

1



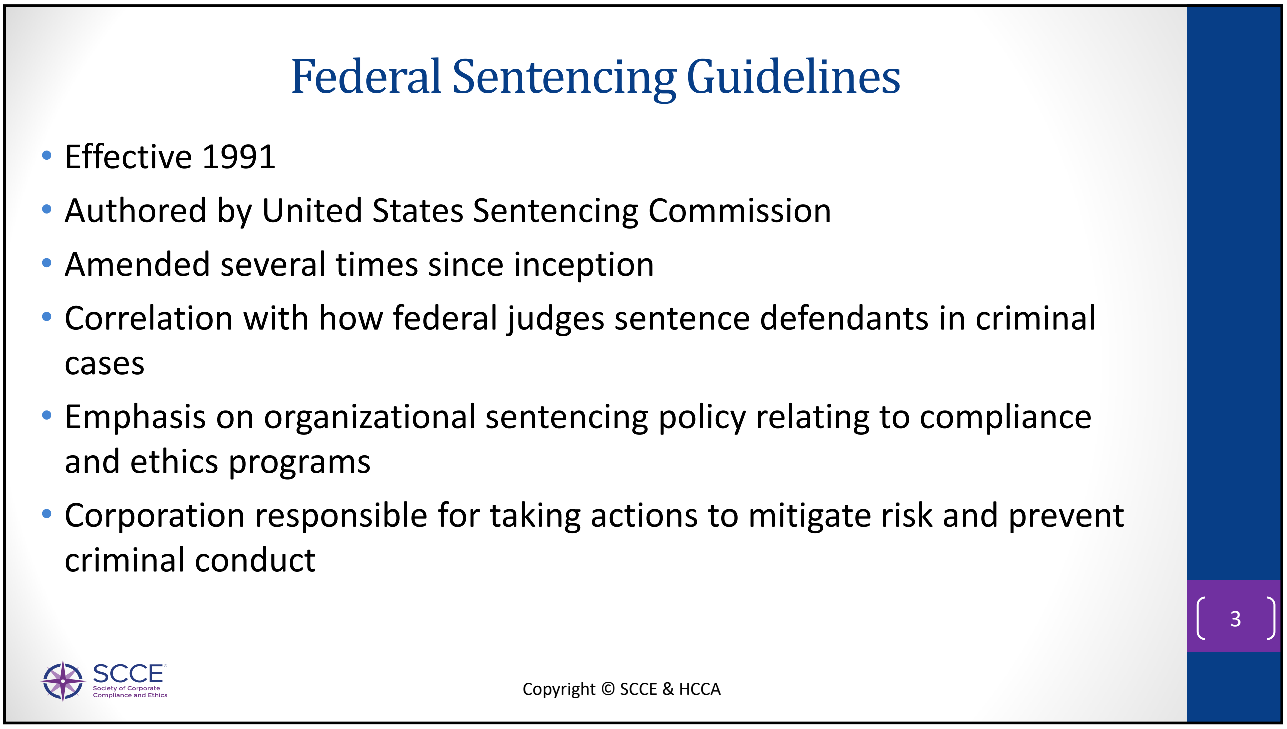
Response to Wrongdoing

Agenda

- Federal Sentencing Guidelines
- 7 Elements of Effective Compliance Program
- Department of Justice Guidance
- Sources of Wrongdoing
- What is a Root Cause Analysis?
- What is a Remediation Plan?
- Benefits of RCA/Remediation Plan
- Elements of RCA
- Elements of Remediation Plan
- Case Study
- Recap

2

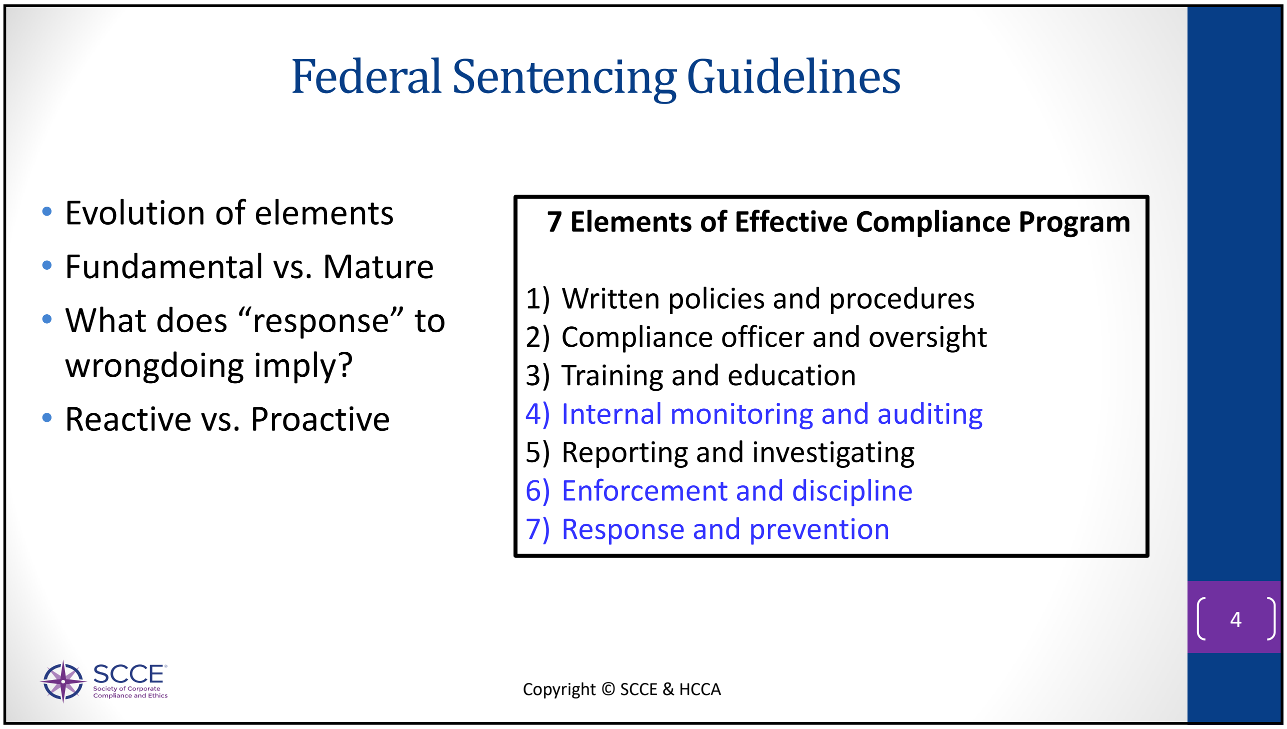
2



Federal Sentencing Guidelines

- Effective 1991
- Authored by United States Sentencing Commission
- Amended several times since inception
- Correlation with how federal judges sentence defendants in criminal cases
- Emphasis on organizational sentencing policy relating to compliance and ethics programs
- Corporation responsible for taking actions to mitigate risk and prevent criminal conduct

3



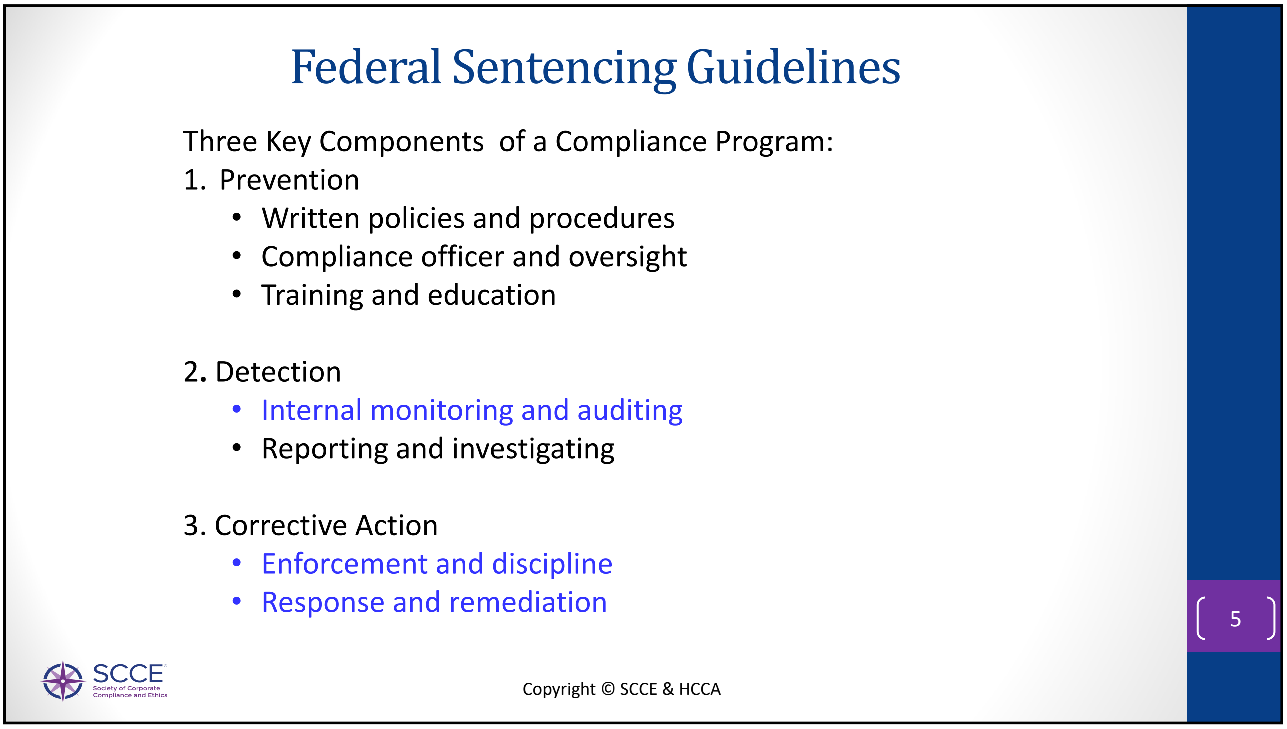
Federal Sentencing Guidelines

- Evolution of elements
- Fundamental vs. Mature
- What does “response” to wrongdoing imply?
- Reactive vs. Proactive

7 Elements of Effective Compliance Program

1) Written policies and procedures
2) Compliance officer and oversight
3) Training and education
4) Internal monitoring and auditing
5) Reporting and investigating
6) Enforcement and discipline
7) Response and prevention

4



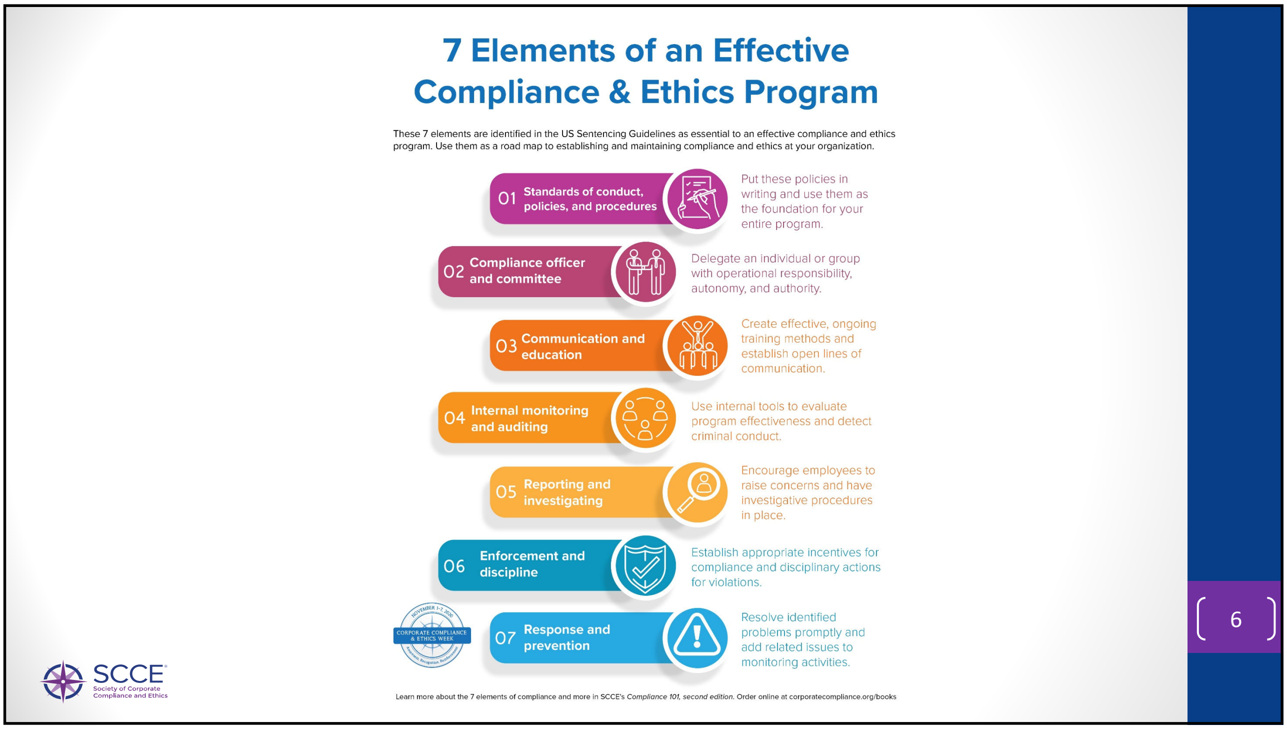
Federal Sentencing Guidelines

Three Key Components of a Compliance Program:

1. Prevention
   - Written policies and procedures
   - Compliance officer and oversight
   - Training and education

2. Detection
   - Internal monitoring and auditing
   - Reporting and investigating

3. Corrective Action
   - Enforcement and discipline
   - Response and remediation



7 Elements of an Effective Compliance & Ethics Program

These 7 elements are identified in the US Sentencing Guidelines as essential to an effective compliance and ethics program. Use them as a road map to establishing and maintaining compliance and ethics at your organization.

01 **Standards of conduct, policies, and procedures** — Put these policies in writing and use them as the foundation for your entire program.

02 **Compliance officer and committee** — Delegate an individual or group with operational responsibility, autonomy, and authority.

03 **Communication and education** — Create effective, ongoing training methods and establish open lines of communication.

04 **Internal monitoring and auditing** — Use internal tools to evaluate program effectiveness and detect criminal conduct.

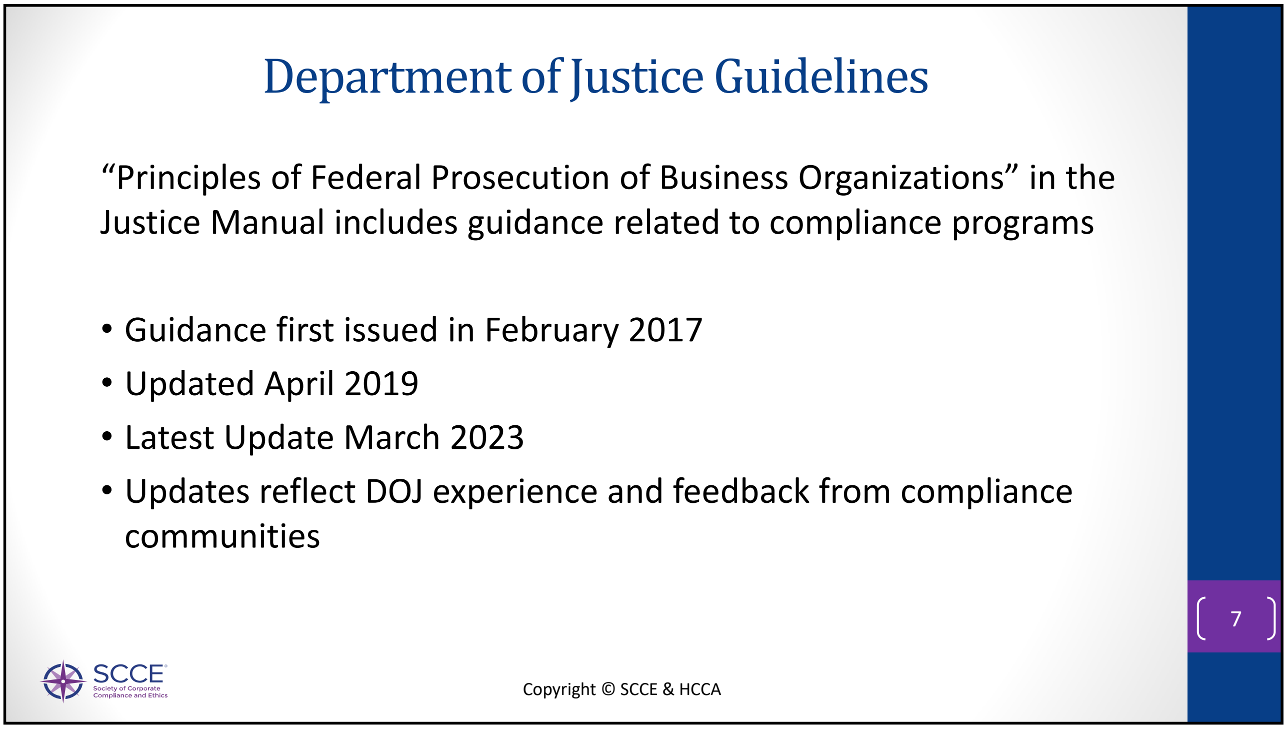
05 **Reporting and investigating** — Encourage employees to raise concerns and have investigative procedures in place.

06 **Enforcement and discipline** — Establish appropriate incentives for compliance and disciplinary actions for violations.

07 **Response and prevention** — Resolve identified problems promptly and add related issues to monitoring activities.

NOVEMBER 1-7, 2020 CORPORATE COMPLIANCE & ETHICS WEEK Awareness, Recognition, Reinforcement

Learn more about the 7 elements of compliance and more in SCCE's *Compliance 101, second edition*. Order online at corporatecompliance.org/books



Department of Justice Guidelines

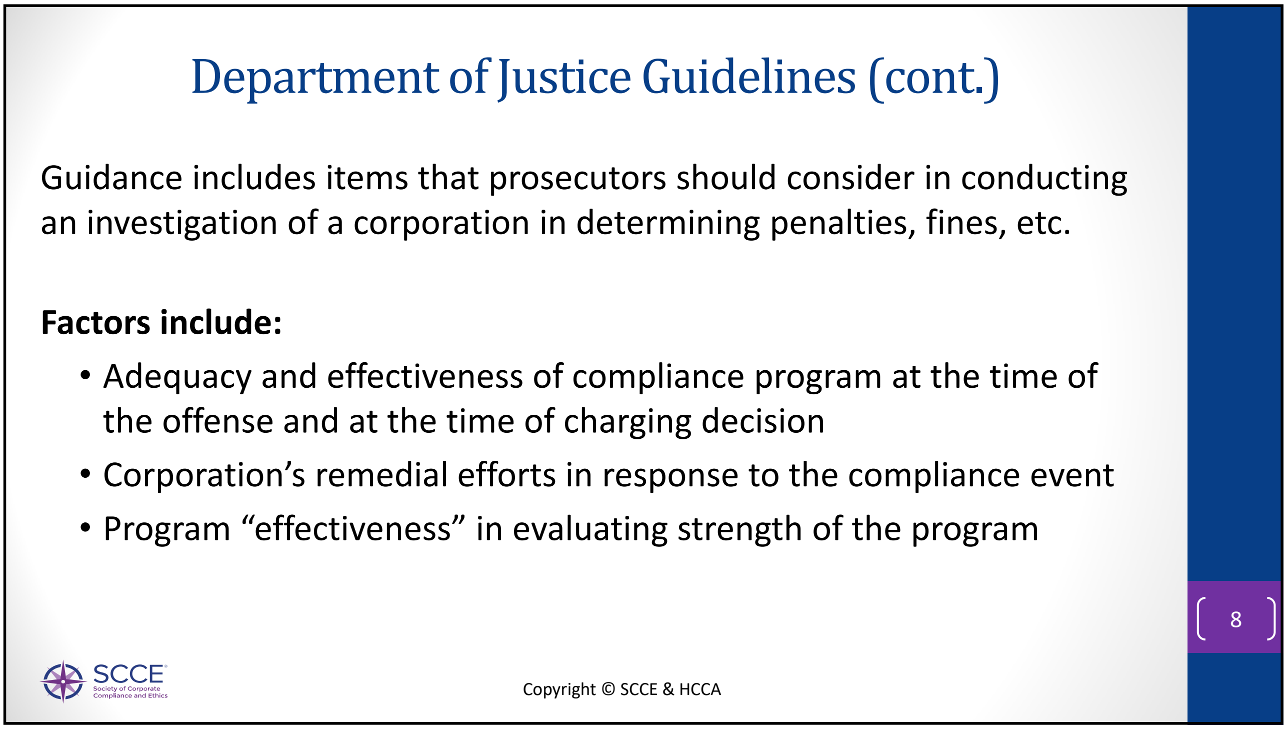
"Principles of Federal Prosecution of Business Organizations" in the Justice Manual includes guidance related to compliance programs

- Guidance first issued in February 2017
- Updated April 2019
- Latest Update March 2023
- Updates reflect DOJ experience and feedback from compliance communities

7

SCCE Society of Corporate Compliance and Ethics

7



Department of Justice Guidelines (cont.)

Guidance includes items that prosecutors should consider in conducting an investigation of a corporation in determining penalties, fines, etc.

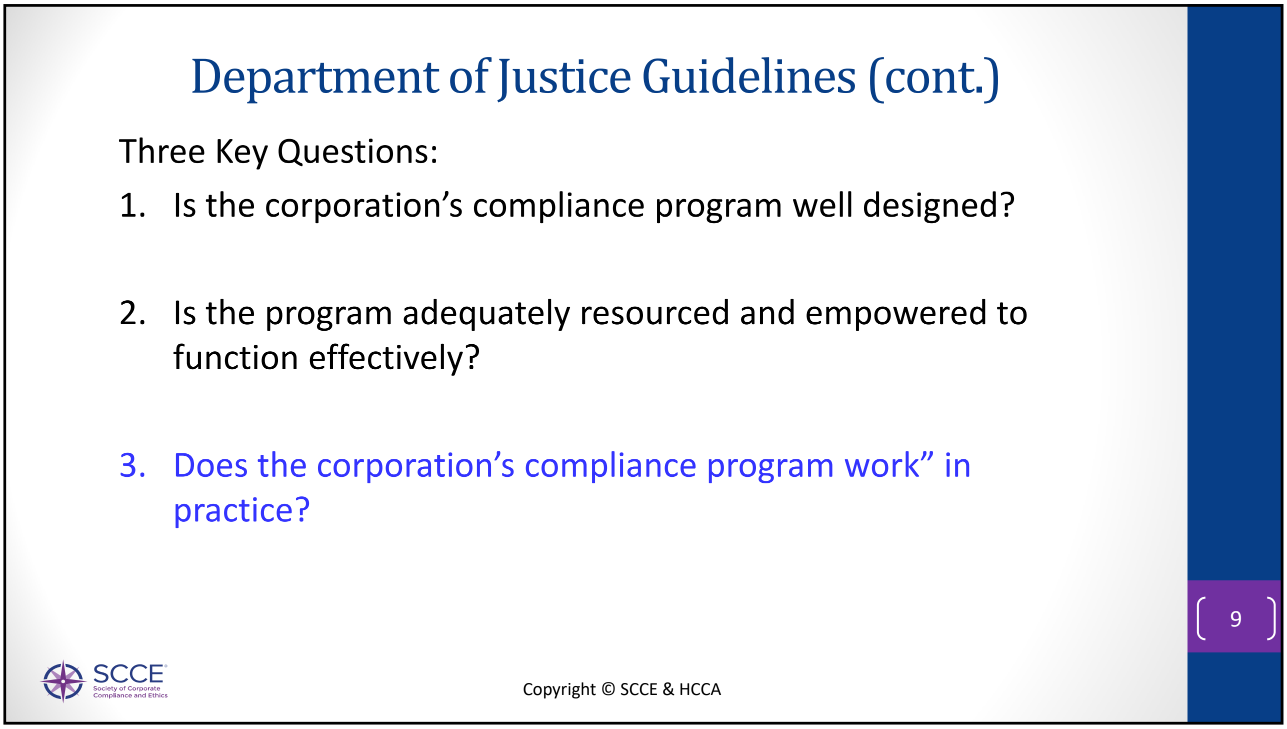
Factors include:

- Adequacy and effectiveness of compliance program at the time of the offense and at the time of charging decision
- Corporation's remedial efforts in response to the compliance event
- Program "effectiveness" in evaluating strength of the program

8

SCCE Society of Corporate Compliance and Ethics

8



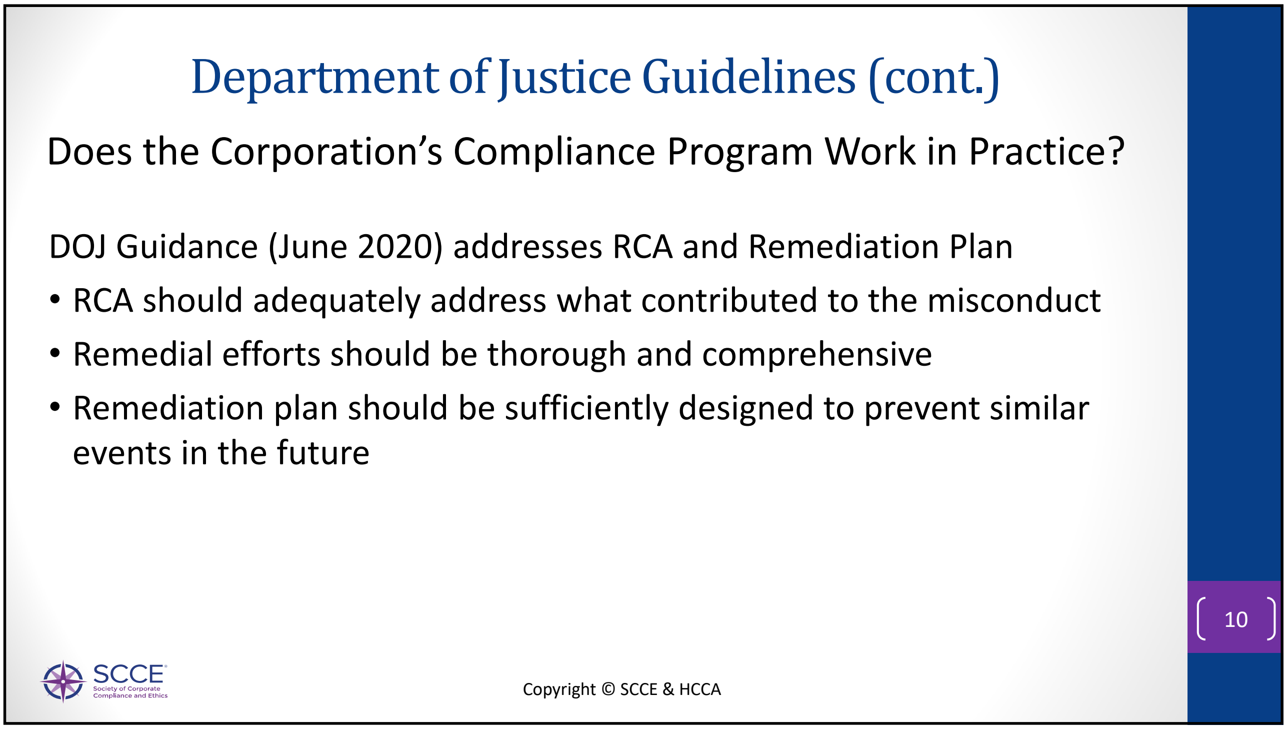
Department of Justice Guidelines (cont.)

Three Key Questions:

1. Is the corporation’s compliance program well designed?

2. Is the program adequately resourced and empowered to function effectively?

3. Does the corporation’s compliance program work” in practice?

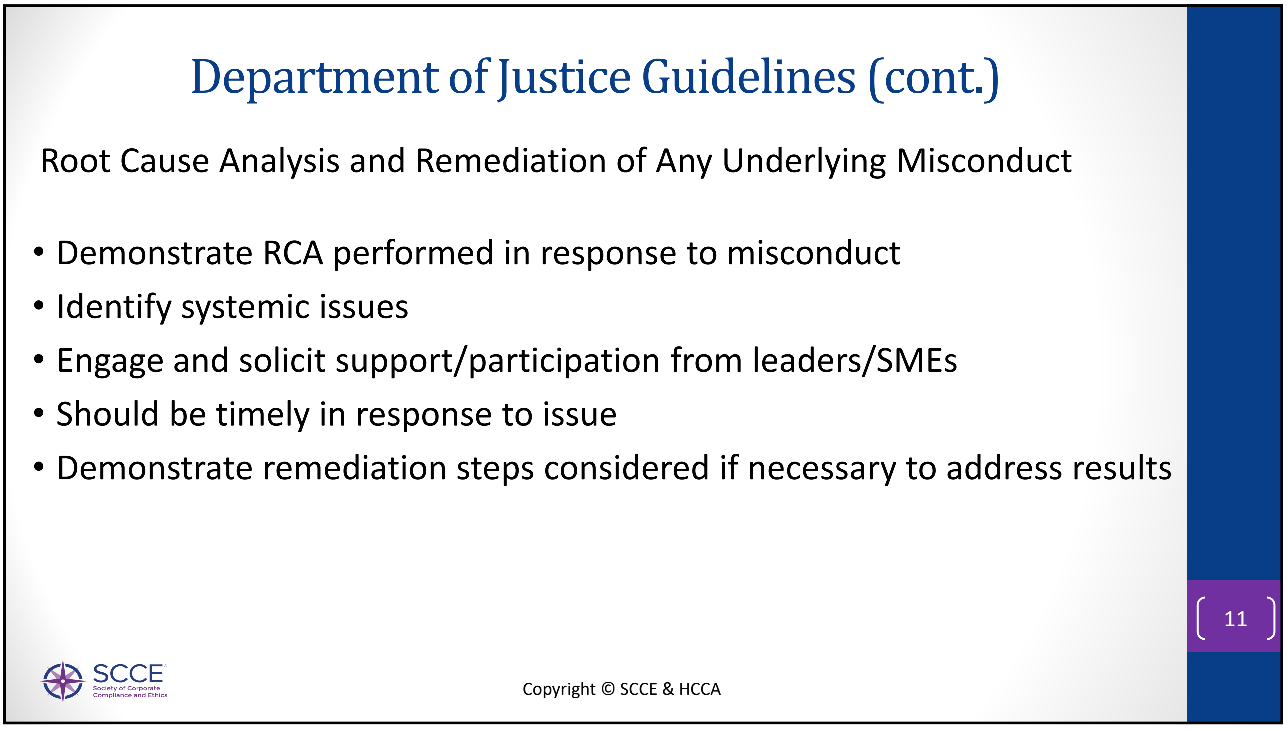


Department of Justice Guidelines (cont.)

Does the Corporation’s Compliance Program Work in Practice?

DOJ Guidance (June 2020) addresses RCA and Remediation Plan

- RCA should adequately address what contributed to the misconduct
- Remedial efforts should be thorough and comprehensive
- Remediation plan should be sufficiently designed to prevent similar events in the future

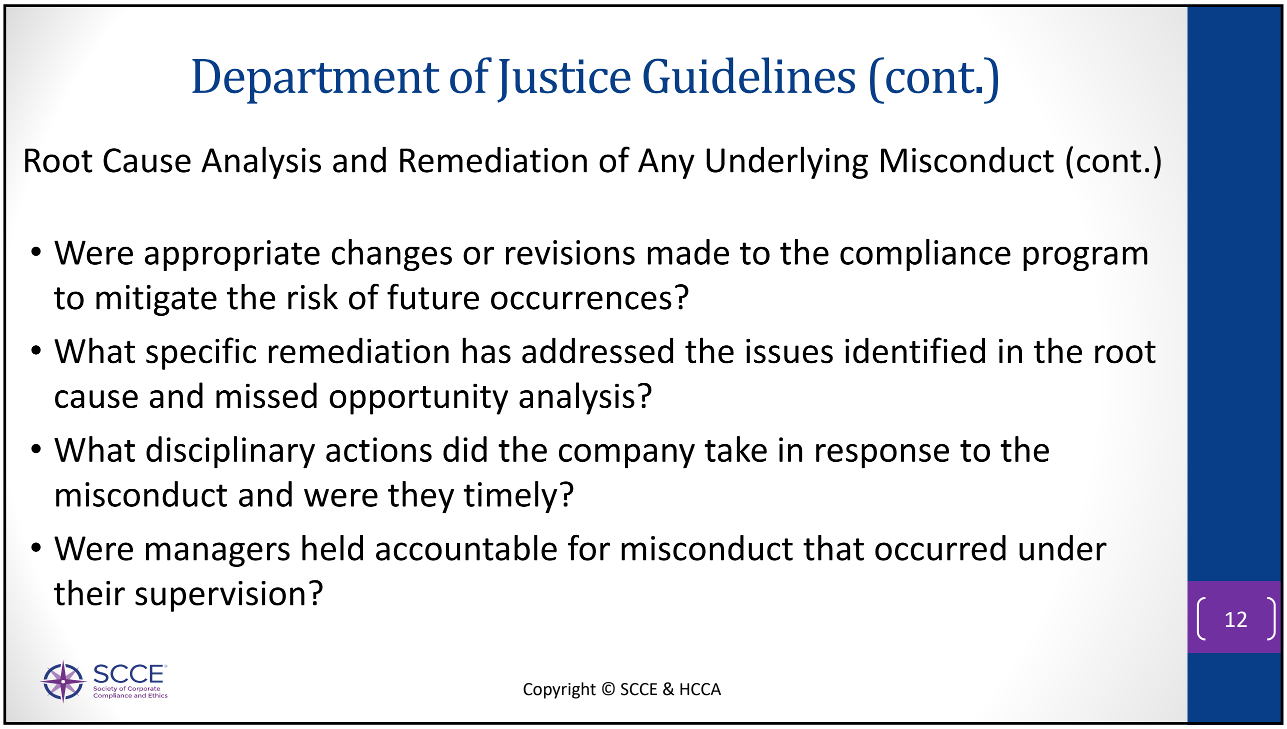


Department of Justice Guidelines (cont.)

Root Cause Analysis and Remediation of Any Underlying Misconduct

- Demonstrate RCA performed in response to misconduct
- Identify systemic issues
- Engage and solicit support/participation from leaders/SMEs
- Should be timely in response to issue
- Demonstrate remediation steps considered if necessary to address results

11

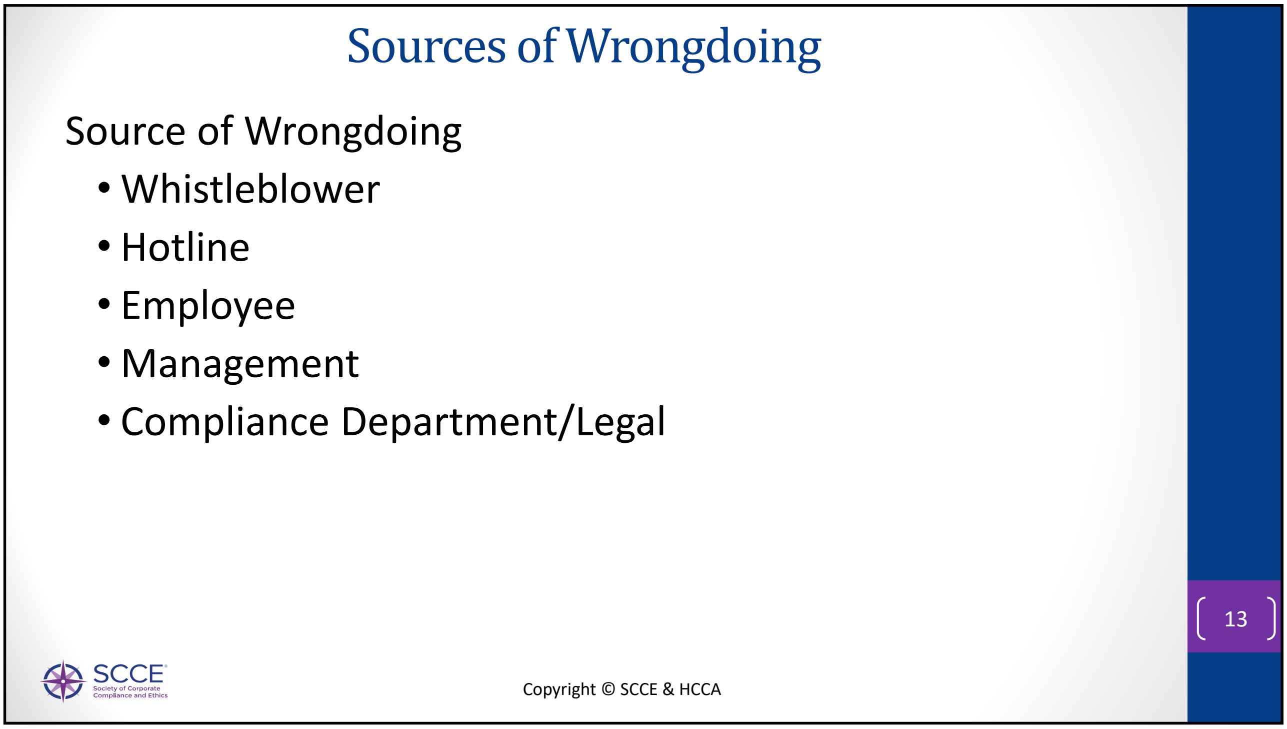


Department of Justice Guidelines (cont.)

Root Cause Analysis and Remediation of Any Underlying Misconduct (cont.)

- Were appropriate changes or revisions made to the compliance program to mitigate the risk of future occurrences?
- What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?
- What disciplinary actions did the company take in response to the misconduct and were they timely?
- Were managers held accountable for misconduct that occurred under their supervision?

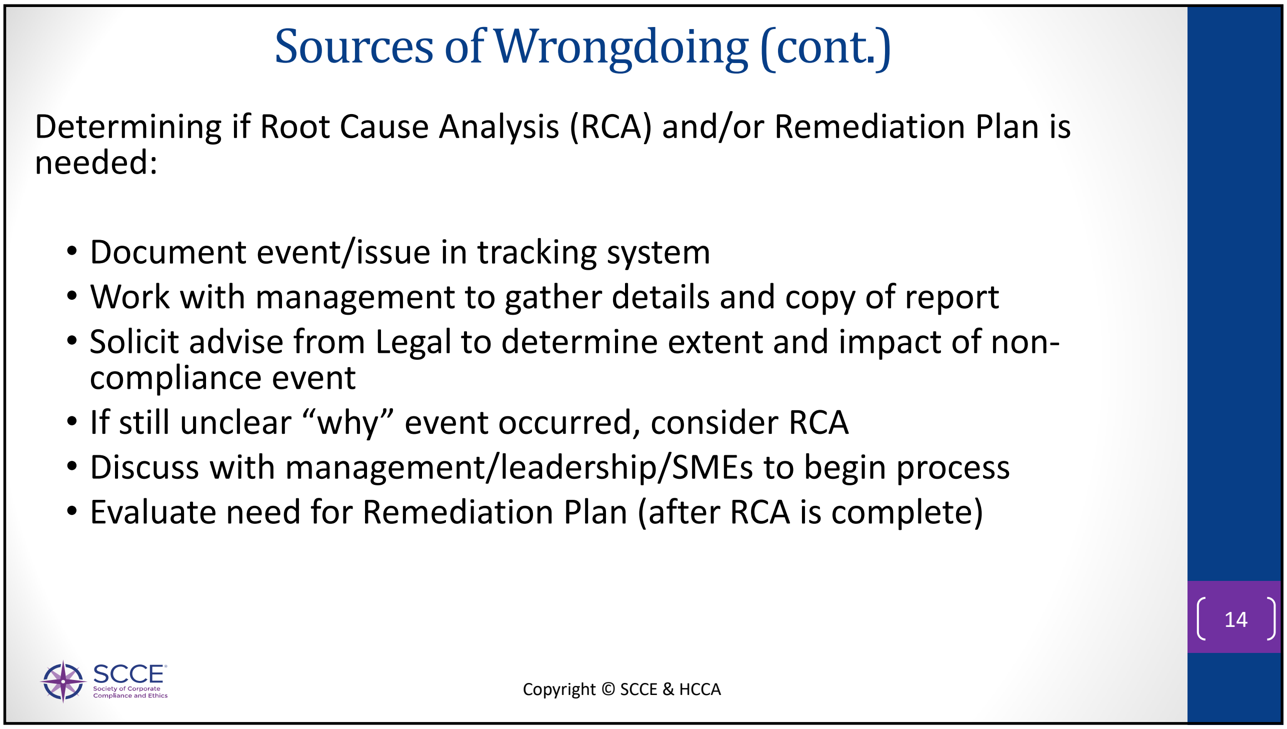
12



Sources of Wrongdoing

Source of Wrongdoing

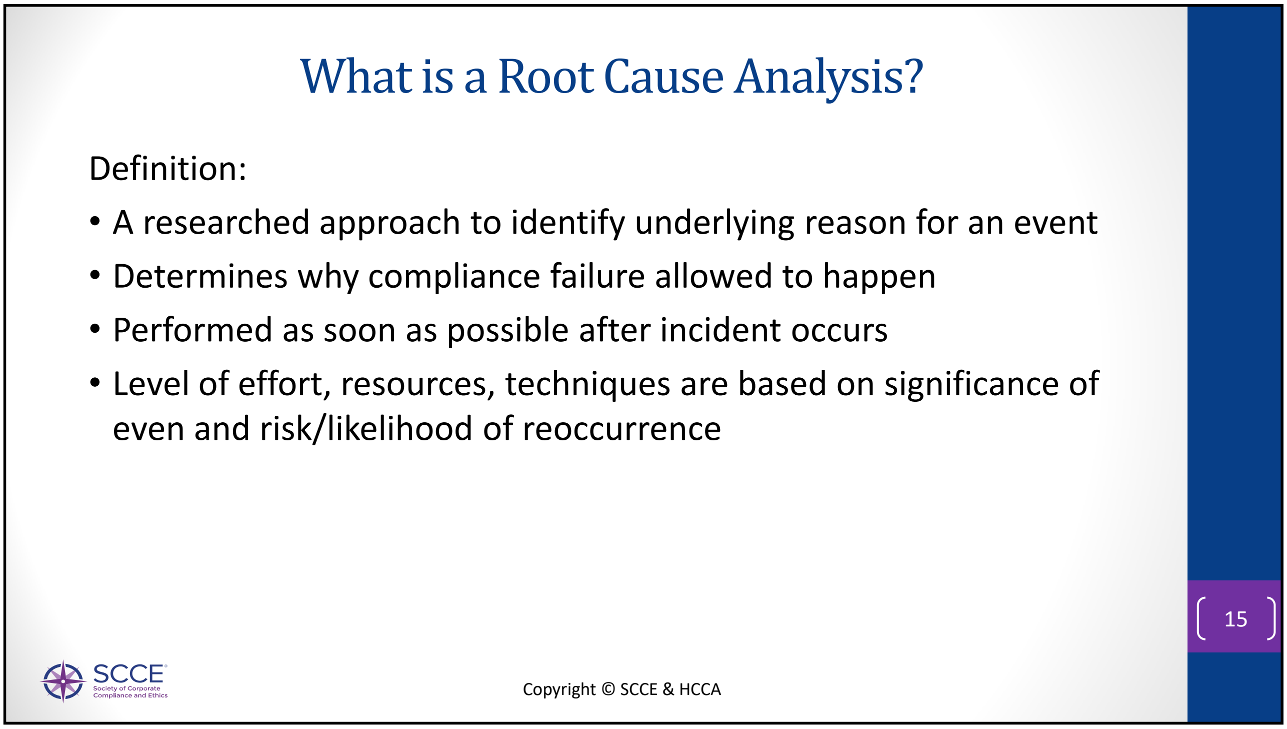
- Whistleblower
- Hotline
- Employee
- Management
- Compliance Department/Legal



Sources of Wrongdoing (cont.)

Determining if Root Cause Analysis (RCA) and/or Remediation Plan is needed:

- Document event/issue in tracking system
- Work with management to gather details and copy of report
- Solicit advise from Legal to determine extent and impact of non-compliance event
- If still unclear "why" event occurred, consider RCA
- Discuss with management/leadership/SMEs to begin process
- Evaluate need for Remediation Plan (after RCA is complete)

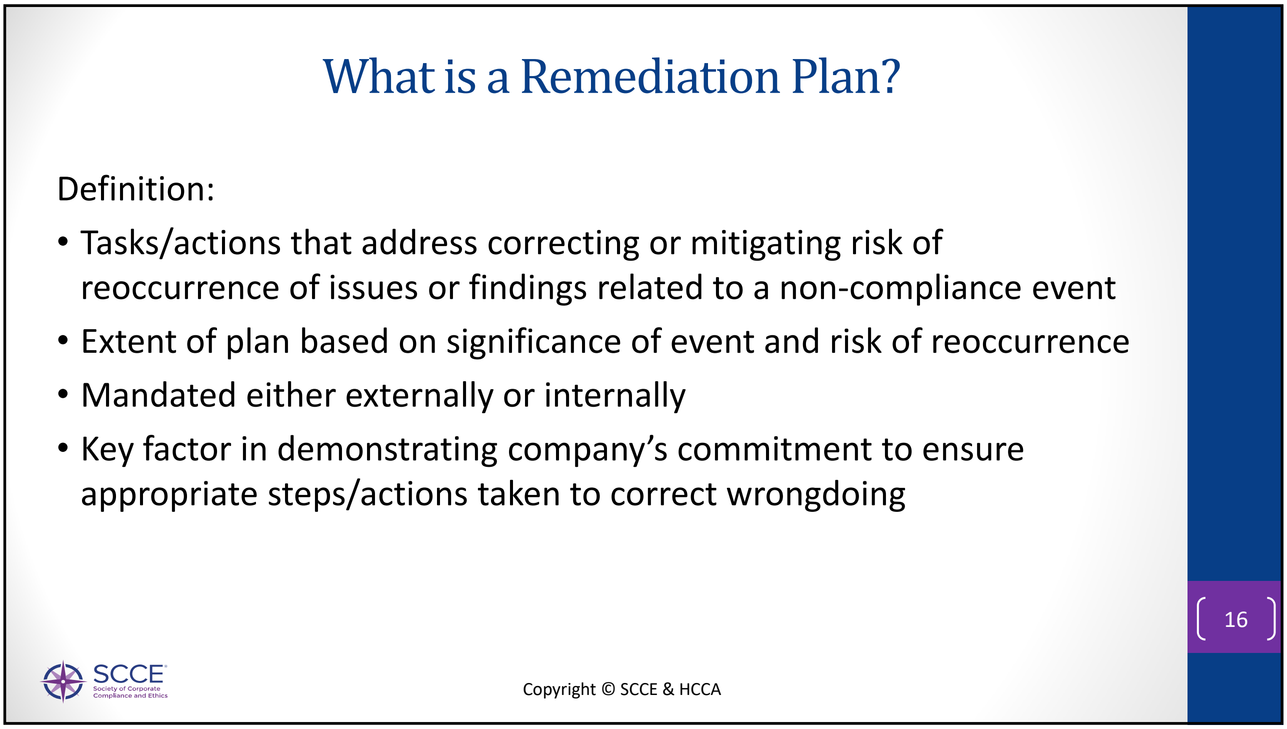


What is a Root Cause Analysis?

Definition:

- A researched approach to identify underlying reason for an event
- Determines why compliance failure allowed to happen
- Performed as soon as possible after incident occurs
- Level of effort, resources, techniques are based on significance of even and risk/likelihood of reoccurrence

15

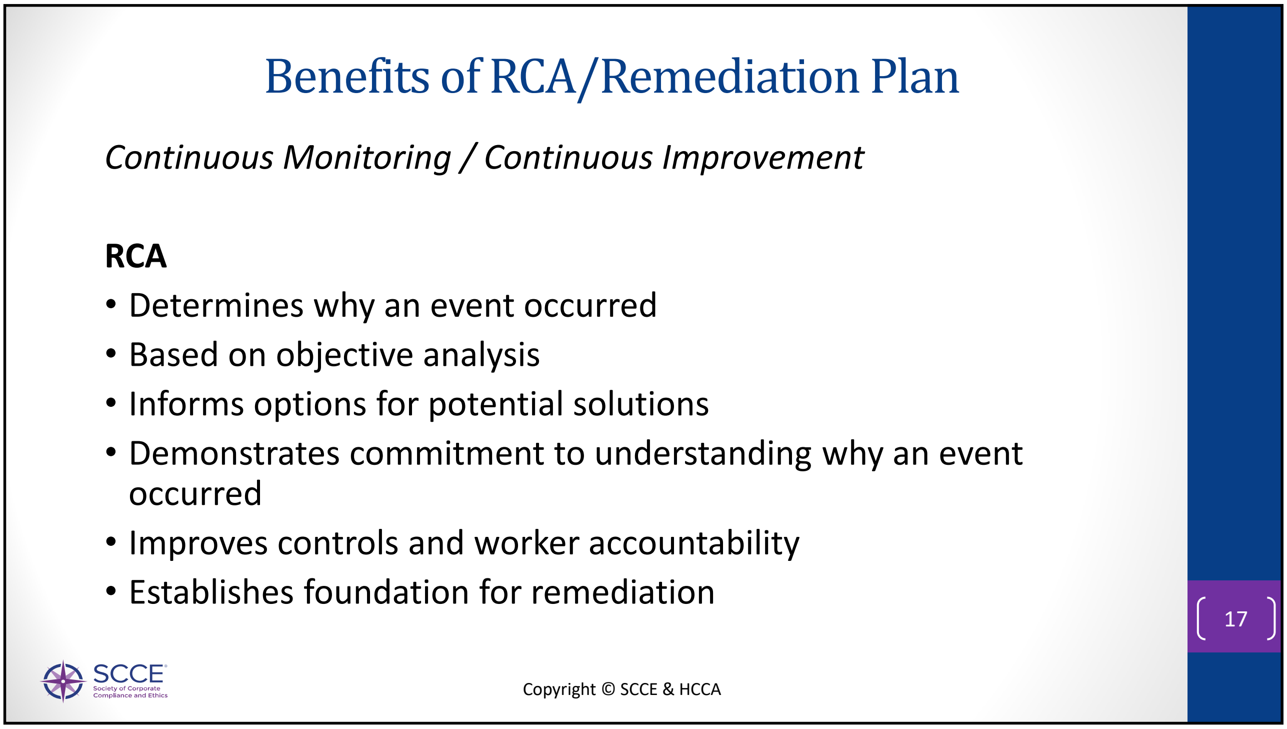


What is a Remediation Plan?

Definition:

- Tasks/actions that address correcting or mitigating risk of reoccurrence of issues or findings related to a non-compliance event
- Extent of plan based on significance of event and risk of reoccurrence
- Mandated either externally or internally
- Key factor in demonstrating company’s commitment to ensure appropriate steps/actions taken to correct wrongdoing

16

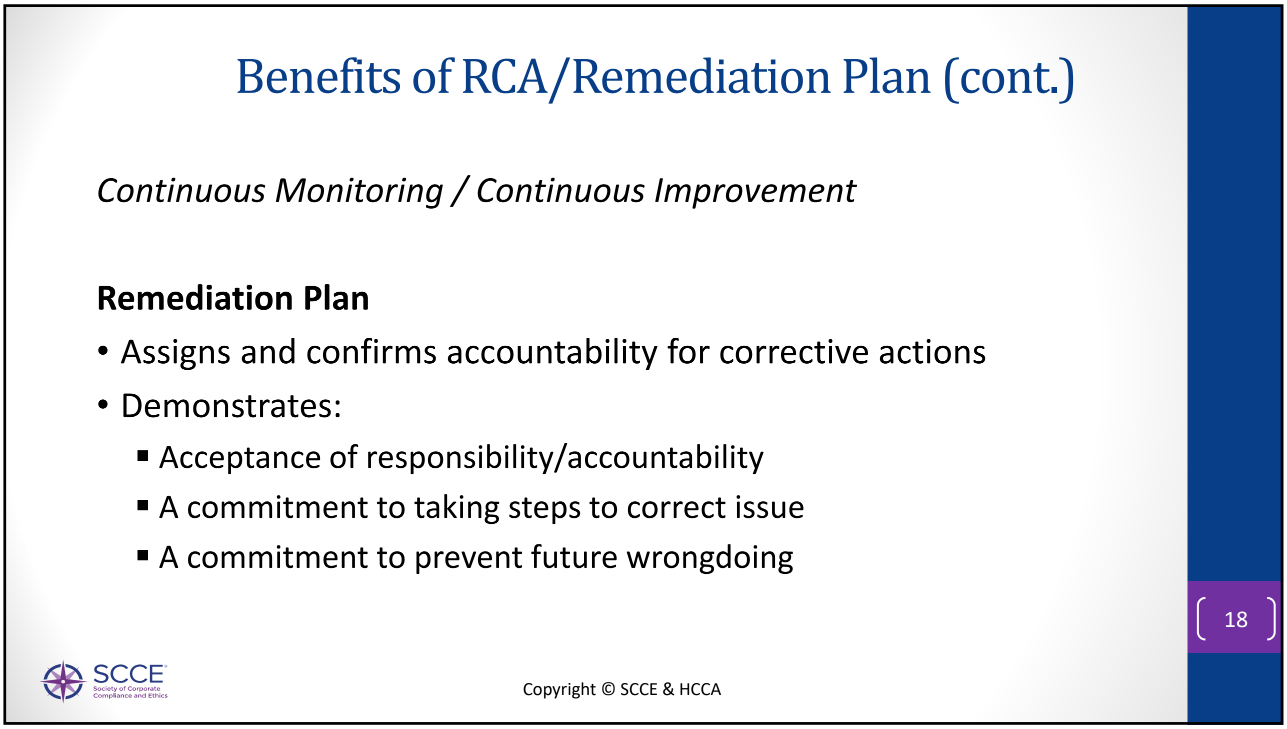


Benefits of RCA/Remediation Plan

Continuous Monitoring / Continuous Improvement

RCA

- Determines why an event occurred
- Based on objective analysis
- Informs options for potential solutions
- Demonstrates commitment to understanding why an event occurred
- Improves controls and worker accountability
- Establishes foundation for remediation

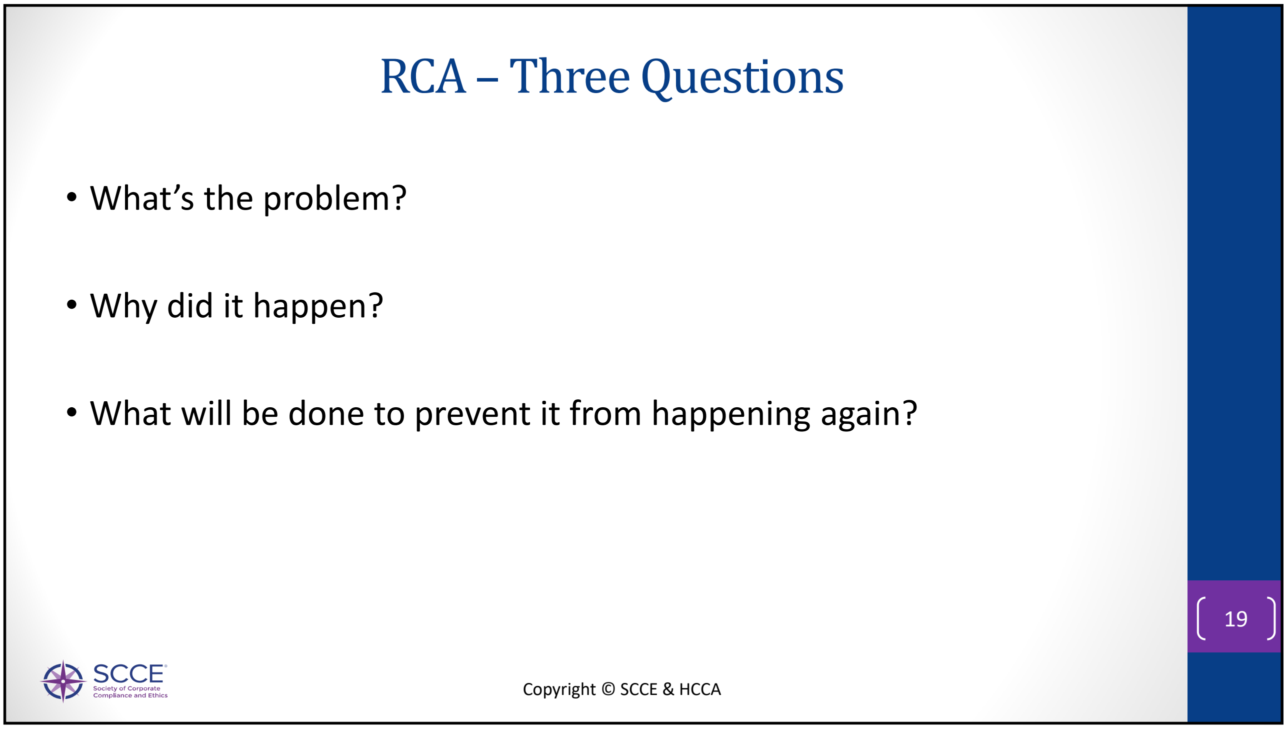


Benefits of RCA/Remediation Plan (cont.)

Continuous Monitoring / Continuous Improvement

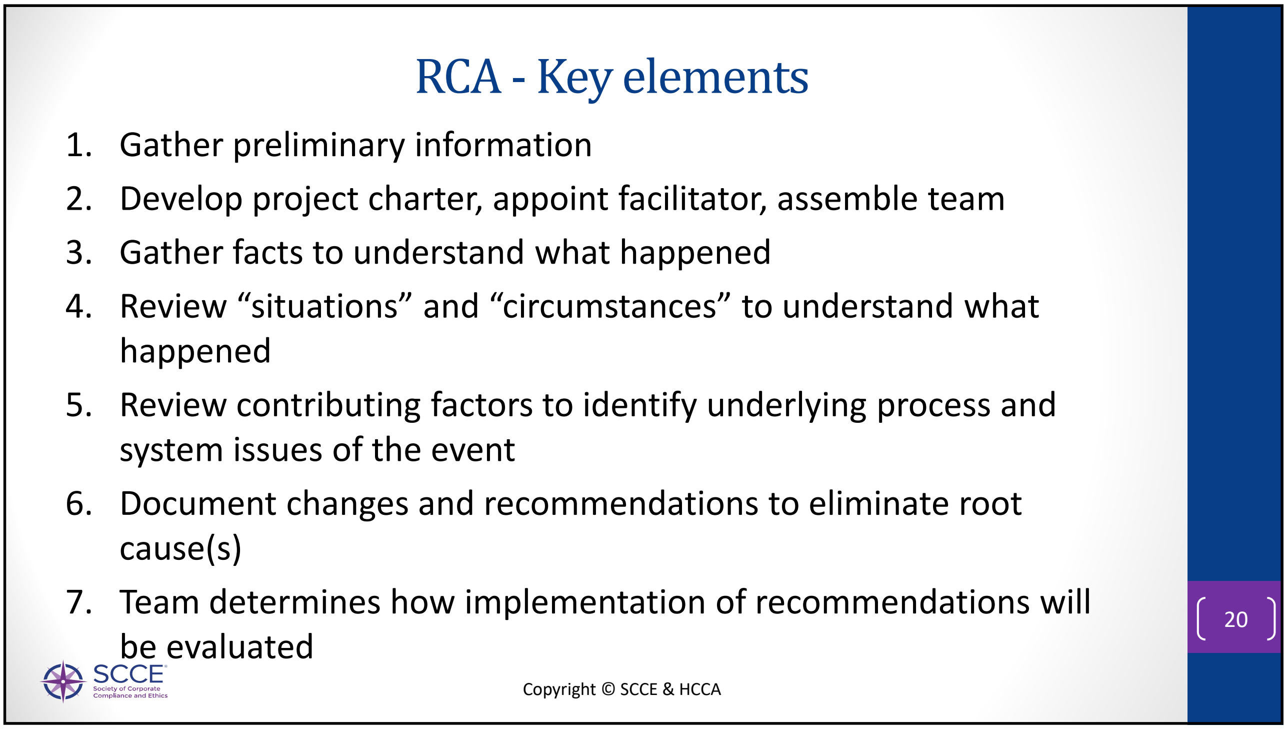
Remediation Plan

- Assigns and confirms accountability for corrective actions
- Demonstrates:
  - Acceptance of responsibility/accountability
  - A commitment to taking steps to correct issue
  - A commitment to prevent future wrongdoing



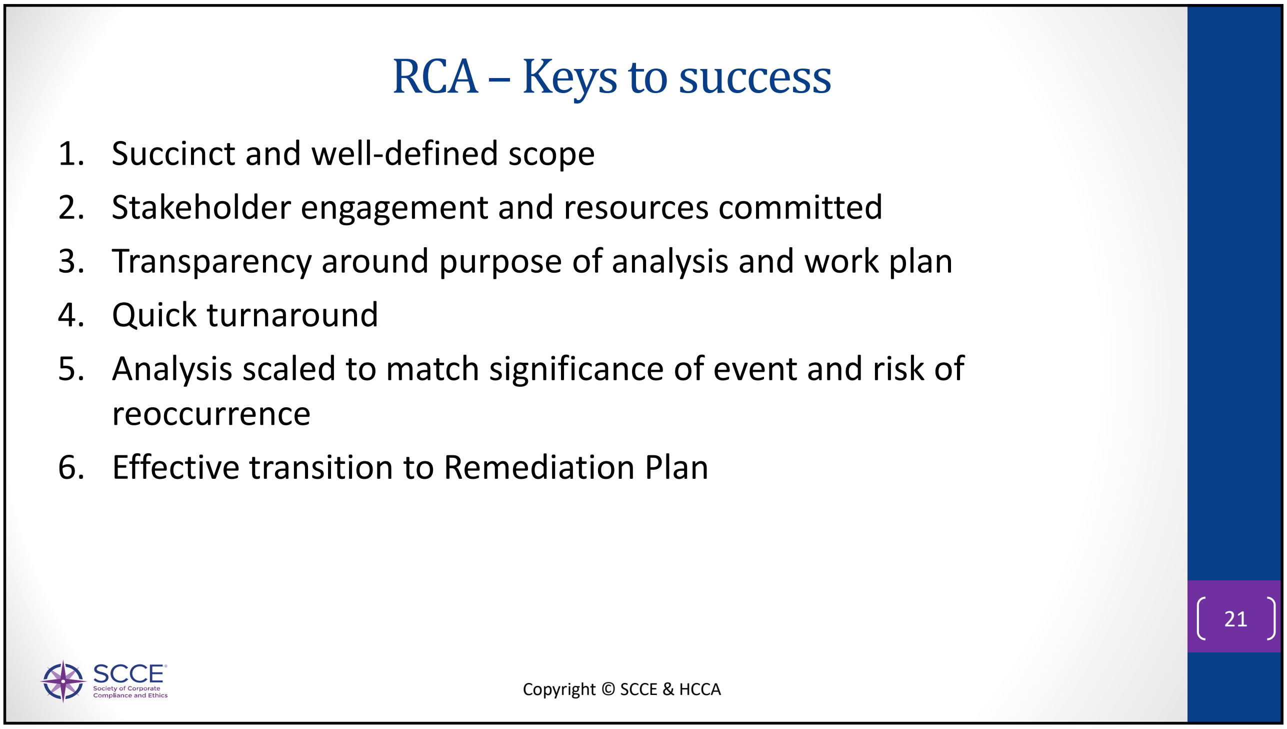
RCA – Three Questions

- What's the problem?
- Why did it happen?
- What will be done to prevent it from happening again?



RCA - Key elements

1. Gather preliminary information
2. Develop project charter, appoint facilitator, assemble team
3. Gather facts to understand what happened
4. Review "situations" and "circumstances" to understand what happened
5. Review contributing factors to identify underlying process and system issues of the event
6. Document changes and recommendations to eliminate root cause(s)
7. Team determines how implementation of recommendations will be evaluated

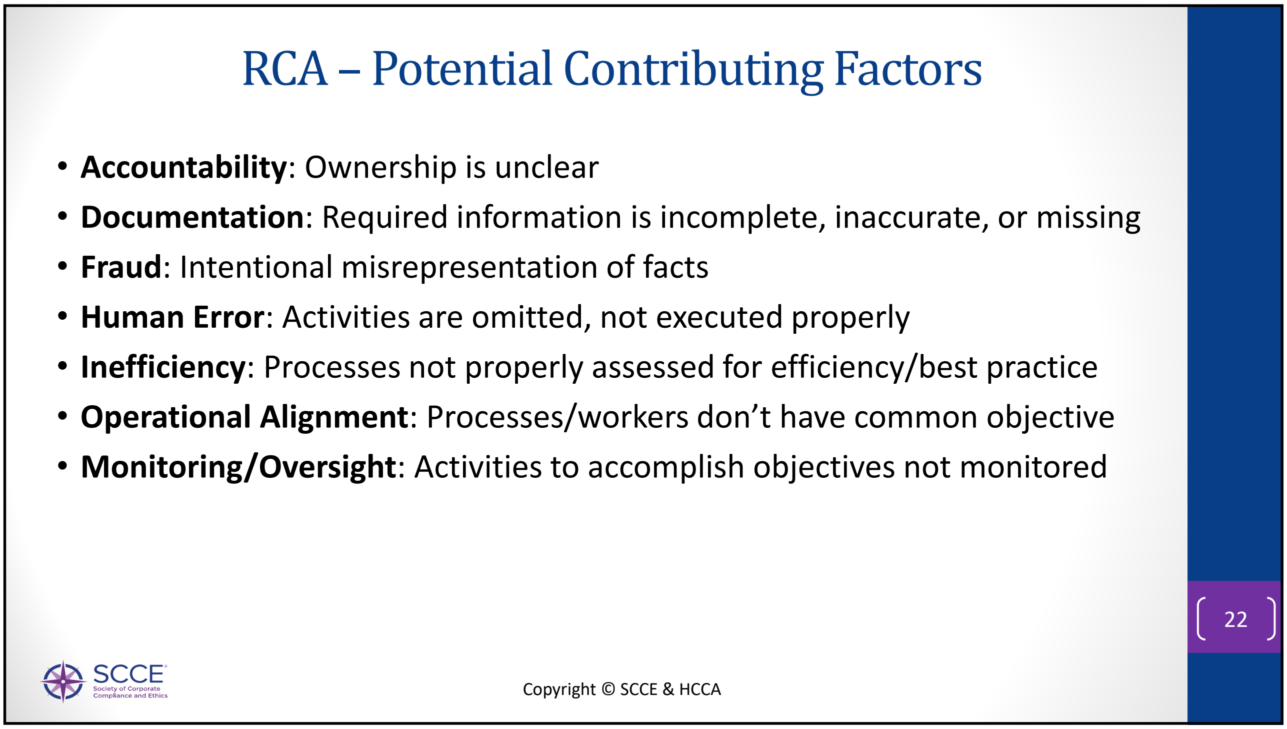


RCA – Keys to success

1. Succinct and well-defined scope
2. Stakeholder engagement and resources committed
3. Transparency around purpose of analysis and work plan
4. Quick turnaround
5. Analysis scaled to match significance of event and risk of reoccurrence
6. Effective transition to Remediation Plan

SCCE Society of Corporate Compliance and Ethics

21

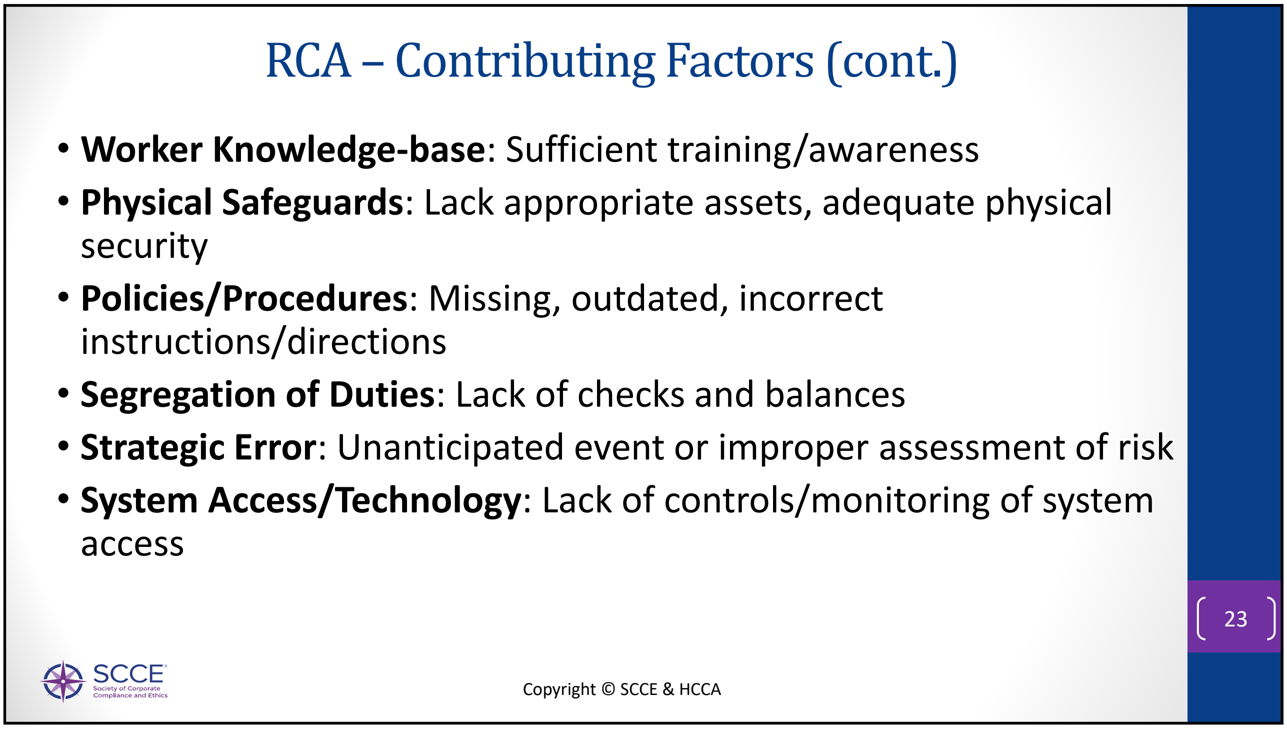


RCA – Potential Contributing Factors

- **Accountability**: Ownership is unclear
- **Documentation**: Required information is incomplete, inaccurate, or missing
- **Fraud**: Intentional misrepresentation of facts
- **Human Error**: Activities are omitted, not executed properly
- **Inefficiency**: Processes not properly assessed for efficiency/best practice
- **Operational Alignment**: Processes/workers don't have common objective
- **Monitoring/Oversight**: Activities to accomplish objectives not monitored

SCCE Society of Corporate Compliance and Ethics

22

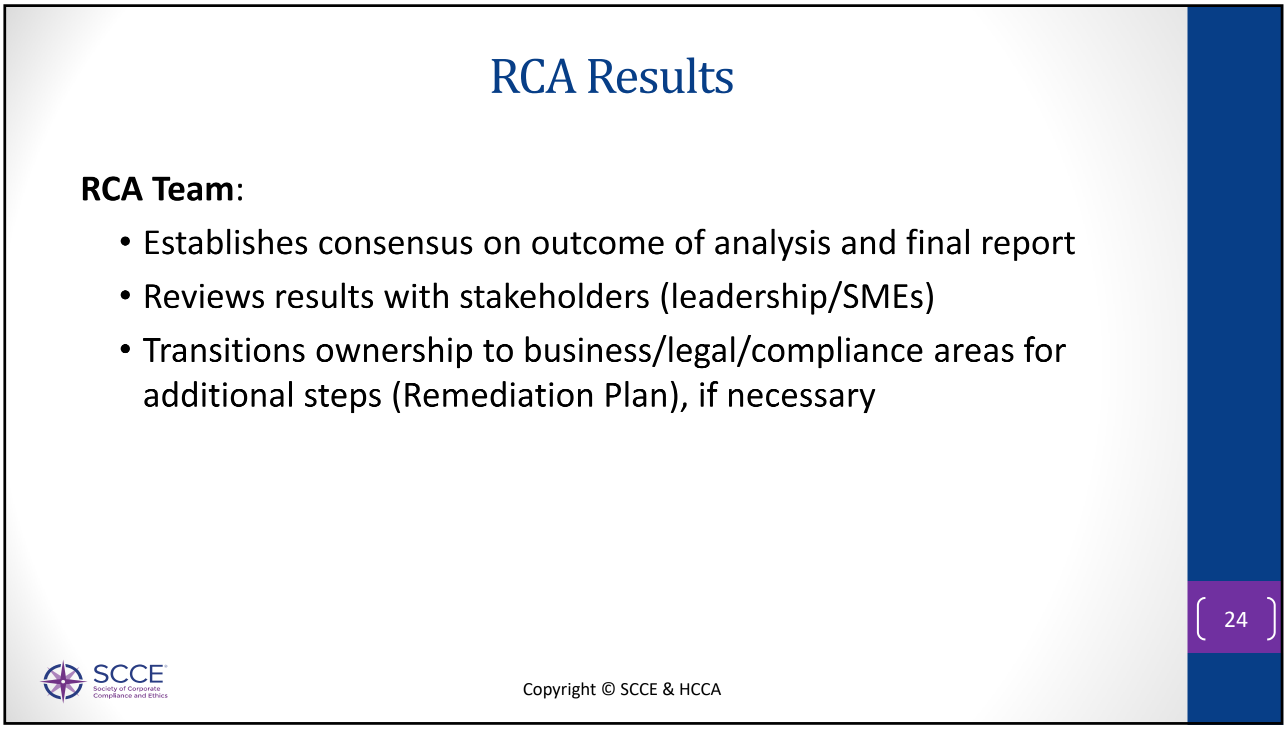


RCA – Contributing Factors (cont.)

- **Worker Knowledge-base**: Sufficient training/awareness
- **Physical Safeguards**: Lack appropriate assets, adequate physical security
- **Policies/Procedures**: Missing, outdated, incorrect instructions/directions
- **Segregation of Duties**: Lack of checks and balances
- **Strategic Error**: Unanticipated event or improper assessment of risk
- **System Access/Technology**: Lack of controls/monitoring of system access

23

23



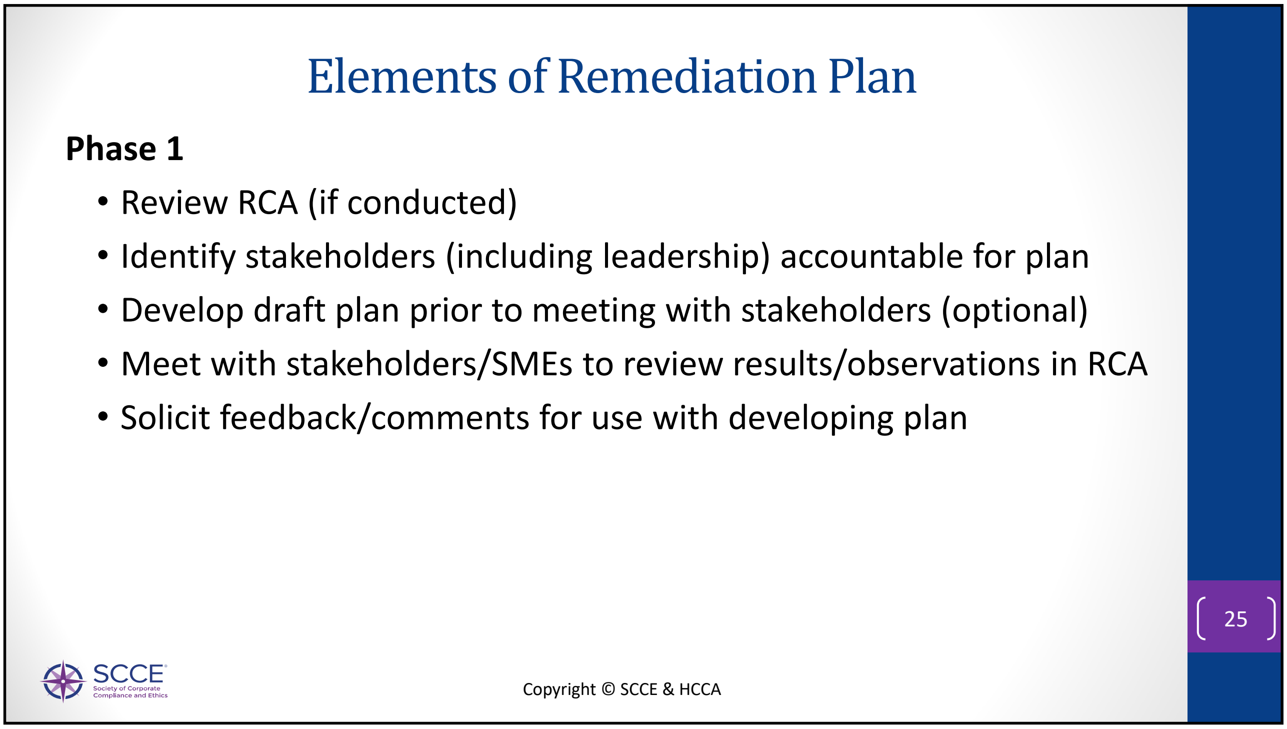
RCA Results

RCA Team:

- Establishes consensus on outcome of analysis and final report
- Reviews results with stakeholders (leadership/SMEs)
- Transitions ownership to business/legal/compliance areas for additional steps (Remediation Plan), if necessary

24

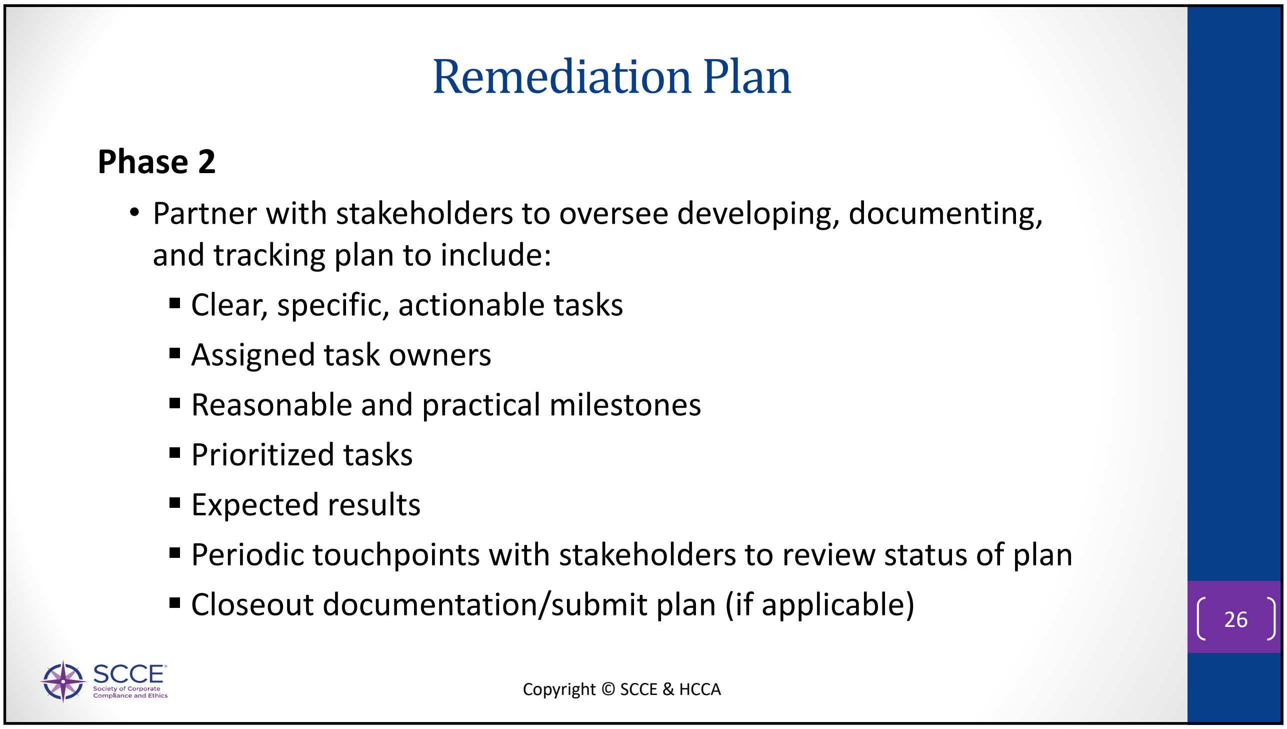
24



Elements of Remediation Plan

Phase 1

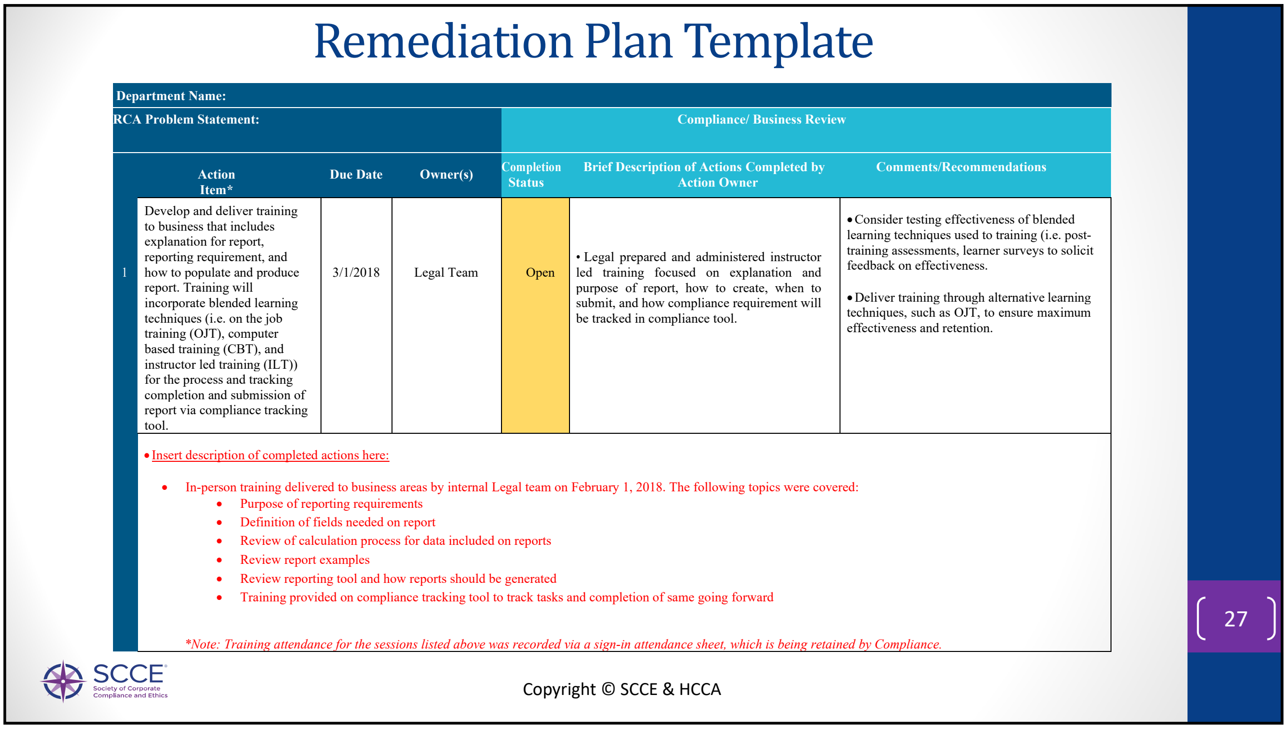
- Review RCA (if conducted)
- Identify stakeholders (including leadership) accountable for plan
- Develop draft plan prior to meeting with stakeholders (optional)
- Meet with stakeholders/SMEs to review results/observations in RCA
- Solicit feedback/comments for use with developing plan



Remediation Plan

Phase 2

- Partner with stakeholders to oversee developing, documenting, and tracking plan to include:
  - Clear, specific, actionable tasks
  - Assigned task owners
  - Reasonable and practical milestones
  - Prioritized tasks
  - Expected results
  - Periodic touchpoints with stakeholders to review status of plan
  - Closeout documentation/submit plan (if applicable)



Remediation Plan Template

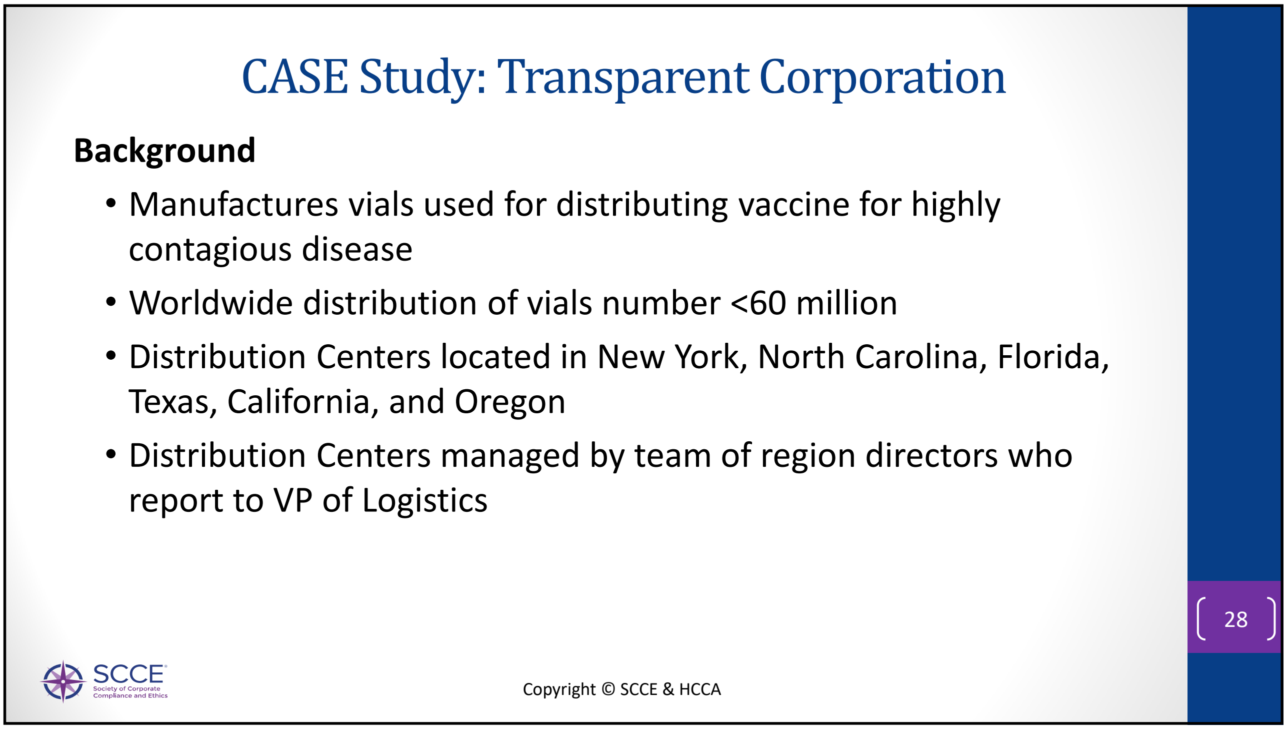
Department Name:						
RCA Problem Statement:				Compliance/ Business Review		
	Action Item*	Due Date	Owner(s)	Completion Status	Brief Description of Actions Completed by Action Owner	Comments/Recommendations
1	Develop and deliver training to business that includes explanation for report, reporting requirement, and how to populate and produce report. Training will incorporate blended learning techniques (i.e. on the job training (OJT), computer based training (CBT), and instructor led training (ILT)) for the process and tracking completion and submission of report via compliance tracking tool.	3/1/2018	Legal Team	Open	• Legal prepared and administered instructor led training focused on explanation and purpose of report, how to create, when to submit, and how compliance requirement will be tracked in compliance tool.	• Consider testing effectiveness of blended learning techniques used to training (i.e. post-training assessments, learner surveys to solicit feedback on effectiveness. • Deliver training through alternative learning techniques, such as OJT, to ensure maximum effectiveness and retention.

- Insert description of completed actions here:

- In-person training delivered to business areas by internal Legal team on February 1, 2018. The following topics were covered:
  - Purpose of reporting requirements
  - Definition of fields needed on report
  - Review of calculation process for data included on reports
  - Review report examples
  - Review reporting tool and how reports should be generated
  - Training provided on compliance tracking tool to track tasks and completion of same going forward

**Note: Training attendance for the sessions listed above was recorded via a sign-in attendance sheet, which is being retained by Compliance.*

27

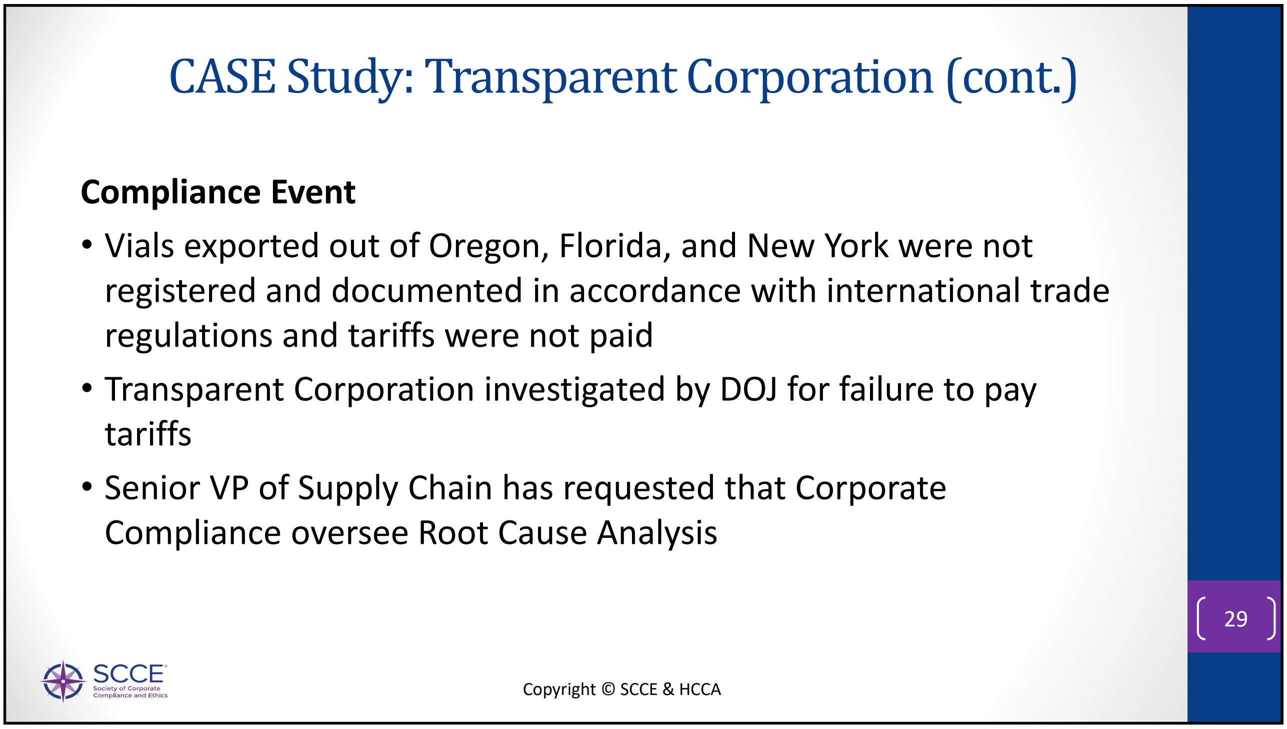


CASE Study: Transparent Corporation

Background

- Manufactures vials used for distributing vaccine for highly contagious disease
- Worldwide distribution of vials number <60 million
- Distribution Centers located in New York, North Carolina, Florida, Texas, California, and Oregon
- Distribution Centers managed by team of region directors who report to VP of Logistics

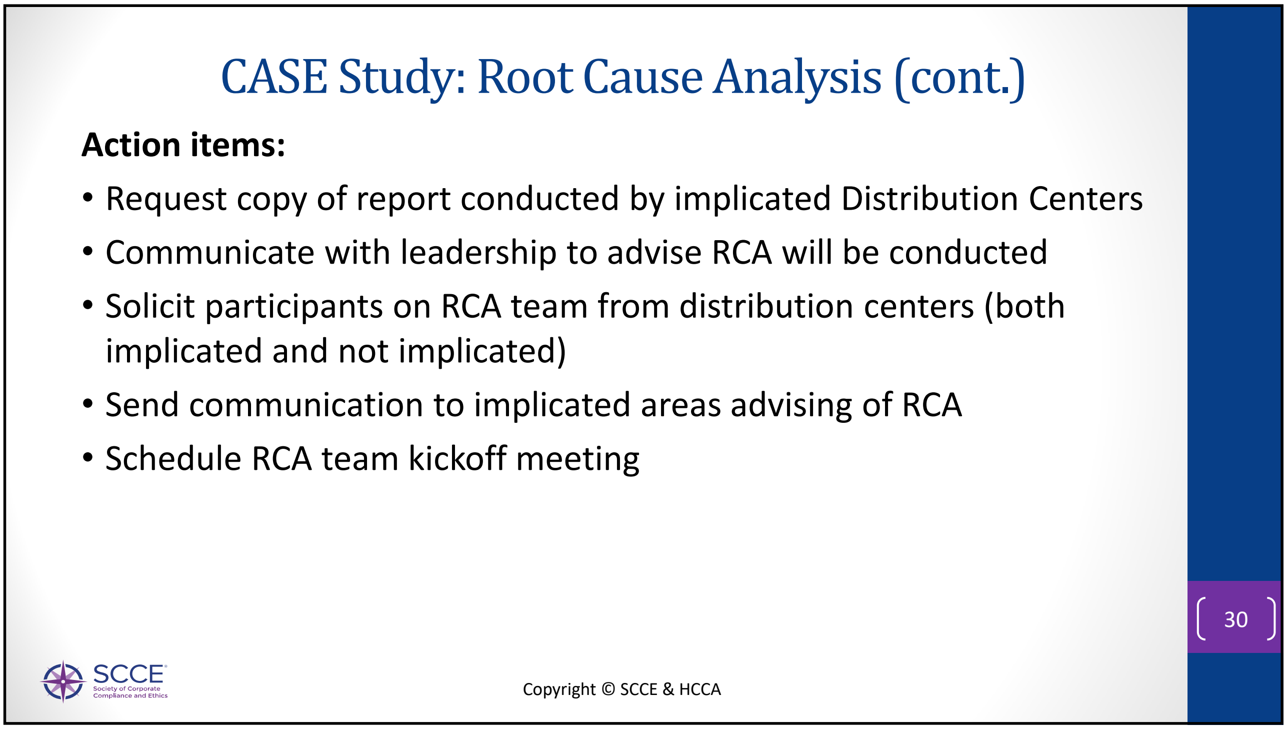
28



CASE Study: Transparent Corporation (cont.)

Compliance Event

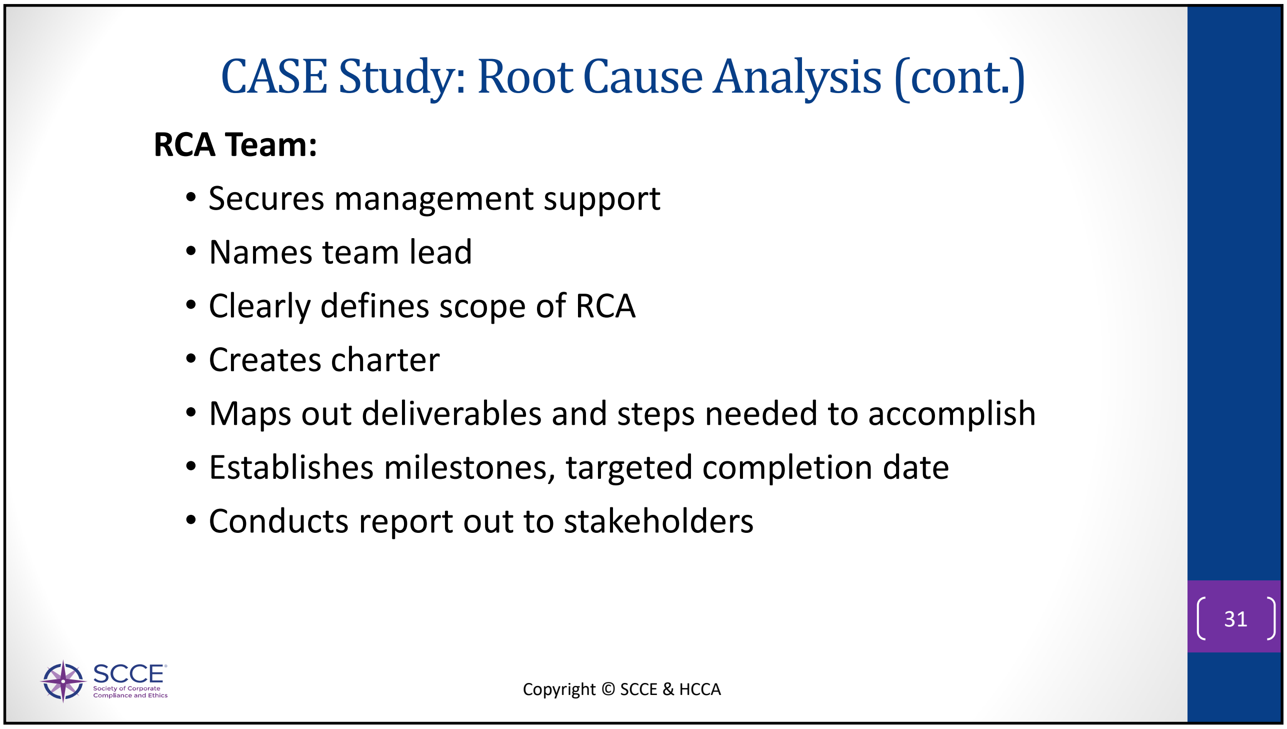
- Vials exported out of Oregon, Florida, and New York were not registered and documented in accordance with international trade regulations and tariffs were not paid
- Transparent Corporation investigated by DOJ for failure to pay tariffs
- Senior VP of Supply Chain has requested that Corporate Compliance oversee Root Cause Analysis



CASE Study: Root Cause Analysis (cont.)

Action items:

- Request copy of report conducted by implicated Distribution Centers
- Communicate with leadership to advise RCA will be conducted
- Solicit participants on RCA team from distribution centers (both implicated and not implicated)
- Send communication to implicated areas advising of RCA
- Schedule RCA team kickoff meeting



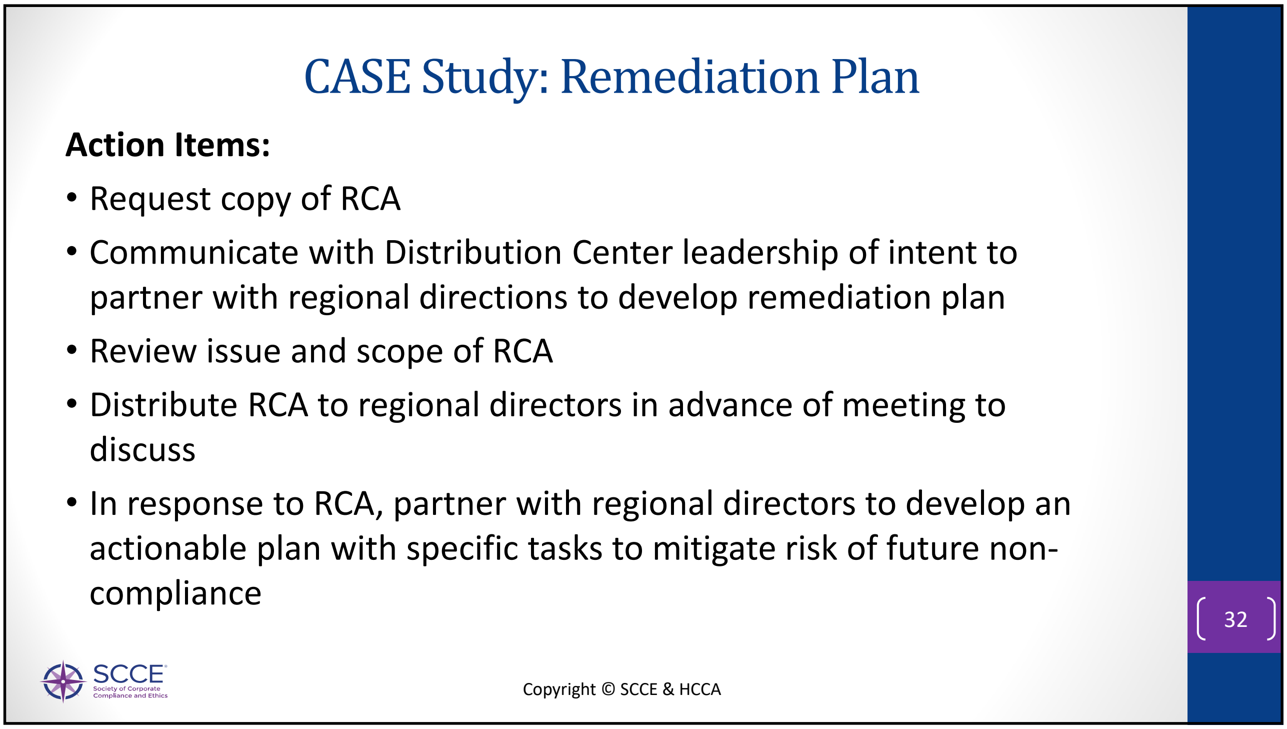
CASE Study: Root Cause Analysis (cont.)

RCA Team:

- Secures management support
- Names team lead
- Clearly defines scope of RCA
- Creates charter
- Maps out deliverables and steps needed to accomplish
- Establishes milestones, targeted completion date
- Conducts report out to stakeholders

31

31



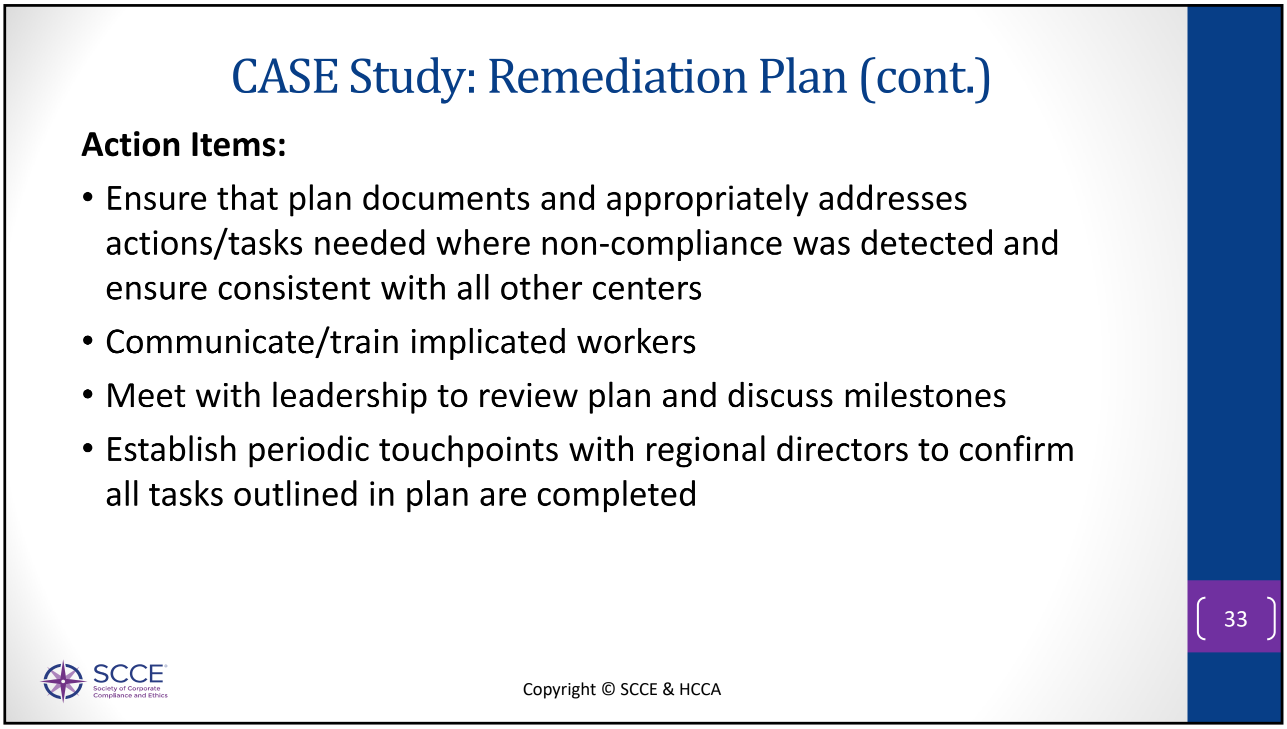
CASE Study: Remediation Plan

Action Items:

- Request copy of RCA
- Communicate with Distribution Center leadership of intent to partner with regional directions to develop remediation plan
- Review issue and scope of RCA
- Distribute RCA to regional directors in advance of meeting to discuss
- In response to RCA, partner with regional directors to develop an actionable plan with specific tasks to mitigate risk of future non-compliance

32

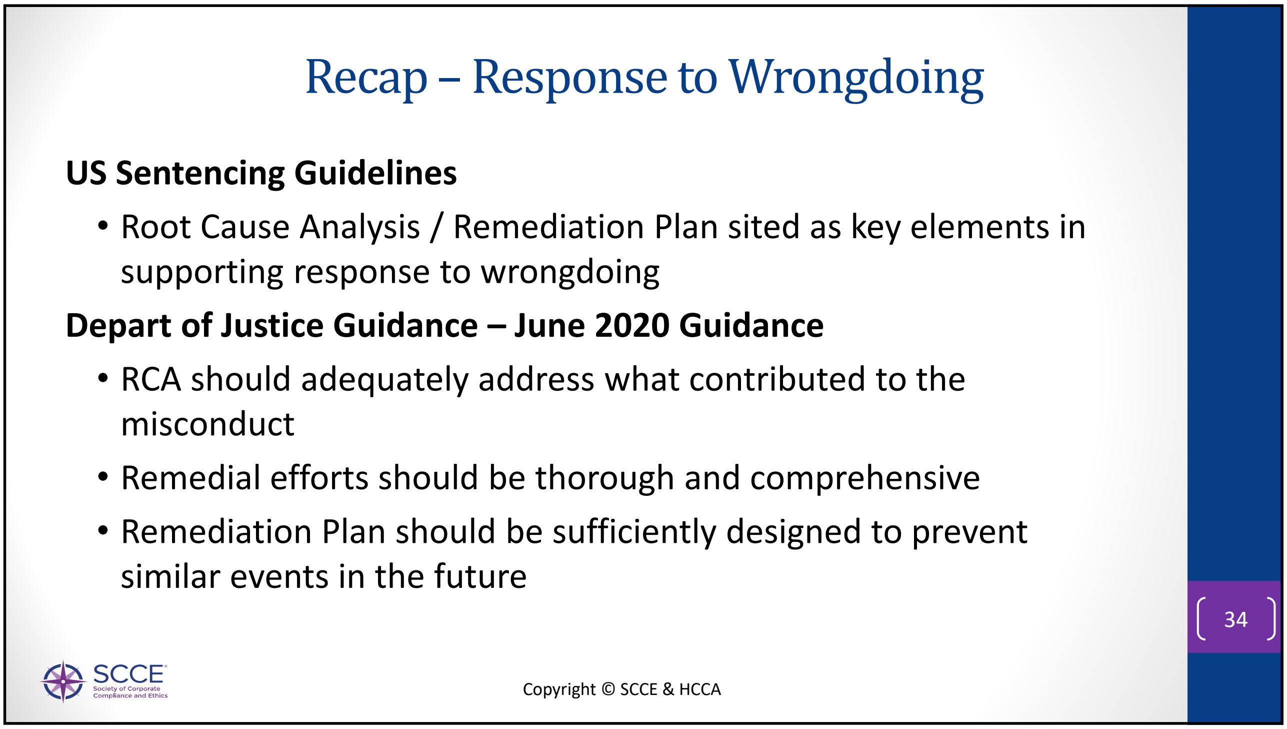
32



CASE Study: Remediation Plan (cont.)

Action Items:

- Ensure that plan documents and appropriately addresses actions/tasks needed where non-compliance was detected and ensure consistent with all other centers
- Communicate/train implicated workers
- Meet with leadership to review plan and discuss milestones
- Establish periodic touchpoints with regional directors to confirm all tasks outlined in plan are completed



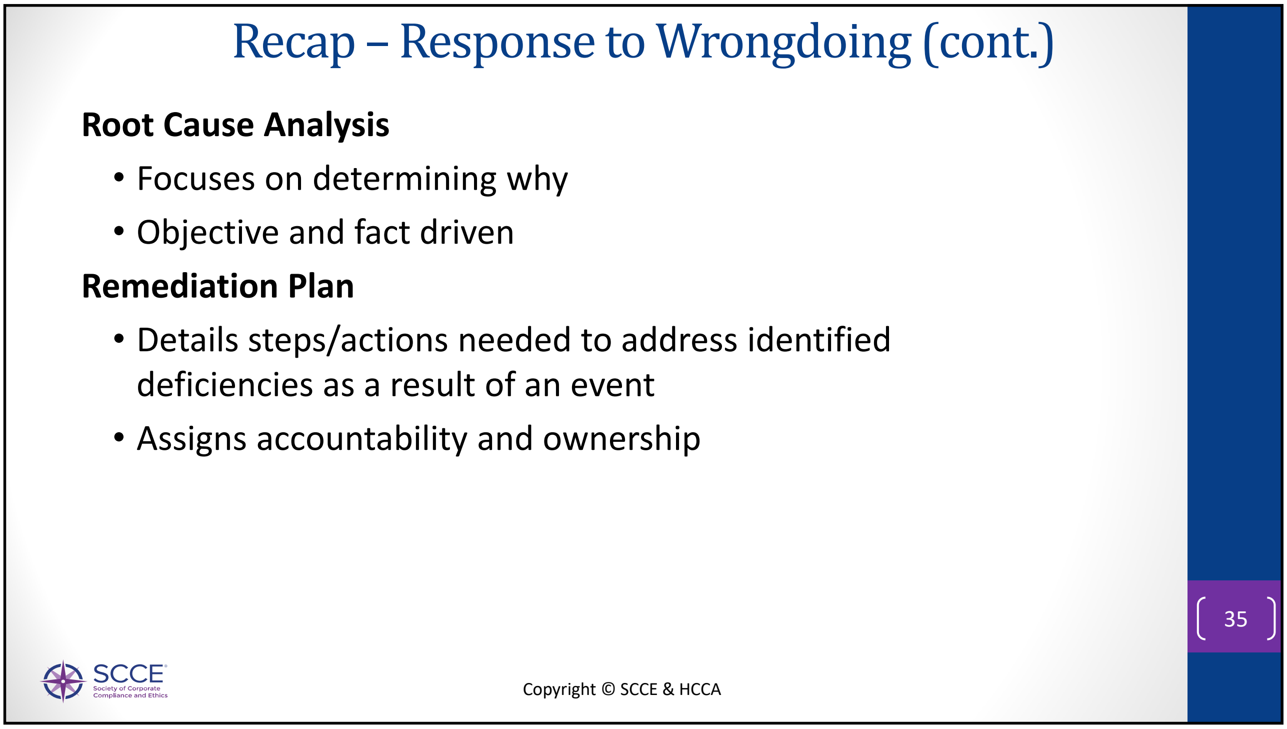
Recap – Response to Wrongdoing

US Sentencing Guidelines

- Root Cause Analysis / Remediation Plan sited as key elements in supporting response to wrongdoing

Depart of Justice Guidance – June 2020 Guidance

- RCA should adequately address what contributed to the misconduct
- Remedial efforts should be thorough and comprehensive
- Remediation Plan should be sufficiently designed to prevent similar events in the future



Recap – Response to Wrongdoing (cont.)

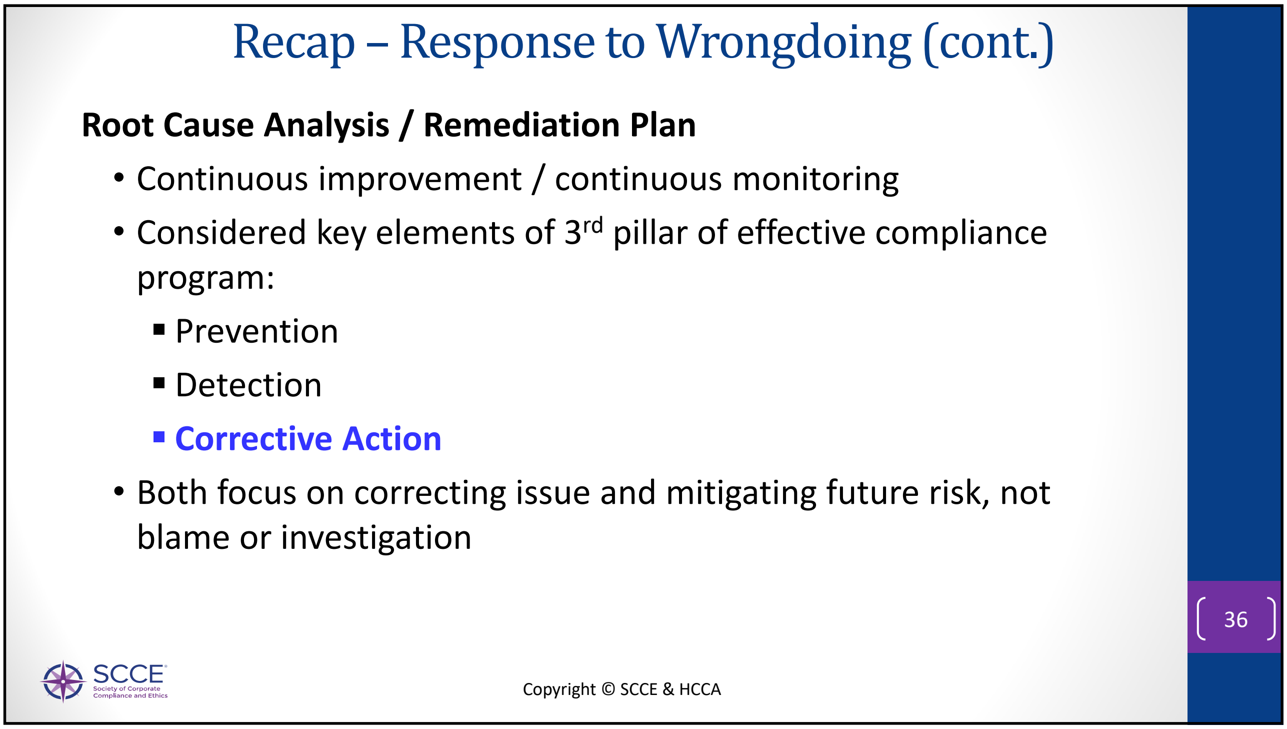
Root Cause Analysis

- Focuses on determining why
- Objective and fact driven

Remediation Plan

- Details steps/actions needed to address identified deficiencies as a result of an event
- Assigns accountability and ownership

35

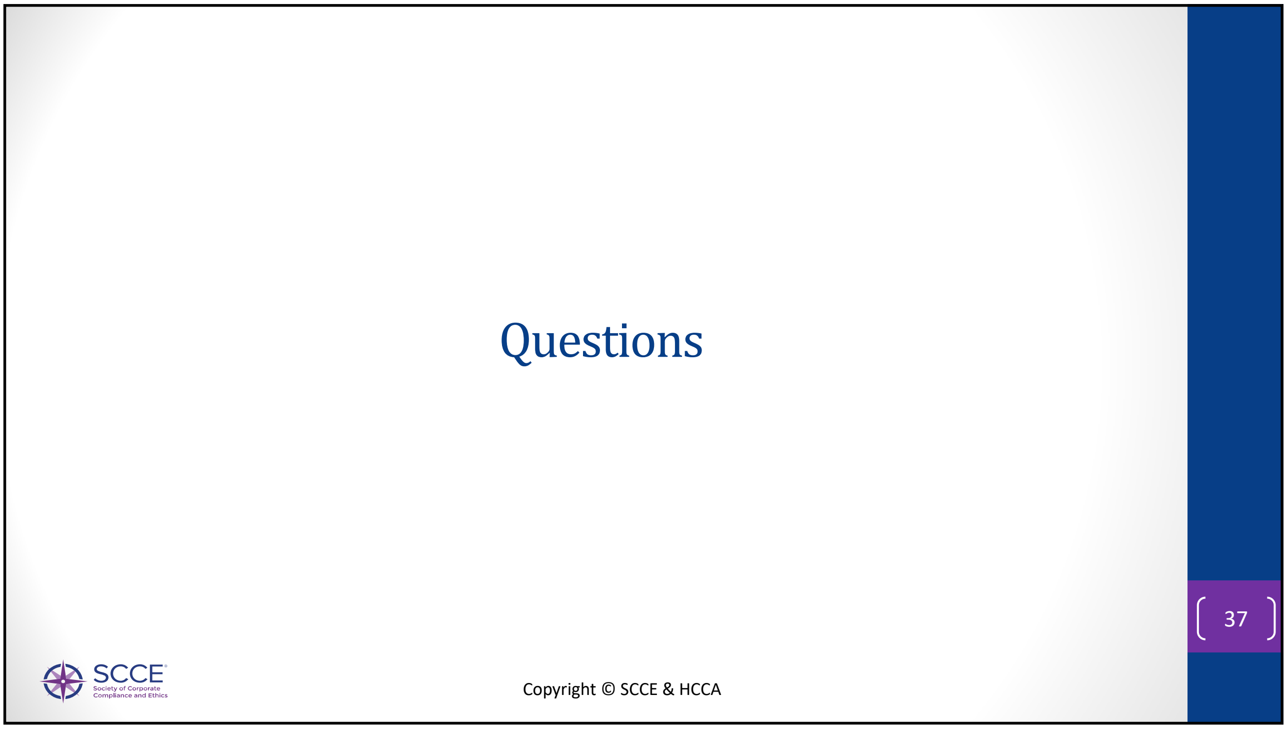


Recap – Response to Wrongdoing (cont.)

Root Cause Analysis / Remediation Plan

- Continuous improvement / continuous monitoring
- Considered key elements of 3rd pillar of effective compliance program:
  - Prevention
  - Detection
  - **Corrective Action**
- Both focus on correcting issue and mitigating future risk, not blame or investigation

36



Questions

SCCE Society of Corporate Compliance and Ethics

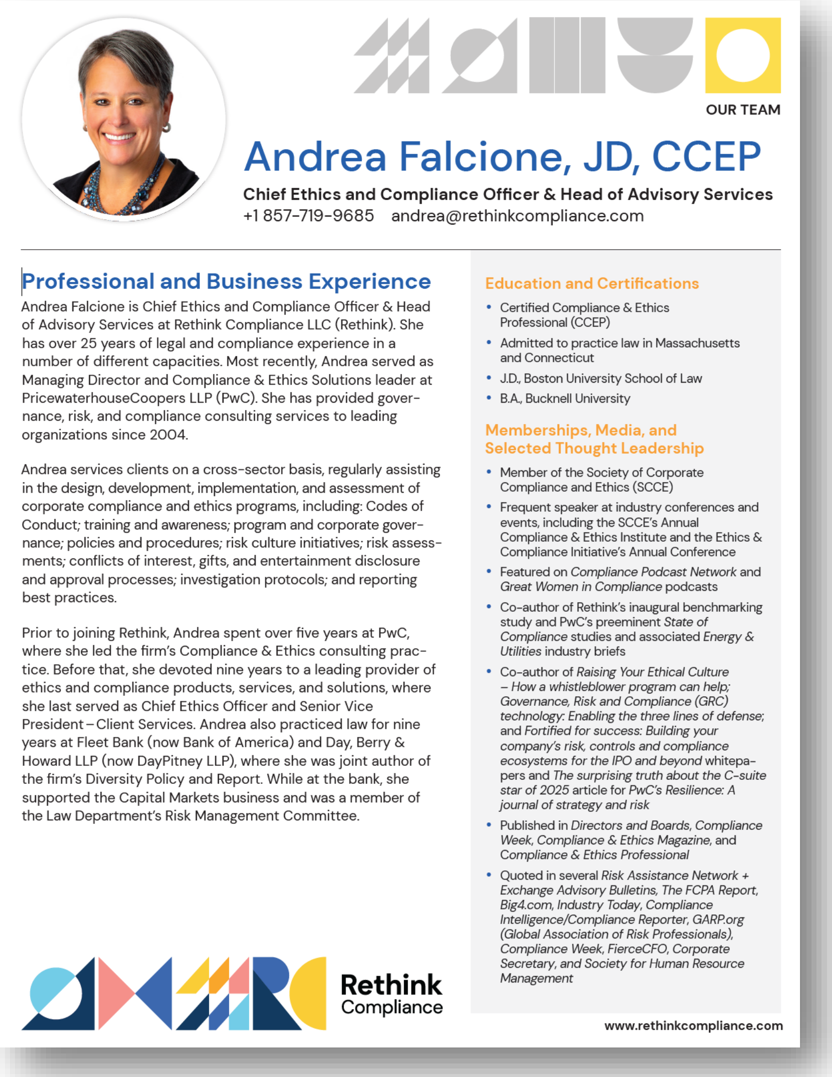
SCCE Compliance & Ethics Essentials Workshop

Hot/Common Compliance Topics

Andrea Falcione

SCCE
Society of Corporate Compliance and Ethics

Introductions



OUR TEAM

Andrea Falcione, JD, CCEP

Chief Ethics and Compliance Officer & Head of Advisory Services
+1 857-719-9685   andrea@rethinkcompliance.com

Professional and Business Experience

Andrea Falcione is Chief Ethics and Compliance Officer & Head of Advisory Services at Rethink Compliance LLC (Rethink). She has over 25 years of legal and compliance experience in a number of different capacities. Most recently, Andrea served as Managing Director and Compliance & Ethics Solutions leader at PricewaterhouseCoopers LLP (PwC). She has provided governance, risk, and compliance consulting services to leading organizations since 2004.

Andrea services clients on a cross-sector basis, regularly assisting in the design, development, implementation, and assessment of corporate compliance and ethics programs, including: Codes of Conduct; training and awareness; program and corporate governance; policies and procedures; risk culture initiatives; risk assessments; conflicts of interest, gifts, and entertainment disclosure and approval processes; investigation protocols; and reporting best practices.

Prior to joining Rethink, Andrea spent over five years at PwC, where she led the firm's Compliance & Ethics consulting practice. Before that, she devoted nine years to a leading provider of ethics and compliance products, services, and solutions, where she last served as Chief Ethics Officer and Senior Vice President – Client Services. Andrea also practiced law for nine years at Fleet Bank (now Bank of America) and Day, Berry & Howard LLP (now DayPitney LLP), where she was joint author of the firm's Diversity Policy and Report. While at the bank, she supported the Capital Markets business and was a member of the Law Department's Risk Management Committee.

Education and Certifications

- Certified Compliance & Ethics Professional (CCEP)
- Admitted to practice law in Massachusetts and Connecticut
- J.D., Boston University School of Law
- B.A., Bucknell University

Memberships, Media, and Selected Thought Leadership

- Member of the Society of Corporate Compliance and Ethics (SCCE)
- Frequent speaker at industry conferences and events, including the SCCE's Annual Compliance & Ethics Institute and the Ethics & Compliance Initiative's Annual Conference
- Featured on *Compliance Podcast Network* and *Great Women in Compliance* podcasts
- Co-author of Rethink's inaugural benchmarking study and PwC's preeminent *State of Compliance* studies and associated *Energy & Utilities* industry briefs
- Co-author of *Raising Your Ethical Culture – How a whistleblower program can help; Governance, Risk and Compliance (GRC) technology: Enabling the three lines of defense;* and *Fortified for success: Building your company's risk, controls and compliance ecosystems for the IPO and beyond* whitepapers and *The surprising truth about the C-suite star of 2025* article for *PwC's Resilience: A journal of strategy and risk*
- Published in *Directors and Boards, Compliance Week, Compliance & Ethics Magazine,* and *Compliance & Ethics Professional*
- Quoted in several *Risk Assistance Network + Exchange Advisory Bulletins, The FCPA Report, Big4.com, Industry Today, Compliance Intelligence/Compliance Reporter, GARP.org (Global Association of Risk Professionals), Compliance Week, FierceCFO, Corporate Secretary, and Society for Human Resource Management*

Rethink Compliance

www.rethinkcompliance.com

What we will cover today

- Ethics and compliance risks in the context of Enterprise Risk Management: 15 min.
- Ethics and compliance risks: 5 min.
- Management of ethics and compliance risks: 20 min.
- Common ethics and compliance risks: 20 min.
- “Hot topics” in ethics and compliance: 15 min.
- TOTAL SESSION TIME: 75 minutes

15 minutes

ETHICS AND COMPLIANCE RISKS IN THE CONTEXT OF ENTERPRISE RISK MANAGEMENT (ERM)

ERM … in a nutshell

Types of Enterprise Risk

1. **External Risk: risks to an organization that are unavoidable and originate outside the organization**
   - Examples: regulatory, geopolitical, cyber
2. **Strategic Risk: choices made by an organization that are intended to provide financial value**
   - Examples: entry into a new market, R&D investment, cost-cutting initiatives
3. **Operational Risk: day-to-day operations, decisions, and actions**
   - Examples: ineffective processes, poor judgment, gaps in staff expertise or knowledge

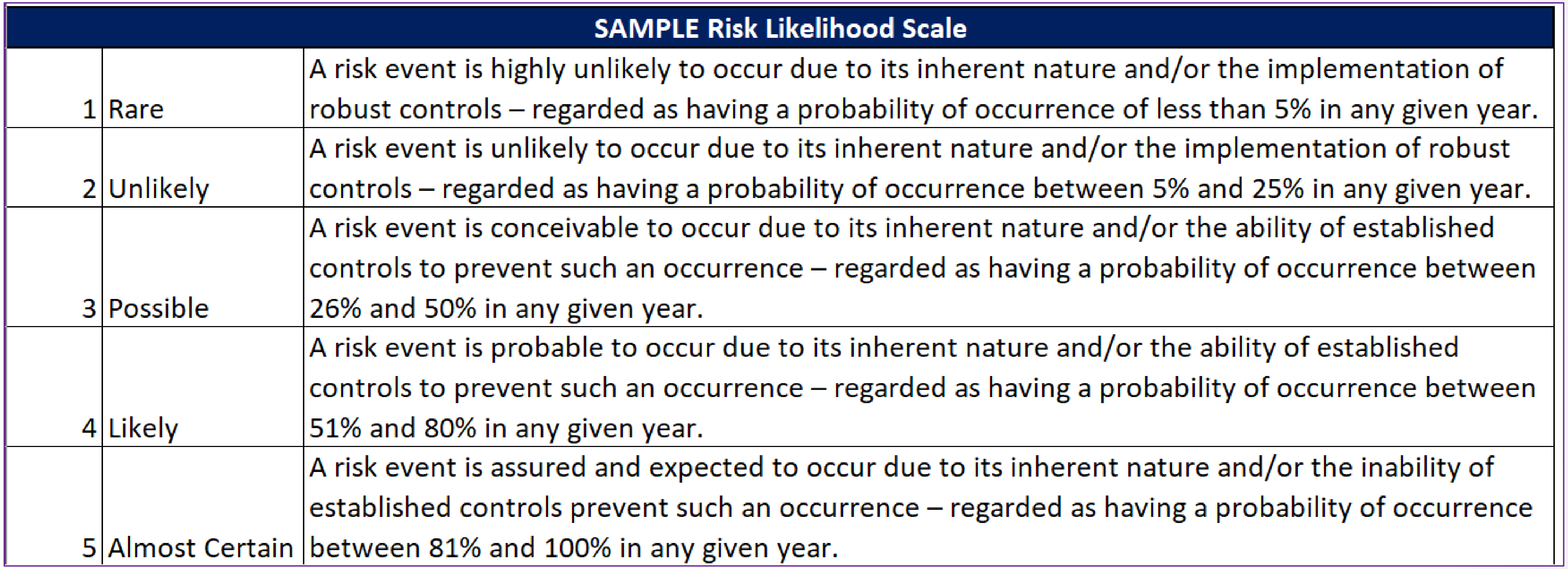
SCCE Society of Corporate Compliance and Ethics

Some important risk management terms

- **Impact:** What happens if the risk becomes a reality?
- **Likelihood:** How likely is the risk to become a reality?
- **Inherent Risk:** Considers Impact and Likelihood *before* considering controls
- **Residual Risk:** Considers Impact and Likelihood *after* applying existing controls

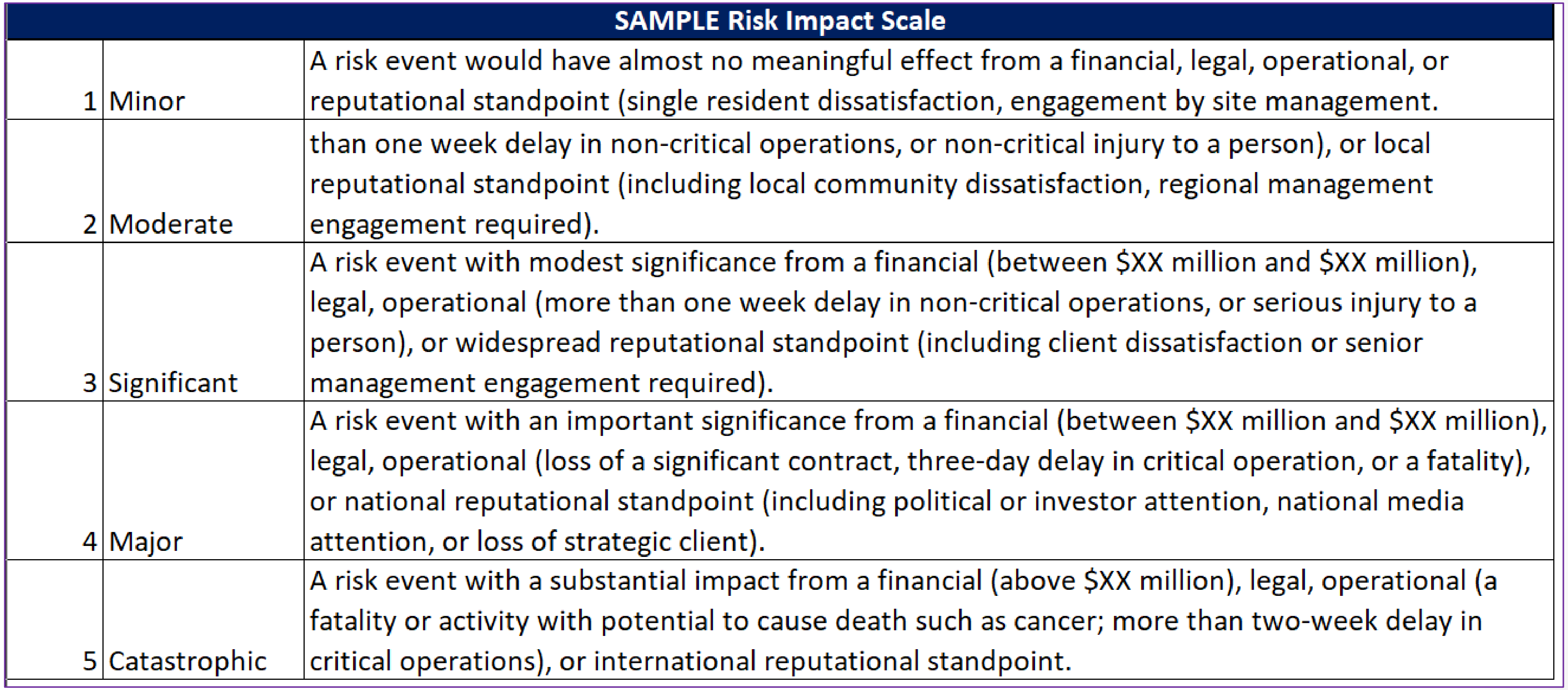
SCCE Society of Corporate Compliance and Ethics

Some samples



SAMPLE Risk Likelihood Scale		
1	Rare	A risk event is highly unlikely to occur due to its inherent nature and/or the implementation of robust controls – regarded as having a probability of occurrence of less than 5% in any given year.
2	Unlikely	A risk event is unlikely to occur due to its inherent nature and/or the implementation of robust controls – regarded as having a probability of occurrence between 5% and 25% in any given year.
3	Possible	A risk event is conceivable to occur due to its inherent nature and/or the ability of established controls to prevent such an occurrence – regarded as having a probability of occurrence between 26% and 50% in any given year.
4	Likely	A risk event is probable to occur due to its inherent nature and/or the ability of established controls to prevent such an occurrence – regarded as having a probability of occurrence between 51% and 80% in any given year.
5	Almost Certain	A risk event is assured and expected to occur due to its inherent nature and/or the inability of established controls prevent such an occurrence – regarded as having a probability of occurrence between 81% and 100% in any given year.

Some samples (cont.)



SAMPLE Risk Impact Scale		
1	Minor	A risk event would have almost no meaningful effect from a financial, legal, operational, or reputational standpoint (single resident dissatisfaction, engagement by site management.
2	Moderate	than one week delay in non-critical operations, or non-critical injury to a person), or local reputational standpoint (including local community dissatisfaction, regional management engagement required).
3	Significant	A risk event with modest significance from a financial (between $XX million and $XX million), legal, operational (more than one week delay in non-critical operations, or serious injury to a person), or widespread reputational standpoint (including client dissatisfaction or senior management engagement required).
4	Major	A risk event with an important significance from a financial (between $XX million and $XX million), legal, operational (loss of a significant contract, three-day delay in critical operation, or a fatality), or national reputational standpoint (including political or investor attention, national media attention, or loss of strategic client).
5	Catastrophic	A risk event with a substantial impact from a financial (above $XX million), legal, operational (a fatality or activity with potential to cause death such as cancer; more than two-week delay in critical operations), or international reputational standpoint.

How our risks fit into the ERM construct

Alas …

it’s difficult

"Depressed musician vintage drawing" by The British Library is marked with CC0 1.0 🅭🄍.

Polling question #1

Q: At my organization, compliance and ethics risks are assessed:

a: Only during the ERM risk assessment process

b: In a stand-alone risk assessment process

c: Not at all

d: I don't know.

SCCE Society of Corporate Compliance and Ethics

Separation anxiety?

ERM

C&E

5 minutes

ETHICS AND COMPLIANCE RISKS

SCCE
Society of Corporate
Compliance and Ethics

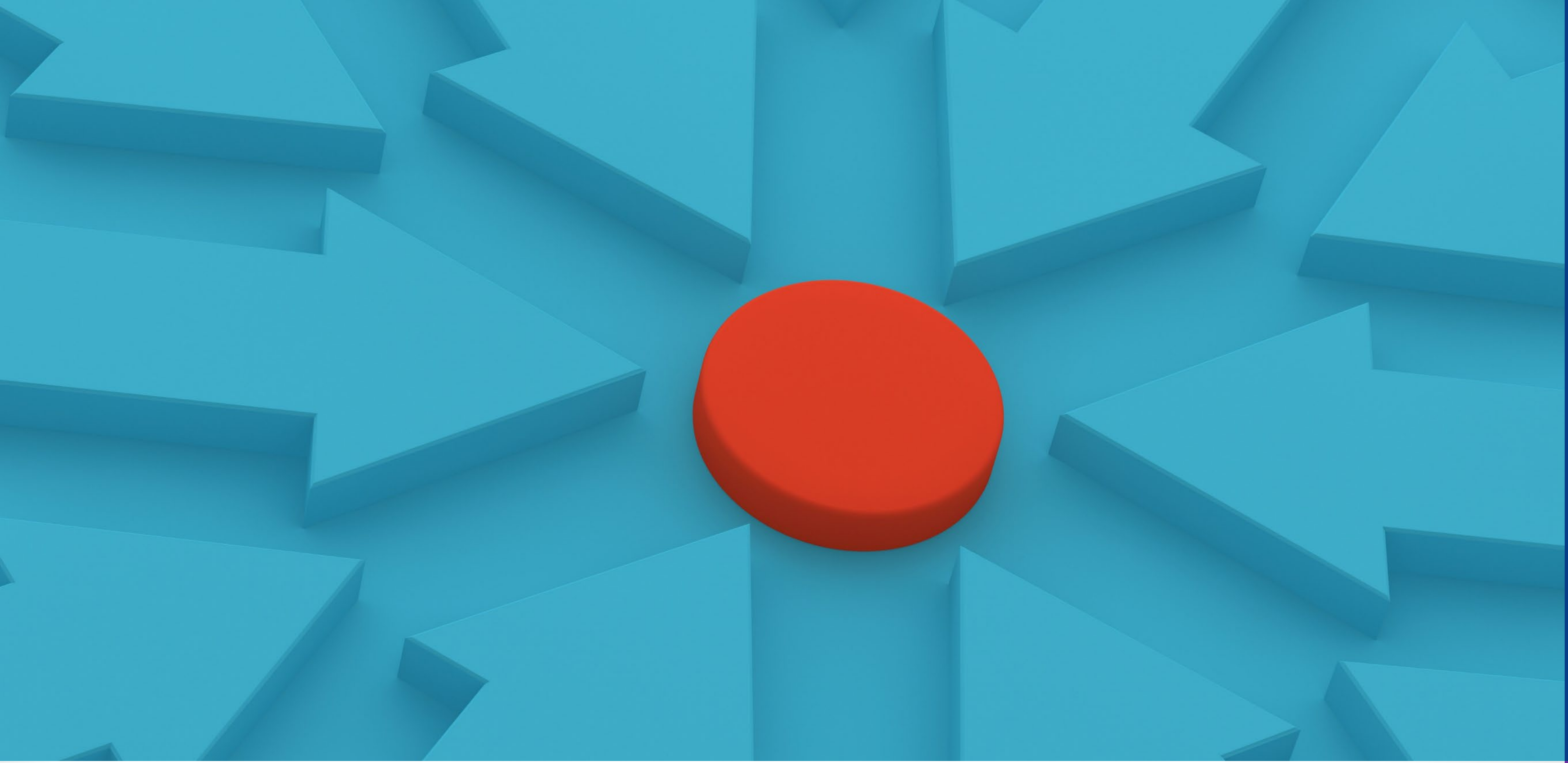
It Starts With an Ethical Mindset

Serving as a true partner to our clients means always acting with integrity.

Table of Contents

- Leadership message 2
- Introduction 3
  - The Rethink Compliance Values
  - It Starts With an Ethical Mindset
  - Why Do We Have a Code?
  - Who Has to Follow the Code?
  - What Happens If I Do Something Prohibited By the Code?
  - Raising Concerns
- When we earn trust, we build successful and lasting relationships. 5
  - Confidential Information
  - Personal Information
  - Cyber Security
  - Company Assets
  - Intellectual Property
- When we communicate thoughtfully and transparently, we demonstrate who we are as a company. 9
  - Business Records
  - Financial Integrity
  - Careful Communication
  - Social Media
- When we show respect, we encourage everyone to contribute their best. 12
  - Inclusivity
  - Respectful Workplace
- When we treat others with fairness, we succeed on the merits of our business. 15
  - Fair Competition
  - Gifts and Entertainment
  - Conflicts of Interest
  - Insider Trading
- When we are thoughtful in our actions, we create a stronger community. 19
  - Political Activities
  - Our Surroundings
  - The Compliance and Ethics Community
- When we speak up, we create a stronger company. 22
  - Questions and Concerns

Industry-specific risks



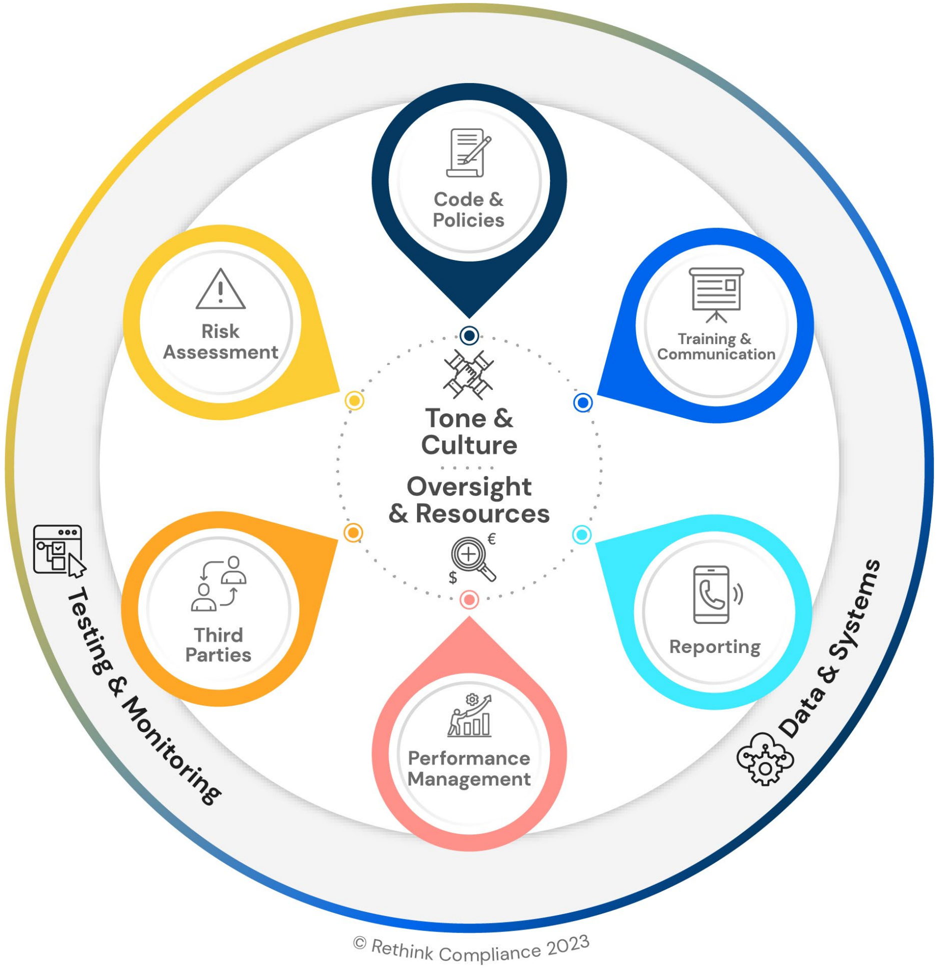
Our focus today

20 minutes

MANAGEMENT OF ETHICS & COMPLIANCE RISKS

Risk-management frameworks

Using a risk-management framework



For example, Rethink's compliance & ethics risk-management framework incorporates criteria from (among other resources):

- The Elements of an Effective Compliance Program set forth in the U.S. Federal Sentencing Guidelines for Organizations
- The U.S. Department of Justice's March 2023 Updated Guidance Document regarding its Evaluation of Corporate Compliance Programs
- The U.S. Department of Health & Human Services Office of Inspector General's November 2023 Seven Fundamental Elements of an Effective Compliance Program
- Compliance Risk Management: Applying the COSO ERM Framework (2020)

Polling question #2

Q: Do you use a risk management framework at your organization?

a: Yes, we utilize a framework we developed.

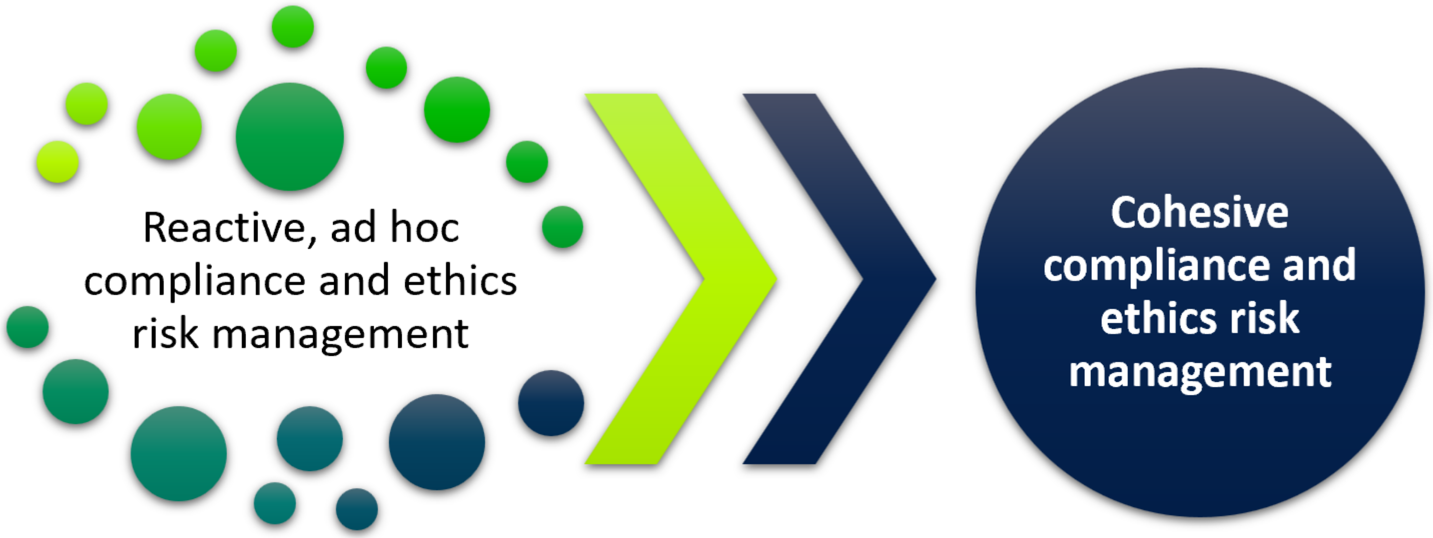
b: Yes, we utilize a framework developed by a third party.

c: No

d: I don’t know.

SCCE Society of Corporate Compliance and Ethics

Goal of using a consistent framework



Reactive, ad hoc compliance and ethics risk management
Cohesive compliance and ethics risk management

Inconsistency

No clarity or coordination

Gaps AND overlaps

Business fatigue

Increasing costs

Enhanced brand value

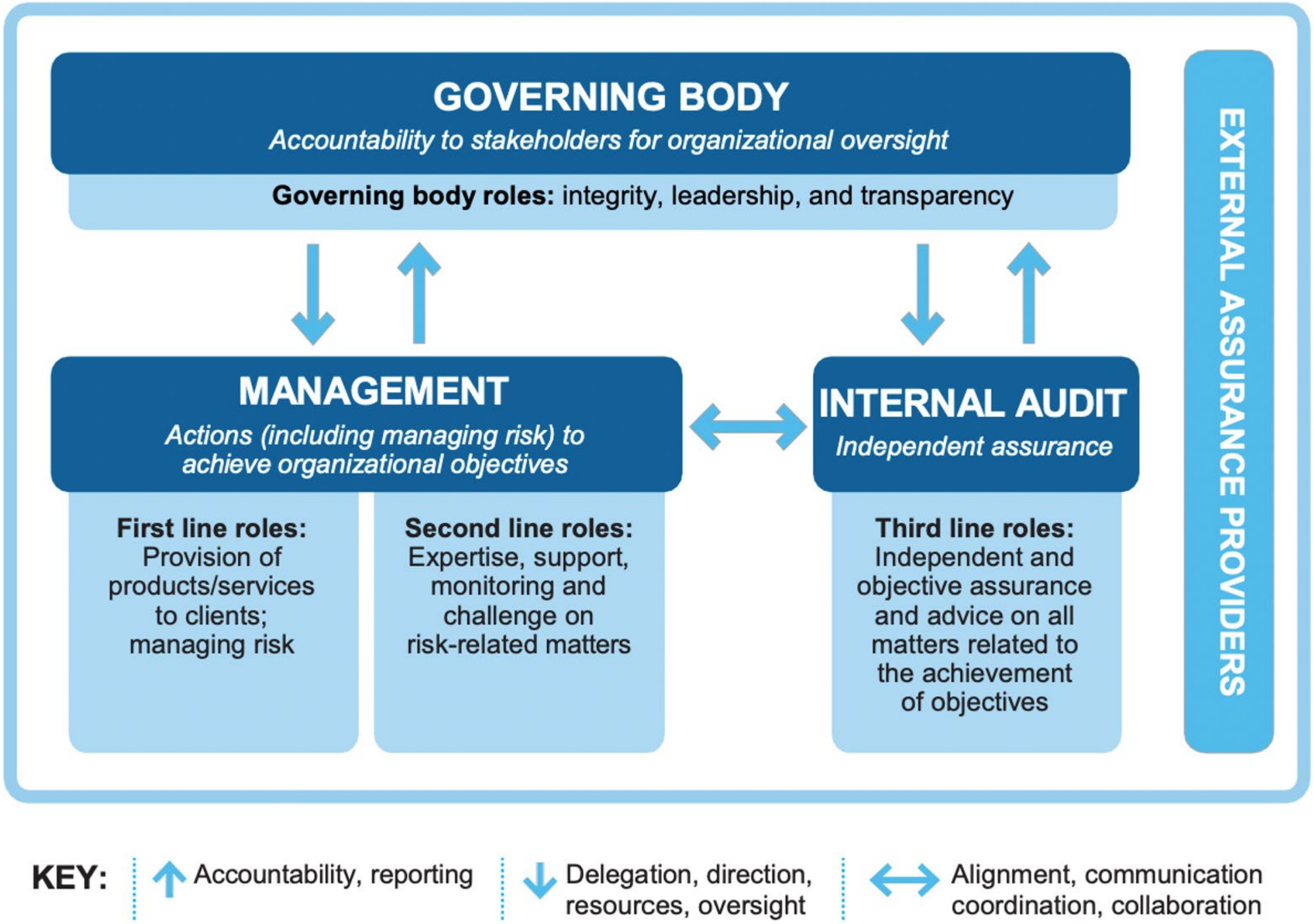
Reputation protection

Proactive risk management

Enhanced risk oversight

Increased risk agility

The IIA’s Three Lines Model



GOVERNING BODY

Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT

Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT

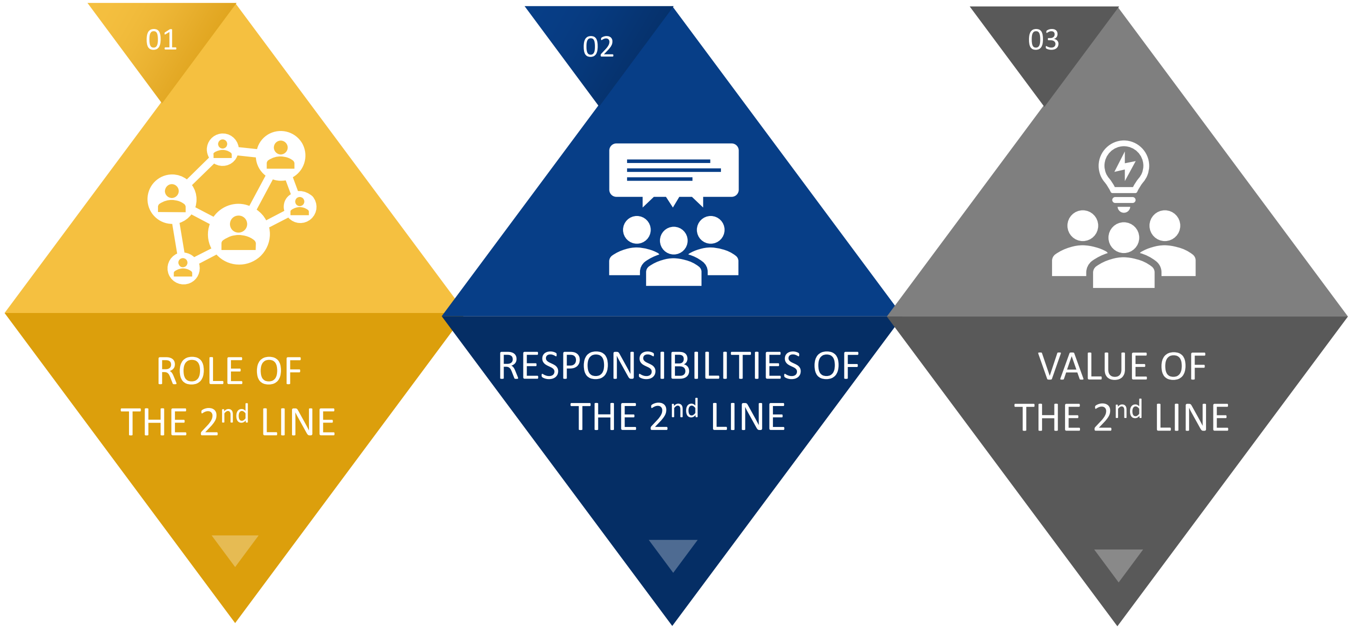
Independent assurance

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY: ↑ Accountability, reporting | ↓ Delegation, direction, resources, oversight | ↔ Alignment, communication coordination, collaboration

The second line



01

ROLE OF THE 2nd LINE

02

RESPONSIBILITIES OF THE 2nd LINE

03

VALUE OF THE 2nd LINE

- ✓ Independent operational risk and compliance functions
- ✓ Enables business performance
- ✓ Fosters collaboration among the various 2nd line functions and activities

- ✓ Provides integrated and consistent risk reporting
- ✓ Uses common risk taxonomy & integrated risk framework
- ✓ Coordinates with third line

- ✓ Identification and remediation of risk management gaps and overlap
- ✓ Leading to enhanced business performance

Controls mapping

20 minutes

COMMON ETHICS & COMPLIANCE RISKS

SCCE Society of Corporate Compliance and Ethics

Common compliance and ethics risks

Topic/Risk: Bribery and Corruption	
High-Level Overview	The act of an organization’s employee – or a third party operating on the organization’s behalf – offering, promising, providing, or receiving anything of value to or from a commercial business partner or government official for the purposes of gaining or maintaining an unfair advantage.
Key Laws, Guidance, Frameworks, and Standards	• U.S. Foreign Corrupt Practices Act (FCPA) and new Foreign Extortion Prevention Act (FEPA) • UK Bribery Act 2010 • Brazilian Clean Company Act • U.S. Department of Justice (DOJ)/Securities and Exchange Commission (SEC) Guidance • OECD Framework • ISO 37001
Key Stakeholders	• Employees, particularly sales representatives, business development and certain operations professionals, and senior leadership • Any third party acting on the organization’s behalf (e.g., customs brokers, freight forwarders, consultants, distributors, etc.) • Enforcement agencies (e.g., U.S. DOJ and SEC) • Shareholders • Non-governmental organizations (NGOs)
Risk Trends, Cautionary Tales, and Lessons Learned	• Bribery and corruption continues to be a top priority for U.S. DOJ/SEC, and prosecutors’ powers to charge foreign public officials is expanded with the new FEPA. • Corporate compliance program guidance has become more detailed and is largely grounded in the FCPA and the management of bribery and corruption risk. • U.S. DOJ has provided more transparency as to its enforcement decisions.

SCCE
Society of Corporate Compliance and Ethics

Common compliance and ethics risks (cont.)

Topic/Risk: Data Privacy and Security, Including Cybersecurity	
High-Level Overview	The risk that confidential or sensitive organizational information (e.g., employee information, customer information, trade secrets, etc.) can be intentionally or inadvertently accessed or provided to a non-authorized third party. Risk is both internal and external.
Key Laws, Guidance, Frameworks, and Standards	• U.S. Health Insurance Portability and Accountability Act (HIPAA) • U.S. Gramm-Leach-Bliley Act • U.S. Homeland Security Act • U.S. Federal Information Security Management Act (FISMA) • Directive on Security of Network and Information Systems (NIS Directive) • EU Cybersecurity Act • EU General Data Protection Regulation (GDPR) • ISO / IEC 27001, 27002 • U.S. National Institute of Standards and Technology (NIST) • Various other international and U.S. federal and state laws
Key Stakeholders	• All employees and third parties operating on behalf of an organization • Enforcement agencies (e.g., European Union Agency for Cybersecurity (ENISA)) • Customers, suppliers, and other business partners • Shareholders • NGOs
Risk Trends, Cautionary Tales, and Lessons Learned	• Over the last few years, many new cybersecurity regulations have been enacted at various levels of government. • These regulations have caused a proliferation of Data Protection Agreements (DPAs), including in instances where they are really not necessary. • Organizations continue to report cyber and data breaches, including (among many others) Toyota Financial Services, VF, Xfinity, Panasonic Aviation, and EasyPark in December of 2023 alone. • Cyber criminals keep at it, constantly developing new ways of accessing systems and data.

Common compliance and ethics risks (cont.)

Topic/Risk: Conflicts of interest (COI)	
High-Level Overview	A perceived or actual COI may arise when employees' personal interests interfere with their professional objectivity, responsibility, or duty to their employer. Many *potential* examples exist, including: • Hiring or supervising a family member • Working simultaneously for a competitor • Outside employment • Investing in a competitor • Romantic relationships in the line of management • Providing or accepting gifts, entertainment, or hospitality from a business partner • Excessive use of company property or assets for personal benefit • Taking corporate opportunities for personal gain
Key Laws, Guidance, Frameworks, and Standards	While there are no over-arching COI laws that cover all examples across all industries and professions, a wide variety of federal and state laws and regulations strive to prevent COIs in a myriad of industries and settings (e.g., physicians, attorneys, bankers, government officials, etc.).
Key Stakeholders	• All employees • Enforcement agencies • Customers, suppliers, and other business partners • Boards of Directors • Shareholders
Risk Trends, Cautionary Tales, and Lessons Learned	• COIs continue to be a key risk area for organizations across industries, with organizations going to greater lengths to contextualize how COIs may arise in the workplace – and to training employees regarding these contexts. • Often, a COI can be *managed* rather than eliminated. • COIs can be very difficult to recognize "in the moment" and, realistically, require independent identification.

Common compliance and ethics risks (cont.)

Topic/Risk: Fair Competition	
High-Level Overview	Competition and antitrust laws promote fair competition in the marketplace, prohibiting practices that restrain trade or free competition, including price fixing, market allocation, bid rigging, cartels, and abuse of dominant position.
Key Laws, Guidance, Frameworks, and Standards	• U.S. Sherman Antitrust Act • U.S. Federal Trade Commission Act • U.S. Clayton Act • U.S. Robinson-Patman Act • U.S. Hart-Scott-Rodino Antitrust Improvements Act • International competition laws • OECD Competition Law Guidance • U.S. DOJ Antitrust Guidelines
Key Stakeholders	• Employees, particularly in sales, marketing, and HR • Competitors • Customers and suppliers • Consumers generally • Enforcement agencies (*e.g.,* U.S. DOJ and Federal Trade Commission)
Risk Trends, Cautionary Tales, and Lessons Learned	• New regulatory focus on non-compete agreements puts the spotlight on hiring practices in the U.S. • Competition risk is both horizonal (among competitors) and vertical (involving companies and their suppliers/dealers). • Regulatory authorities have been known to monitor trade shows and industry conferences, looking for pricing discussions or other evidence of anti-competitive behavior. • Often, regulators will focus on a particular industry (*e.g.,* tech, healthcare, pharma) for investigation and enforcement – and they remain active.

Common compliance and ethics risks (cont.)

Topic/Risk: Trade Compliance	
High-Level Overview	Trade compliance covers both import and export transactions. Organizations must follow applicable international import and tariff laws and regulations as well as export and sanctions laws and regulations. Export controls help promote a safer, more secure world by controlling the transfer of certain products, technical data, and other information to particular people, groups, and destinations. Sanctions restrict trade with certain countries, entities, or individuals that pose a threat to national security. The U.S., UK, EU, and other jurisdictions use sanctions as a foreign policy tool, imposing economic pressure to influence unfavorable policy decisions or otherwise change behavior. In the U.S., there also are strict anti-boycott laws that prohibit companies from complying with aspects of *other countries'* sanctions that the U.S. does not support.
Key Laws, Guidance, Frameworks, and Standards	• U.S. Export Administration Regulation (EAR) • U.S. International Traffic in Arms Regulations (ITAR) • U.S. Department of Commerce's Bureau of Industry and Security (BIS) List • U.S. Specially Designated Nationals (SDN) and Blocked Persons List • U.S. Harmonized Tariff Schedule • International trade laws, rules, and regulations
Key Stakeholders	• Employees involved in the importing and exporting of products, services, and information • Customers, suppliers, and other business partners • Enforcement agencies (*e.g.,* Office of Foreign Assets Control (OFAC) of U.S. Treasury Department, U.S. Department of State, Office of Trade of U.S. Customs and Border Control, International Trade Administration) • Foreign governments
Risk Trends, Cautionary Tales, and Lessons Learned	• Trade compliance is a technical, complicated, and ever-evolving area, impacted by the geopolitical environment (*e.g.,* Russia's invasion of Ukraine, U.S. arms sales to Taiwan). • We are seeing an increased enforcement focus in this area. • Often, companies maintain stand-alone trade compliance programs due to the technical, regulatory nature of this risk area.

Common compliance and ethics risks (cont.)

Topic/Risk: Whistleblower Protection	
High-Level Overview	There are many, many laws protecting whistleblowers – in the U.S. and abroad. In general, those laws protect whistleblowers from retaliation (*e.g.,* dismissal, demotion, suspension, intimidation) for reporting potential violations of law to external regulatory authorities. Some of the laws also set forth requirements for internal whistleblower programs.
Key Laws, Guidance, Frameworks, and Standards	• U.S. Whistleblower Protection Act • U.S. Dodd-Frank Act • U.S. False Claims Act • EU Whistleblower Protection Directive • Japan's Amended Whistleblower Protection Act • Other U.S. Federal, state, and local laws and regulations • Other international laws and regulations
Key Stakeholders	• All employees, customers, suppliers, and other third-party business partners • Boards of Directors • Regulators and enforcement agencies (*e.g.,* U.S. SEC, U.S. FTC, U.S. Occupational Safety and Health Commission, U.S. Department of Labor, U.S. Office of Federal Contract Compliance Programs, U.S. Department of Homeland Security, U.S. Commodity Futures Trading Commission)
Risk Trends, Cautionary Tales, and Lessons Learned	• Monetary rewards for successful prosecutions directly resulting from a whistleblower's report incentivize external – rather than internal – reporting. • Investigations and case management protocols – including the technology to support them – are important considerations in this area.

15 minutes

“HOT TOPICS” IN ETHICS AND COMPLIANCE

Data analytics

- Regulator expectations
- Example uses in compliance programs

Artificial intelligence (AI)

- Consider how to use AI in your compliance and ethics program
- Understand how your business operations and support functions (including HR and IT) are using AI – and whether AI risk is being managed appropriately

SCCE
Society of Corporate Compliance and Ethics

Polling question #3

Q: Do you use AI in your compliance and ethics program?

a: Yes, we're ahead of the curve!

b: Not yet, but we're planning to soon.

c: No way!

d: I don't know.

Diversity, Equity & Inclusion (DEI)

Environmental, social & governance (ESG)

- What is it?
- What's the role of Compliance & Ethics?

SCCE Society of Corporate Compliance and Ethics

Ephemeral messaging

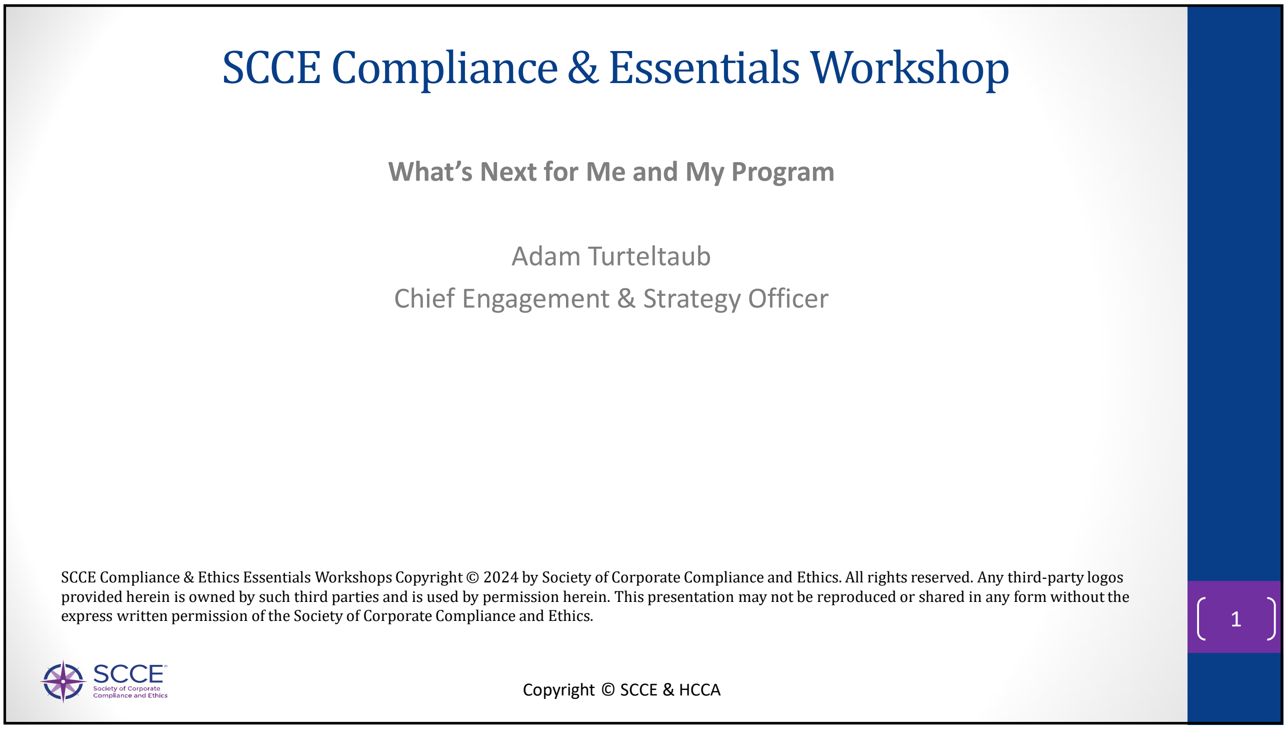
SCCE Society of Corporate Compliance and Ethics

Clawbacks

Considerations in a U.S. Election Year

- Conflicts of interest
- Respectful workplace
- Changes in enforcement priorities
- Reputational considerations in a social media world

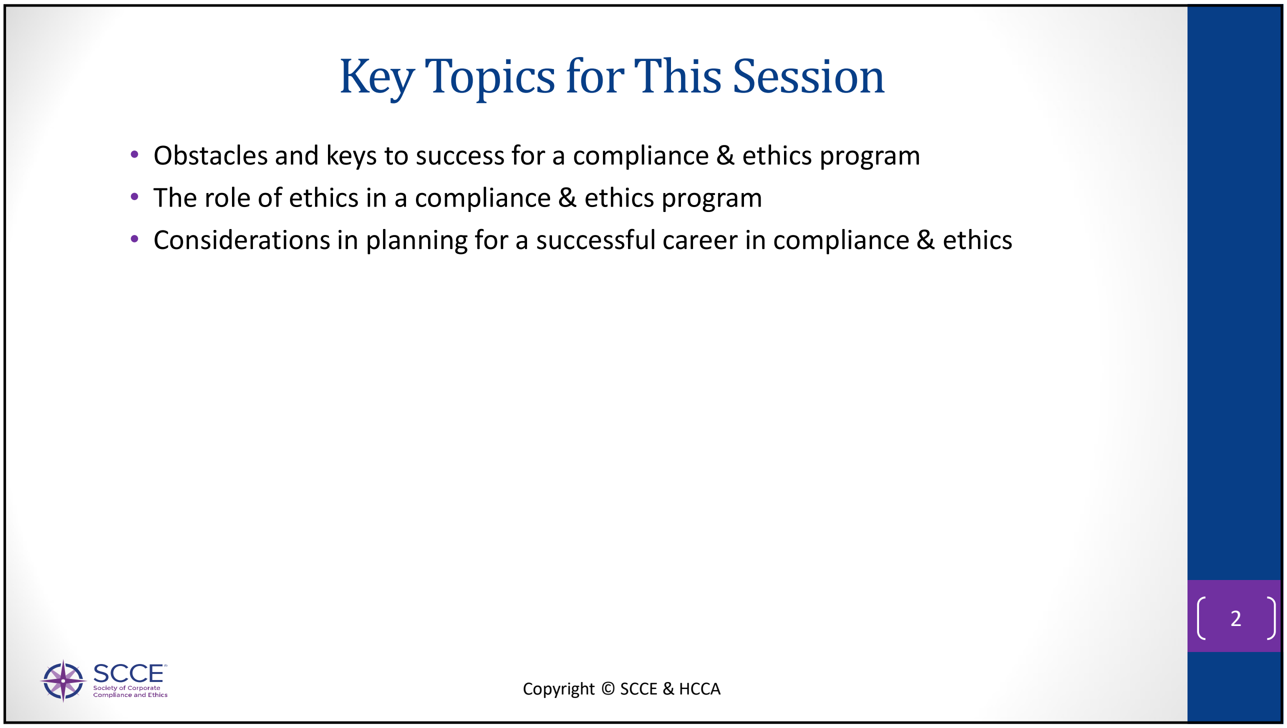
THANK YOU!



SCCE Compliance & Essentials Workshop

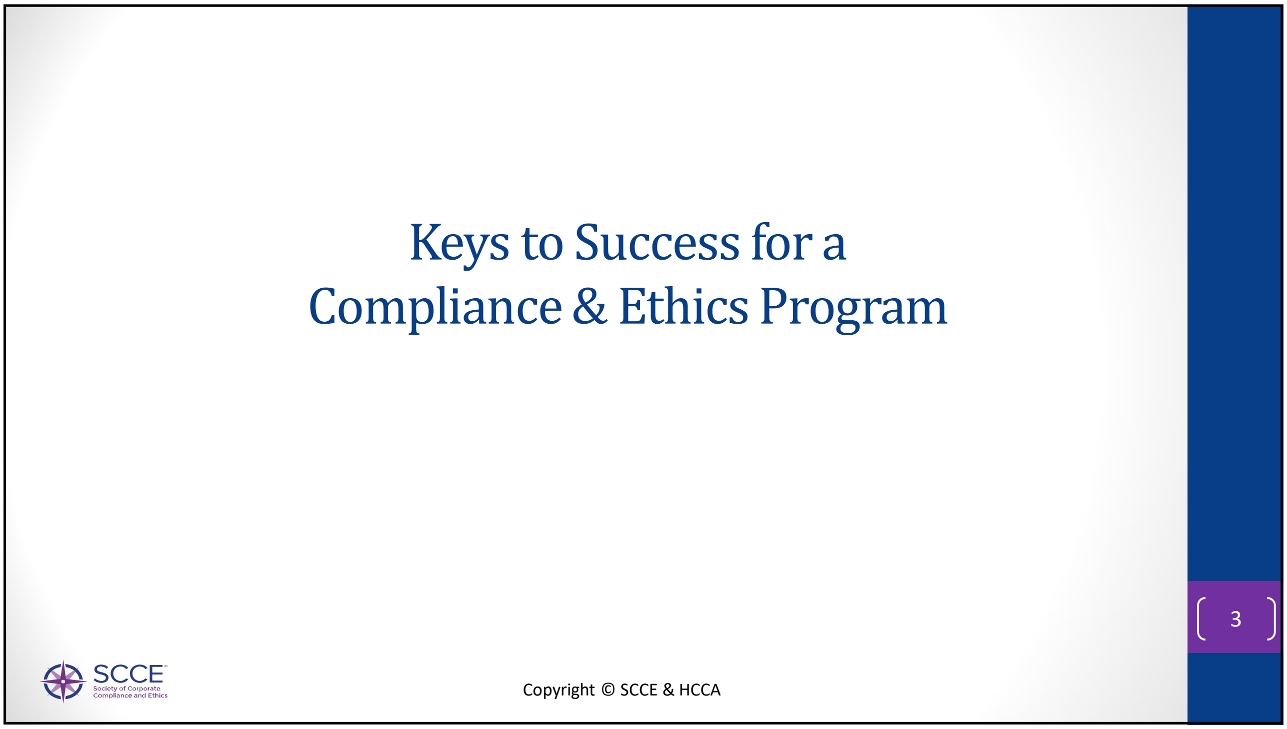
What's Next for Me and My Program

Adam Turteltaub
Chief Engagement & Strategy Officer



Key Topics for This Session

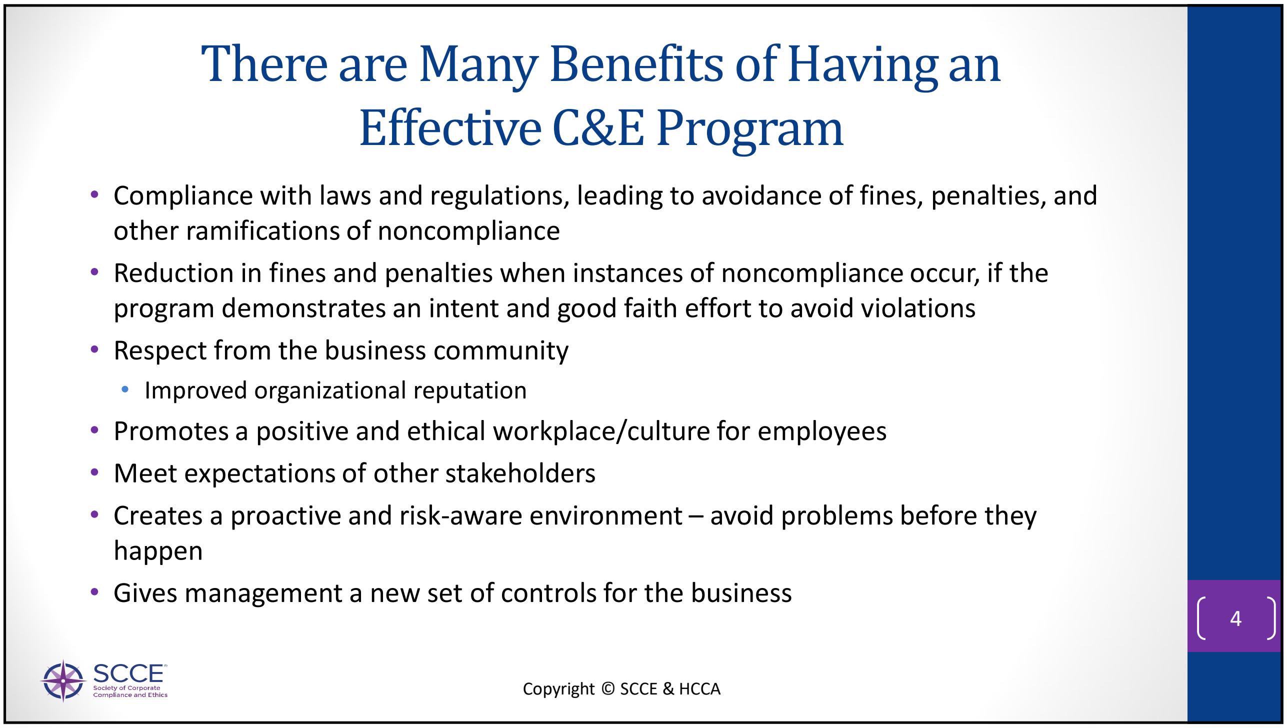
- Obstacles and keys to success for a compliance & ethics program
- The role of ethics in a compliance & ethics program
- Considerations in planning for a successful career in compliance & ethics



Keys to Success for a Compliance & Ethics Program

3

3

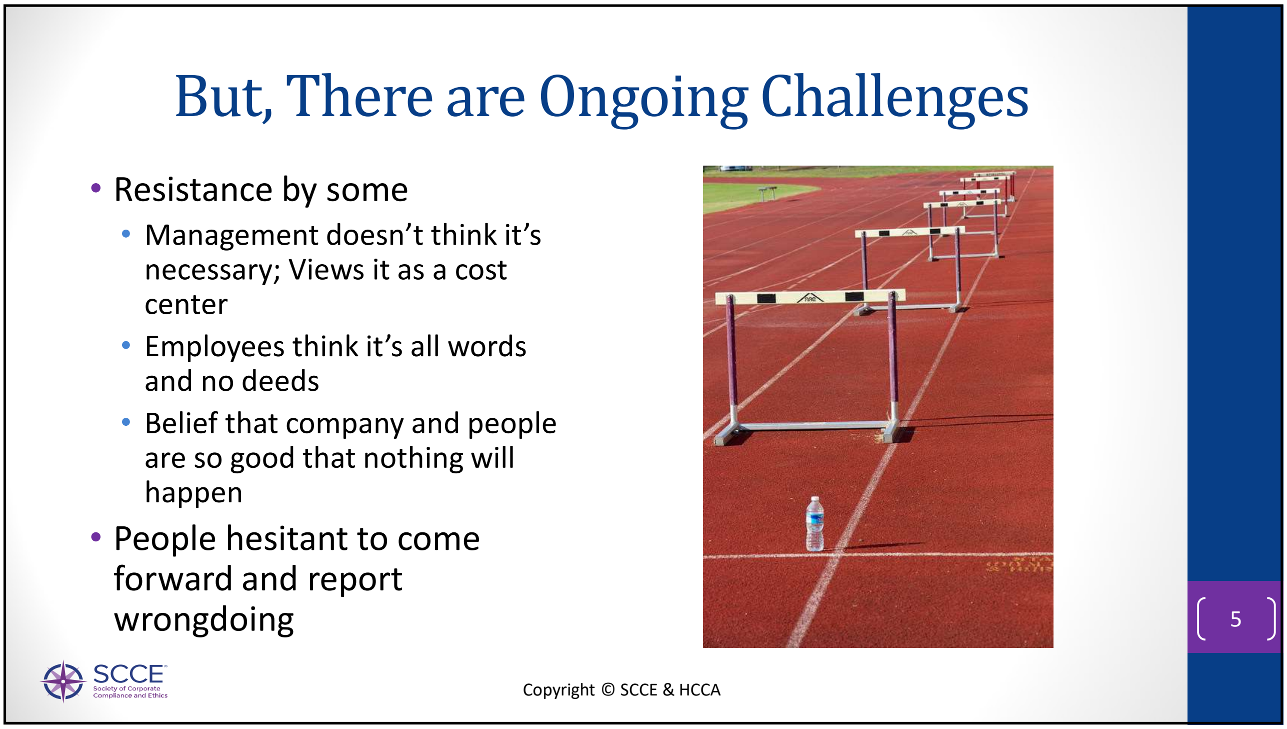


There are Many Benefits of Having an Effective C&E Program

- Compliance with laws and regulations, leading to avoidance of fines, penalties, and other ramifications of noncompliance
- Reduction in fines and penalties when instances of noncompliance occur, if the program demonstrates an intent and good faith effort to avoid violations
- Respect from the business community
  - Improved organizational reputation
- Promotes a positive and ethical workplace/culture for employees
- Meet expectations of other stakeholders
- Creates a proactive and risk-aware environment – avoid problems before they happen
- Gives management a new set of controls for the business

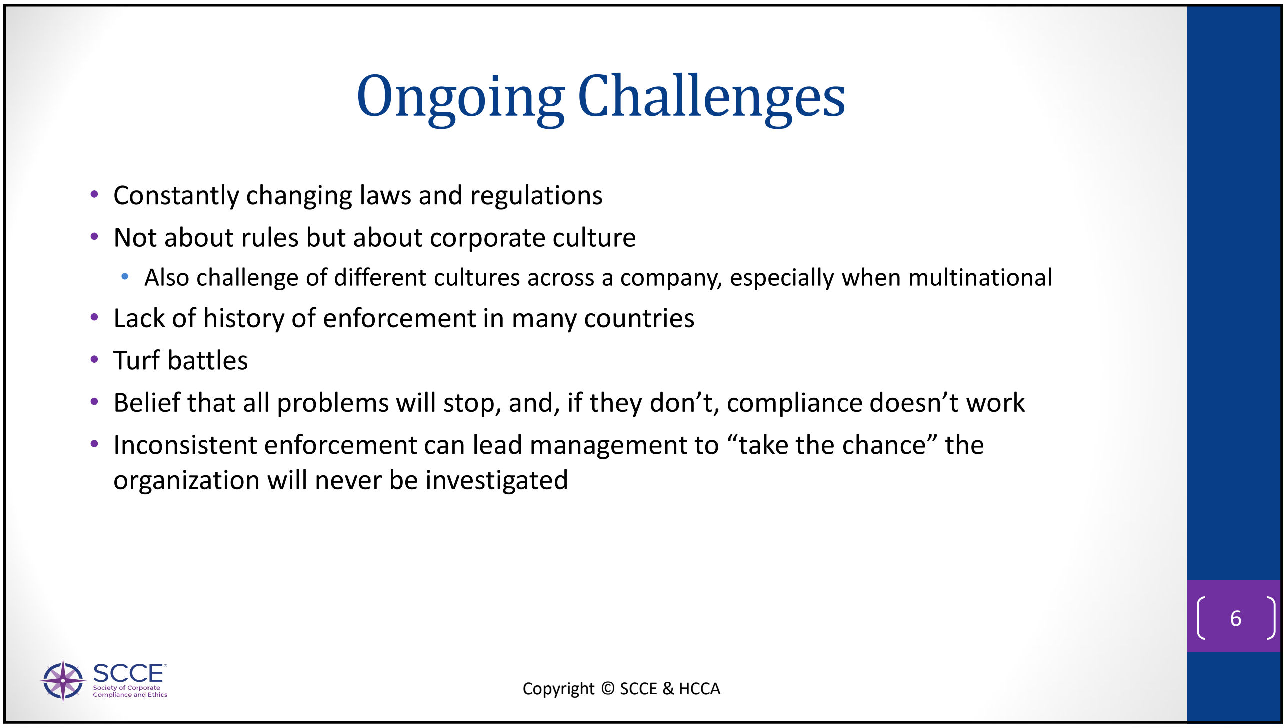
4

4



But, There are Ongoing Challenges

- Resistance by some
  - Management doesn't think it's necessary; Views it as a cost center
  - Employees think it's all words and no deeds
  - Belief that company and people are so good that nothing will happen
- People hesitant to come forward and report wrongdoing



Ongoing Challenges

- Constantly changing laws and regulations
- Not about rules but about corporate culture
  - Also challenge of different cultures across a company, especially when multinational
- Lack of history of enforcement in many countries
- Turf battles
- Belief that all problems will stop, and, if they don't, compliance doesn't work
- Inconsistent enforcement can lead management to "take the chance" the organization will never be investigated

Changing Scope of C&E Programs

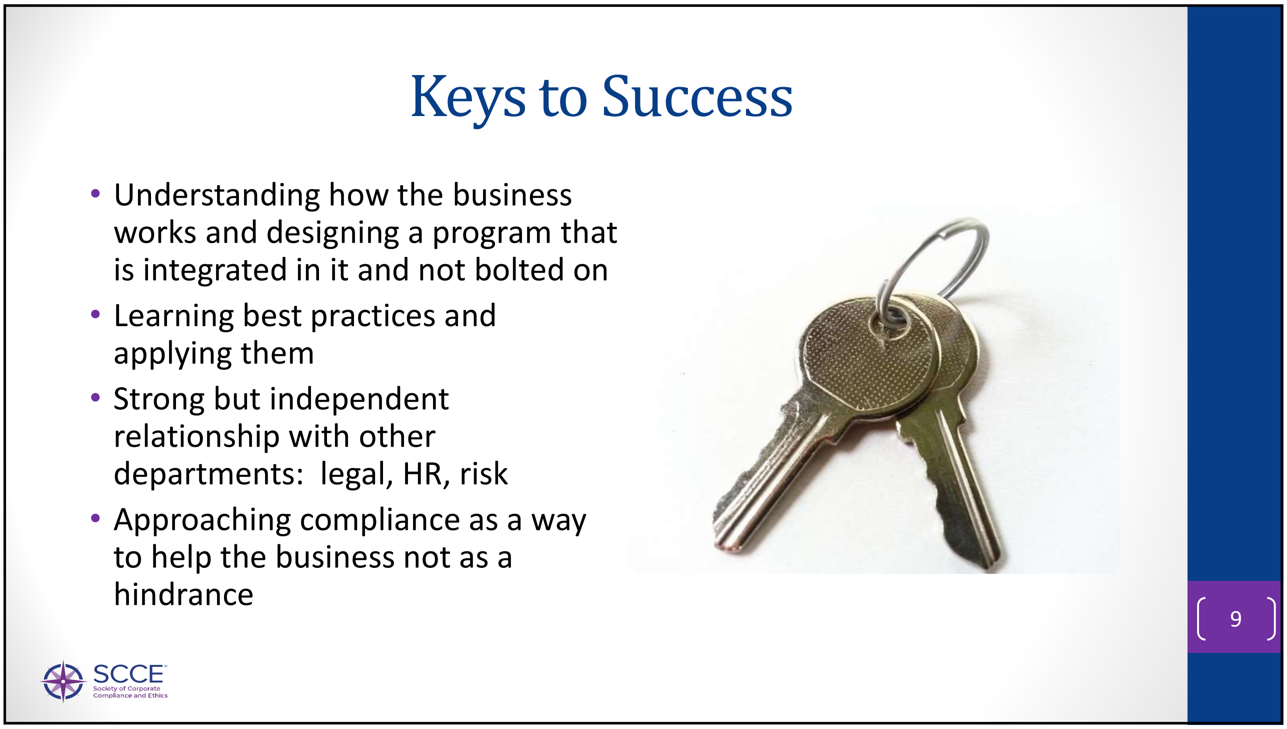
- The history of C&E programs began with bribery and corruption
- Now, C&E programs may address:
  - Antitrust
  - Contracts and agreements
  - False Claims Act
  - Tax compliance
  - Employment laws
  - Environmental
  - Conflicts of interest
  - Product/patient/student safety
  - Privacy
  - Economic sanctions
  - Many other laws and regulations

SCCE Society of Corporate Compliance and Ethics

Keys to Success

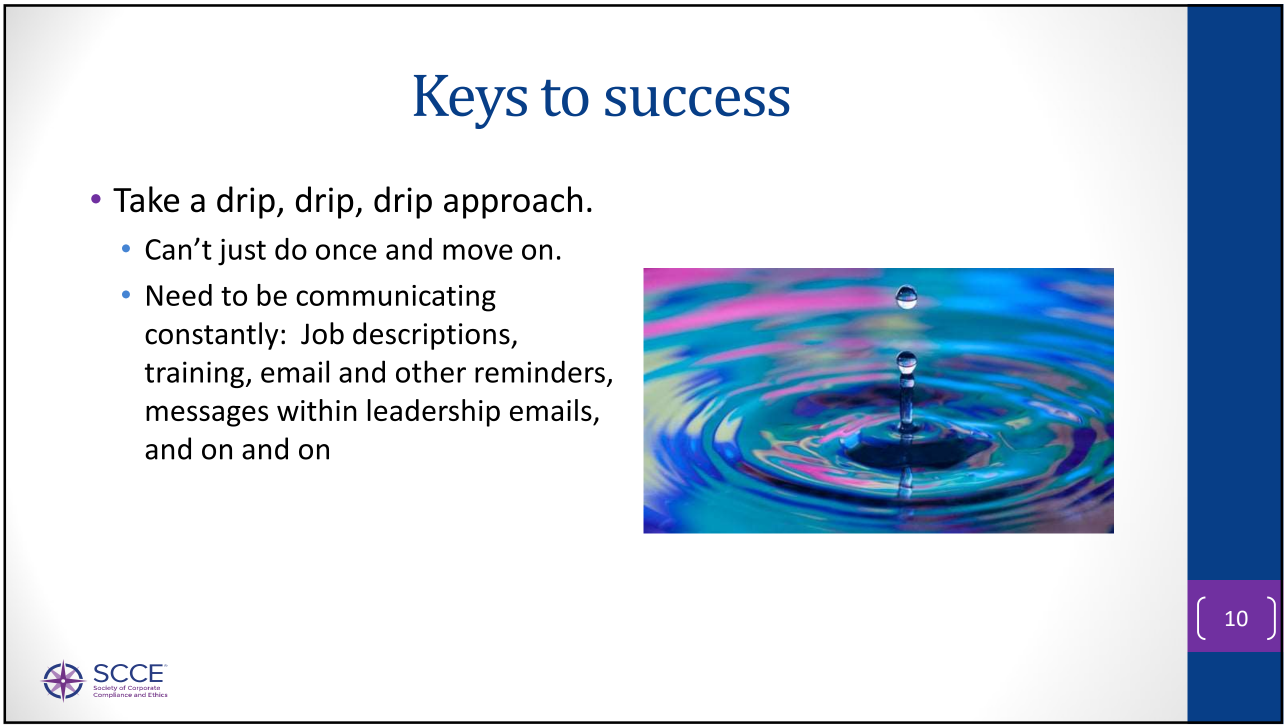
- Securing buy in from the board and direct line to it
- Strong tone at the top
- Ensuring that tone cascades to the middle
- Open lines of communication and acting on it so employees see response
- Consistent discipline
- Willingness to own problems and not hide them

SCCE Society of Corporate Compliance and Ethics



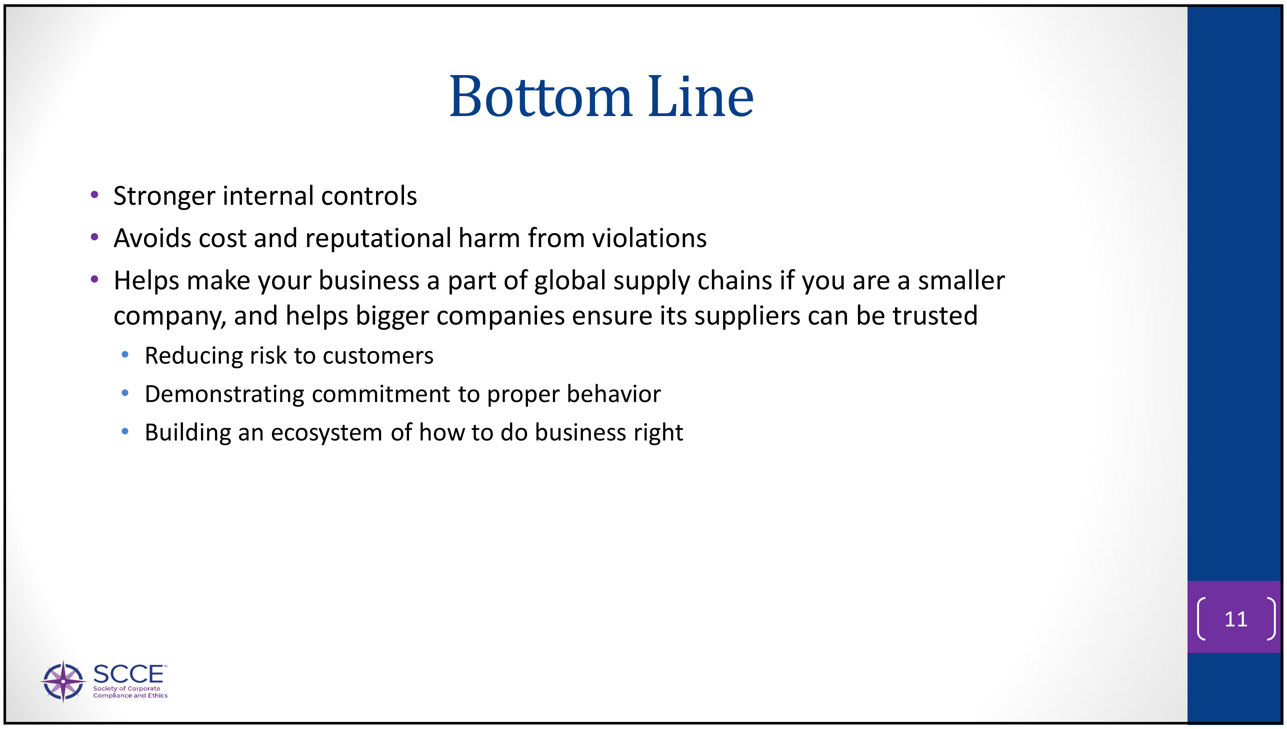
Keys to Success

- Understanding how the business works and designing a program that is integrated in it and not bolted on
- Learning best practices and applying them
- Strong but independent relationship with other departments: legal, HR, risk
- Approaching compliance as a way to help the business not as a hindrance



Keys to success

- Take a drip, drip, drip approach.
  - Can't just do once and move on.
  - Need to be communicating constantly: Job descriptions, training, email and other reminders, messages within leadership emails, and on and on

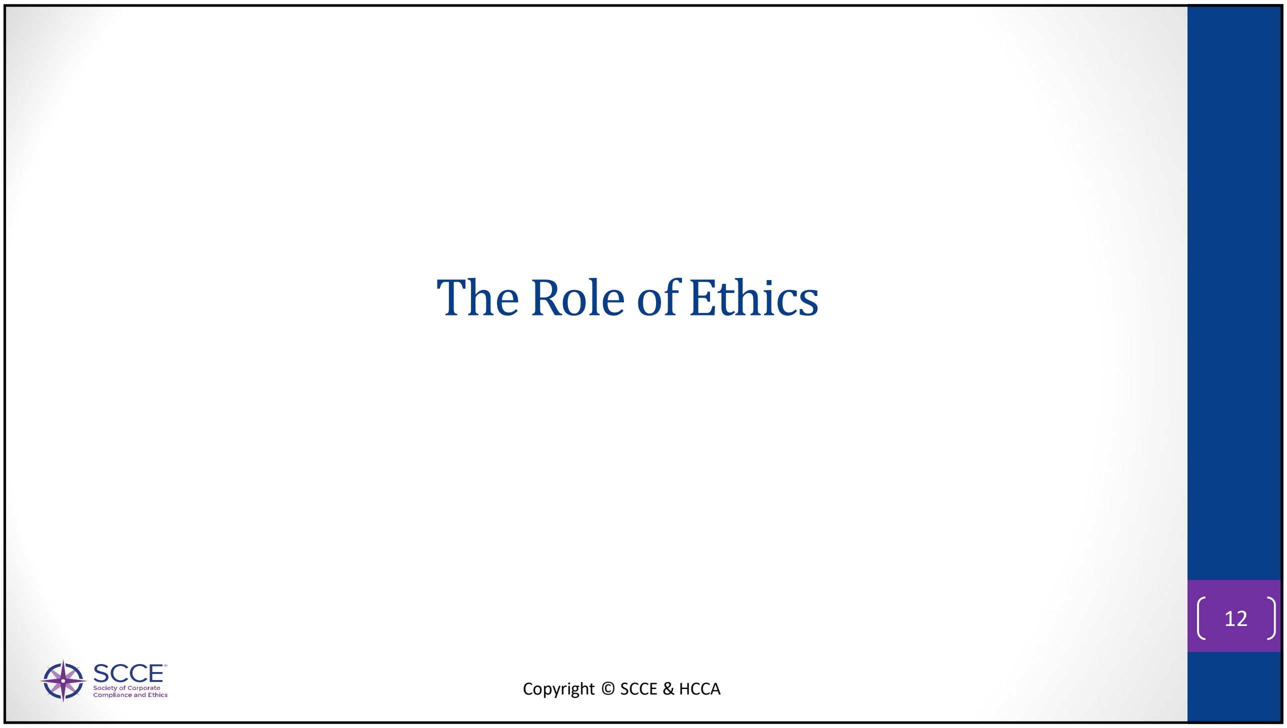


Bottom Line

- Stronger internal controls
- Avoids cost and reputational harm from violations
- Helps make your business a part of global supply chains if you are a smaller company, and helps bigger companies ensure its suppliers can be trusted
  - Reducing risk to customers
  - Demonstrating commitment to proper behavior
  - Building an ecosystem of how to do business right

11

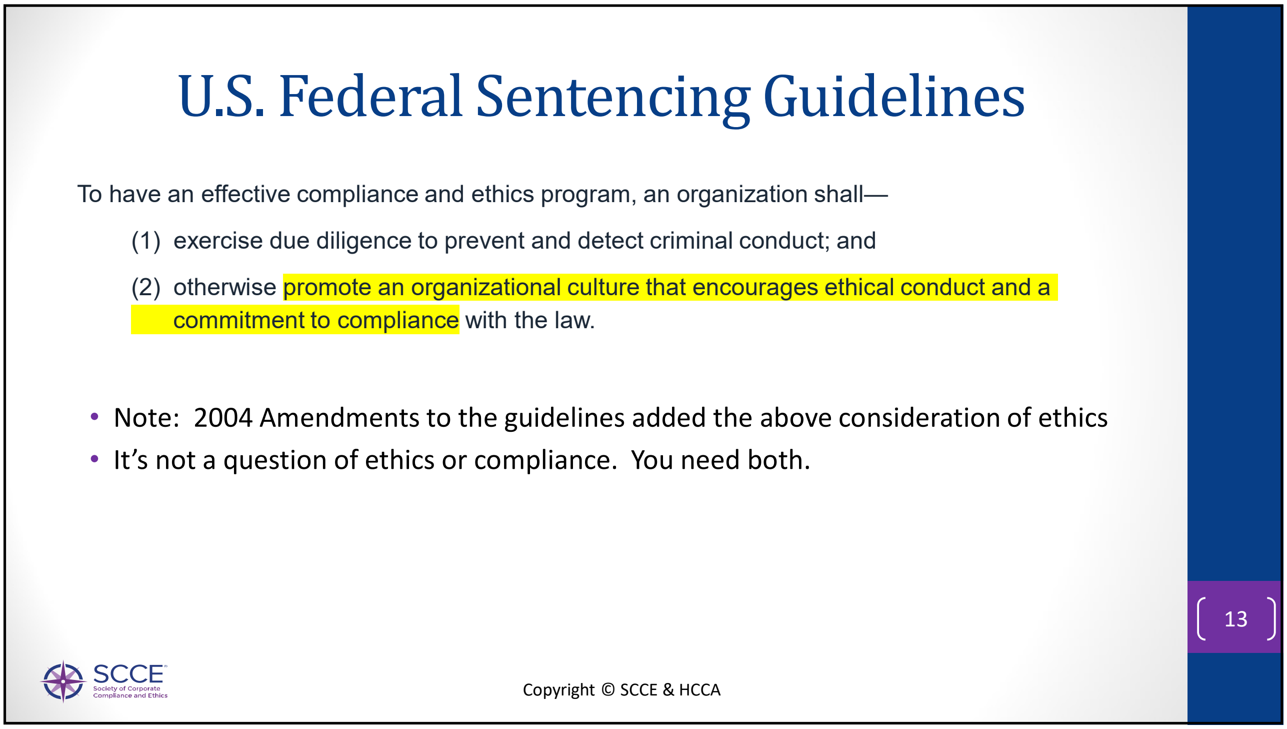
11



The Role of Ethics

12

12



U.S. Federal Sentencing Guidelines

To have an effective compliance and ethics program, an organization shall—

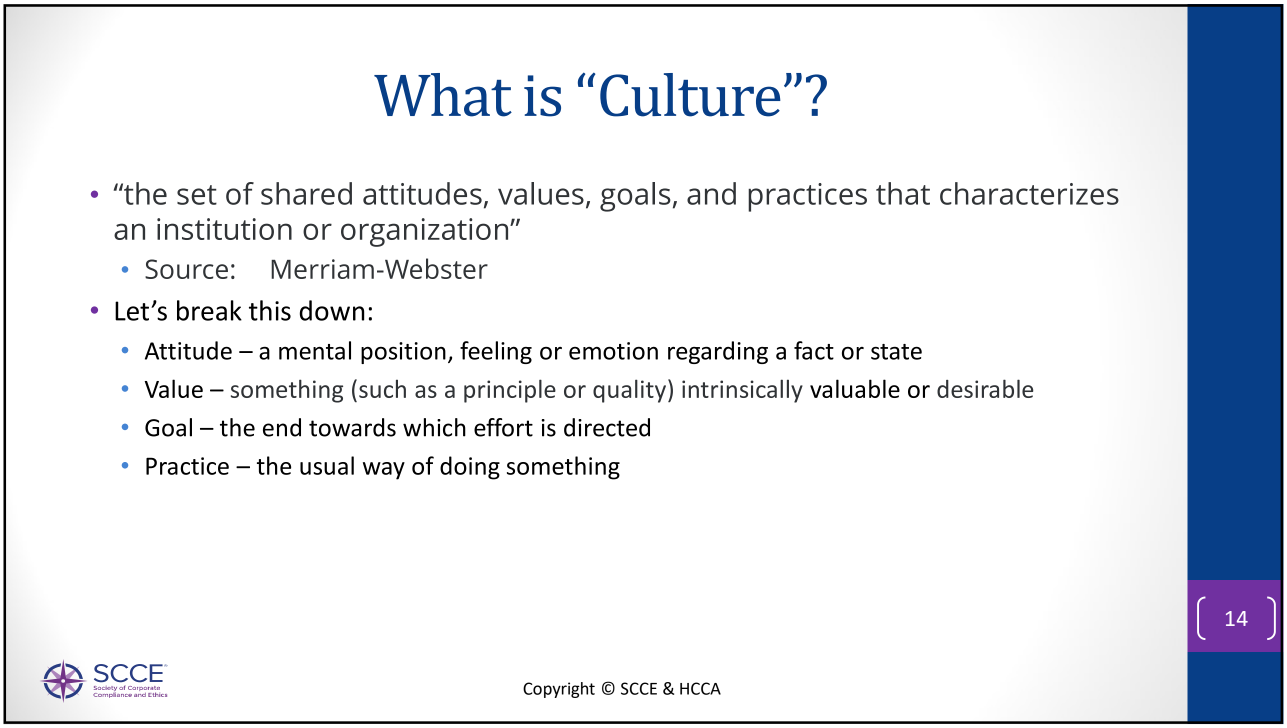
(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

- Note: 2004 Amendments to the guidelines added the above consideration of ethics
- It's not a question of ethics or compliance. You need both.

13

13

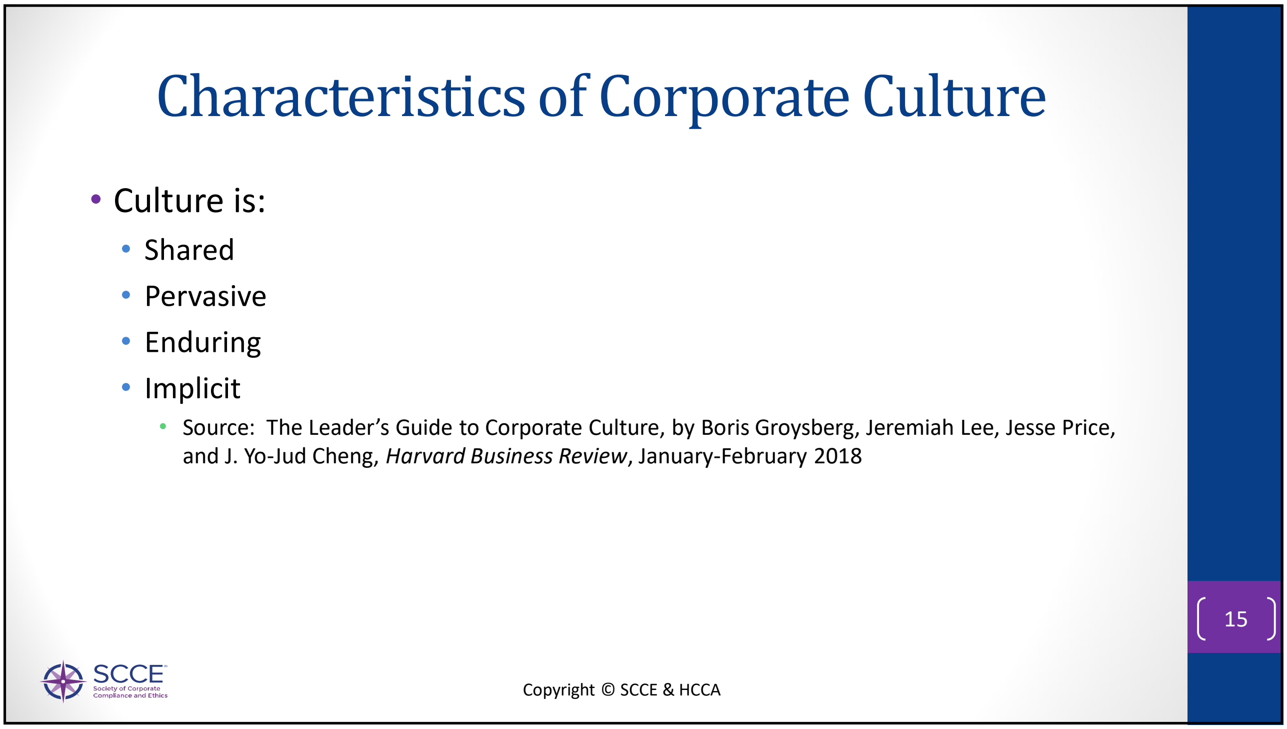


What is "Culture"?

- "the set of shared attitudes, values, goals, and practices that characterizes an institution or organization"
  - Source: Merriam-Webster
- Let's break this down:
  - Attitude – a mental position, feeling or emotion regarding a fact or state
  - Value – something (such as a principle or quality) intrinsically valuable or desirable
  - Goal – the end towards which effort is directed
  - Practice – the usual way of doing something

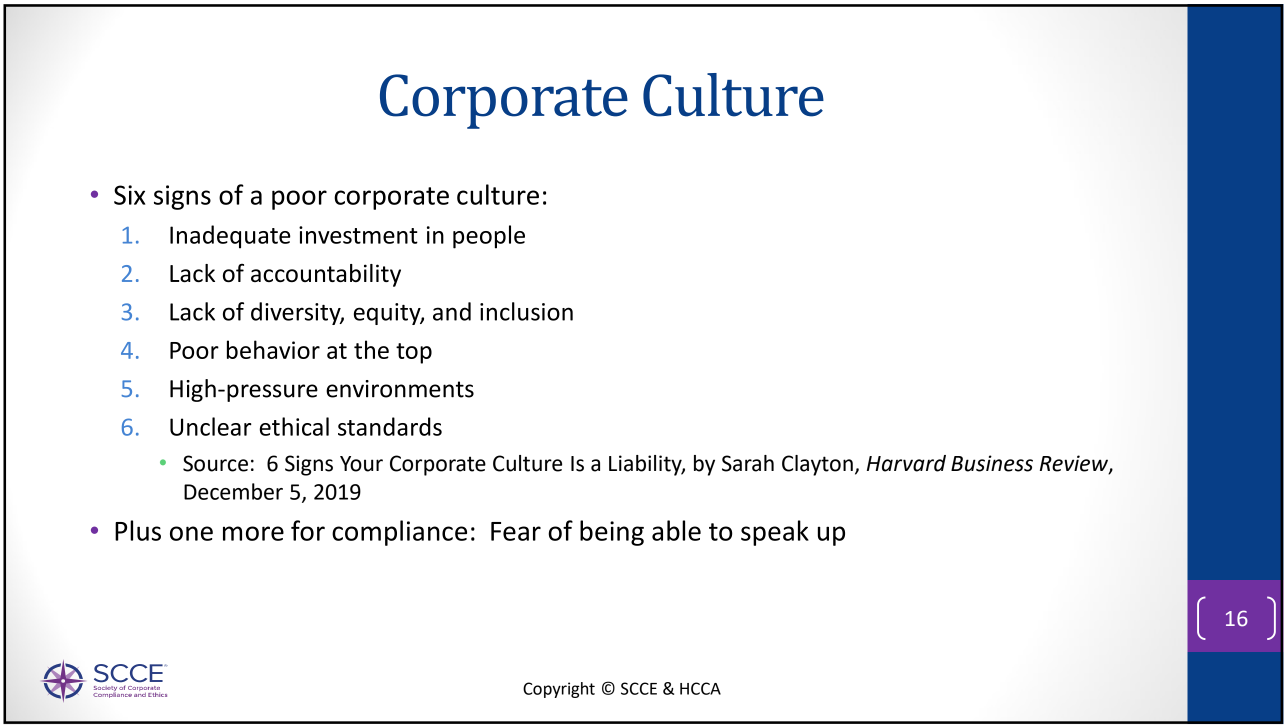
14

14



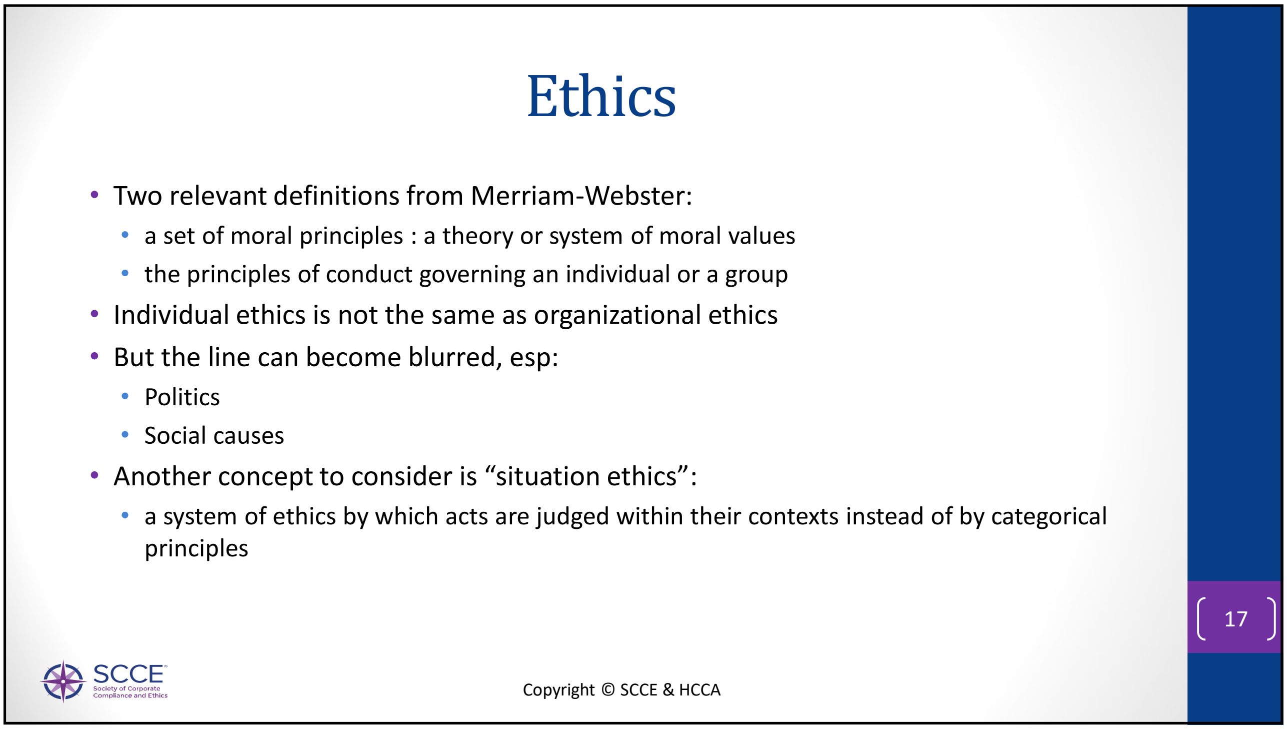
Characteristics of Corporate Culture

- Culture is:
  - Shared
  - Pervasive
  - Enduring
  - Implicit
    - Source: The Leader’s Guide to Corporate Culture, by Boris Groysberg, Jeremiah Lee, Jesse Price, and J. Yo-Jud Cheng, *Harvard Business Review*, January-February 2018



Corporate Culture

- Six signs of a poor corporate culture:
  1. Inadequate investment in people
  2. Lack of accountability
  3. Lack of diversity, equity, and inclusion
  4. Poor behavior at the top
  5. High-pressure environments
  6. Unclear ethical standards
     - Source: 6 Signs Your Corporate Culture Is a Liability, by Sarah Clayton, *Harvard Business Review*, December 5, 2019
- Plus one more for compliance: Fear of being able to speak up



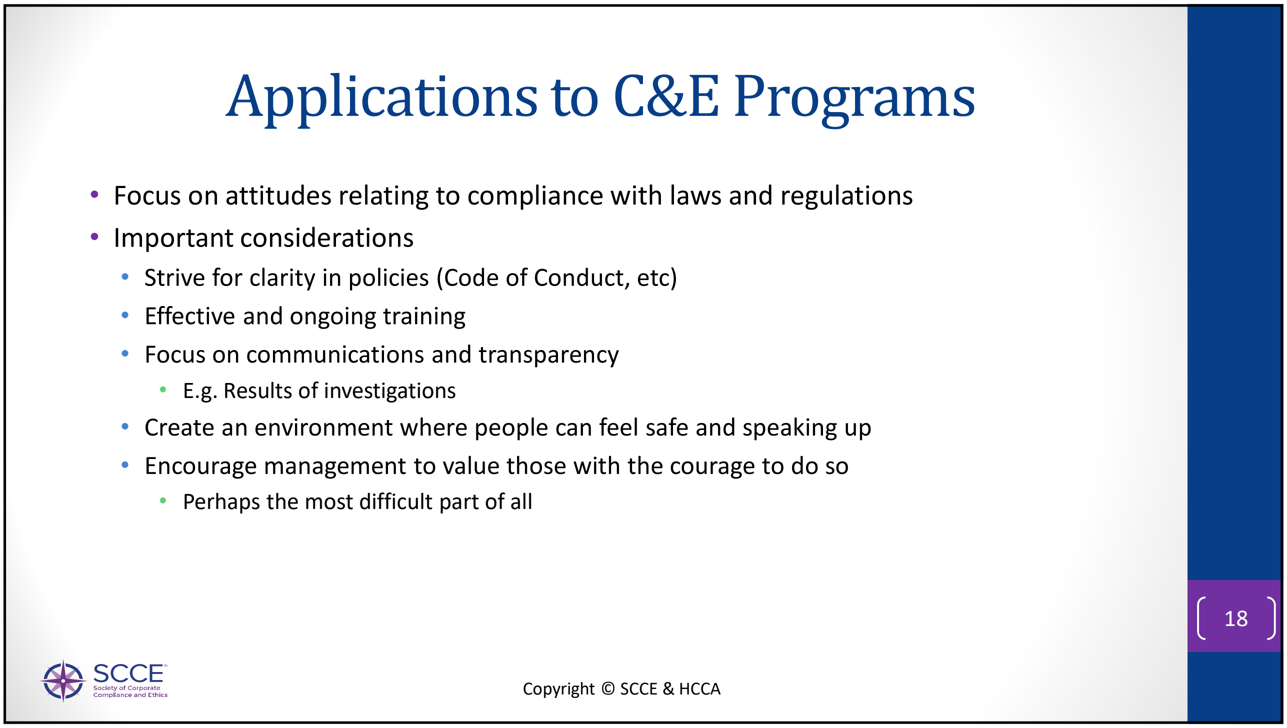
Ethics

- Two relevant definitions from Merriam-Webster:
  - a set of moral principles : a theory or system of moral values
  - the principles of conduct governing an individual or a group
- Individual ethics is not the same as organizational ethics
- But the line can become blurred, esp:
  - Politics
  - Social causes
- Another concept to consider is “situation ethics”:
  - a system of ethics by which acts are judged within their contexts instead of by categorical principles

17

SCCE Society of Corporate Compliance and Ethics

17



Applications to C&E Programs

- Focus on attitudes relating to compliance with laws and regulations
- Important considerations
  - Strive for clarity in policies (Code of Conduct, etc)
  - Effective and ongoing training
  - Focus on communications and transparency
    - E.g. Results of investigations
  - Create an environment where people can feel safe and speaking up
  - Encourage management to value those with the courage to do so
    - Perhaps the most difficult part of all

18

SCCE Society of Corporate Compliance and Ethics

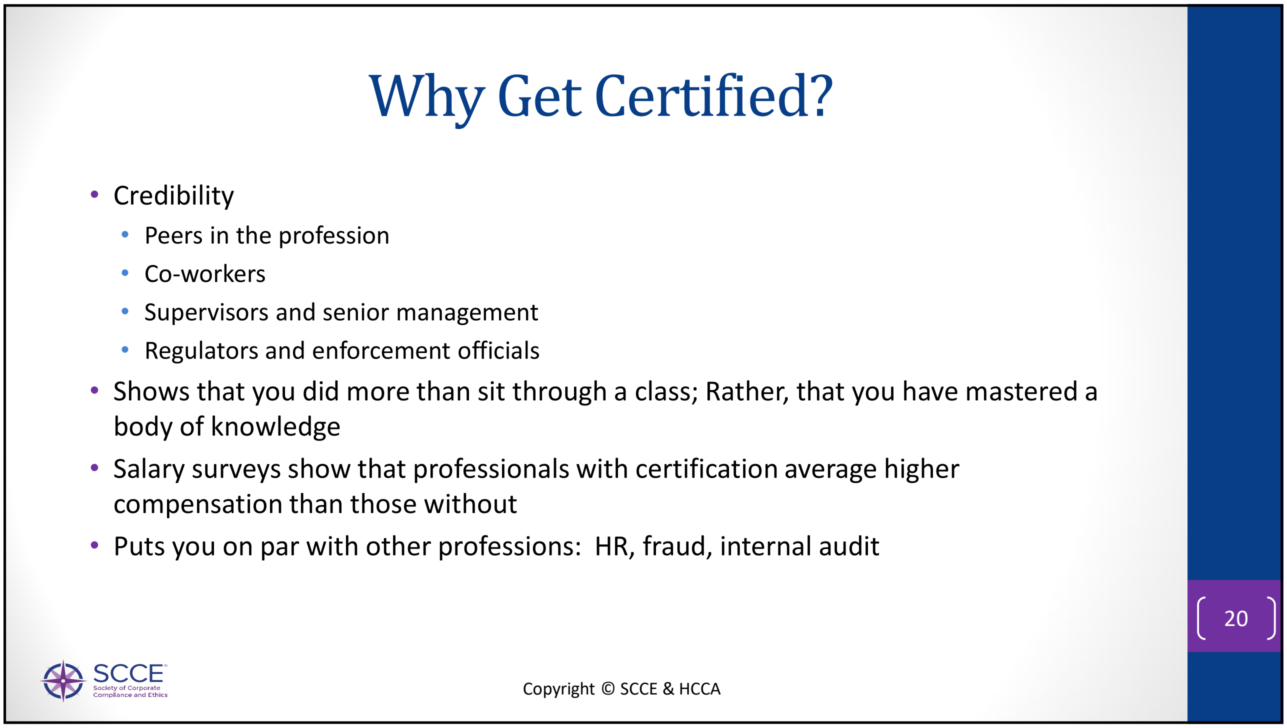
18

Building Your Career as a Compliance & Ethics Professional

- Certification
- Networking
- Additional or specialized training
- Developing a career plan

19

19

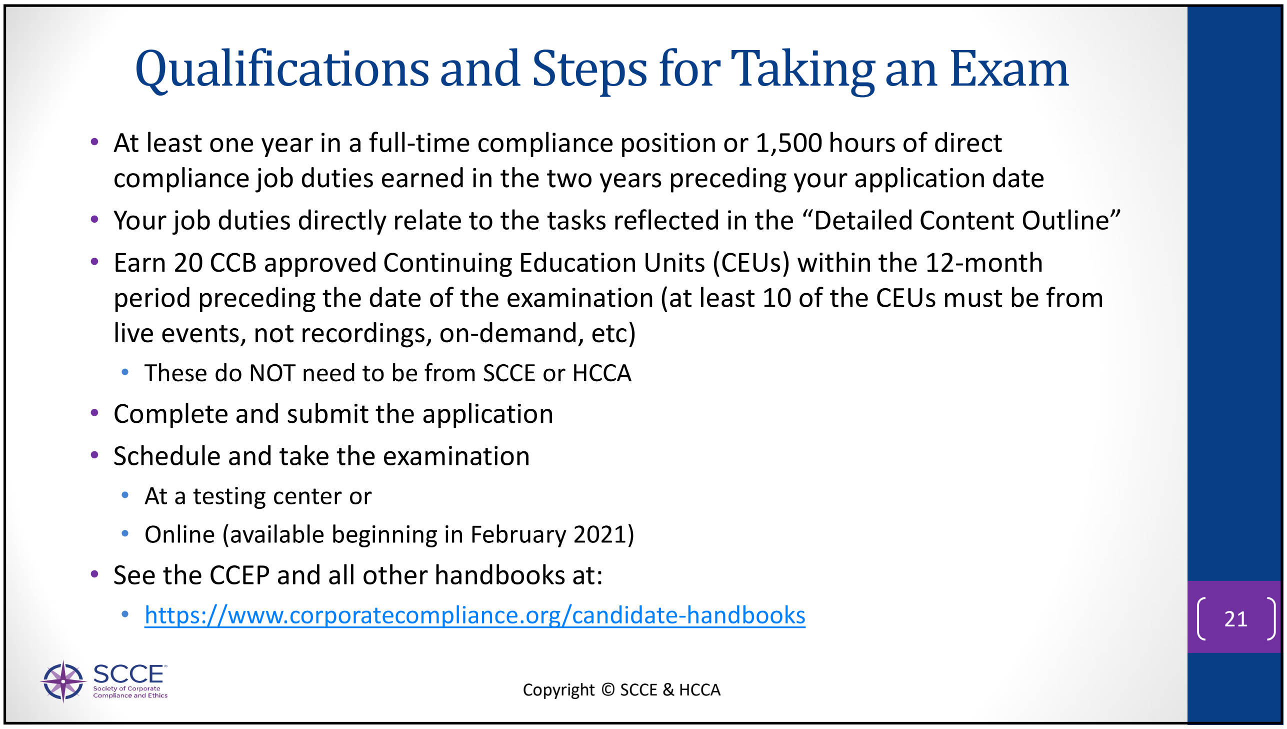


Why Get Certified?

- Credibility
  - Peers in the profession
  - Co-workers
  - Supervisors and senior management
  - Regulators and enforcement officials
- Shows that you did more than sit through a class; Rather, that you have mastered a body of knowledge
- Salary surveys show that professionals with certification average higher compensation than those without
- Puts you on par with other professions: HR, fraud, internal audit

20

20

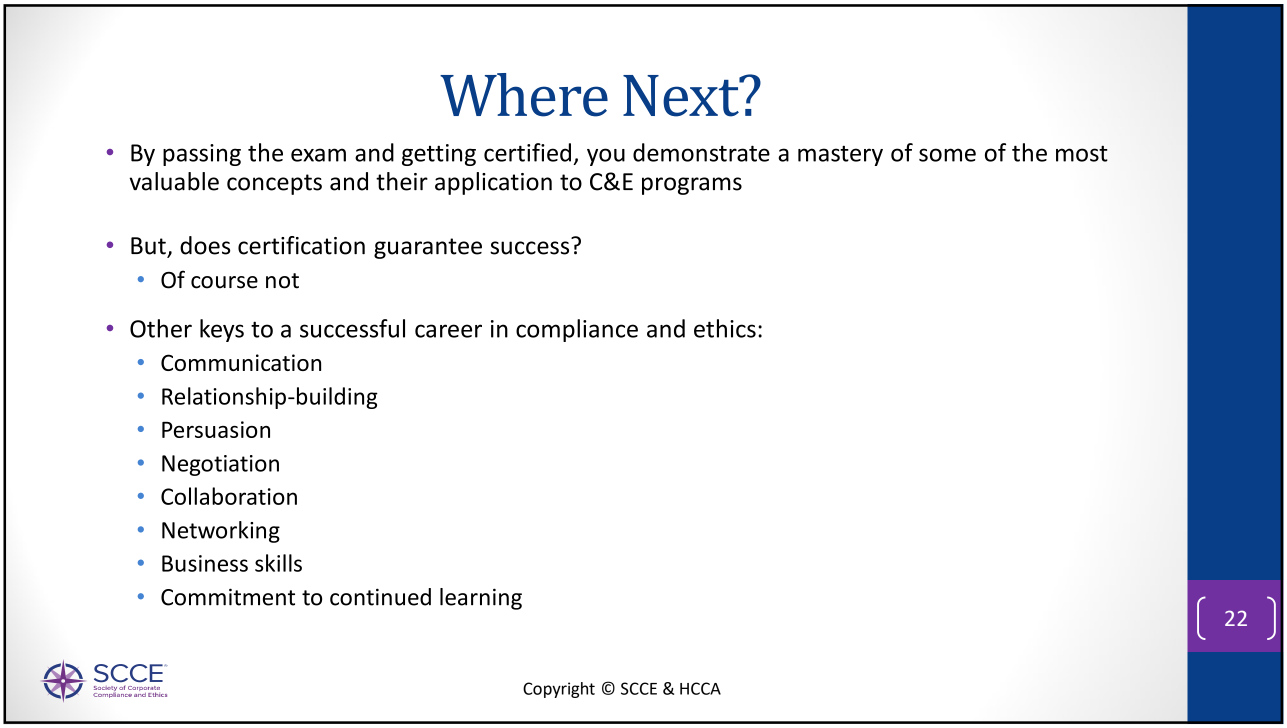


Qualifications and Steps for Taking an Exam

- At least one year in a full-time compliance position or 1,500 hours of direct compliance job duties earned in the two years preceding your application date
- Your job duties directly relate to the tasks reflected in the “Detailed Content Outline”
- Earn 20 CCB approved Continuing Education Units (CEUs) within the 12-month period preceding the date of the examination (at least 10 of the CEUs must be from live events, not recordings, on-demand, etc)
  - These do NOT need to be from SCCE or HCCA
- Complete and submit the application
- Schedule and take the examination
  - At a testing center or
  - Online (available beginning in February 2021)
- See the CCEP and all other handbooks at:
  - https://www.corporatecompliance.org/candidate-handbooks

21

21

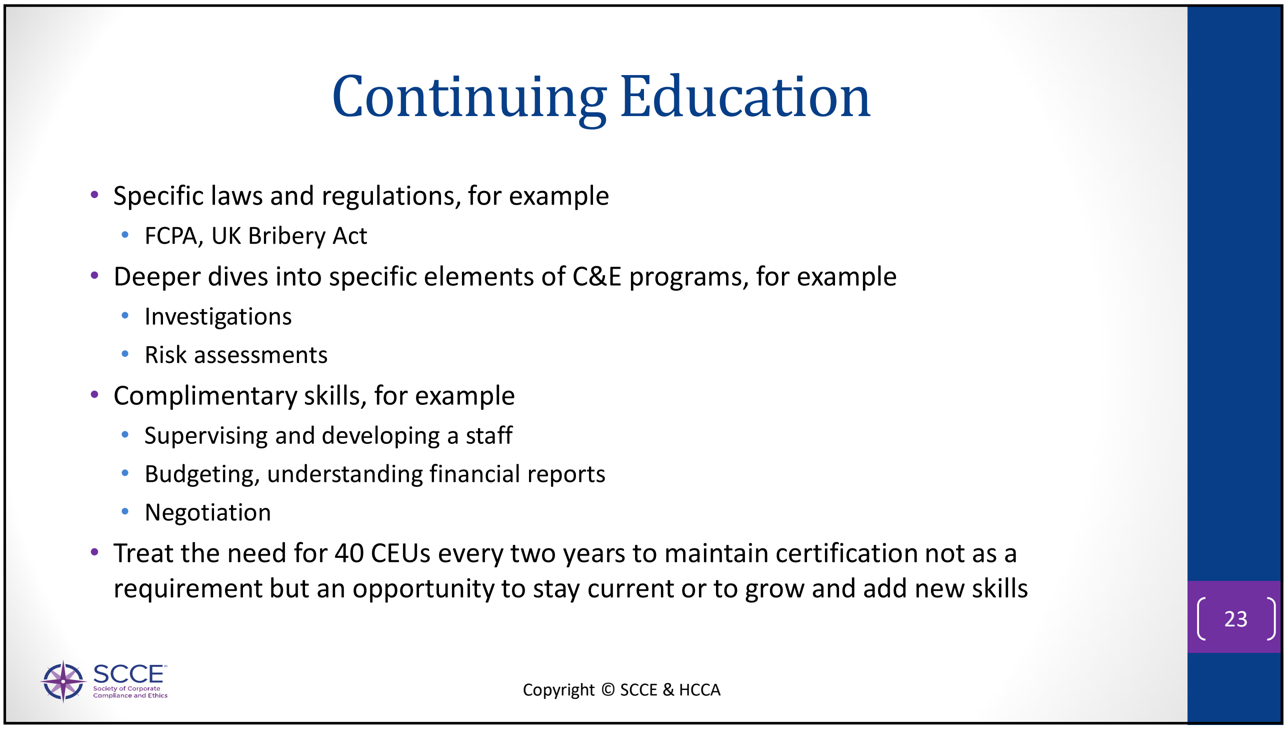


Where Next?

- By passing the exam and getting certified, you demonstrate a mastery of some of the most valuable concepts and their application to C&E programs
- But, does certification guarantee success?
  - Of course not
- Other keys to a successful career in compliance and ethics:
  - Communication
  - Relationship-building
  - Persuasion
  - Negotiation
  - Collaboration
  - Networking
  - Business skills
  - Commitment to continued learning

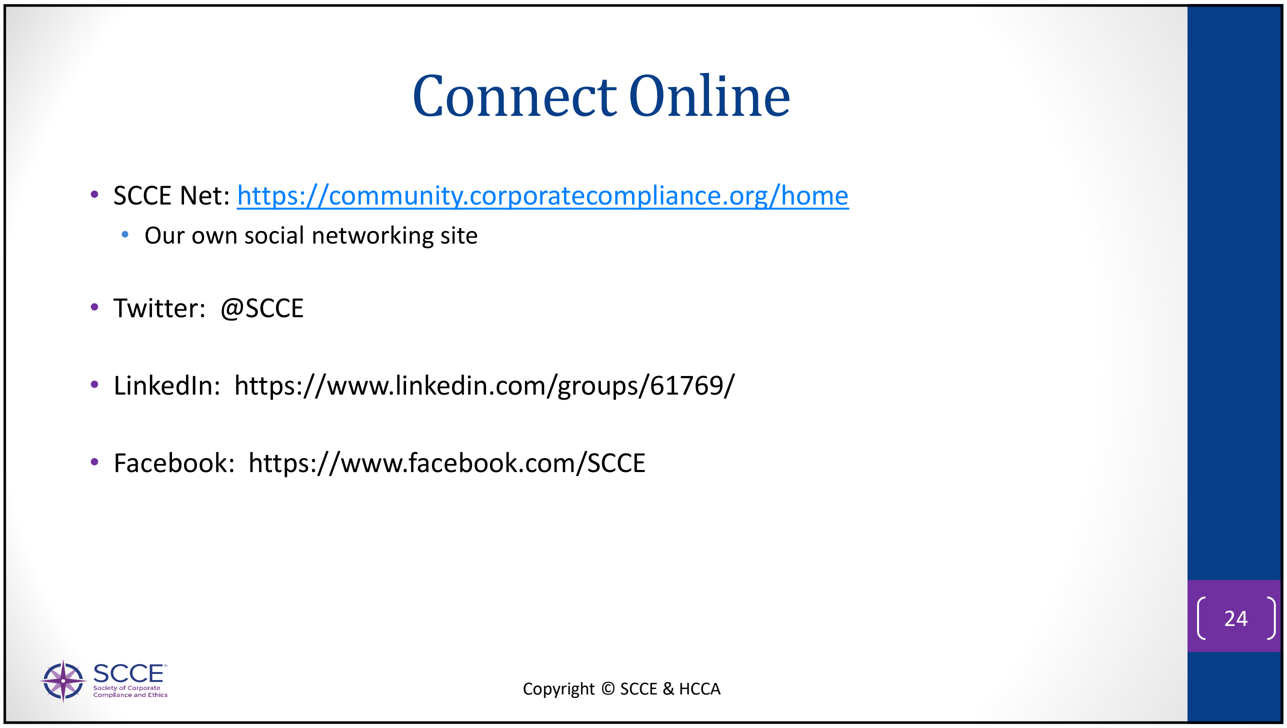
22

22



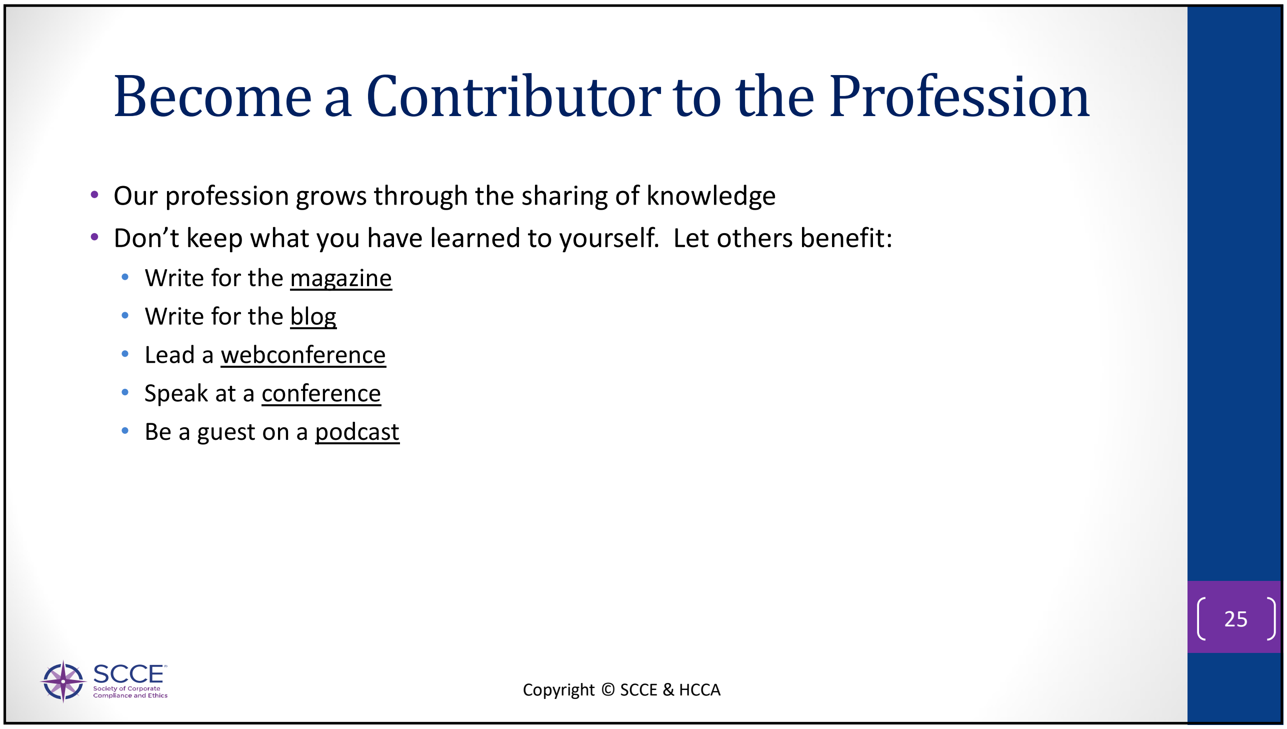
Continuing Education

- Specific laws and regulations, for example
  - FCPA, UK Bribery Act
- Deeper dives into specific elements of C&E programs, for example
  - Investigations
  - Risk assessments
- Complimentary skills, for example
  - Supervising and developing a staff
  - Budgeting, understanding financial reports
  - Negotiation
- Treat the need for 40 CEUs every two years to maintain certification not as a requirement but an opportunity to stay current or to grow and add new skills



Connect Online

- SCCE Net: https://community.corporatecompliance.org/home
  - Our own social networking site
- Twitter: @SCCE
- LinkedIn: https://www.linkedin.com/groups/61769/
- Facebook: https://www.facebook.com/SCCE



Become a Contributor to the Profession

- Our profession grows through the sharing of knowledge
- Don’t keep what you have learned to yourself. Let others benefit:
  - Write for the magazine
  - Write for the blog
  - Lead a webconference
  - Speak at a conference
  - Be a guest on a podcast

25

25

Questions ?

adam.turteltaub@corporatecompliance.org

26

26