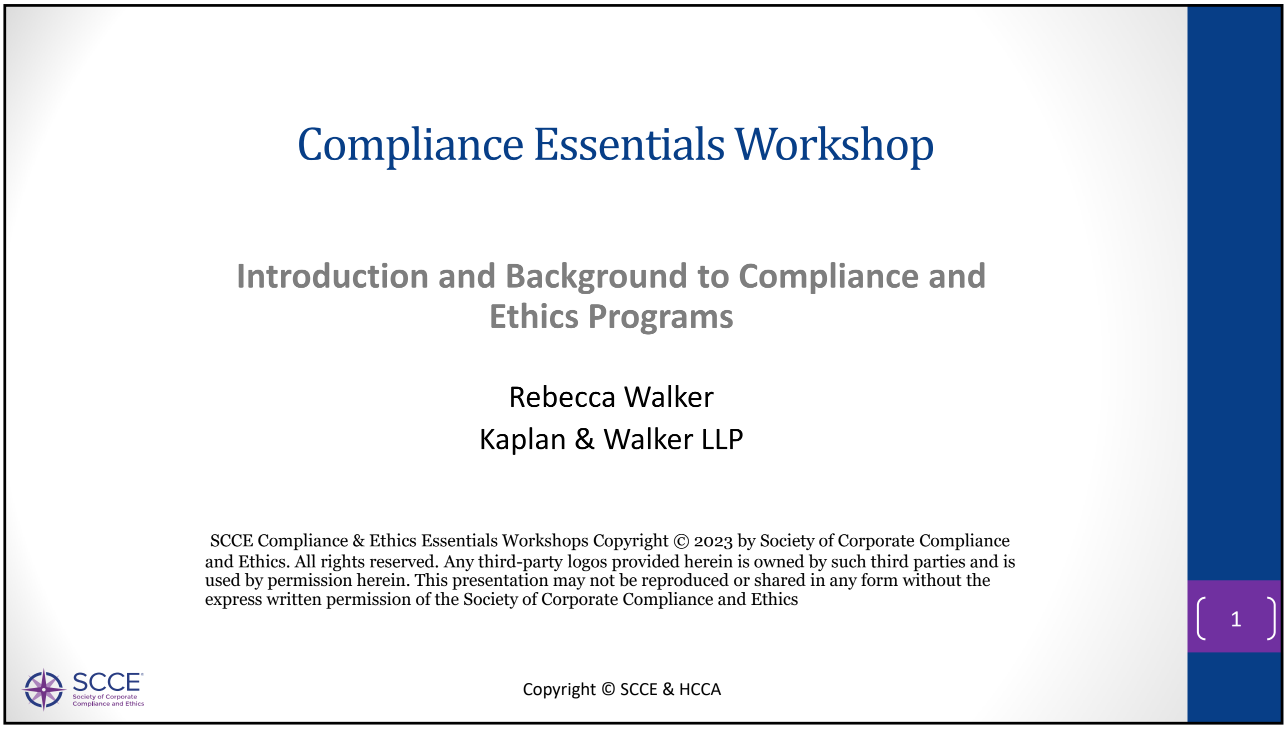
SCCE Compliance & Ethics Essentials Workshop

All PDF Presentations Combined



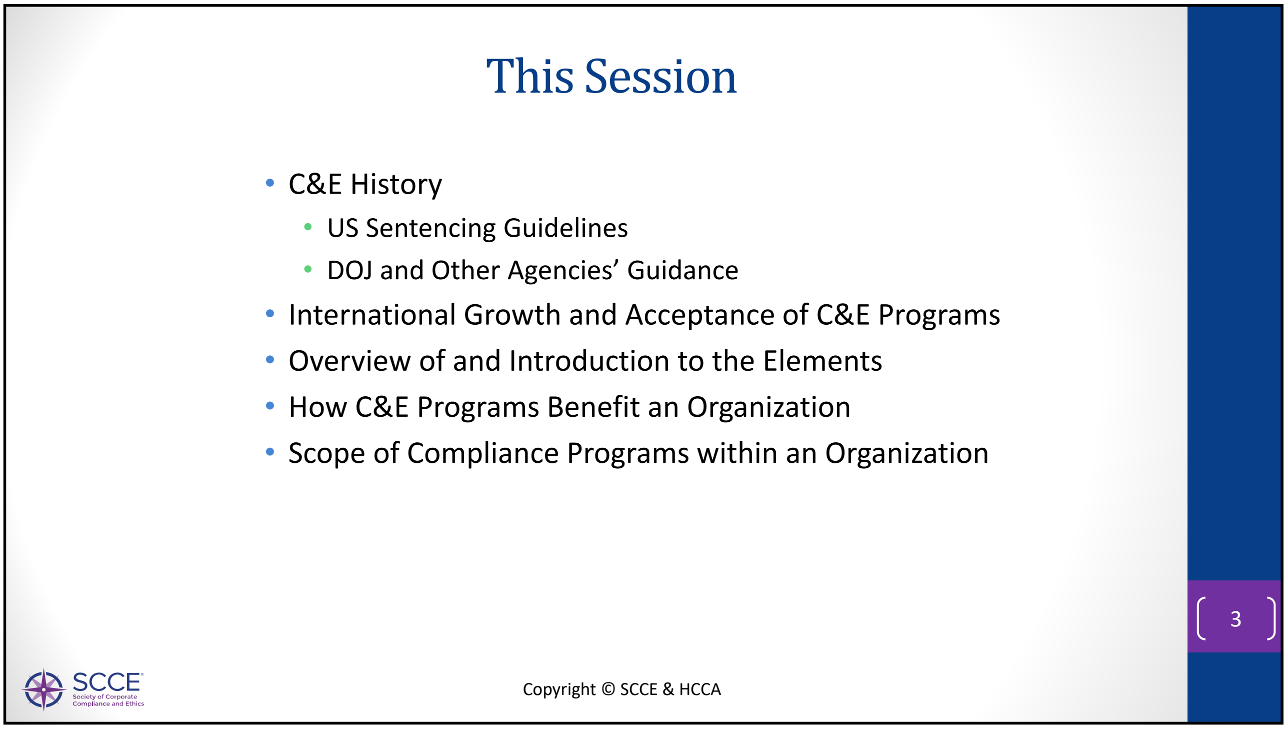
Compliance Essentials Workshop

Introduction and Background to Compliance and Ethics Programs

Rebecca Walker
Kaplan & Walker LLP

Welcome!

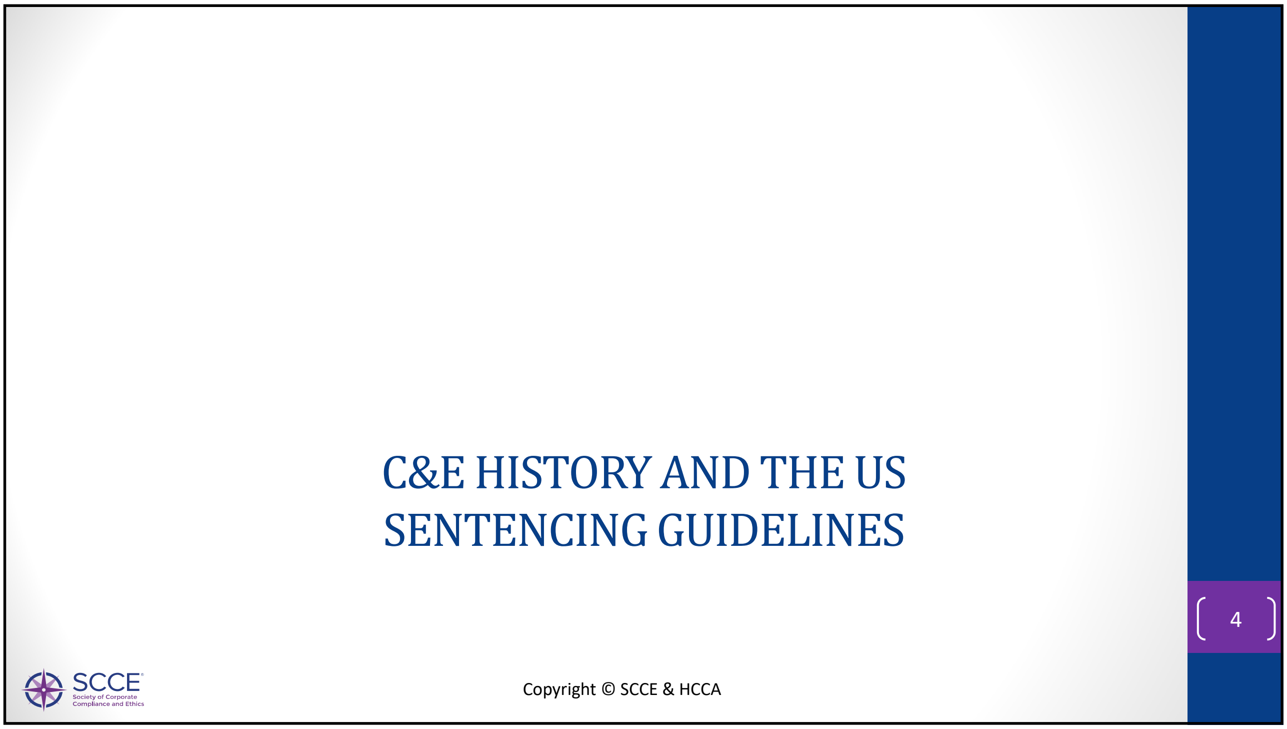
- This is the first of 13 sessions in the SCCE Compliance Essentials Workshop
  - Day 1
    - Introduction & background to compliance & ethics programs
    - Standards and procedures
    - Governance, oversight, authority
  - Day 2
    - Risk assessment
    - Due diligence in delegation of authority
    - 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

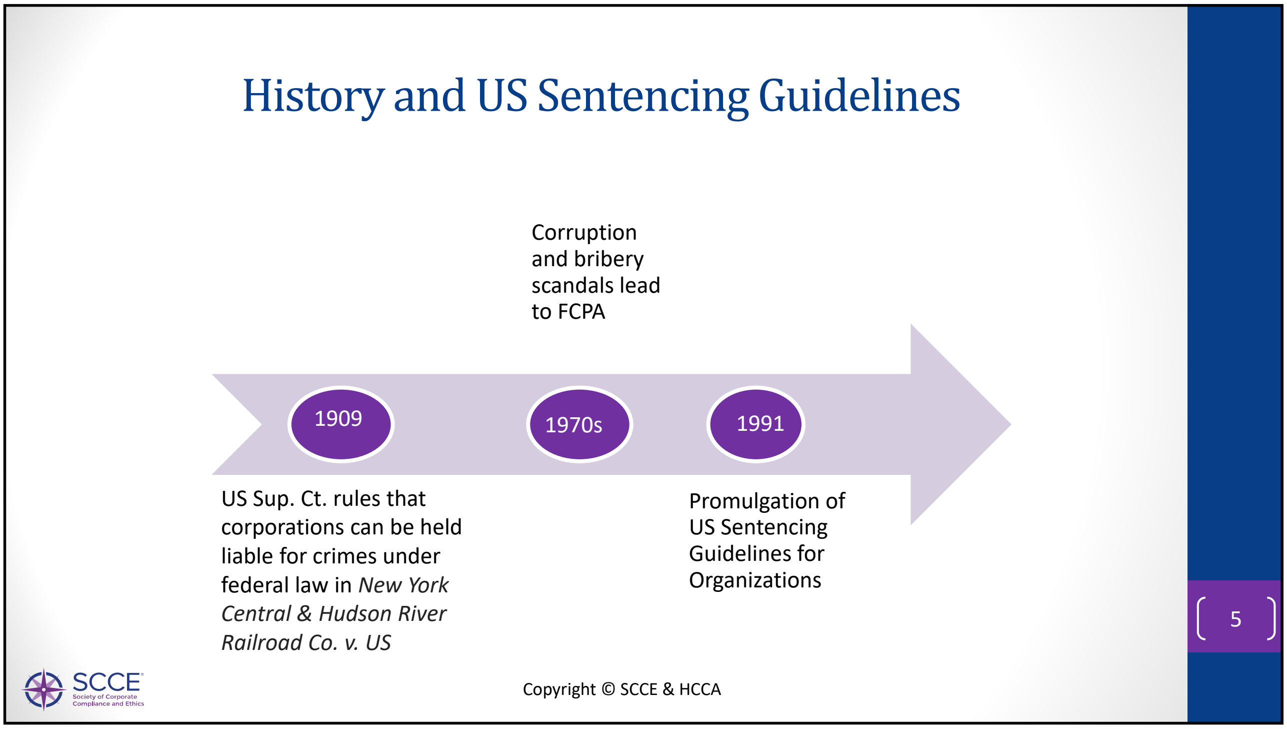
- C&E History
  - US Sentencing Guidelines
  - DOJ and Other Agencies’ Guidance
- International Growth and Acceptance of C&E Programs
- Overview of and Introduction to the Elements
- How C&E Programs Benefit an Organization
- Scope of Compliance Programs within an Organization

3



C&E HISTORY AND THE US SENTENCING GUIDELINES

4

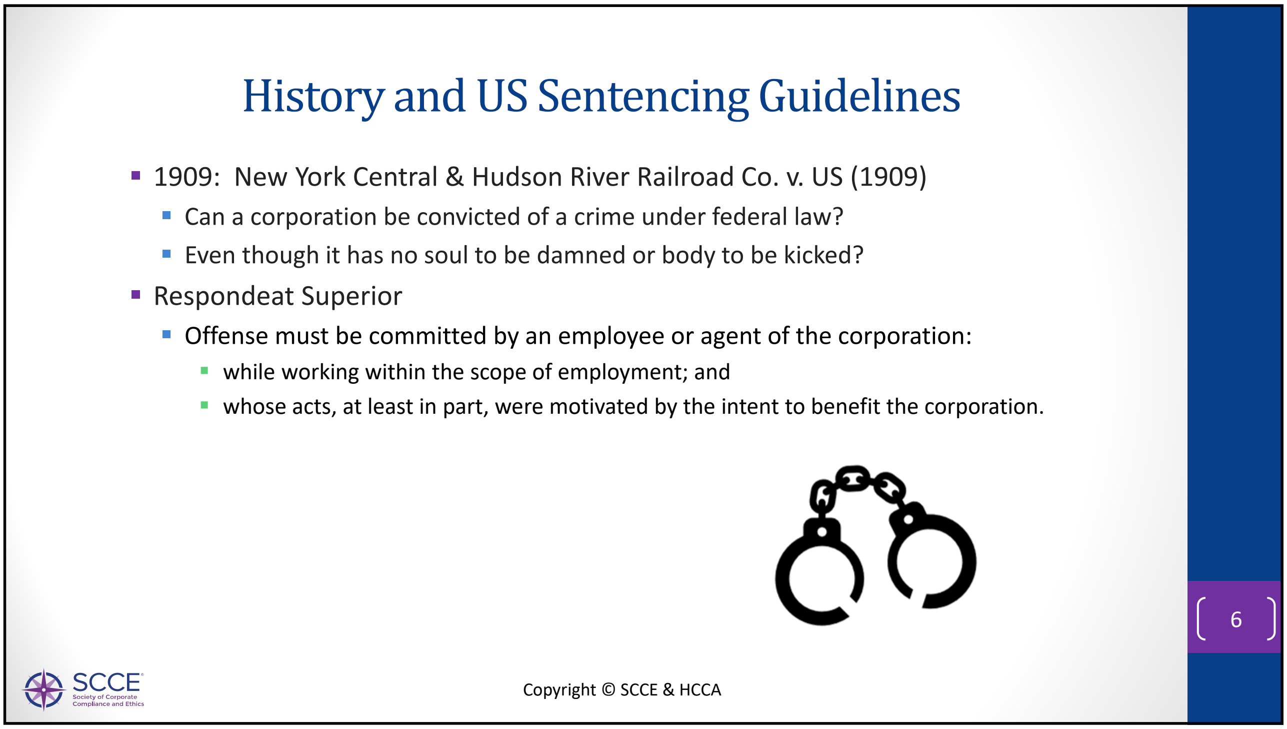


History and US Sentencing Guidelines

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*

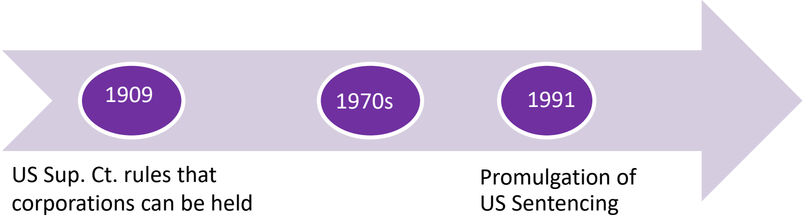
Promulgation of US Sentencing Guidelines for Organizations



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.

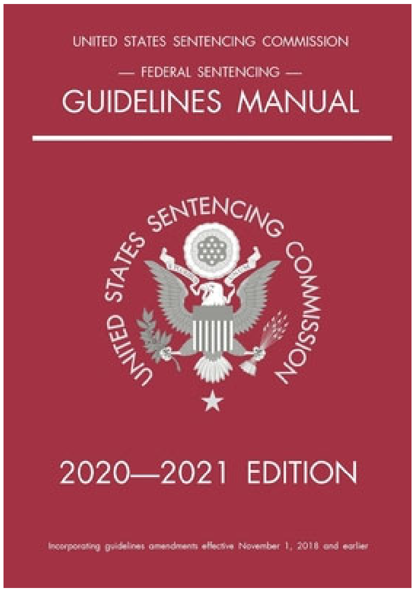
History and US Sentencing Guidelines



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



UNITED STATES SENTENCING COMMISSION

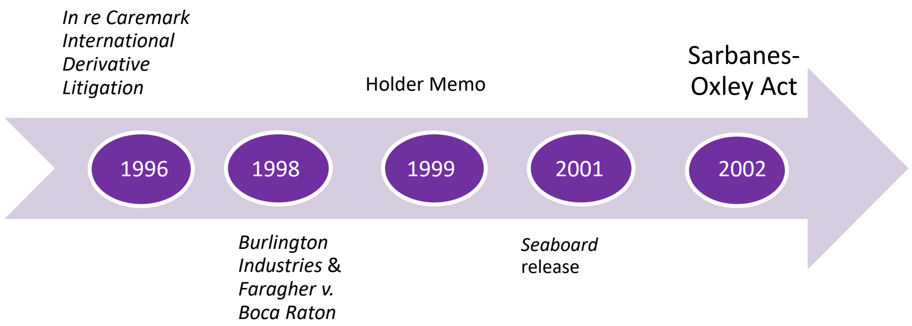
— FEDERAL SENTENCING —

GUIDELINES MANUAL

2020—2021 EDITION

Incorporating guidelines amendments effective November 1, 2018 and earlier

History and US Sentencing Guidelines

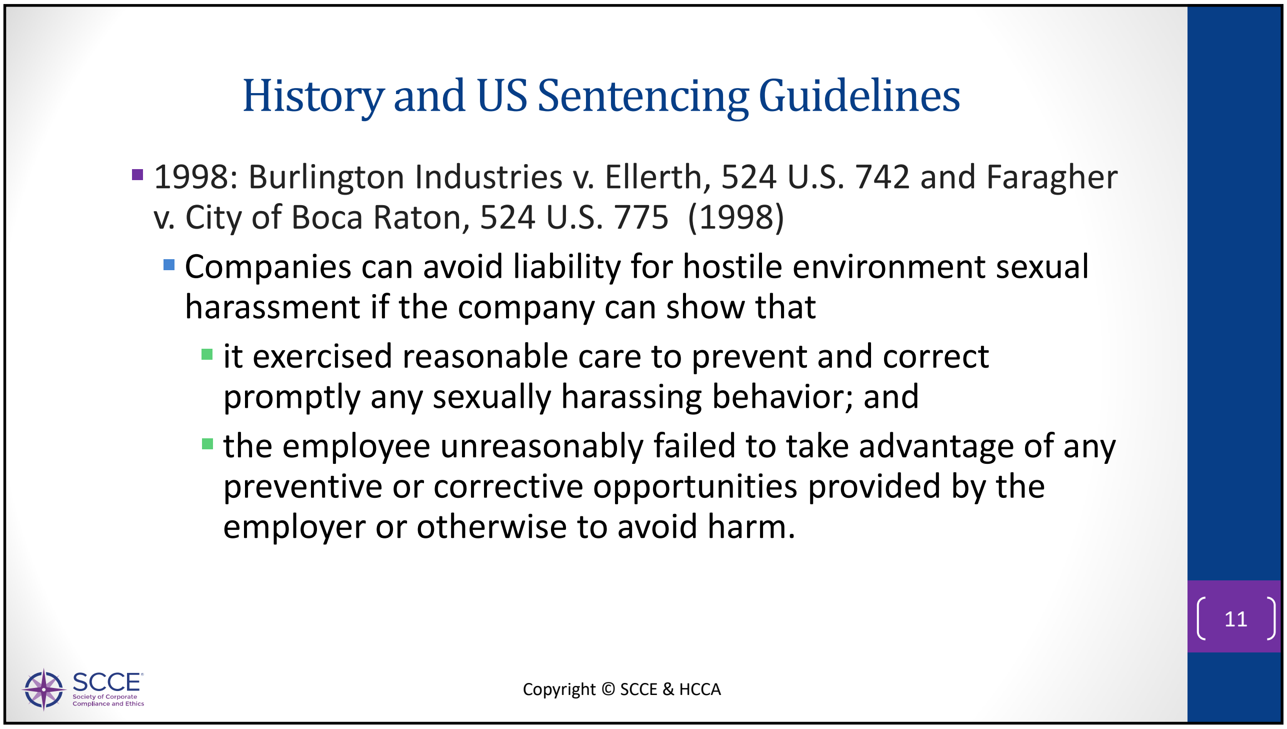

In re Caremark International Derivative Litigation
1996
1998
Burlington Industries & *Faragher v. Boca Raton*
Holder Memo
1999
2001
Seaboard release
Sarbanes-Oxley Act
2002

SCCE Society of Corporate Compliance and Ethics

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."

SCCE Society of Corporate Compliance and Ethics

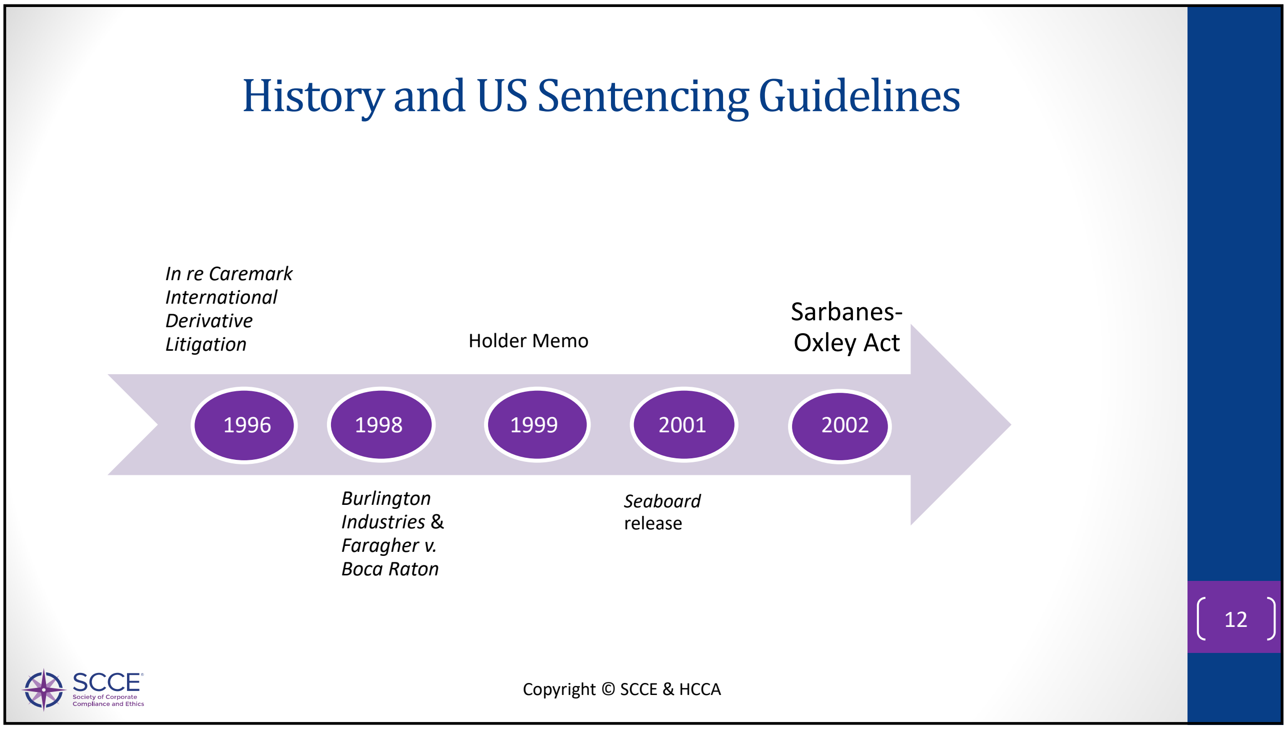


History and US Sentencing Guidelines

- 1998: Burlington Industries v. Ellerth, 524 U.S. 742 and Faragher v. City of Boca Raton, 524 U.S. 775 (1998)
  - Companies can avoid liability for hostile environment sexual harassment if the company can show that
    - it exercised reasonable care to prevent and correct promptly any sexually harassing behavior; and
    - the employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or otherwise to avoid harm.

11

11



History and US Sentencing Guidelines

In re Caremark International Derivative Litigation

Holder Memo

Sarbanes-Oxley Act

1996

1998

1999

2001

2002

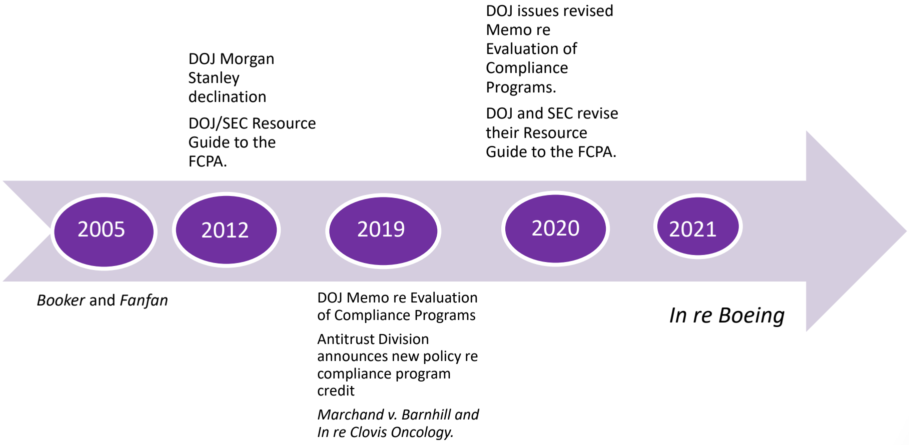
Burlington Industries & Faragher v. Boca Raton

Seaboard release

12

12

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.

2020

DOJ issues revised Memo re Evaluation of Compliance Programs.

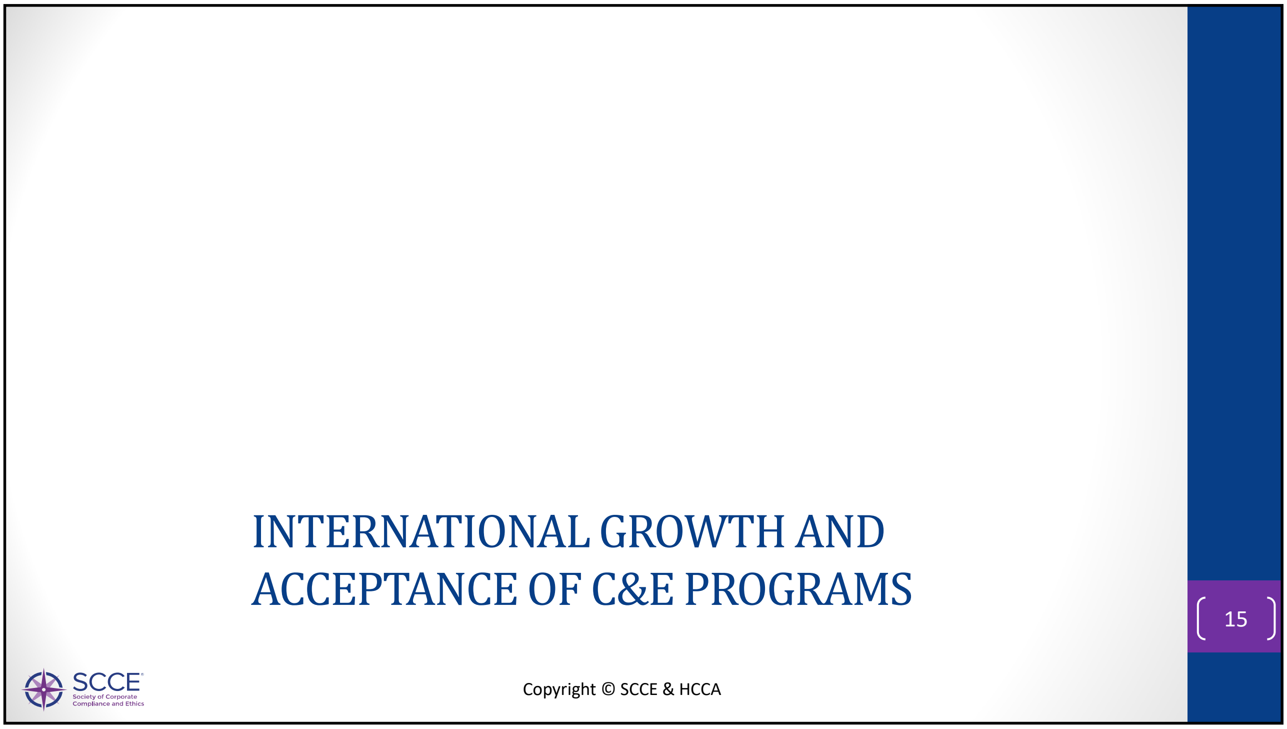
DOJ and SEC revise their Resource Guide to the FCPA.

2021

In re Boeing

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



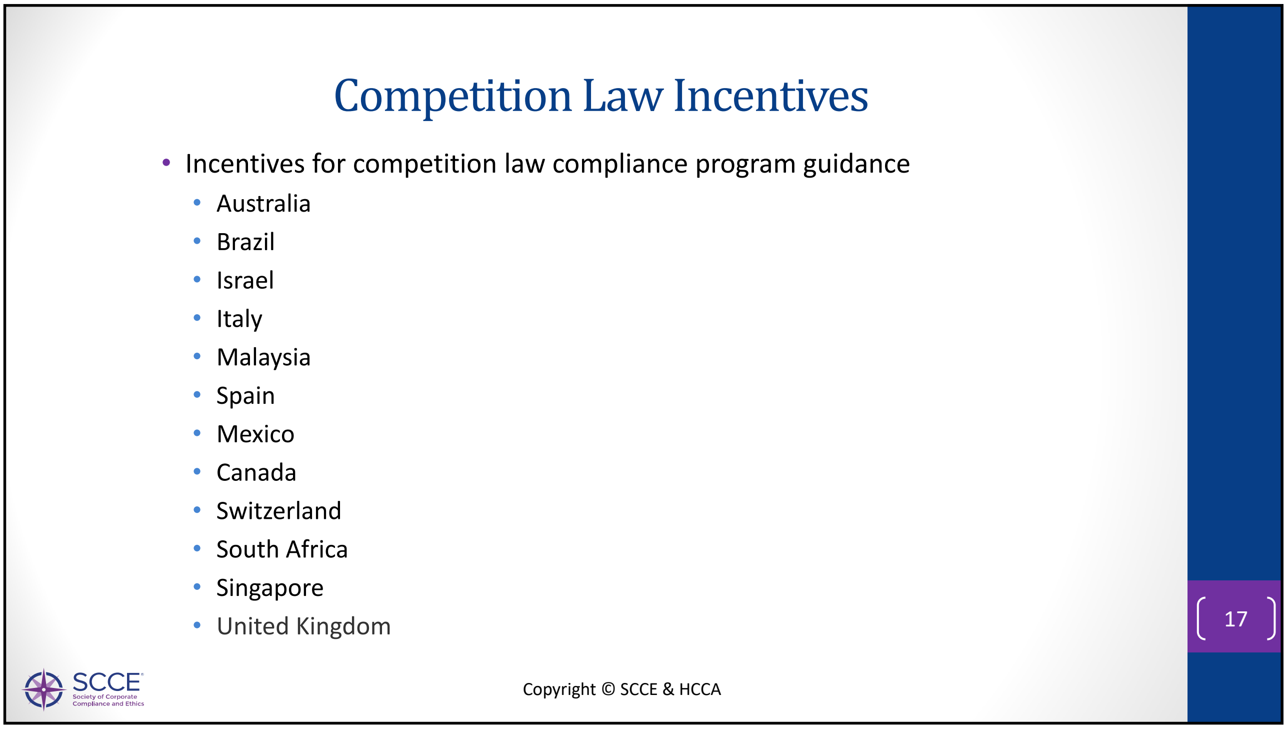
INTERNATIONAL GROWTH AND ACCEPTANCE OF C&E PROGRAMS

15

Anti-Bribery Compliance Programs

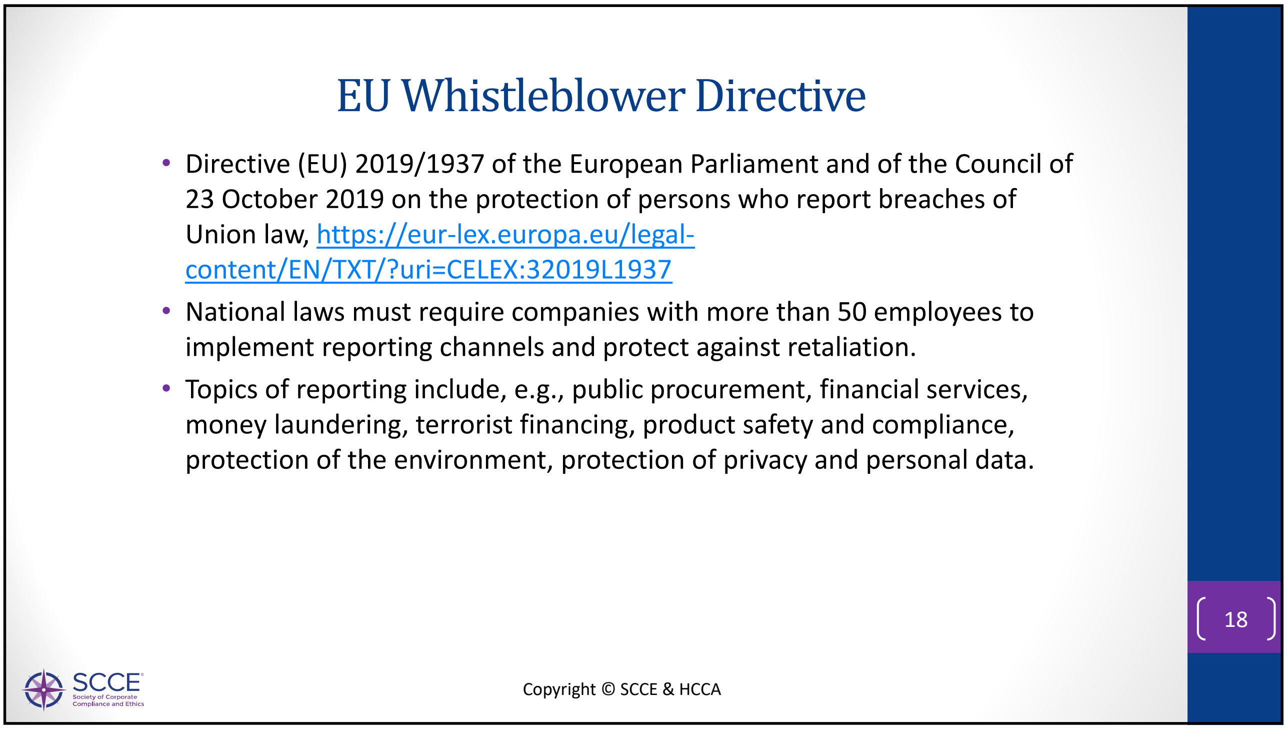
- OECD Good Practice Guidance for Anti-Bribery Compliance Programs (2009)
- UK Bribery Act of 2010
  - Adequate Procedures Guidance
  - SFO publishes Guidance on Deferred Prosecution Agreements (October 23, 2020)
    - https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/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

16



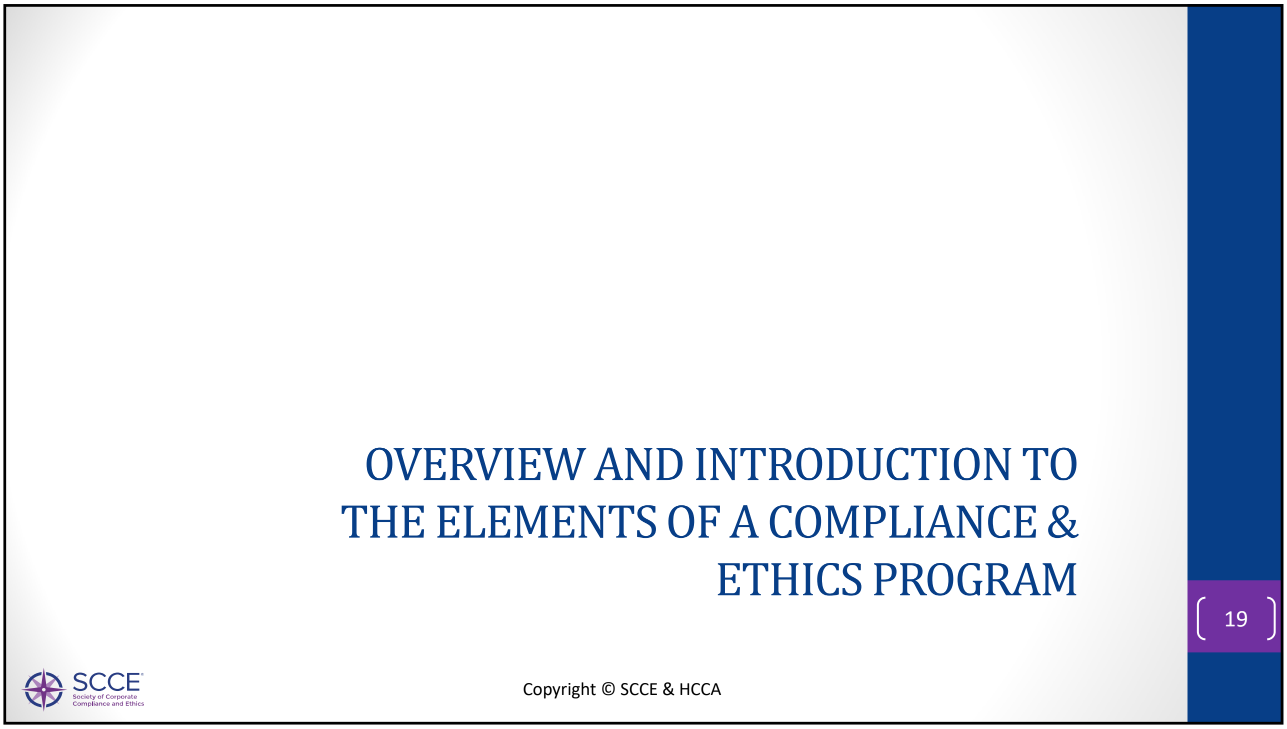
Competition Law Incentives

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

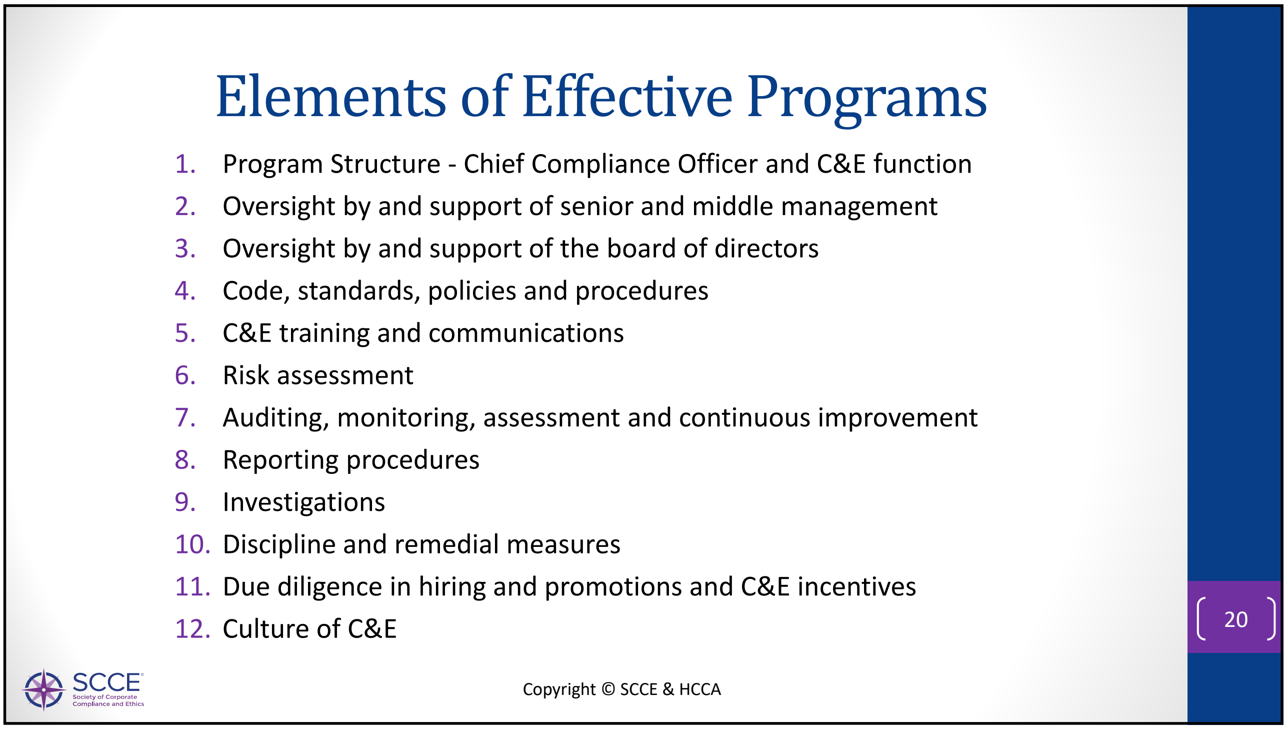


EU Whistleblower Directive

- 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.

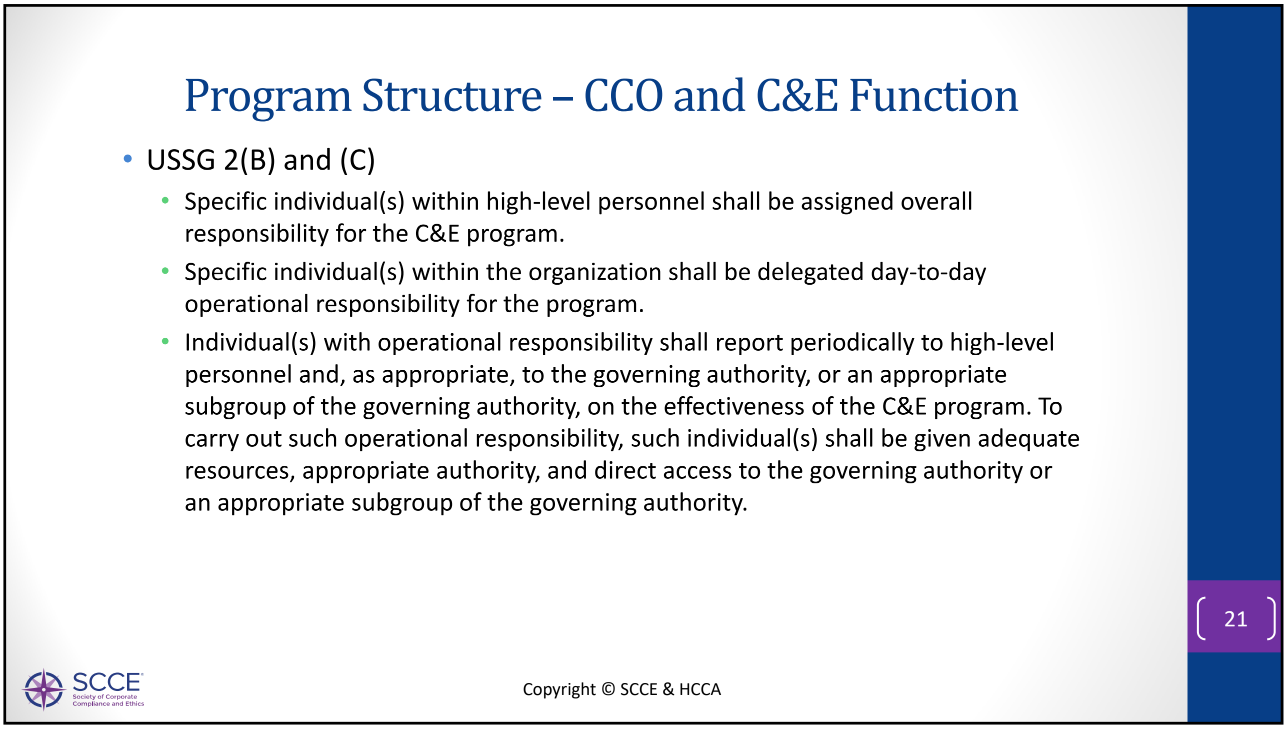


OVERVIEW AND INTRODUCTION TO THE ELEMENTS OF A COMPLIANCE & ETHICS PROGRAM



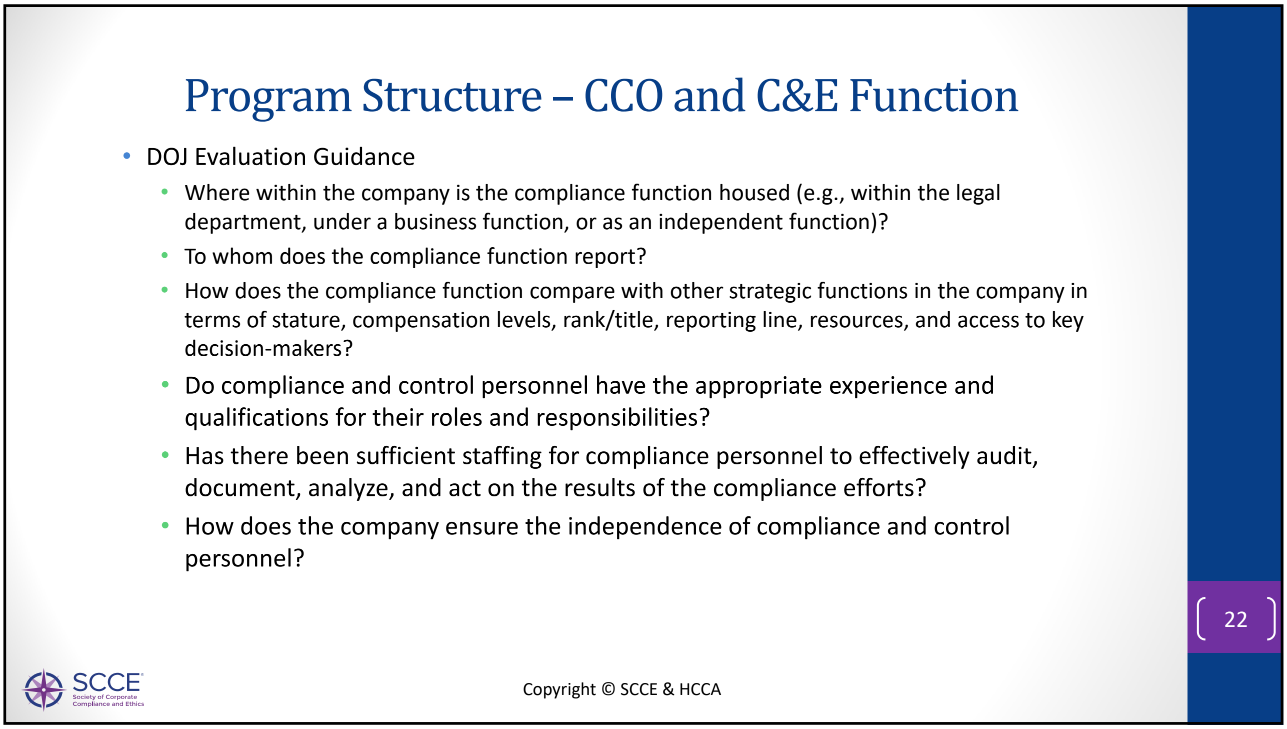
Elements of Effective Programs

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



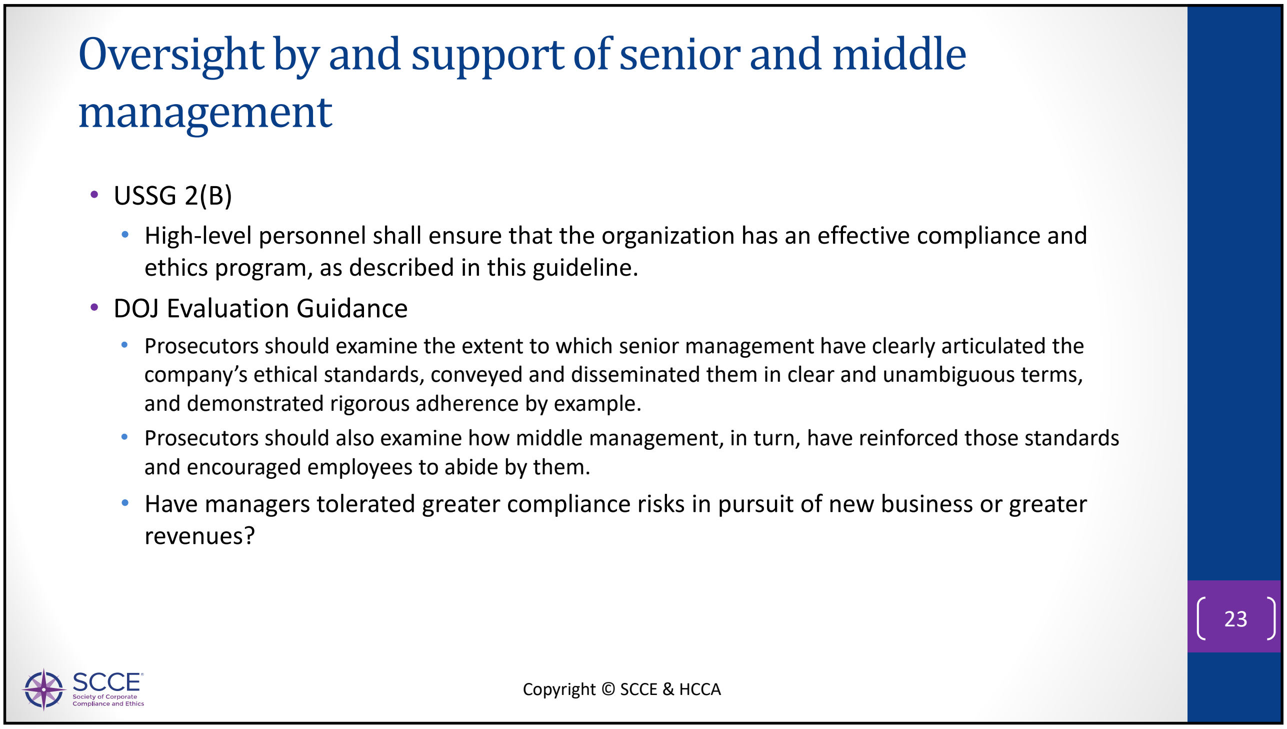
Program Structure – CCO and C&E Function

- 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.



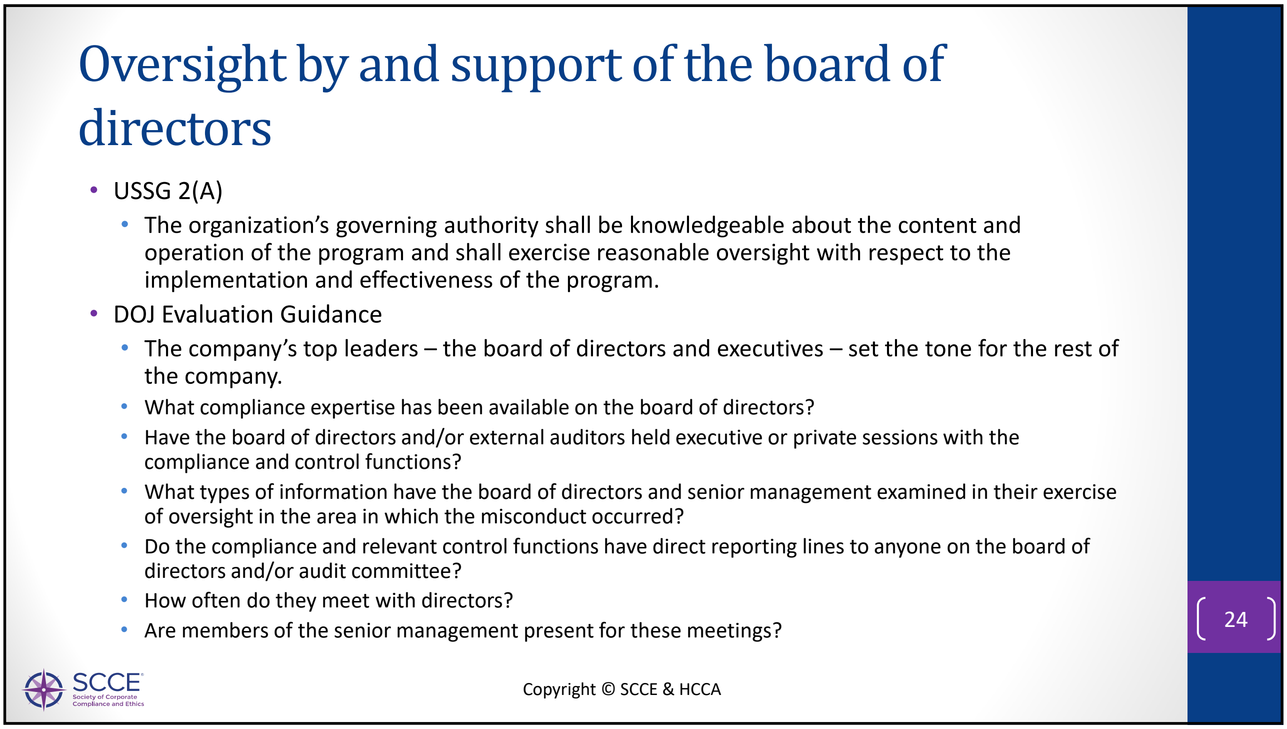
Program Structure – CCO and C&E Function

- 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?



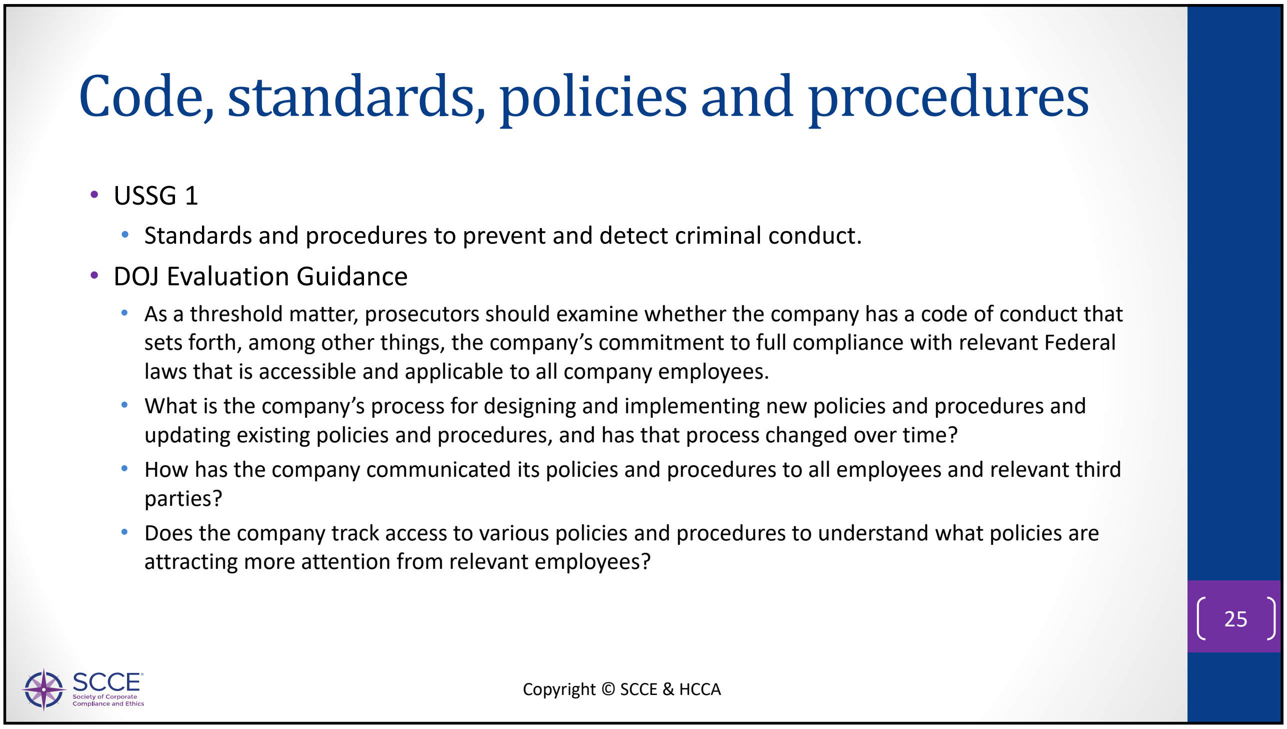
Oversight by and support of senior and middle management

- 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?

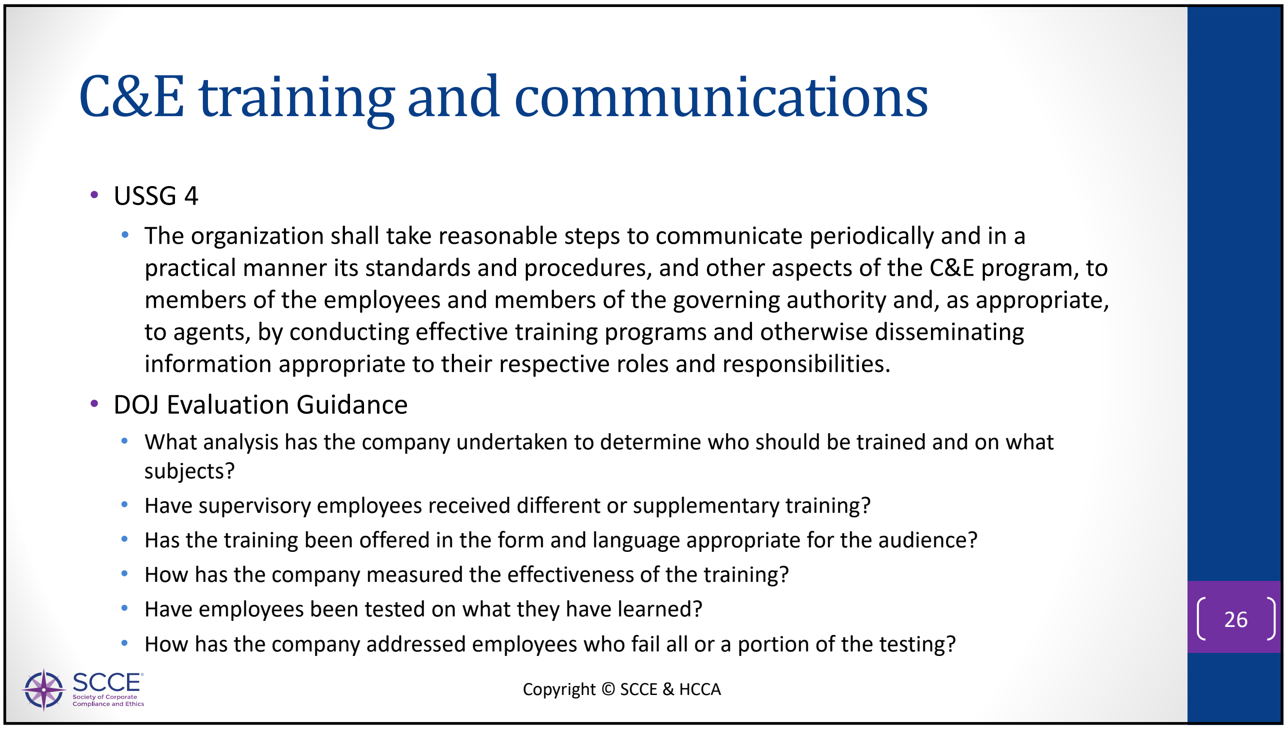


Code, standards, policies and procedures

- 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?

25

25

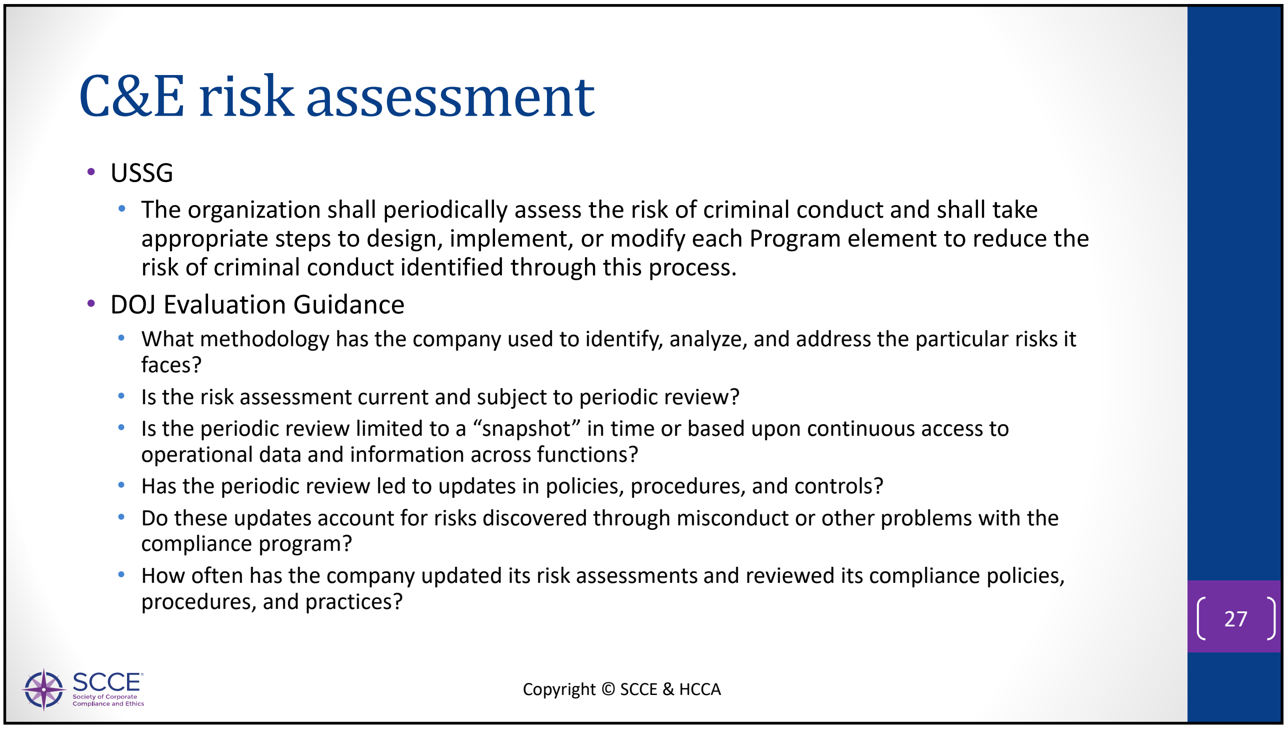


C&E training and communications

- 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?

26

26

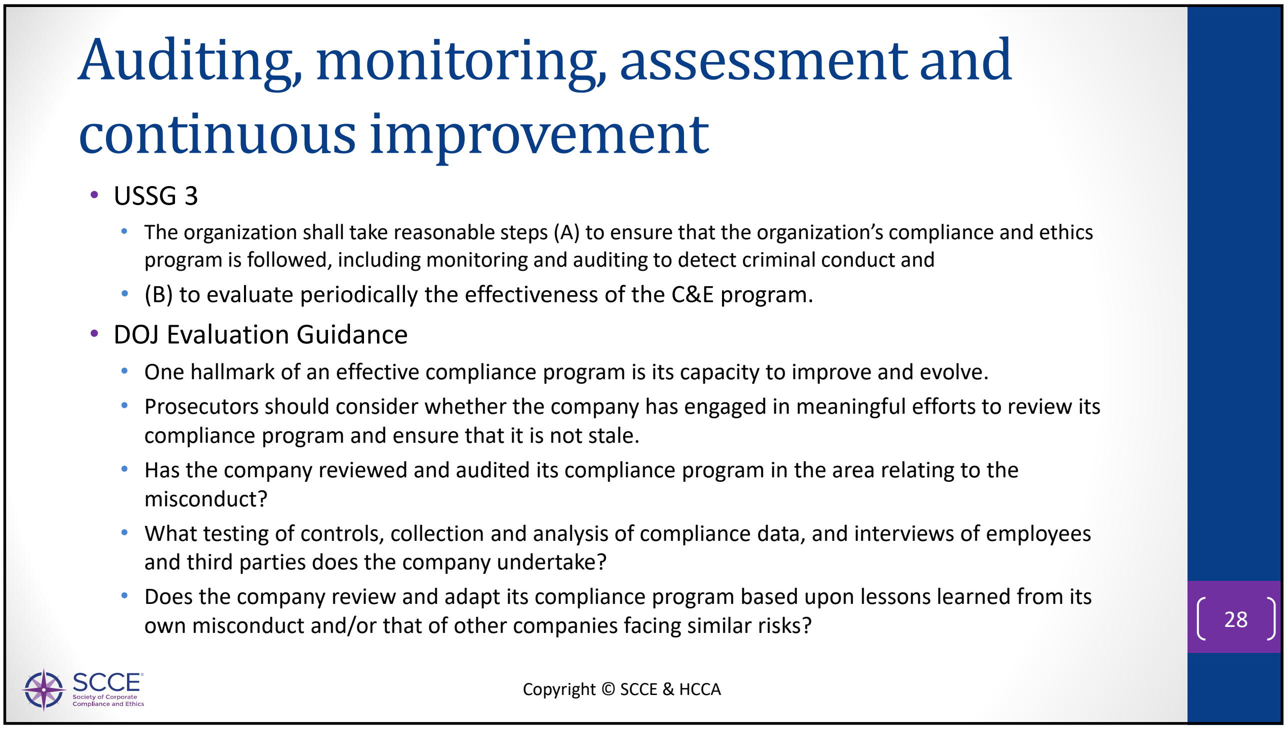


C&E risk assessment

- 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?

27

27

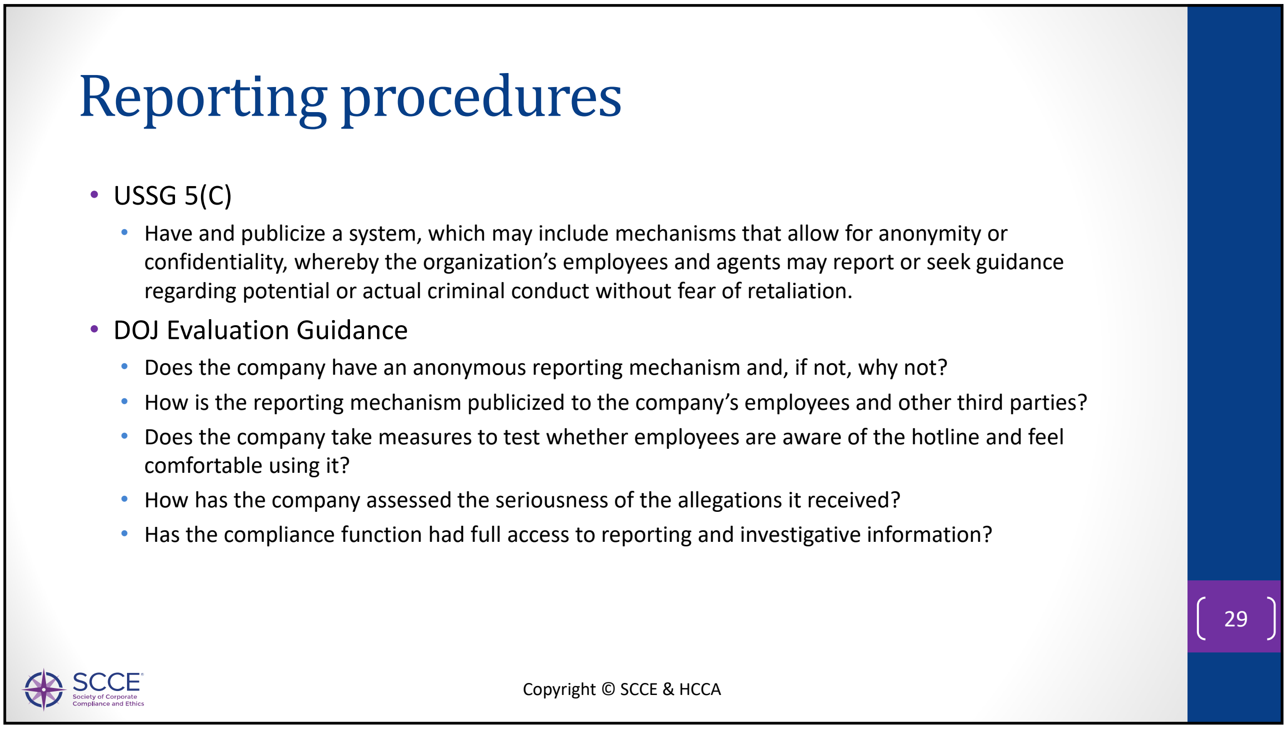


Auditing, monitoring, assessment and continuous improvement

- 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?

28

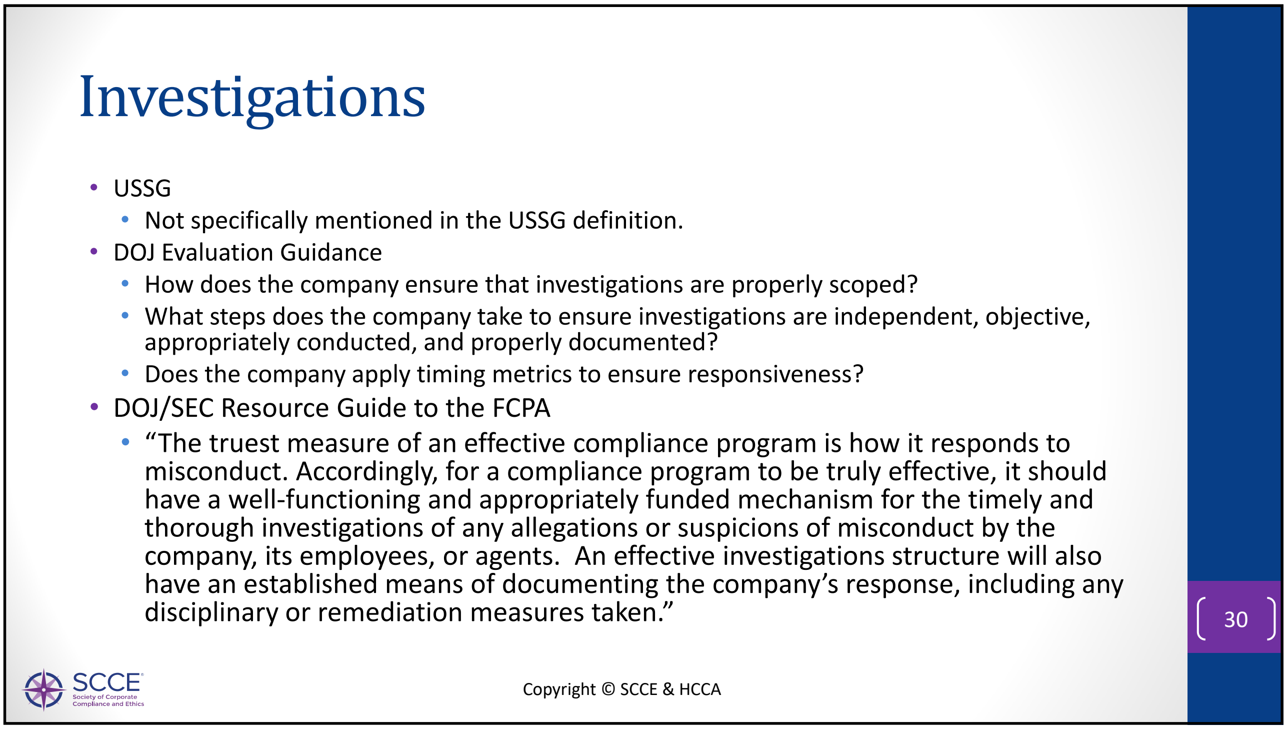
28



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?

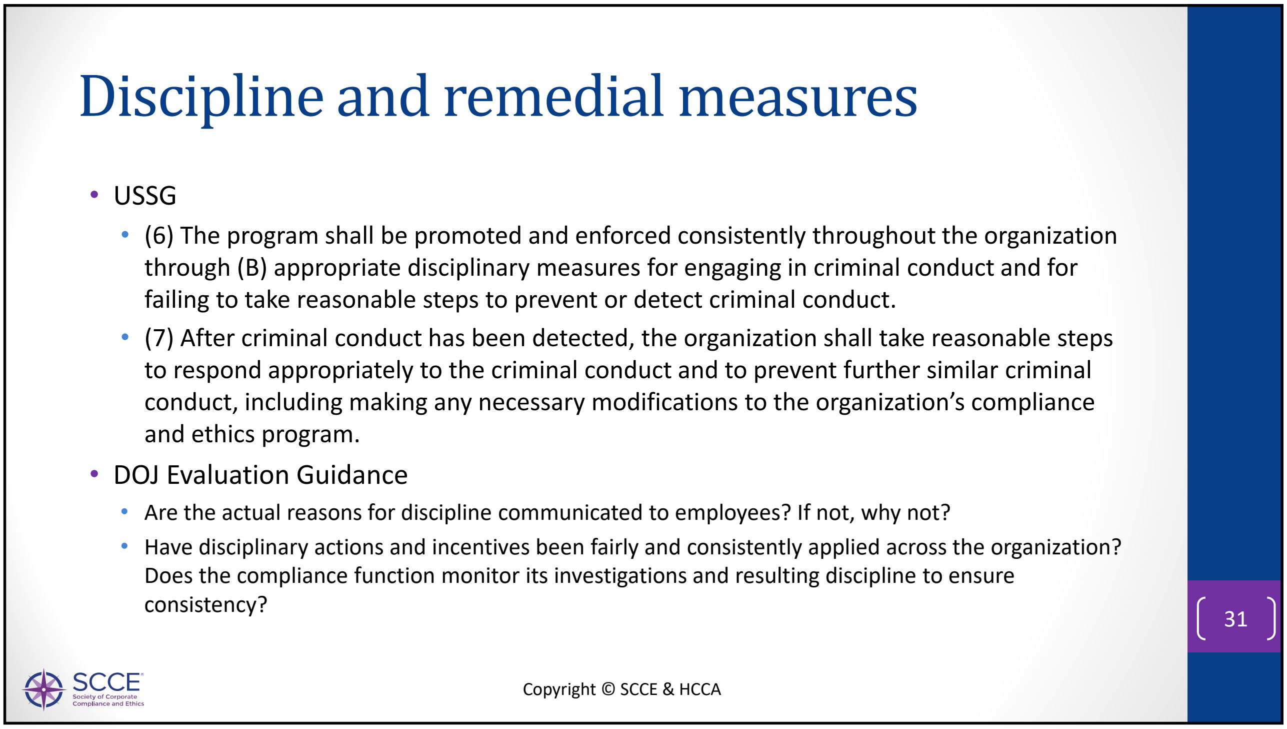
29



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."

30

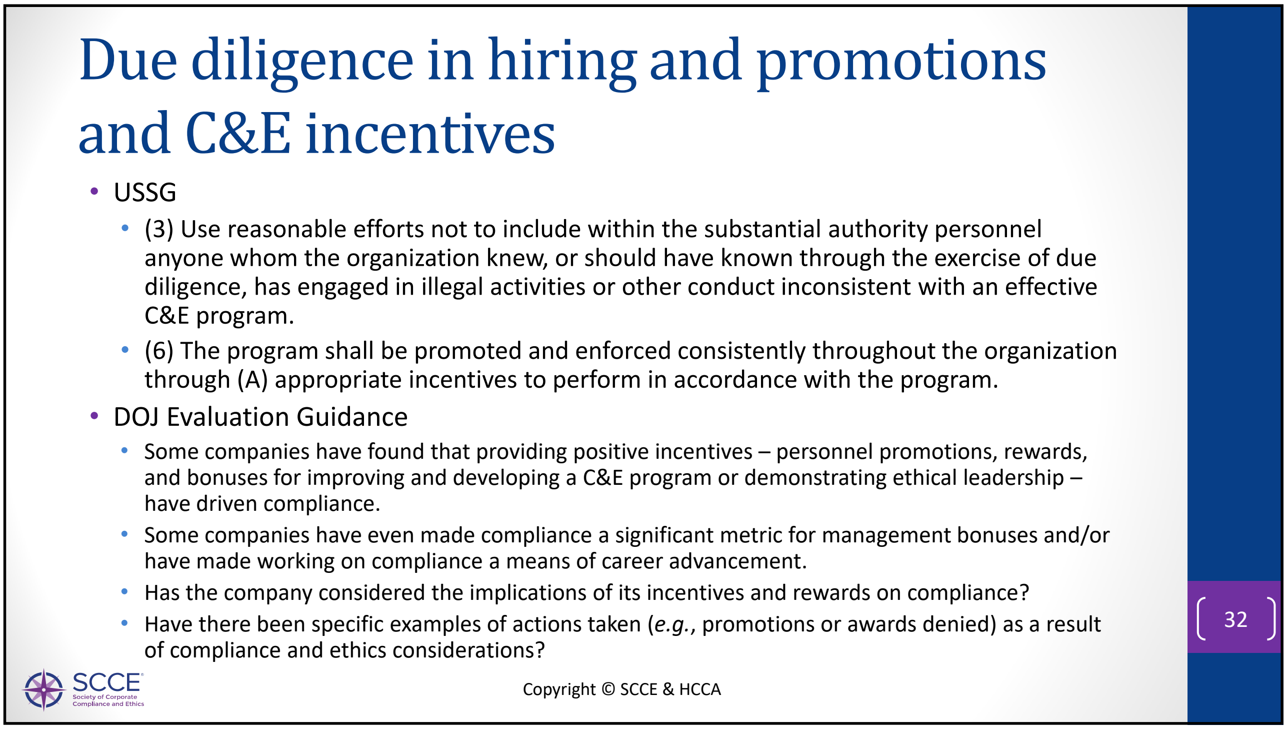


Discipline and remedial measures

- 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?

31

31



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?

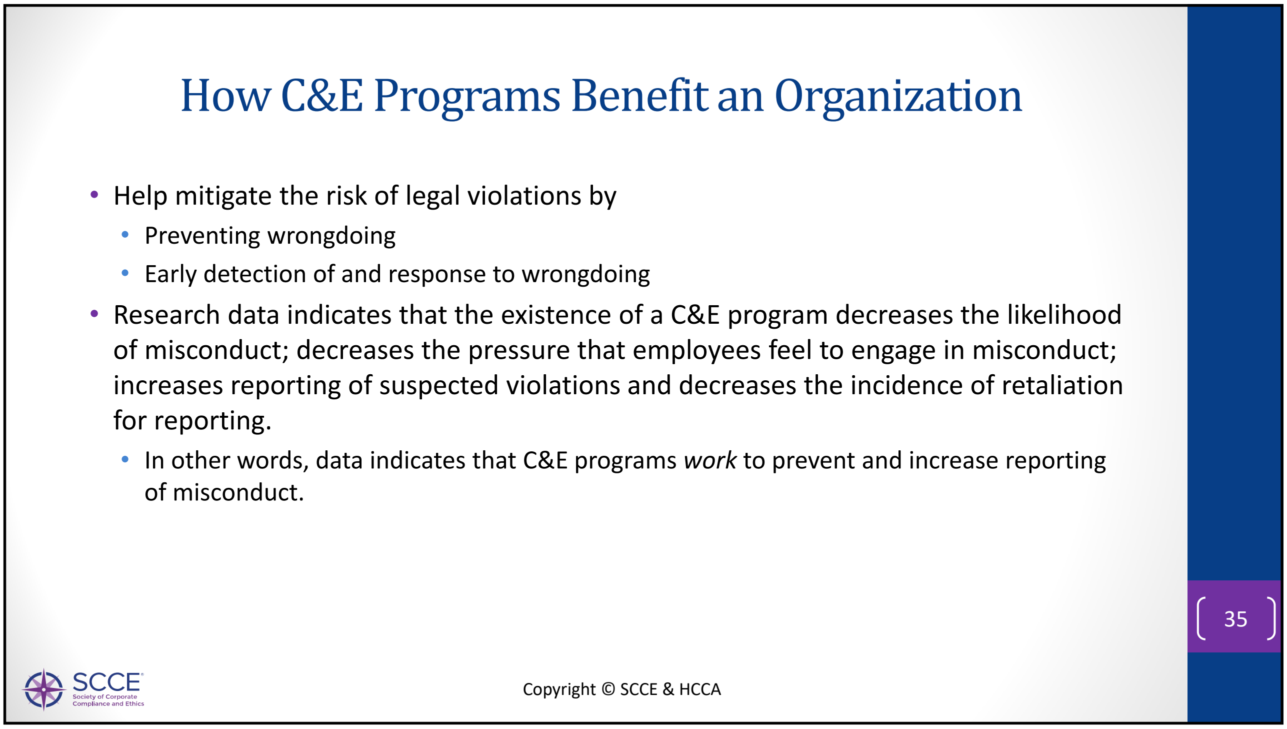
32

32

Culture of C&E

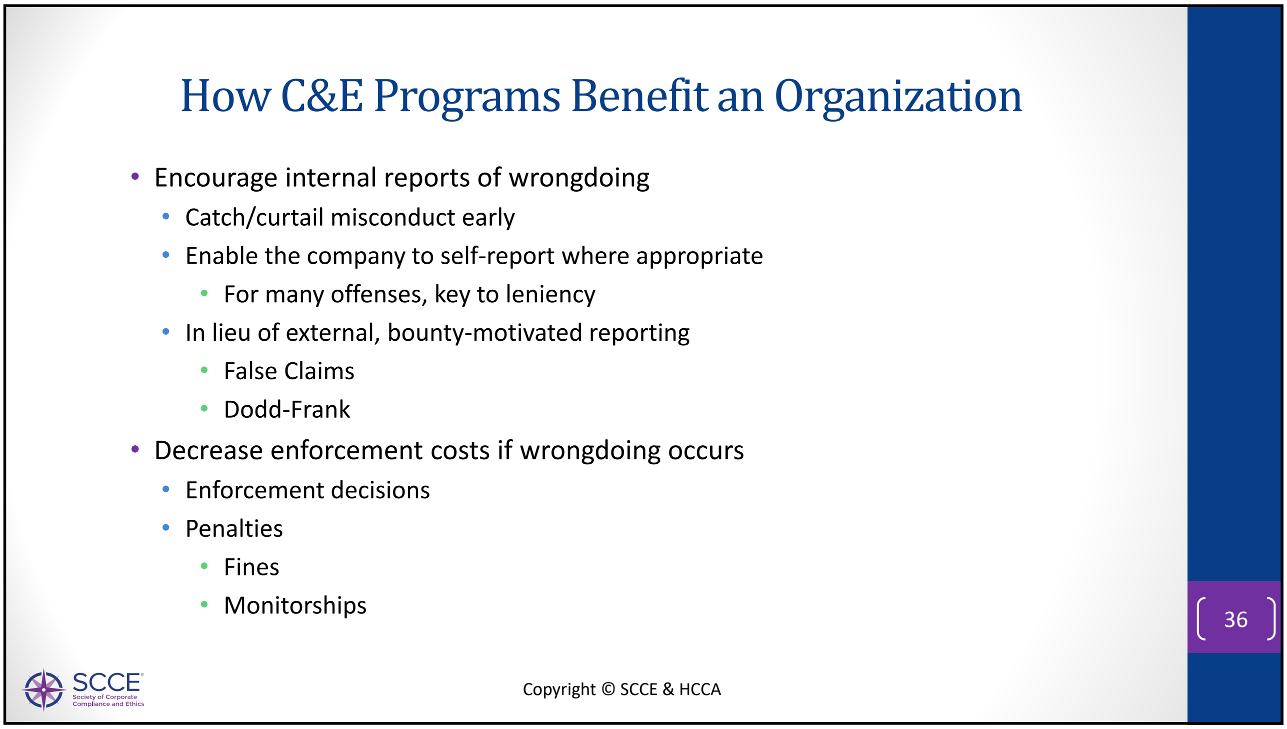
- USSG
  - Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.
- DOJ Evaluation Guidance
  - How often and how does the company measure its culture of compliance?
  - Does the company seek input from all levels of employees to determine whether 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?

HOW C&E PROGRAMS BENEFIT AN ORGANIZATION



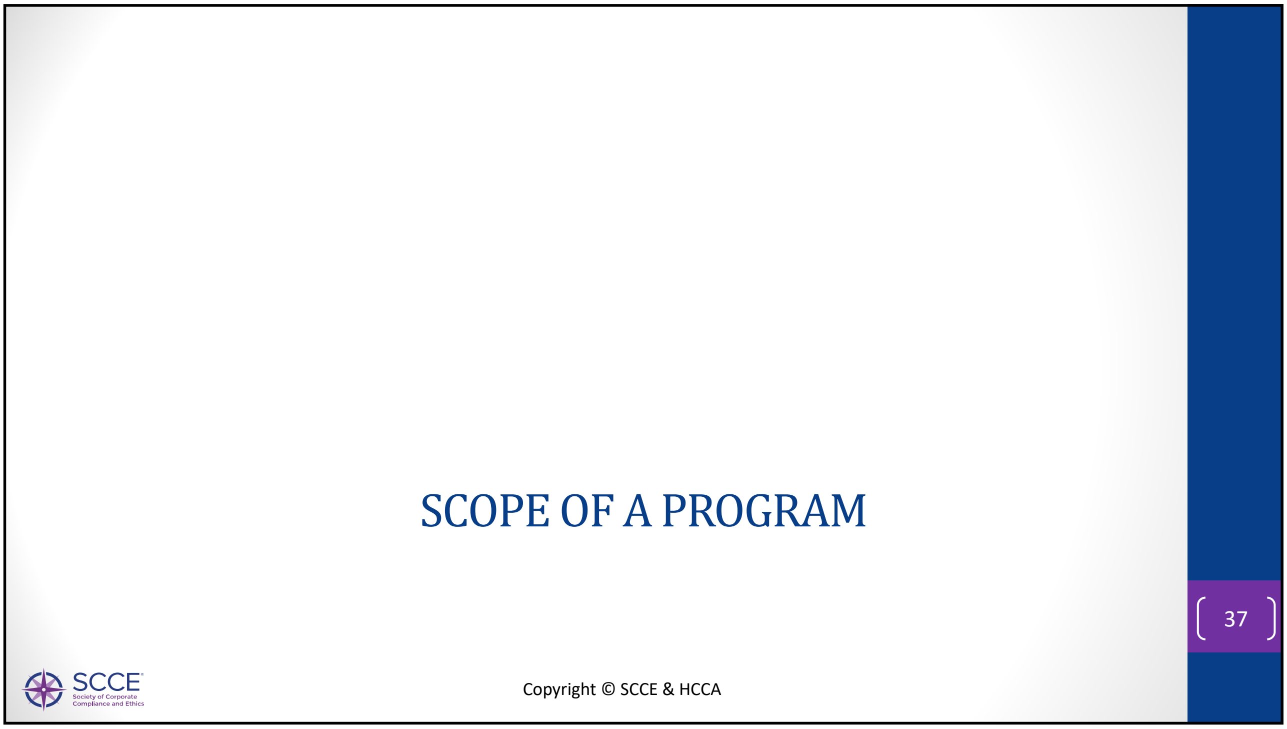
How C&E Programs Benefit an Organization

- Help mitigate the risk of legal violations by
  - Preventing wrongdoing
  - Early detection of and response to wrongdoing
- Research data indicates that the existence of a C&E program decreases the likelihood of misconduct; decreases the pressure that employees feel to engage in misconduct; increases reporting of suspected violations and decreases the incidence of retaliation for reporting.
  - In other words, data indicates that C&E programs *work* to prevent and increase reporting of misconduct.

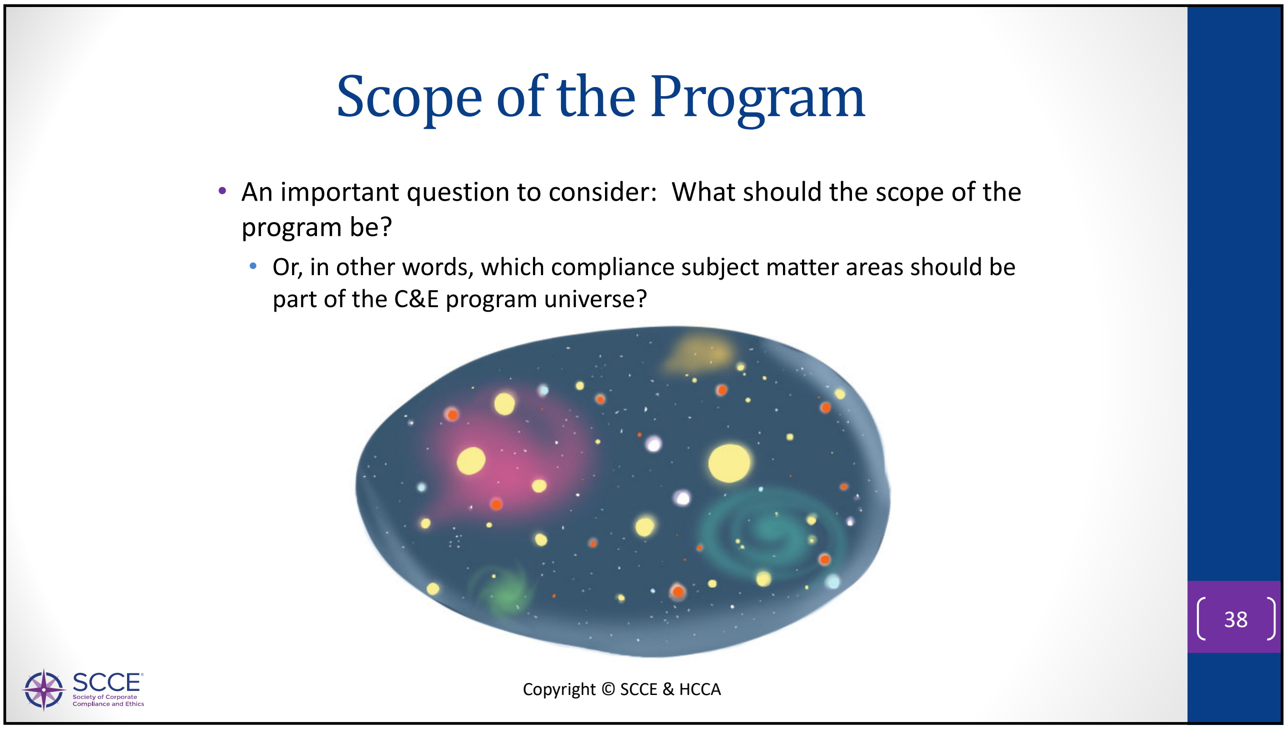


How C&E Programs Benefit an Organization

- 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

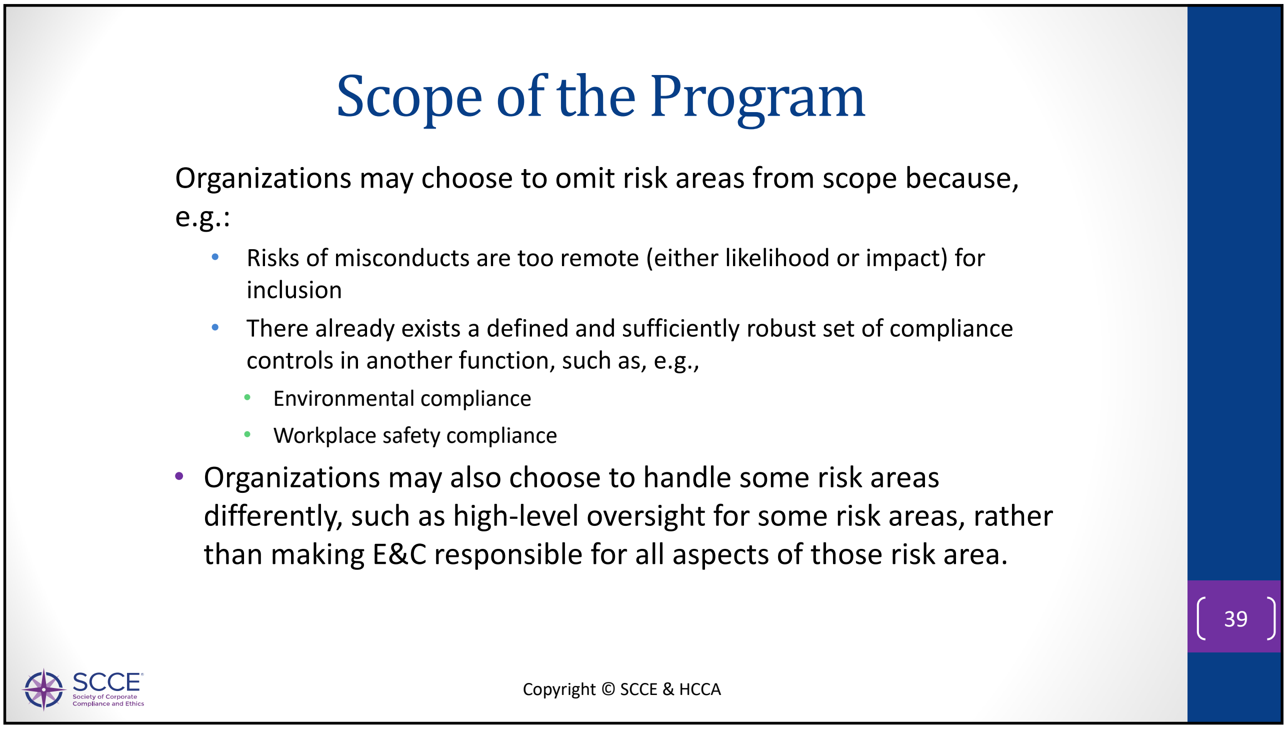


SCOPE OF A PROGRAM



Scope of the Program

- An important question to consider: What should the scope of the program be?
  - Or, in other words, which compliance subject matter areas should be part of the C&E program universe?



Scope of the Program

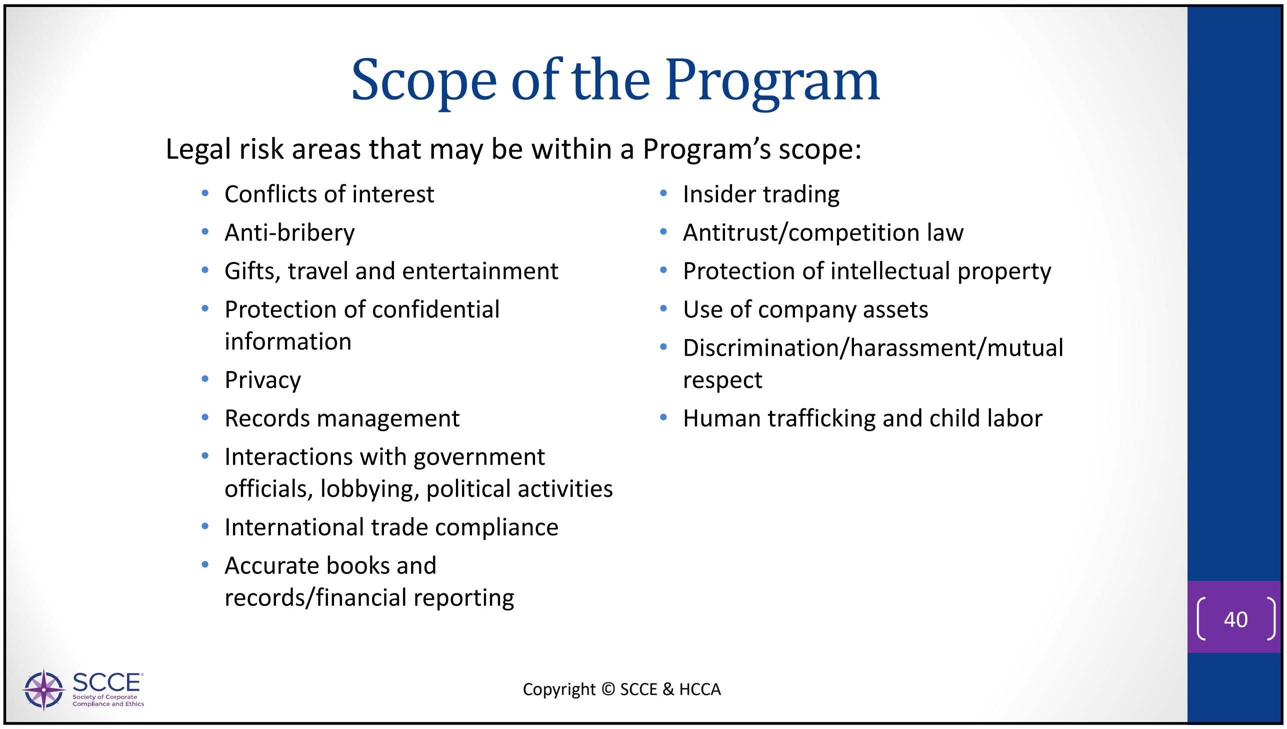
Organizations may choose to omit risk areas from scope because, e.g.:

- Risks of misconducts are too remote (either likelihood or impact) for inclusion
- There already exists a defined and sufficiently robust set of compliance controls in another function, such as, e.g.,
  - Environmental compliance
  - Workplace safety compliance

- Organizations may also choose to handle some risk areas differently, such as high-level oversight for some risk areas, rather than making E&C responsible for all aspects of those risk area.

39

39



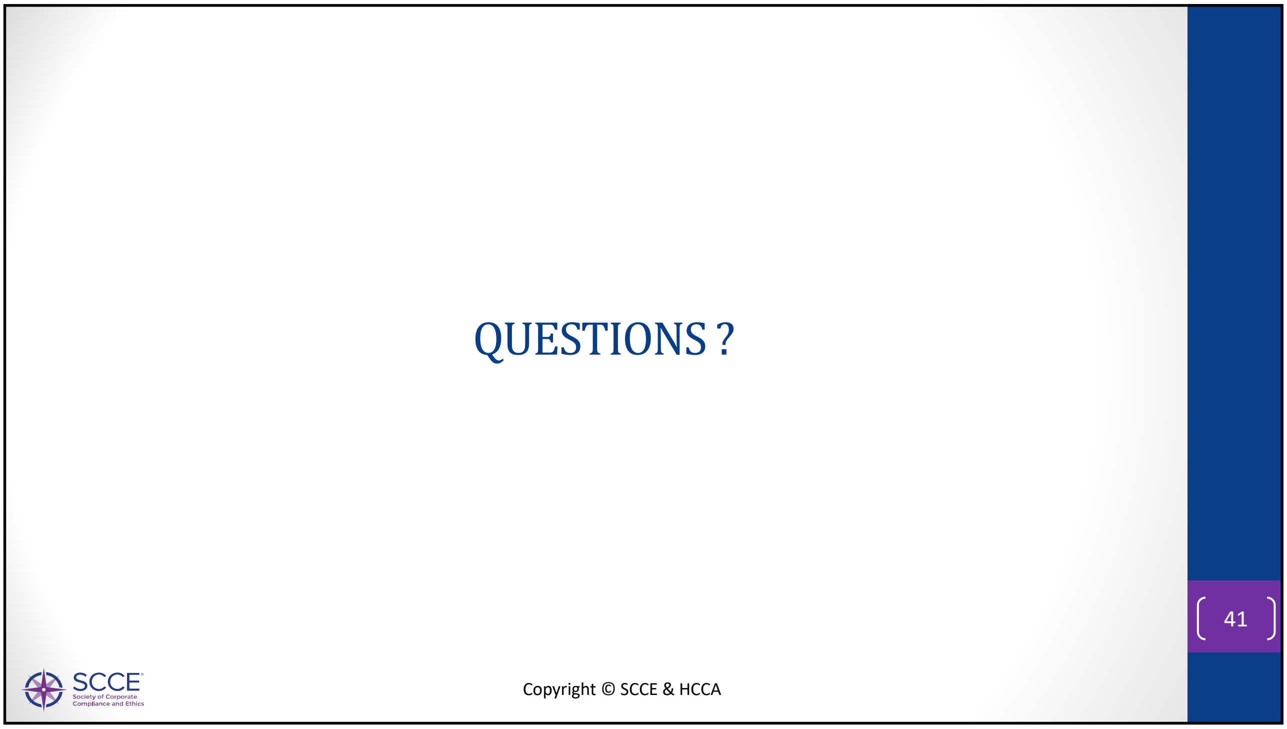
Scope of the Program

Legal risk areas that may be within a Program's 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

40

40



QUESTIONS ?

41

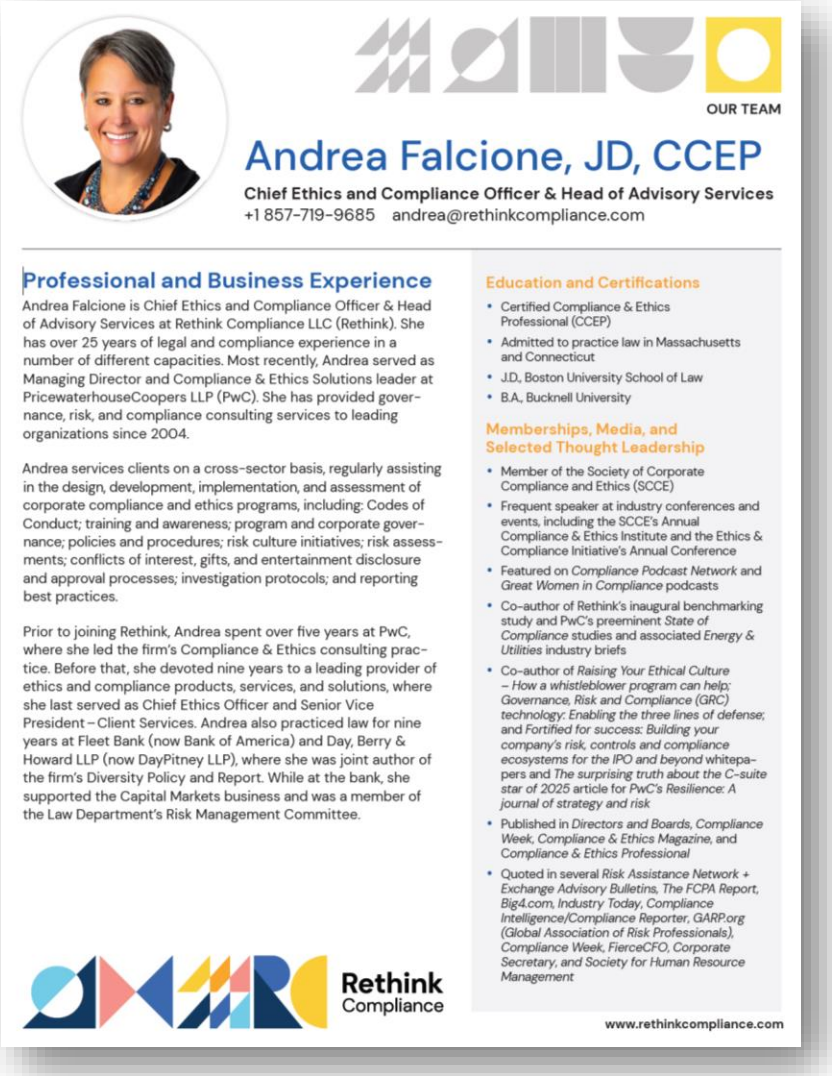
SCCE Compliance & Ethics Essentials Workshop

Standards and Procedures (Element no. 1)

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

SCCE Society of Corporate Compliance and Ethics

What we will cover today

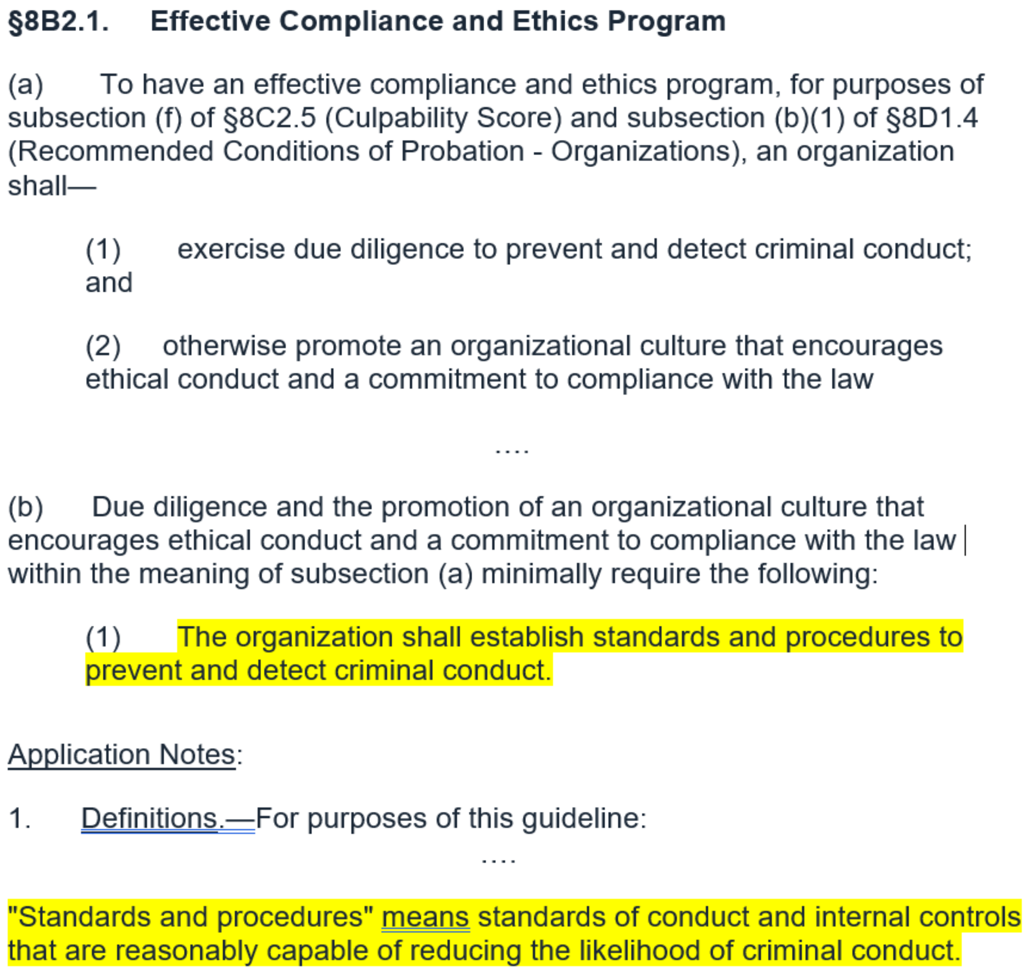
- Standards and Procedures (Element No. 1): 2 min.
- Code of Ethics / Conduct: 35 min.
- Policies v. procedures: 20 min.
- Structural v. substantive: 5 min.
- Format, style, references, etc.: 3 min.
- Documentation for each element of a CEP: 10 min.
- From policies / procedures to a culture of compliance: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

2 minutes

STANDARDS AND PROCEDURES (ELEMENT NO. 1)

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:

(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

This Photo by Unknown Author is licensed under CC BY-SA-NC

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 ….

This Photo by Unknown Author is licensed under CC BY-NC-ND

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.

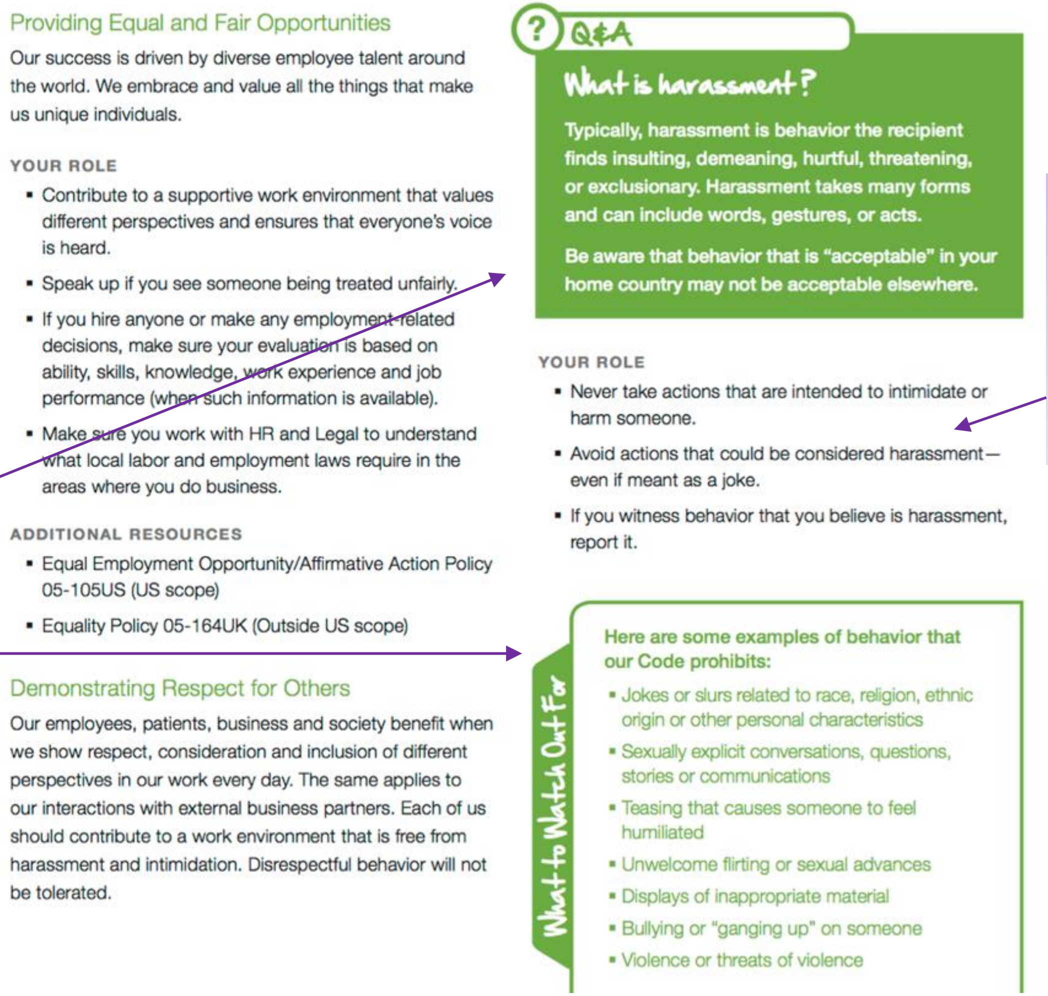
We will never take illegal or unethical actions, even if it helps us win.

Here are some key concepts....

SCCE Society of Corporate Compliance and Ethics

A better example

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



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

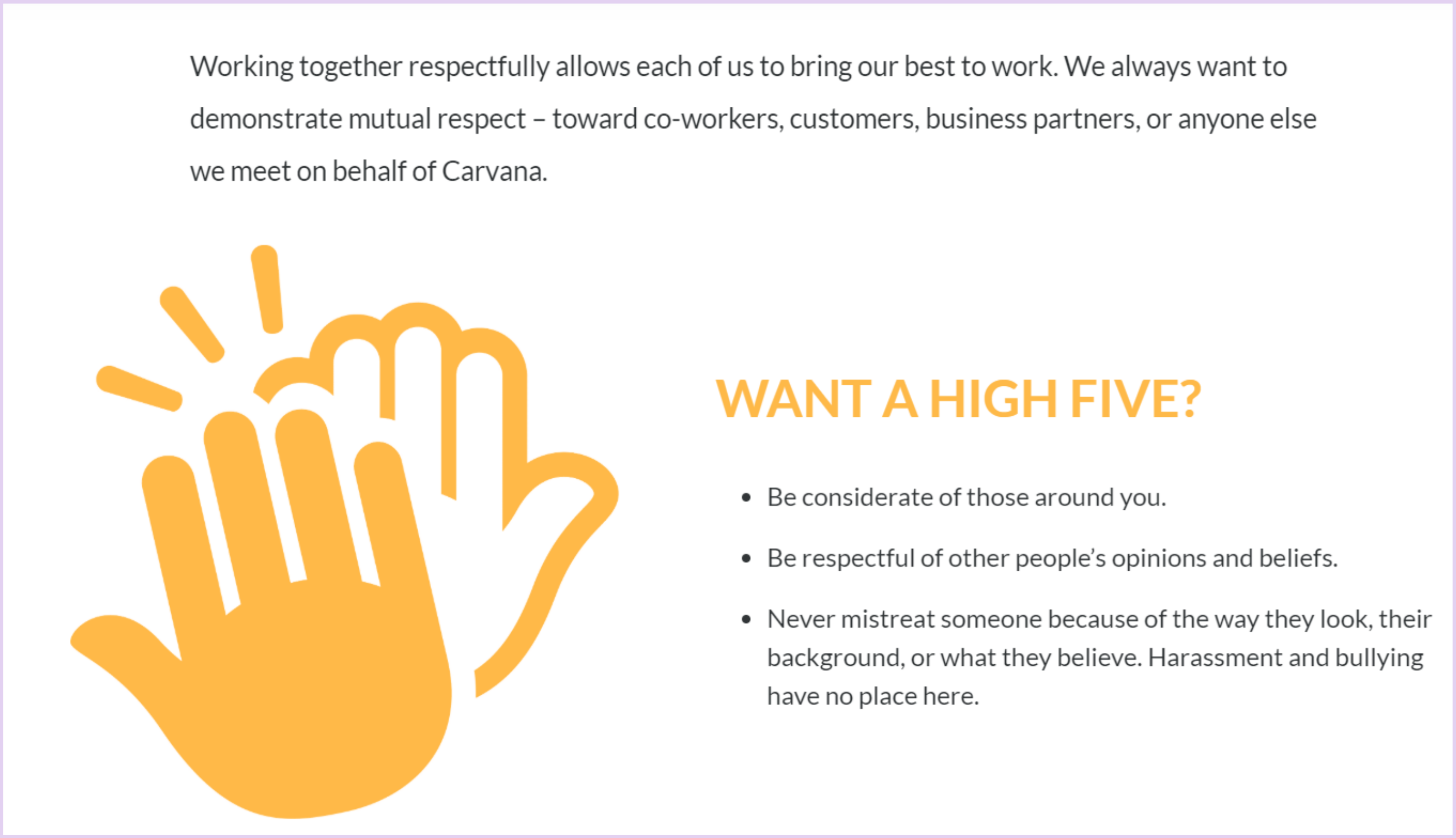
Here are some examples of behavior that our Code prohibits:

- 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.

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

An even better example



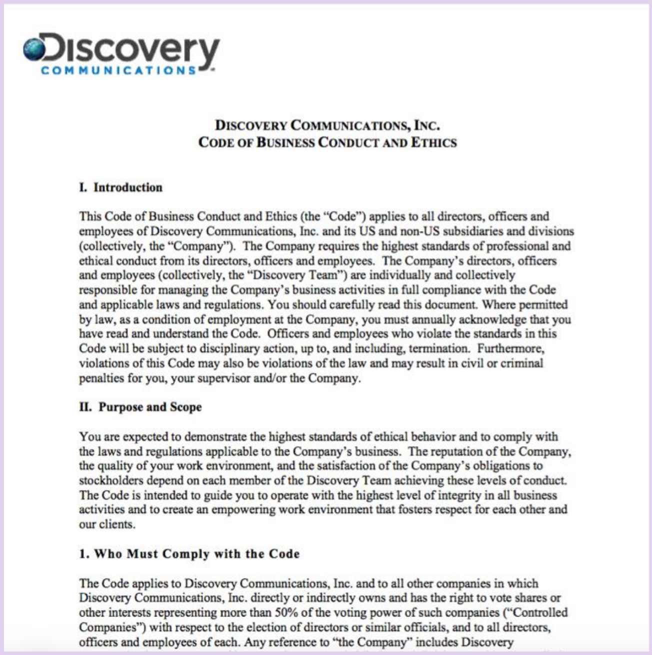
Working together respectfully allows each of us to bring our best to work. We always want to demonstrate mutual respect – toward co-workers, customers, business partners, or anyone else we meet on behalf of Carvana.

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

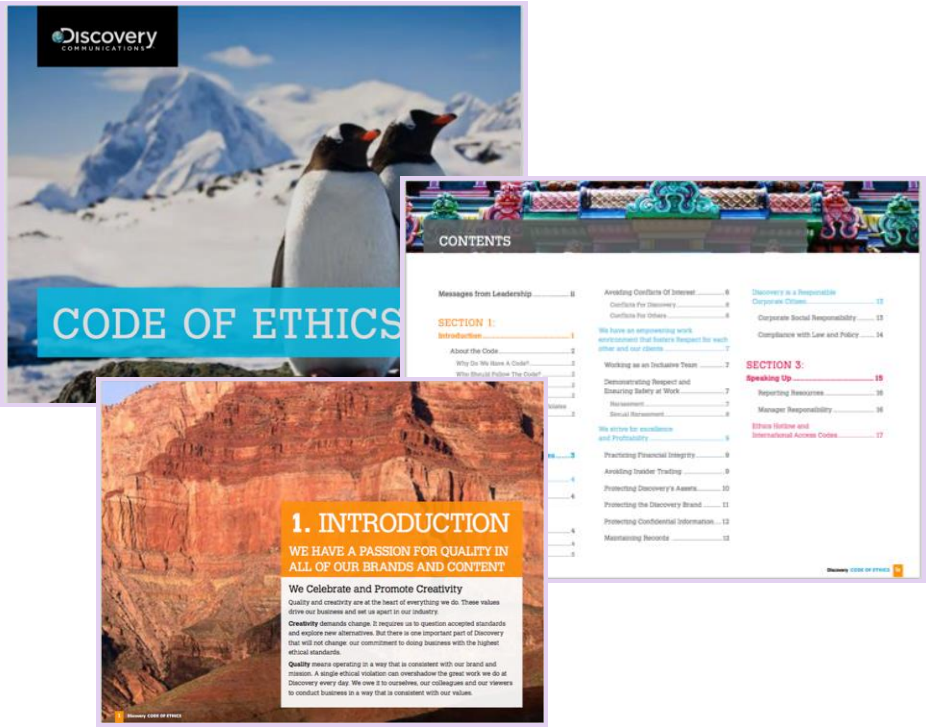
This Code of Business Conduct and Ethics (the "Code") applies to all directors, officers and employees of Discovery Communications, Inc. and its US and non-US subsidiaries and divisions (collectively, the "Company"). The Company requires the highest standards of professional and ethical conduct from 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



CODE OF ETHICS

CONTENTS

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.

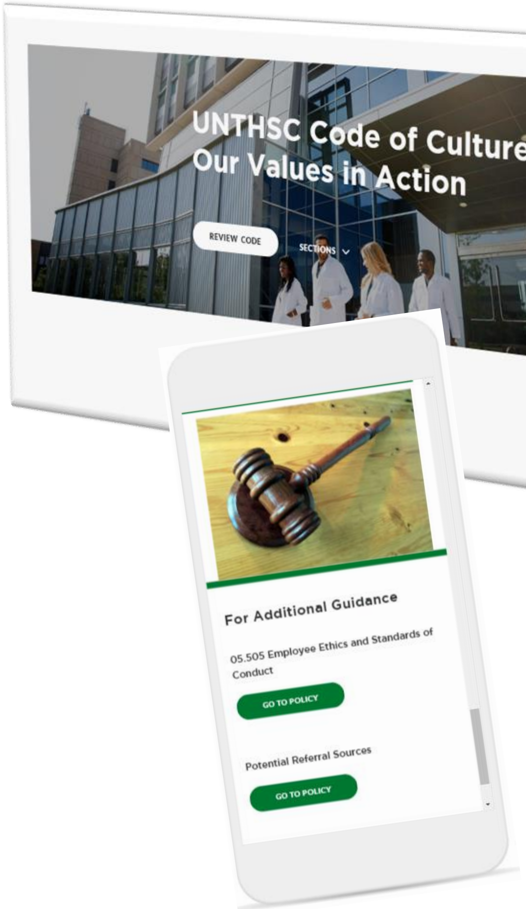
Creativity demands change. It requires us to question accepted standards and explore new alternatives. But there is one important part of Discovery that will not change: our commitment to doing business with the highest ethical standards.

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



UNTHSC Code of Culture: Our Values in Action

For Additional Guidance

05.505 Employee Ethics and Standards of Conduct

Potential Referral Sources

Succeeding Together

Our Guide to Ethical Business Conduct at Shion

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

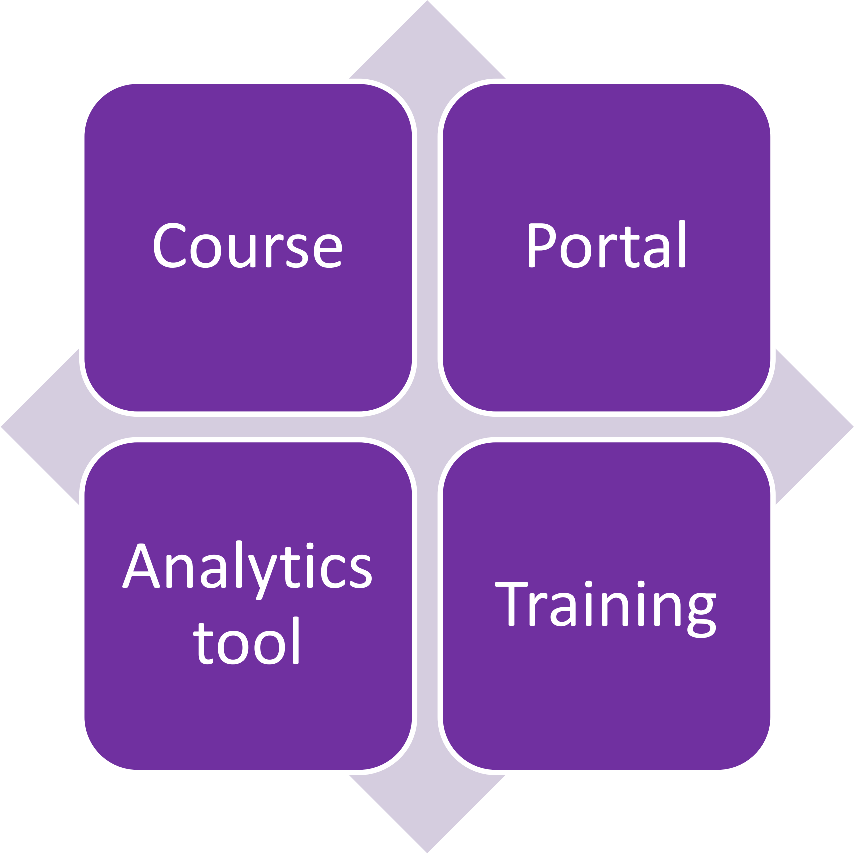
All this = competition for ANY content, including our Code of Ethics / Conduct

This Photo by Unknown Author is licensed under CC BY-NC-ND

How has our audience changed?

SCCE Society of Corporate Compliance and Ethics

Additional benefits



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

This Photo by Unknown Author is licensed under CC BY

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

This Photo by Unknown Author is licensed under CC BY-SA

The current state of affairs …

Leading practices

What are your expectations for accountability???

Leading practices (cont.)

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

SCCE Society of Corporate Compliance and Ethics

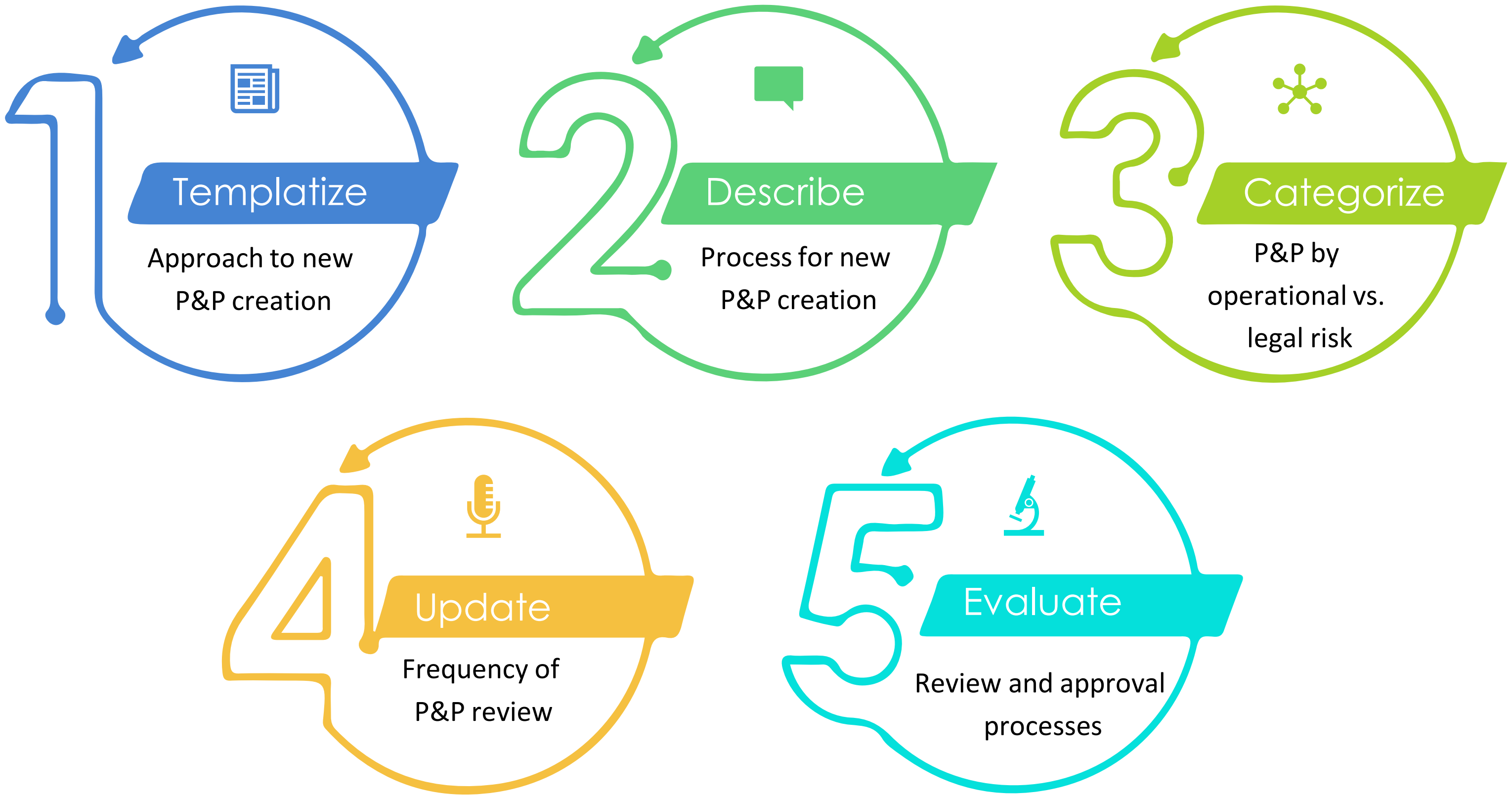
Leading practices (cont.)

Remember: shorter is better!

This Photo by Unknown Author is licensed under CC BY-NC

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.)

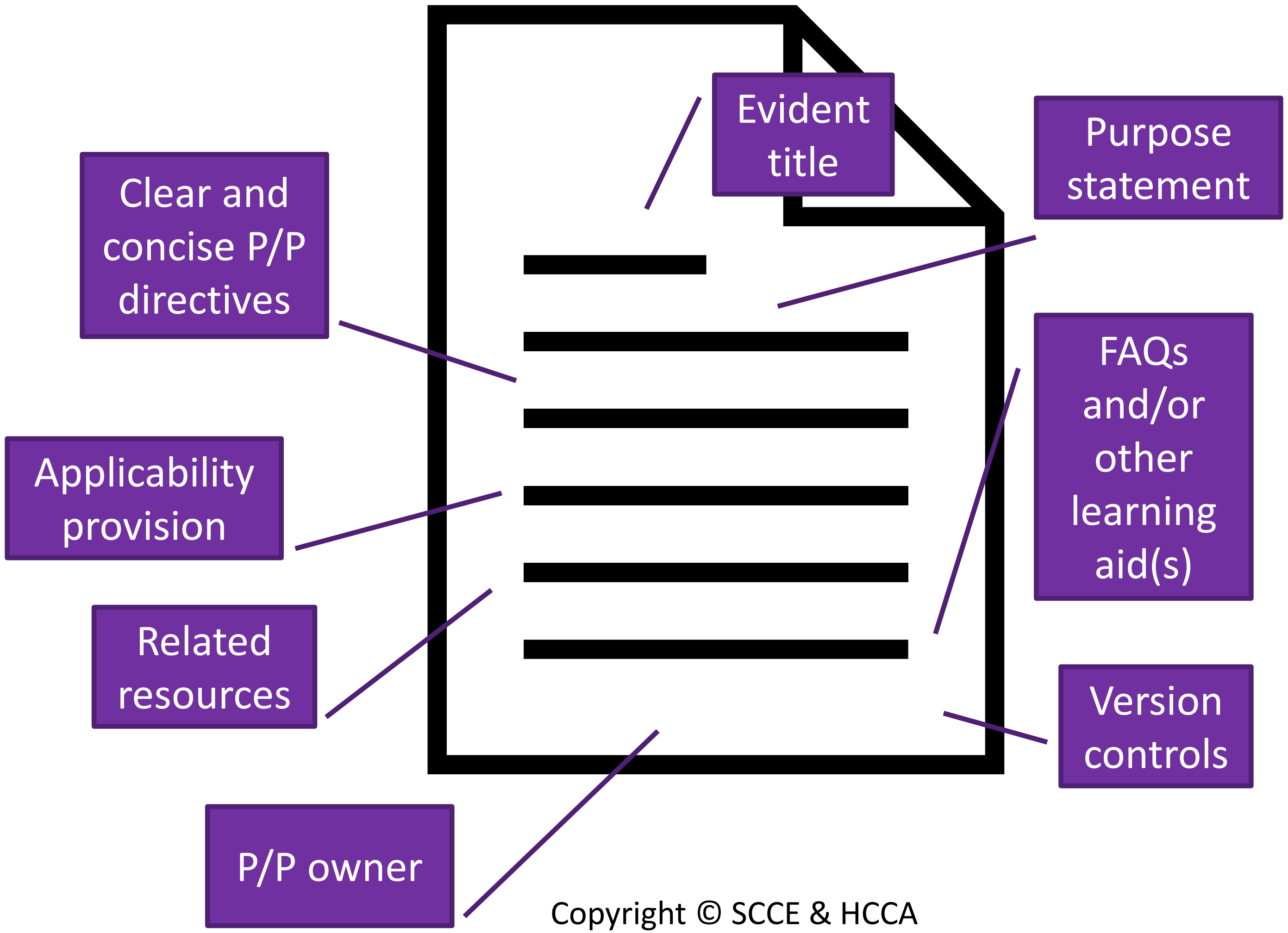
Important elements of P&P management

- 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



Evident title

Purpose statement

Clear and concise P/P directives

FAQs and/or other learning aid(s)

Applicability provision

Related resources

Version controls

P/P owner

3 minutes

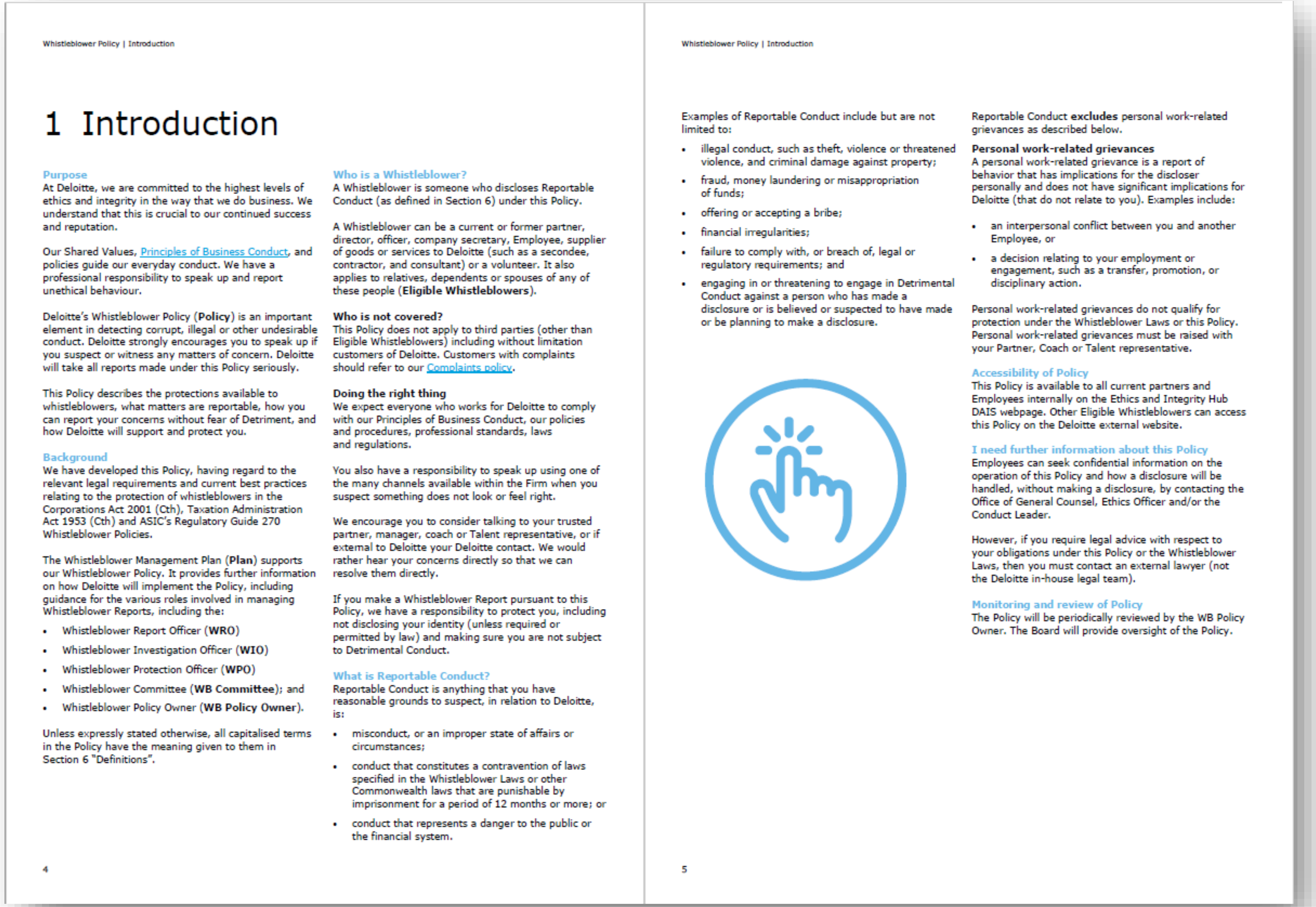
FORMAT, STYLE, REFERENCES, ETC.

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.

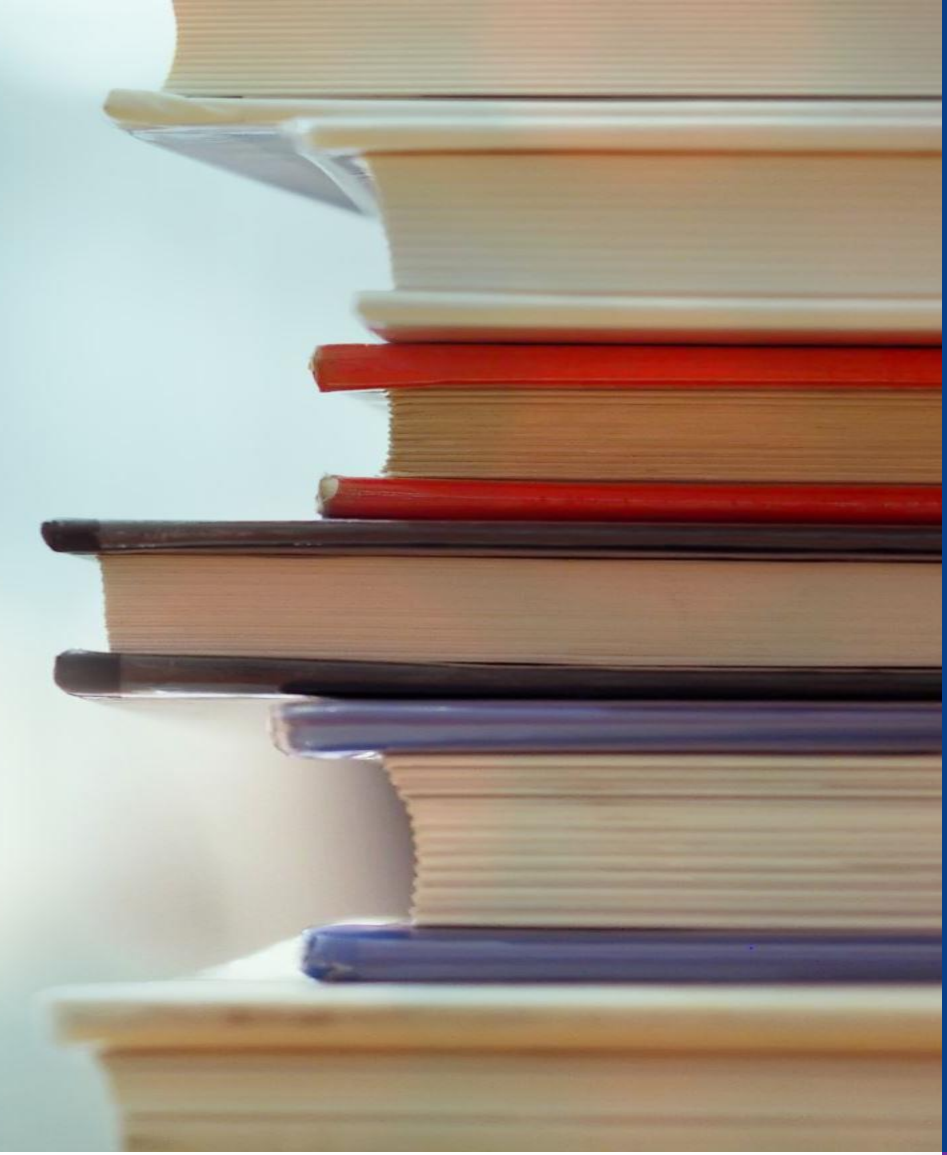
I need further information about this Policy

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

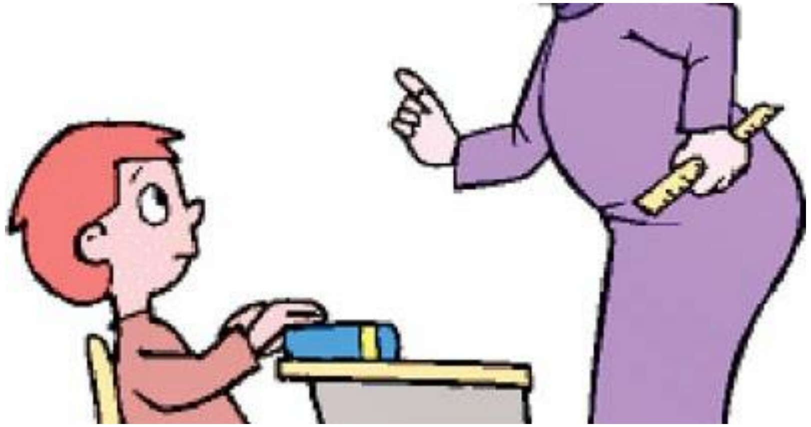
DOCUMENTATION FOR EACH ELEMENT OF A CEP

Why document?

This Photo by Unknown Author is licensed under CC BY

This Photo by Unknown Author is licensed under CC BY-SA

This Photo by Unknown Author is licensed under CC BY-SA



This Photo by Unknown Author is licensed under CC BY-NC

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

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

Framing the issue

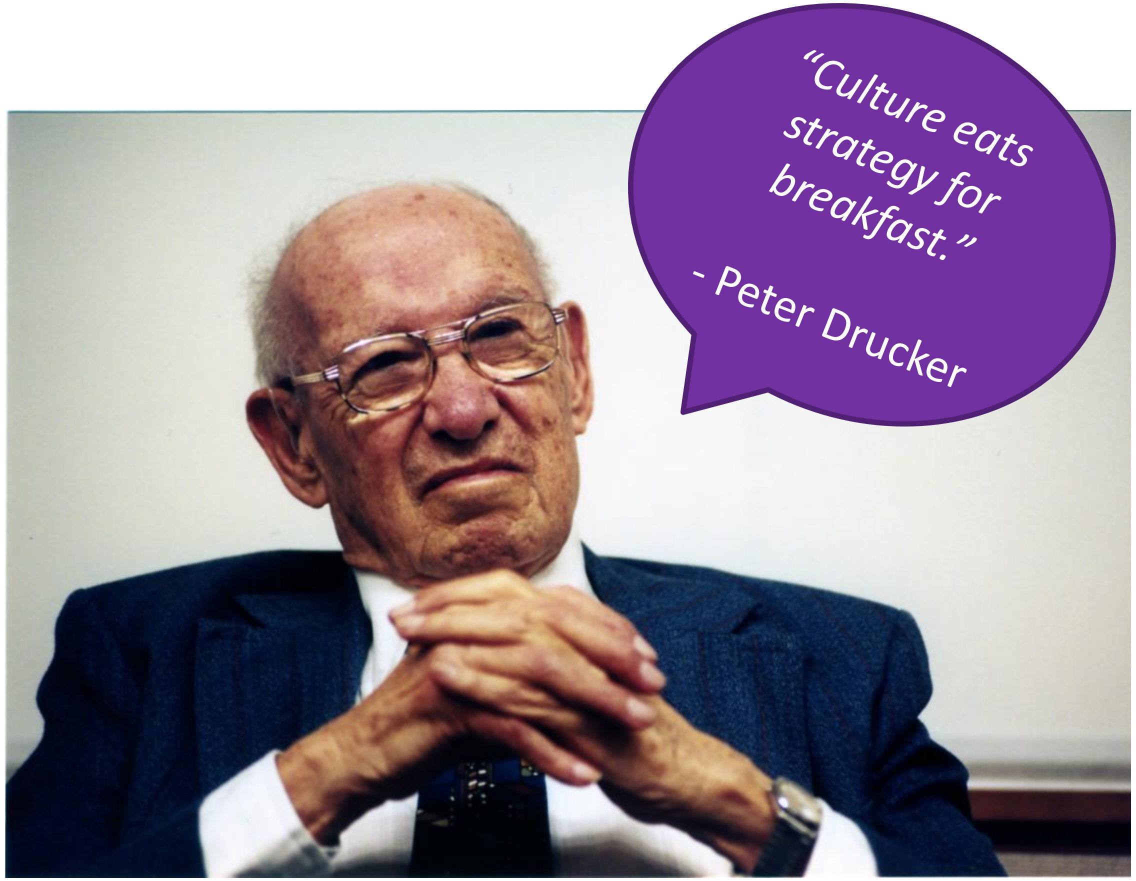
Policies and procedures

- 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



This Photo by Unknown Author is licensed under CC BY

This Photo by Unknown Author is licensed under CC BY-SA

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

This Photo by Unknown Author is licensed under CC BY-SA

How do we make decisions?

This Photo by Unknown Author is licensed under CC BY

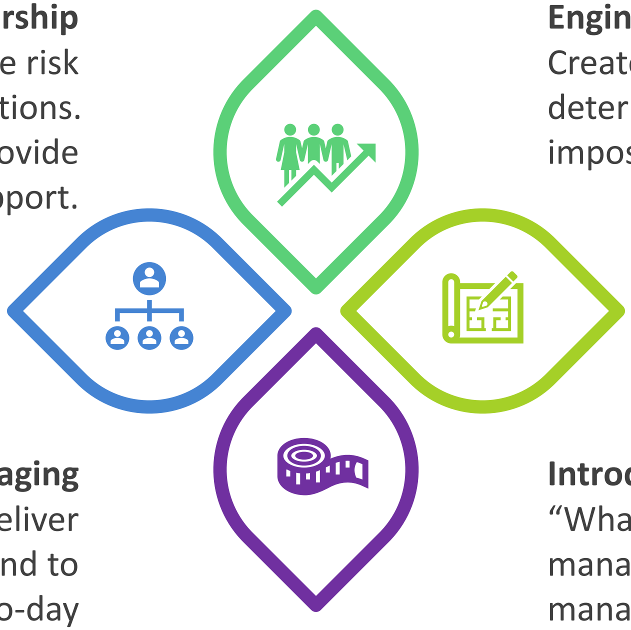
Milgram experiment

This Photo by Unknown Author is licensed under CC BY-SA-NC

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.

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

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

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).

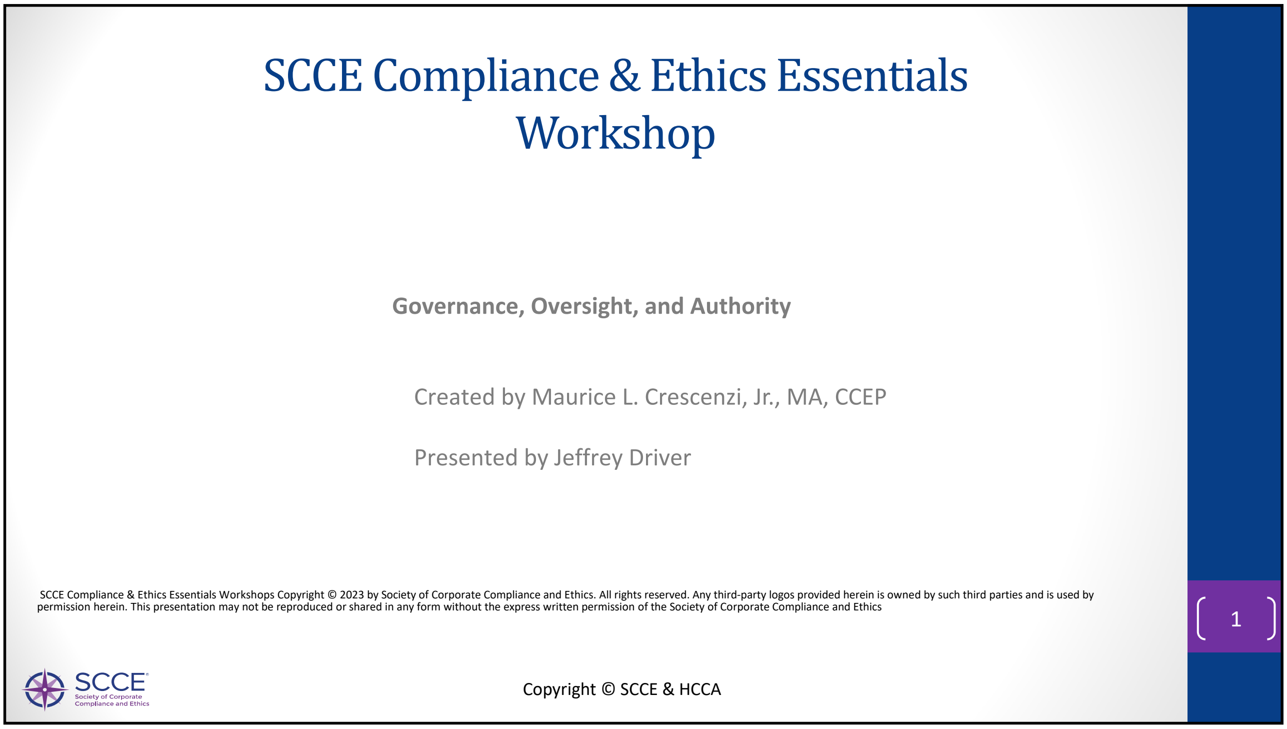
Use Key Messages
Once you know your audience, you can put your message in their terms.

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

Created by Maurice L. Crescenzi, Jr., MA, CCEP

Presented by Jeffrey Driver

1

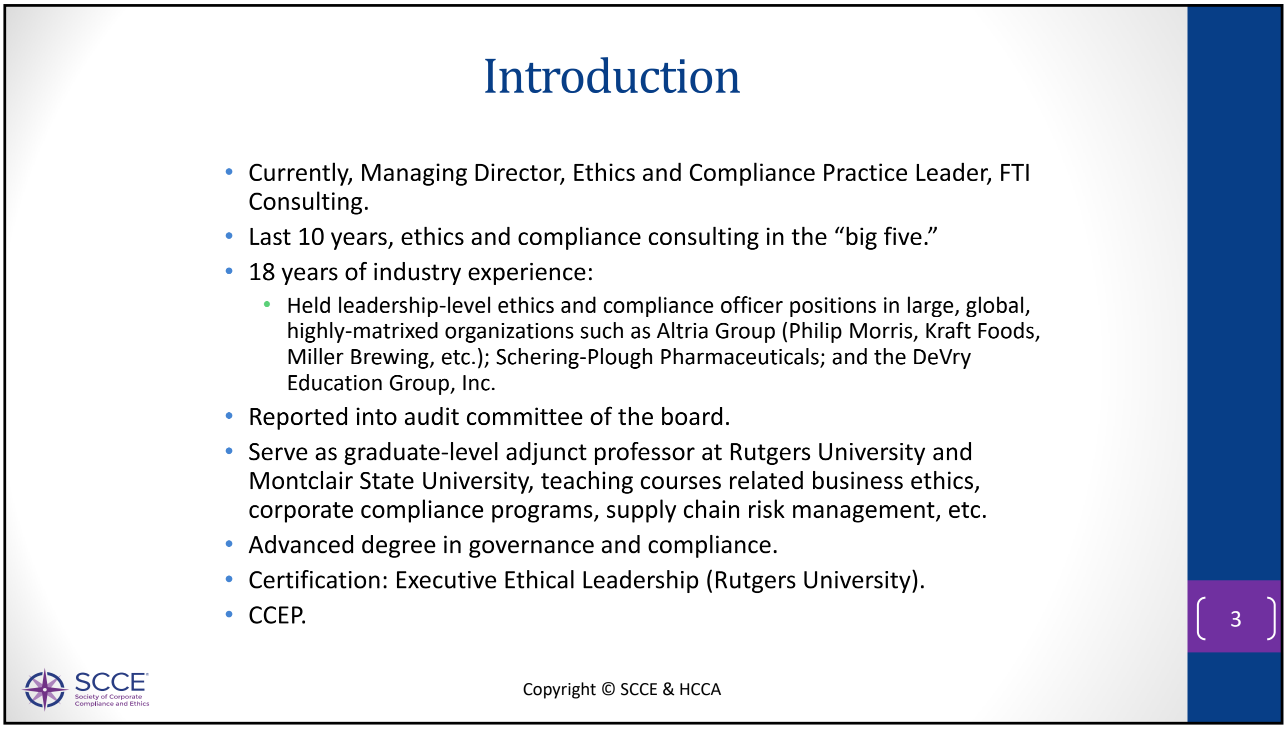
1

Agenda / Table of Contents

- Introduction
- Learning objectives
- Corporations
  - History of corporations
  - Basic structure
  - Paradigm shift – command and control to stakeholder engagement
- Compliance oversight
  - Board
  - Compliance leadership
  - Day-to-day compliance management
- Key take-aways
- Q&A

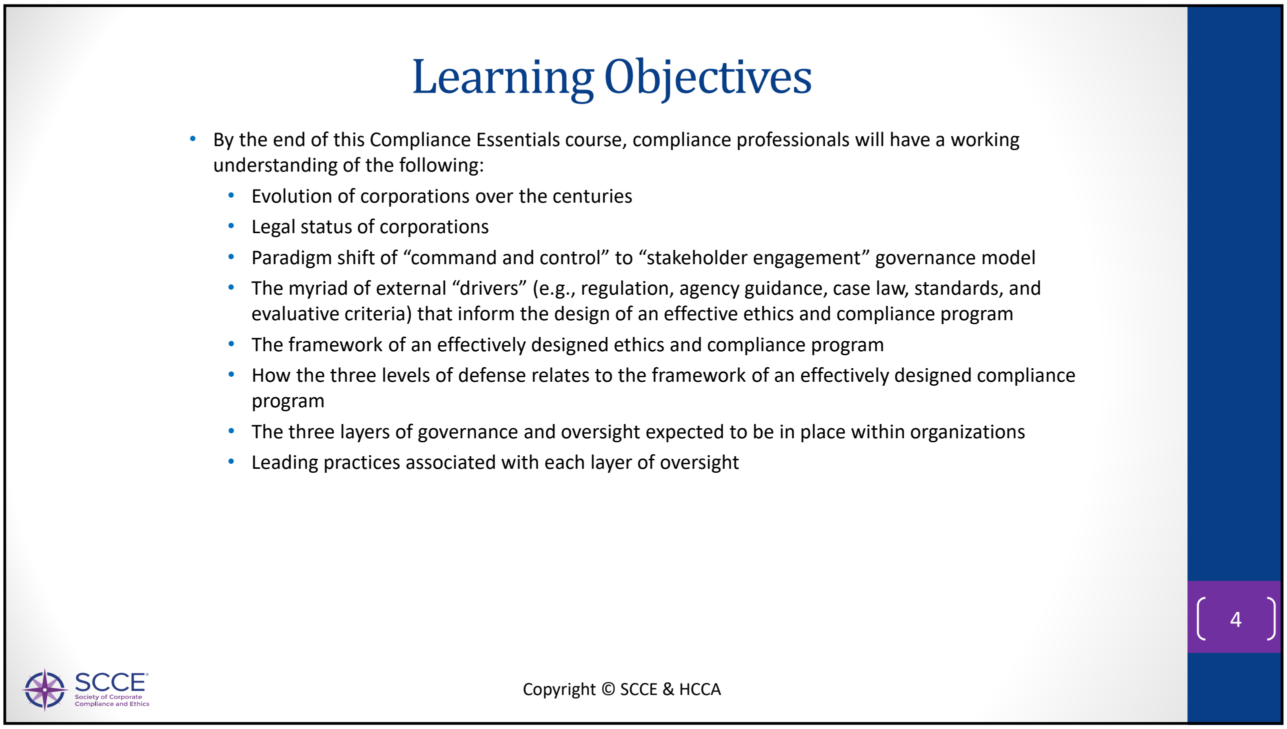
2

2



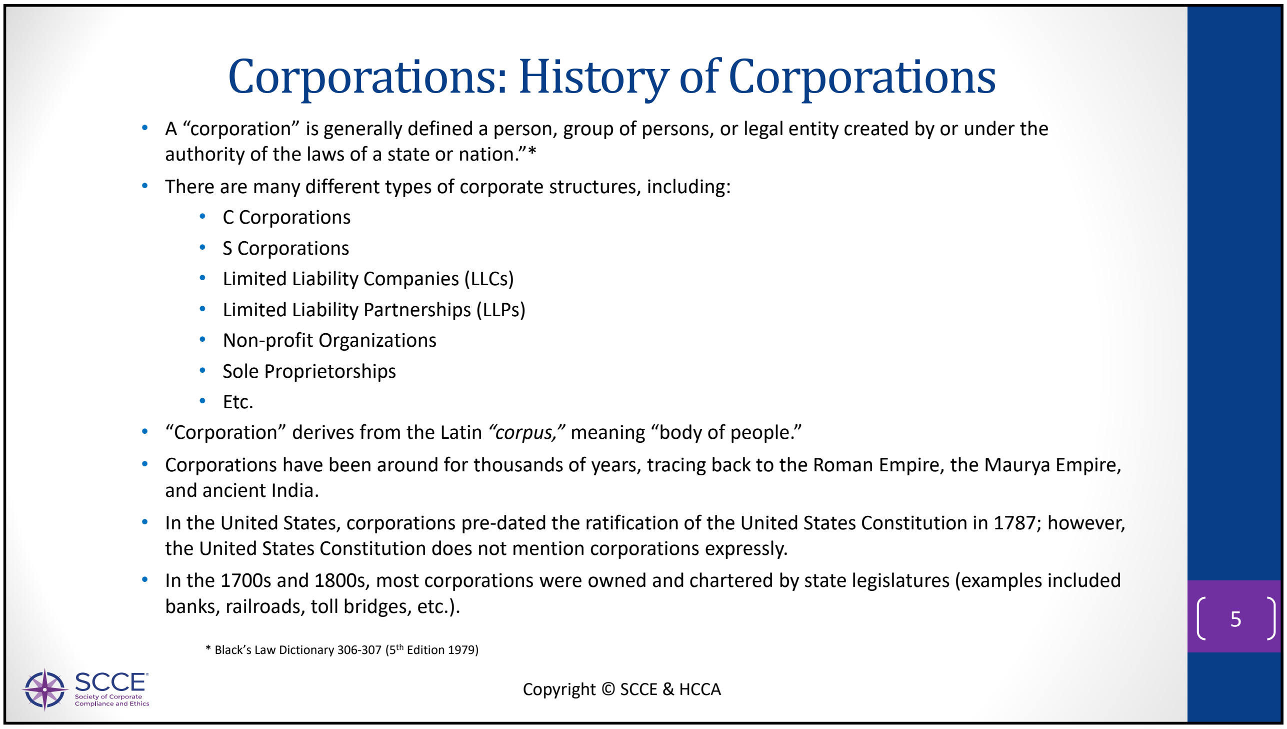
Introduction

- Currently, Managing Director, Ethics and Compliance Practice Leader, FTI Consulting.
- Last 10 years, ethics and compliance consulting in the "big five."
- 18 years of industry experience:
  - Held leadership-level ethics and compliance officer positions in large, global, highly-matrixed organizations such as Altria Group (Philip Morris, Kraft Foods, Miller Brewing, etc.); Schering-Plough Pharmaceuticals; and the DeVry Education Group, Inc.
- Reported into audit committee of the board.
- Serve as graduate-level adjunct professor at Rutgers University and Montclair State University, teaching courses related business ethics, corporate compliance programs, supply chain risk management, etc.
- Advanced degree in governance and compliance.
- Certification: Executive Ethical Leadership (Rutgers University).
- CCEP.



Learning Objectives

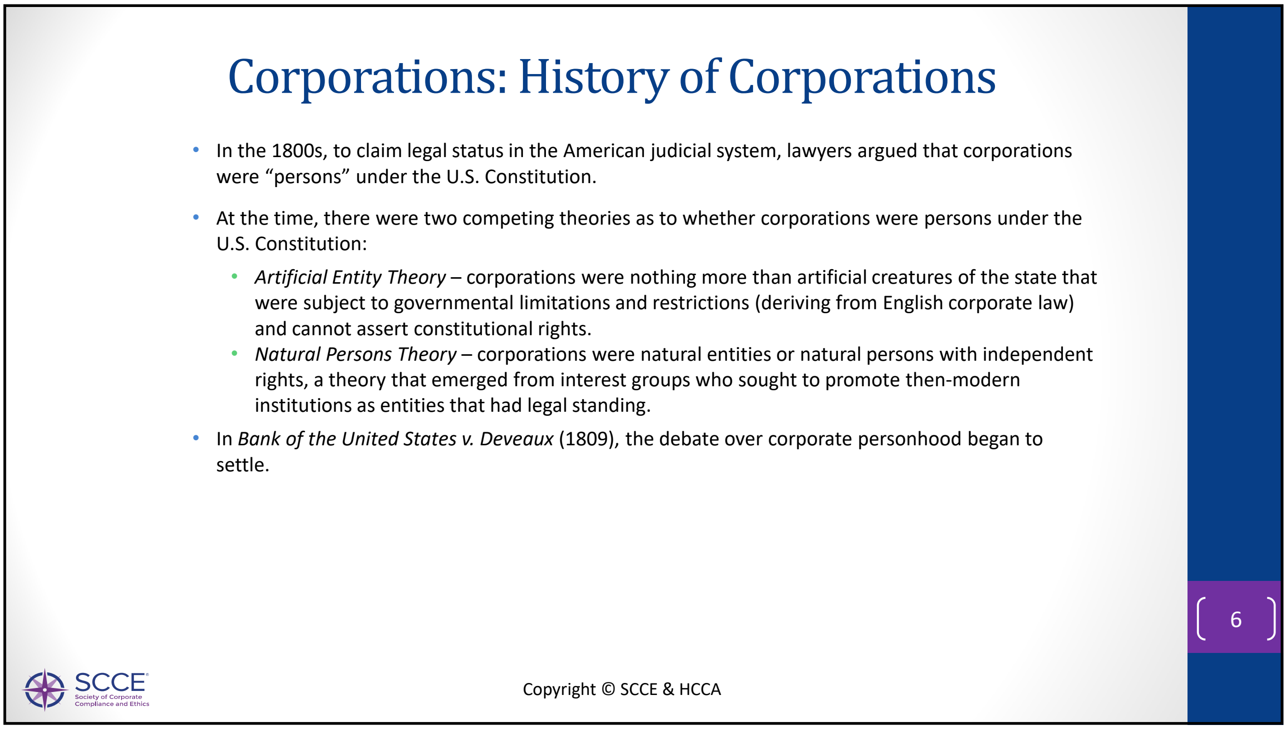
- By the end of this Compliance Essentials course, compliance professionals will have a working understanding of the following:
  - Evolution of corporations over the centuries
  - Legal status of corporations
  - Paradigm shift of "command and control" to "stakeholder engagement" governance model
  - The myriad of external "drivers" (e.g., regulation, agency guidance, case law, standards, and evaluative criteria) that inform the design of an effective ethics and compliance program
  - The framework of an effectively designed ethics and compliance program
  - How the three levels of defense relates to the framework of an effectively designed compliance program
  - The three layers of governance and oversight expected to be in place within organizations
  - Leading practices associated with each layer of oversight



Corporations: History of Corporations

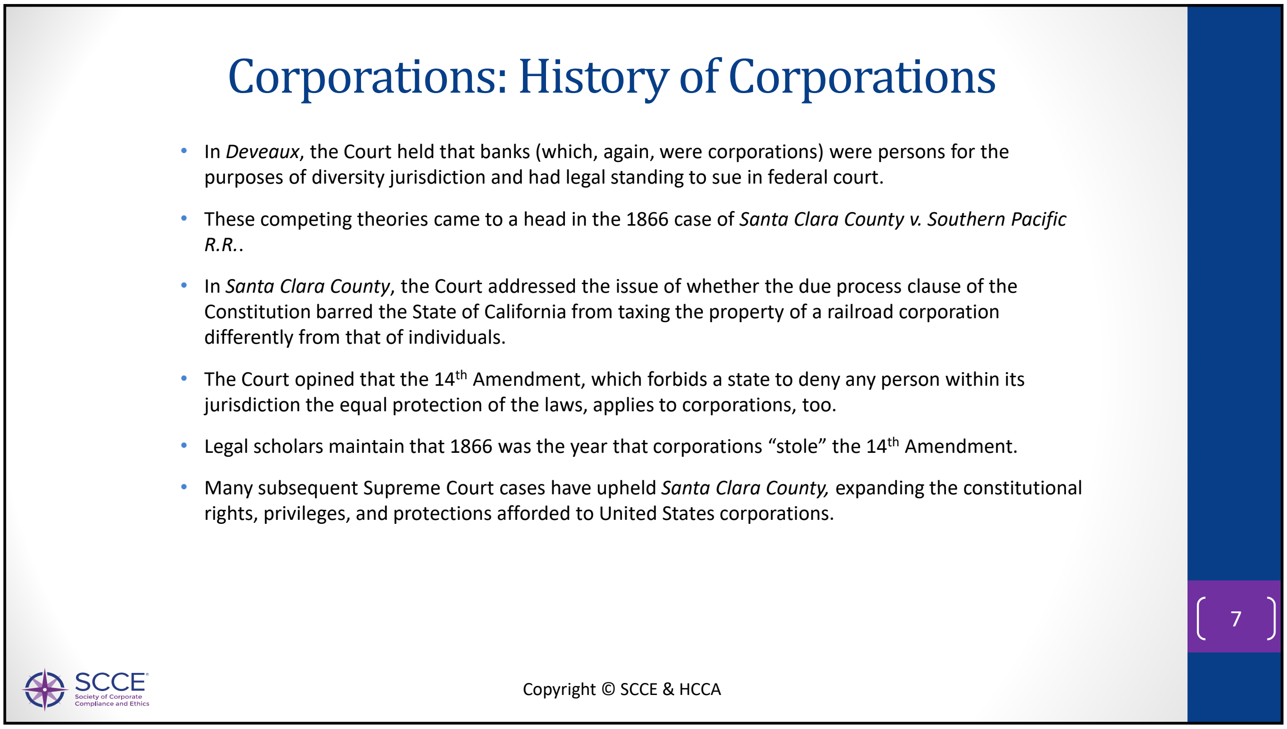
- A "corporation" is generally defined a person, group of persons, or legal entity created by or under the authority of the laws of a state or nation."*
- There are many different types of corporate structures, including:
  - C Corporations
  - S Corporations
  - Limited Liability Companies (LLCs)
  - Limited Liability Partnerships (LLPs)
  - Non-profit Organizations
  - Sole Proprietorships
  - Etc.
- "Corporation" derives from the Latin *"corpus,"* meaning "body of people."
- Corporations have been around for thousands of years, tracing back to the Roman Empire, the Maurya Empire, and ancient India.
- In the United States, corporations pre-dated the ratification of the United States Constitution in 1787; however, the United States Constitution does not mention corporations expressly.
- In the 1700s and 1800s, most corporations were owned and chartered by state legislatures (examples included banks, railroads, toll bridges, etc.).

* Black's Law Dictionary 306-307 (5th Edition 1979)



Corporations: History of Corporations

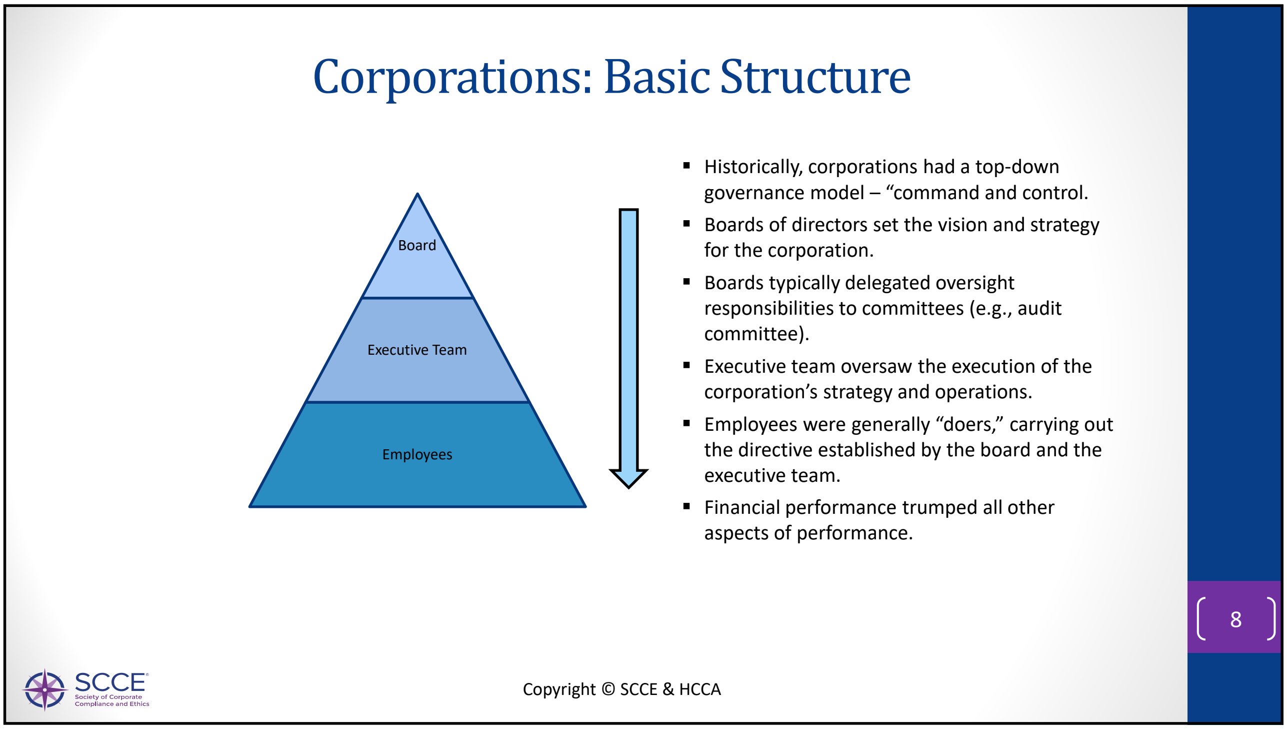
- In the 1800s, to claim legal status in the American judicial system, lawyers argued that corporations were "persons" under the U.S. Constitution.
- At the time, there were two competing theories as to whether corporations were persons under the U.S. Constitution:
  - *Artificial Entity Theory* – corporations were nothing more than artificial creatures of the state that were subject to governmental limitations and restrictions (deriving from English corporate law) and cannot assert constitutional rights.
  - *Natural Persons Theory* – corporations were natural entities or natural persons with independent rights, a theory that emerged from interest groups who sought to promote then-modern institutions as entities that had legal standing.
- In *Bank of the United States v. Deveaux* (1809), the debate over corporate personhood began to settle.



Corporations: History of Corporations

- In *Deveaux*, the Court held that banks (which, again, were corporations) were persons for the purposes of diversity jurisdiction and had legal standing to sue in federal court.
- These competing theories came to a head in the 1866 case of *Santa Clara County v. Southern Pacific R.R.*.
- In *Santa Clara County*, the Court addressed the issue of whether the due process clause of the Constitution barred the State of California from taxing the property of a railroad corporation differently from that of individuals.
- The Court opined that the 14th Amendment, which forbids a state to deny any person within its jurisdiction the equal protection of the laws, applies to corporations, too.
- Legal scholars maintain that 1866 was the year that corporations "stole" the 14th Amendment.
- Many subsequent Supreme Court cases have upheld *Santa Clara County,* expanding the constitutional rights, privileges, and protections afforded to United States corporations.

7

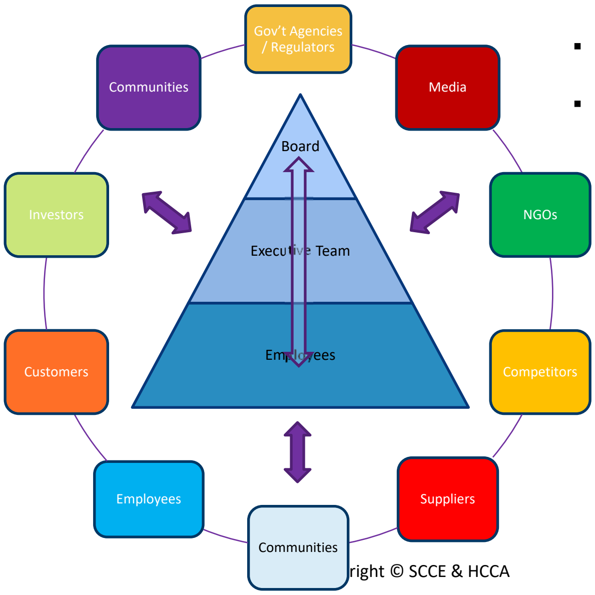


Corporations: Basic Structure

- Historically, corporations had a top-down governance model – "command and control.
- Boards of directors set the vision and strategy for the corporation.
- Boards typically delegated oversight responsibilities to committees (e.g., audit committee).
- Executive team oversaw the execution of the corporation's strategy and operations.
- Employees were generally "doers," carrying out the directive established by the board and the executive team.
- Financial performance trumped all other aspects of performance.

8

Corporations: Basic Structure



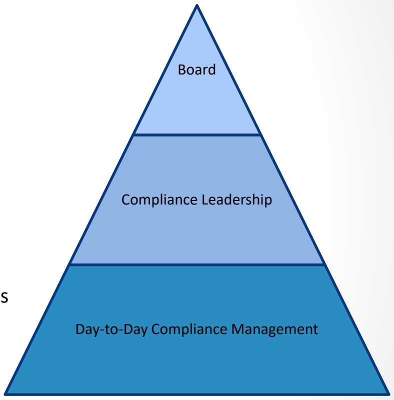
- Over time, the paradigm has shifted to a "stakeholder engagement" model.
- This shift is due to, among other factors:
  - Evolution of corporate personhood
  - Unions / workers' rights
  - Legislation / regulation
  - Globalization
  - Access to information / Internet
  - Technological advancements
  - Corporate scandals
  - Global enforcement and cooperation
  - Increased expectations of stakeholders
  - NGO activity

SCCE Society of Corporate Compliance and Ethics

right © SCCE & HCCA

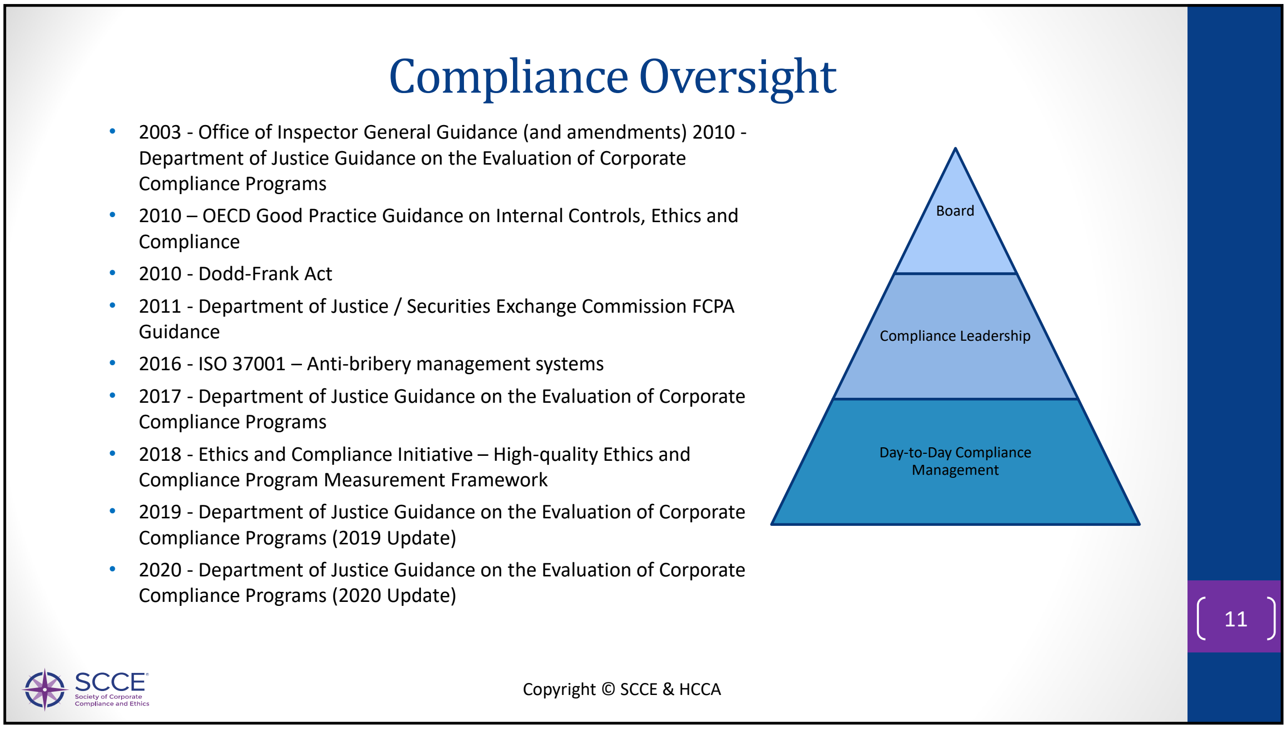
Compliance Oversight

- A wide variety of external drivers require or expect that an organization's compliance program will be overseen at three levels:
  - The governing authority level (typically the board or a board committee)
  - The executive level (e.g., a CCO, a compliance committee, etc.)
  - At the line manager level (e.g., risk owners, day-to-day compliance managers)
- These drivers include, but are not limited to, the following:
  - 1997 - Foreign Corrupt Practices Act (and related guidance)
  - 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)



SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA



Compliance Oversight

- 2003 - Office of Inspector General Guidance (and amendments) 2010 - Department of Justice Guidance on the Evaluation of Corporate Compliance Programs
- 2010 – OECD Good Practice Guidance on Internal Controls, Ethics and Compliance
- 2010 - Dodd-Frank Act
- 2011 - Department of Justice / Securities Exchange Commission FCPA Guidance
- 2016 - ISO 37001 – Anti-bribery management systems
- 2017 - Department of Justice Guidance on the Evaluation of Corporate Compliance Programs
- 2018 - Ethics and Compliance Initiative – High-quality Ethics and Compliance Program Measurement Framework
- 2019 - Department of Justice Guidance on the Evaluation of Corporate Compliance Programs (2019 Update)
- 2020 - Department of Justice Guidance on the Evaluation of Corporate Compliance Programs (2020 Update)

Board

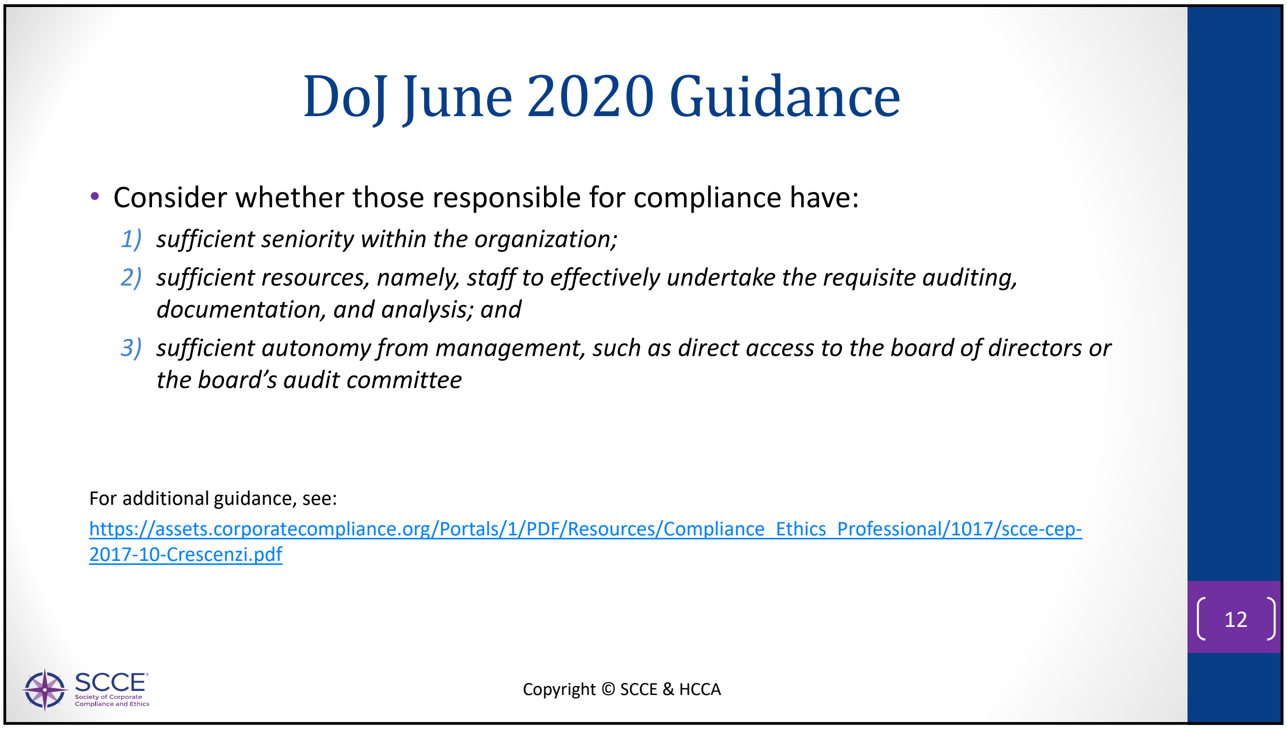
Compliance Leadership

Day-to-Day Compliance Management

11

SCCE Society of Corporate Compliance and Ethics

11



DoJ June 2020 Guidance

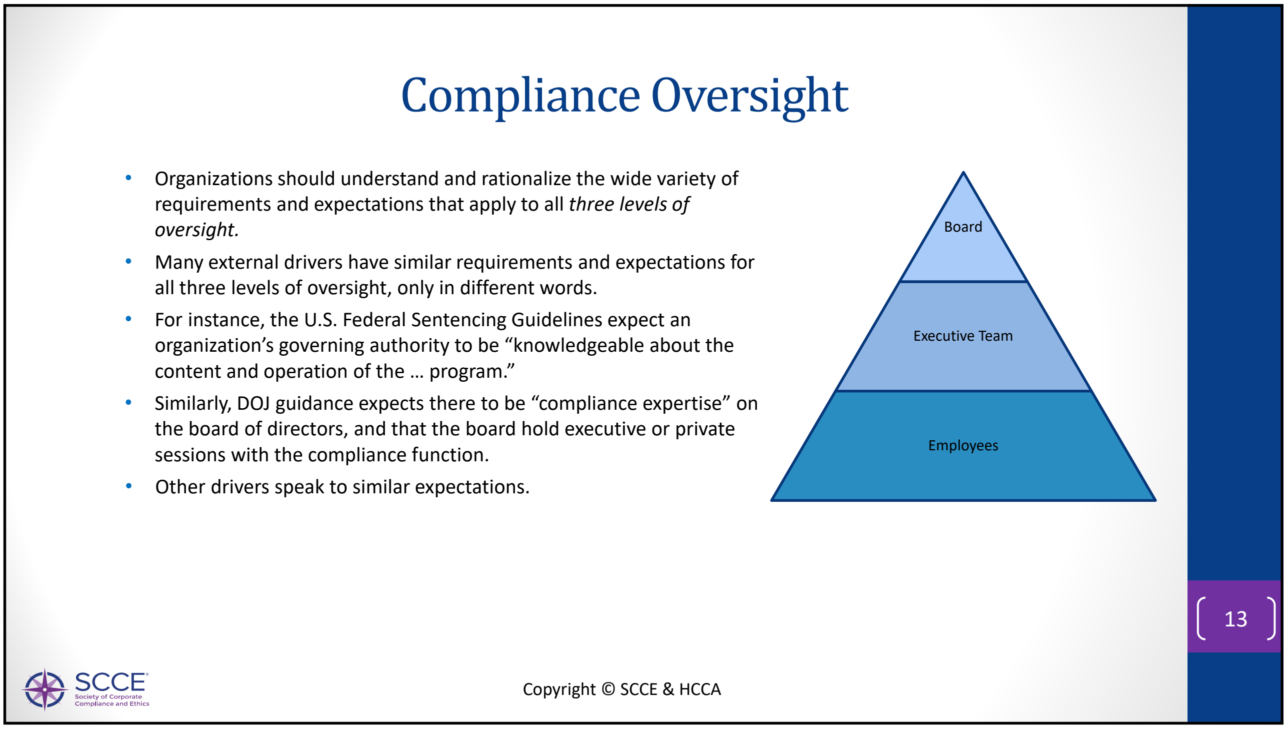
- Consider whether those responsible for compliance have:
  1) *sufficient seniority within the organization;*
  2) *sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and*
  3) *sufficient autonomy from management, such as direct access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

12

SCCE Society of Corporate Compliance and Ethics

12



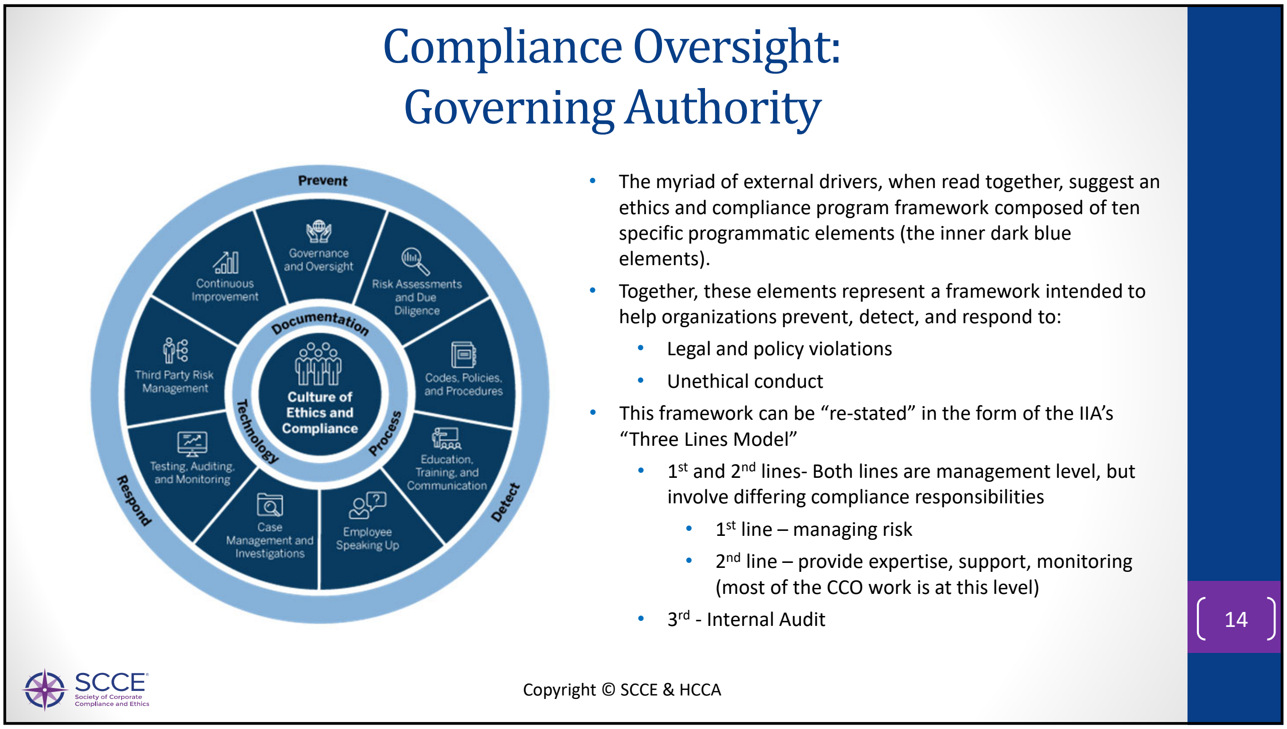
Compliance Oversight

- Organizations should understand and rationalize the wide variety of requirements and expectations that apply to all *three levels of oversight.*
- Many external drivers have similar requirements and expectations for all three levels of oversight, only in different words.
- For instance, the U.S. Federal Sentencing Guidelines expect an organization's governing authority to be "knowledgeable about the content and operation of the … program."
- Similarly, DOJ guidance expects there to be "compliance expertise" on the board of directors, and that the board hold executive or private sessions with the compliance function.
- Other drivers speak to similar expectations.

Board

Executive Team

Employees



Compliance Oversight: Governing Authority

Prevent

Governance and Oversight

Risk Assessments and Due Diligence

Codes, Policies, and Procedures

Education, Training, and Communication

Detect

Employee Speaking Up

Case Management and Investigations

Testing, Auditing, and Monitoring

Respond

Third Party Risk Management

Continuous Improvement

Documentation

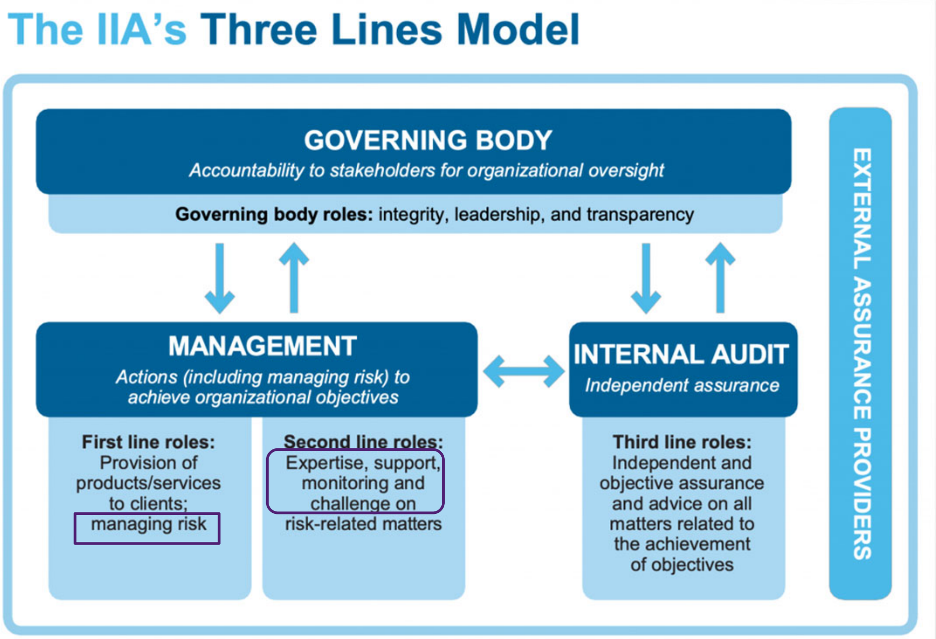
Process

Technology

Culture of Ethics and Compliance

- The myriad of external drivers, when read together, suggest an ethics and compliance program framework composed of ten specific programmatic elements (the inner dark blue elements).
- Together, these elements represent a framework intended to help organizations prevent, detect, and respond to:
  - Legal and policy violations
  - Unethical conduct
- This framework can be "re-stated" in the form of the IIA's "Three Lines Model"
  - 1st and 2nd lines- Both lines are management level, but involve differing compliance responsibilities
    - 1st line – managing risk
    - 2nd line – provide expertise, support, monitoring (most of the CCO work is at this level)
  - 3rd - Internal Audit

Source: The IIA's 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

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

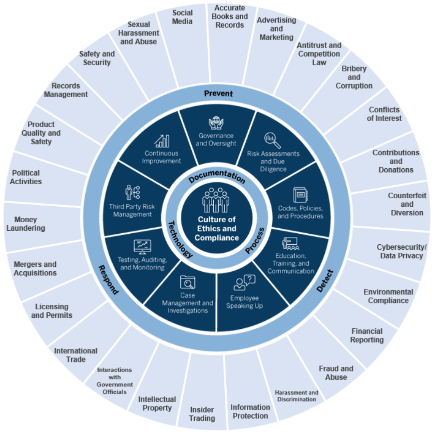
Independent assurance

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

EXTERNAL ASSURANCE PROVIDERS

SCCE Society of Corporate Compliance and Ethics

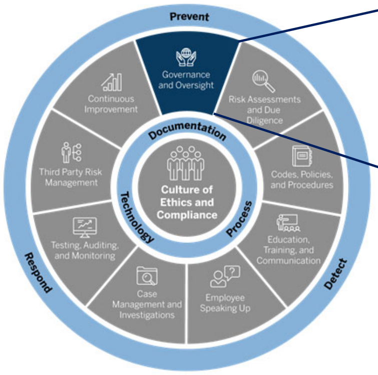
Compliance Oversight: Governing Authority

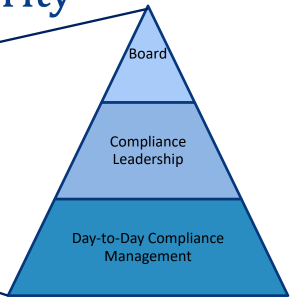

Culture of Ethics and Compliance
Documentation
Process
Technology
Governance and Oversight
Risk Assessments and Due Diligence
Codes, Policies, and Procedures
Education, Training, and Communication
Employee Speaking Up
Case Management and Investigations
Testing, Auditing, and Monitoring
Third Party Risk Management
Continuous Improvement
Prevent
Detect
Respond
Accurate Books and Records
Advertising and Marketing
Antitrust and Competition Law
Bribery and Corruption
Conflicts of Interest
Contributions and Donations
Counterfeit and Diversion
Cybersecurity/ Data Privacy
Environmental Compliance
Financial Reporting
Fraud and Abuse
Harassment and Discrimination
Information Protection
Insider Trading
Intellectual Property
Interactions with Government Officials
International Trade
Licensing and Permits
Mergers and Acquisitions
Money Laundering
Political Activities
Product Quality and Safety
Records Management
Safety and Security
Sexual Harassment and Abuse
Social Media

- The framework that represents an effectively designed ethics and compliance program framework is intended to be applied – in a consistent manner – to an organization's ethics and compliance risk profile.
- In other words, for the key areas of ethics and compliance risk, organizations should have each of the ten elements in place.

SCCE Society of Corporate Compliance and Ethics

Compliance Oversight: Governing Authority


Prevent
Governance and Oversight
Risk Assessments and Due Diligence
Codes, Policies, and Procedures
Education, Training, and Communication
Employee Speaking Up
Case Management and Investigations
Testing, Auditing, and Monitoring
Third Party Risk Management
Continuous Improvement
Documentation
Process
Technology
Culture of Ethics and Compliance
Detect
Respond

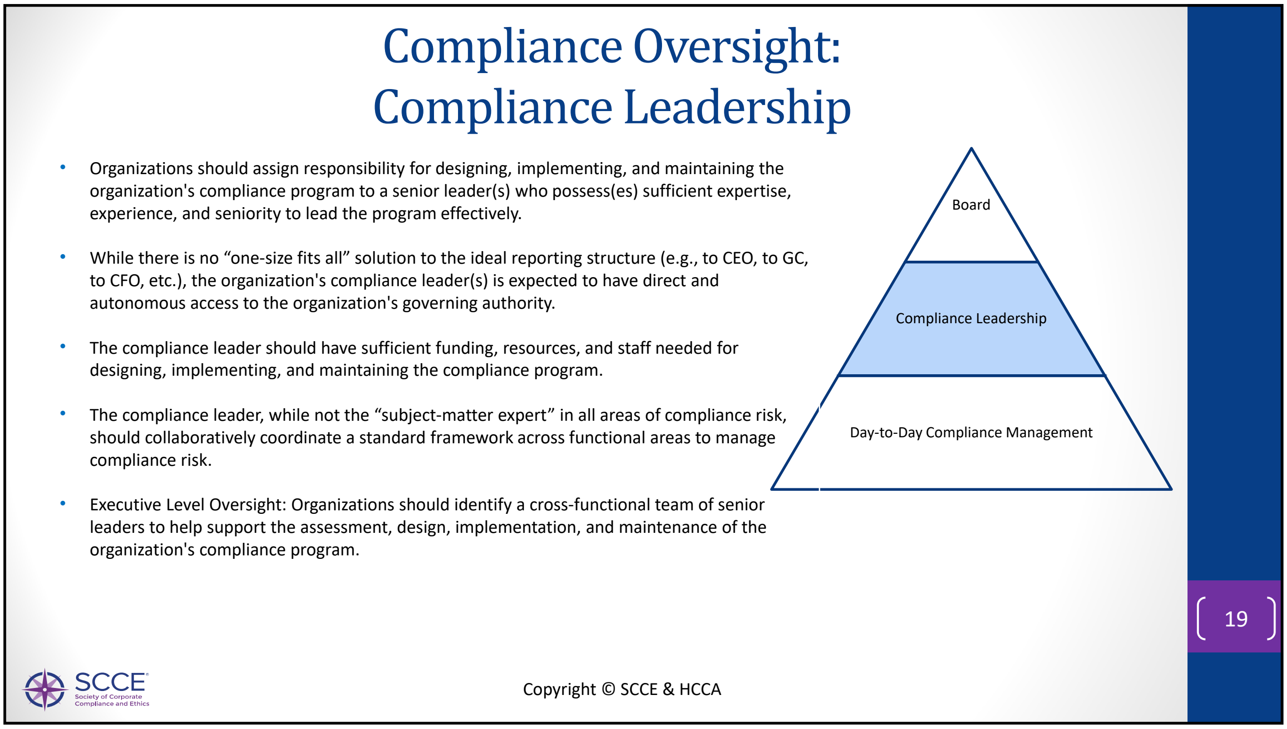


- Effectively designed ethics and compliance programs have a governance and oversight structure at three levels:
  - Board
  - Compliance leadership
  - Day-to-day risk ownership
- There are certain leading practices associated with each level of governance and oversight.

Compliance Oversight: Governing Authority (Board)

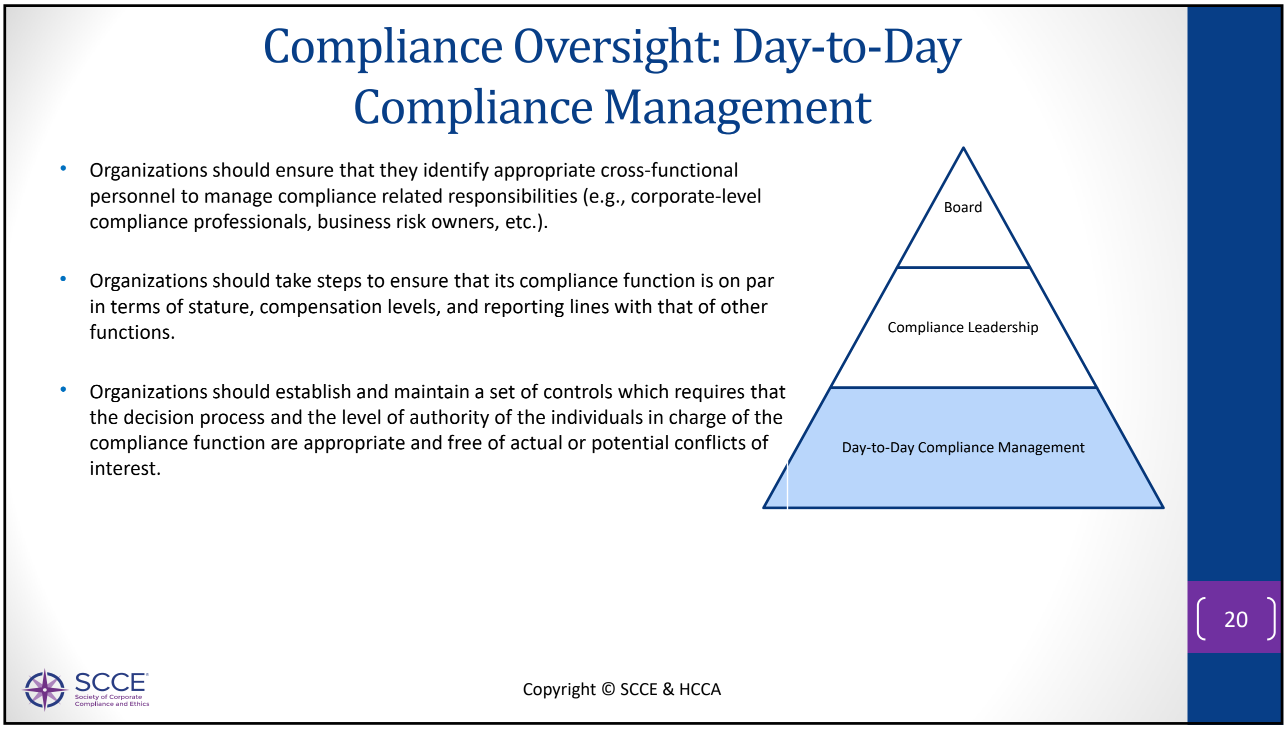
- Governing authority (typically the board of directors) has a fiduciary duty of care to the organization with which it is affiliated.
- Governing authority is expected to exercise high-level oversight of all elements of the organization's compliance program and is knowledgeable about the content and operation of the program.
- Governing authority is expected to exercise oversight such that the organization's compliance leader has direct and autonomous reporting access to the governing authority (e.g., straight line reporting, executive sessions, etc.).
- Governing authority is expected to direct and oversee a periodic review of the organization's compliance program.

Board
Compliance Leadership
Day-to-Day Compliance Management



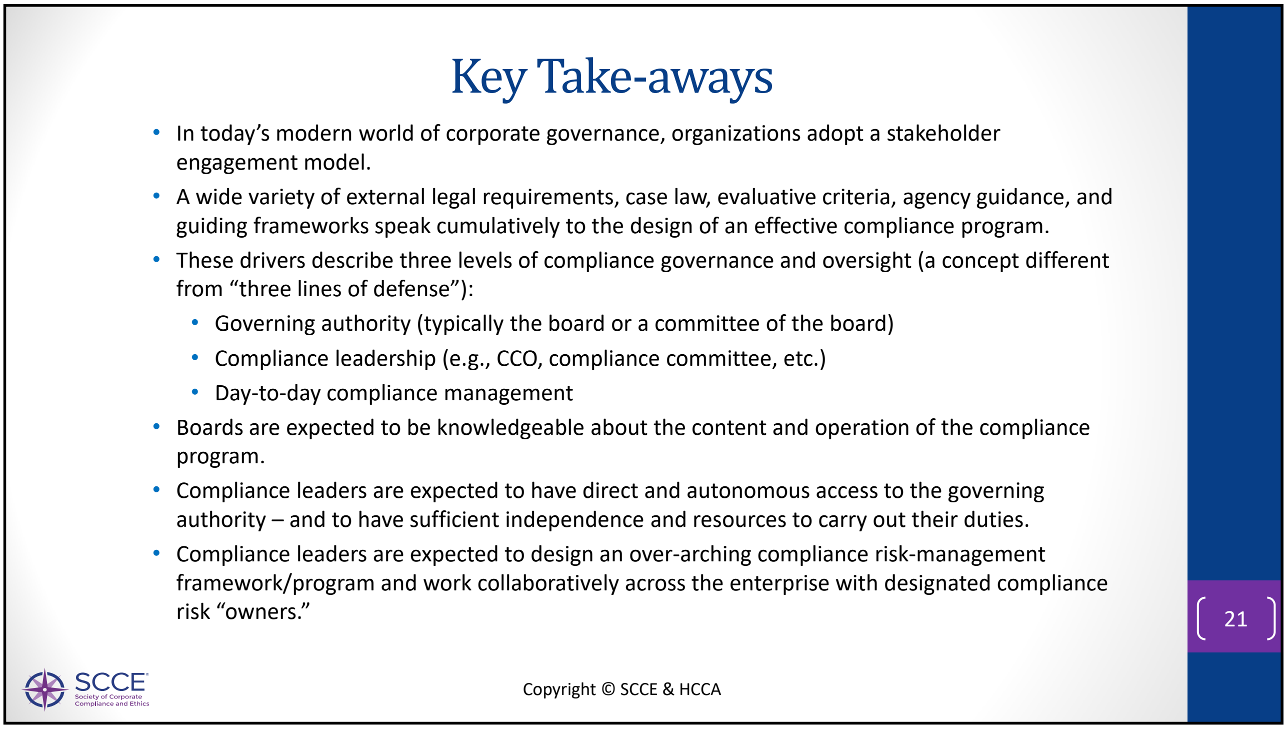
Compliance Oversight: Compliance Leadership

- 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.
- Executive Level Oversight: Organizations should identify a cross-functional team of senior leaders to help support the assessment, design, implementation, and maintenance of the organization's compliance program.



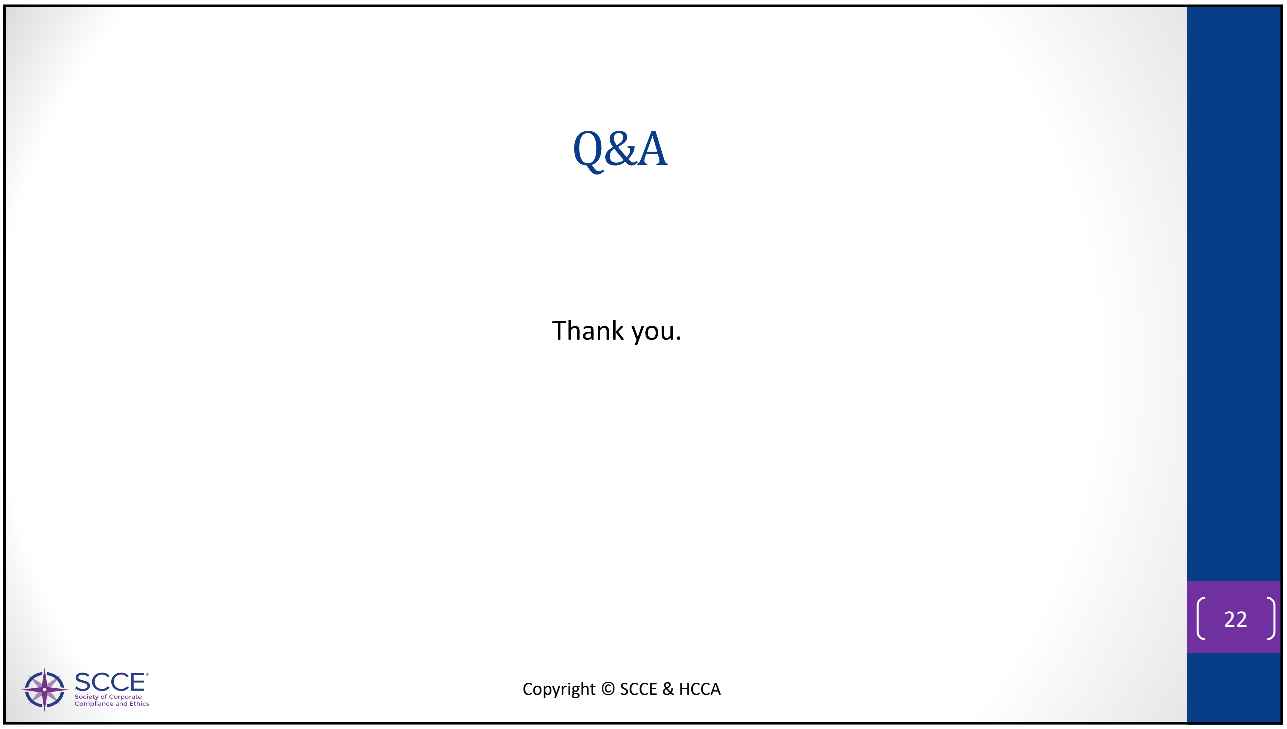
Compliance Oversight: Day-to-Day Compliance Management

- Organizations should ensure that they identify appropriate cross-functional personnel to manage compliance related responsibilities (e.g., corporate-level compliance professionals, business risk owners, etc.).
- Organizations should take steps to ensure that its compliance function is on par in terms of stature, compensation levels, and reporting lines with that of other functions.
- Organizations should establish and maintain a set of controls which requires that the decision process and the level of authority of the individuals in charge of the compliance function are appropriate and free of actual or potential conflicts of interest.



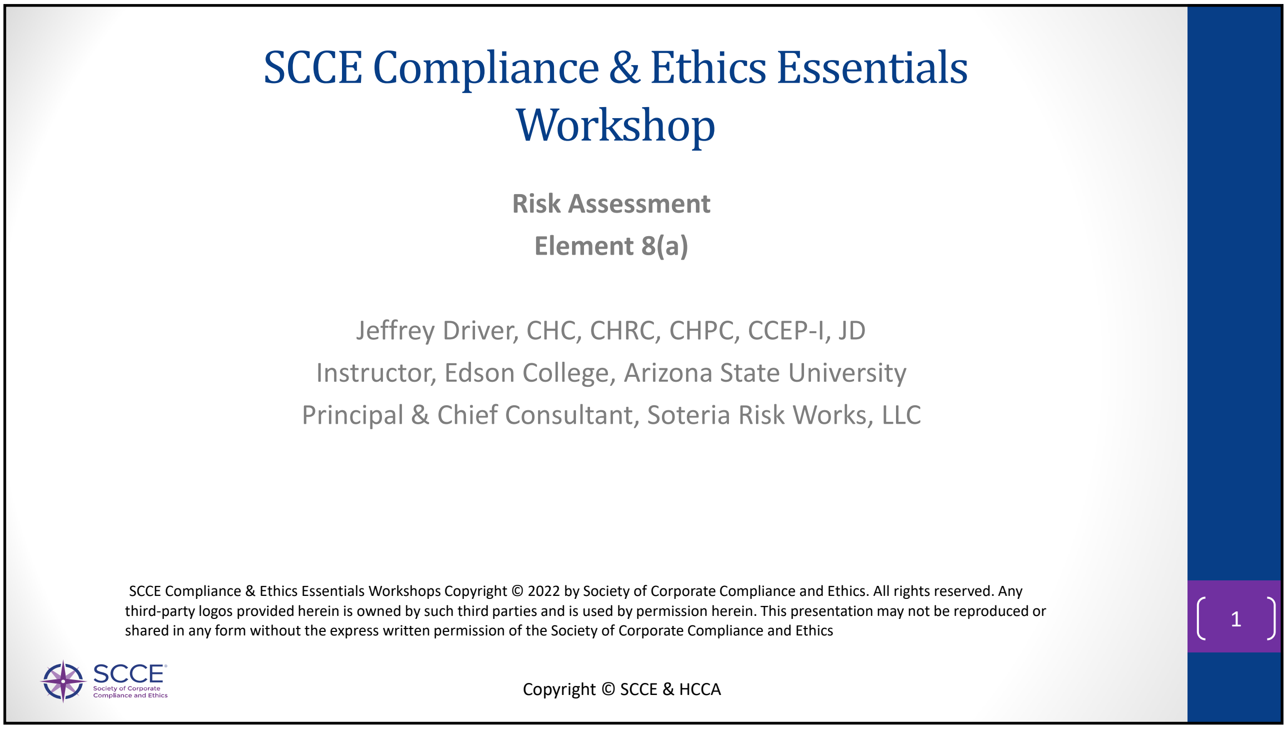
Key Take-aways

- In today’s modern world of corporate governance, organizations adopt a stakeholder engagement model.
- 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 three 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)
  - Compliance leadership (e.g., CCO, compliance committee, etc.)
  - Day-to-day compliance management
- Boards 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.

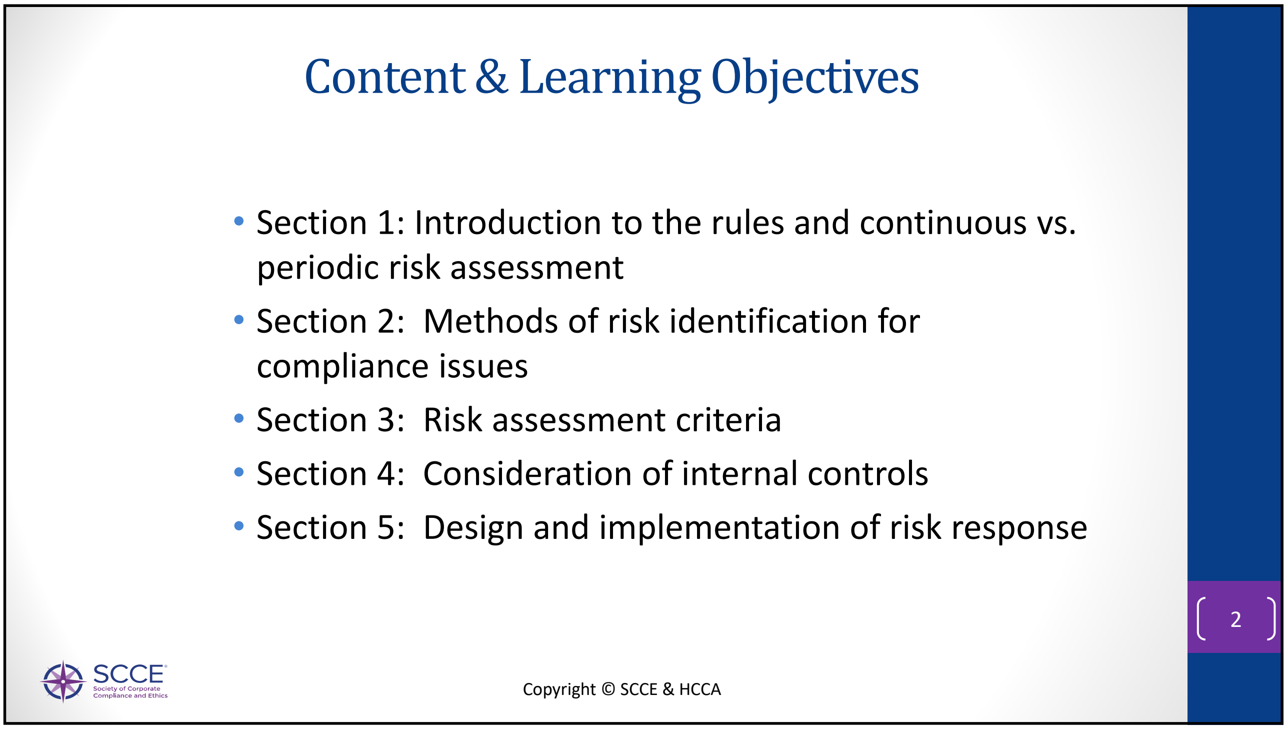


SCCE Compliance & Ethics Essentials Workshop

Risk Assessment

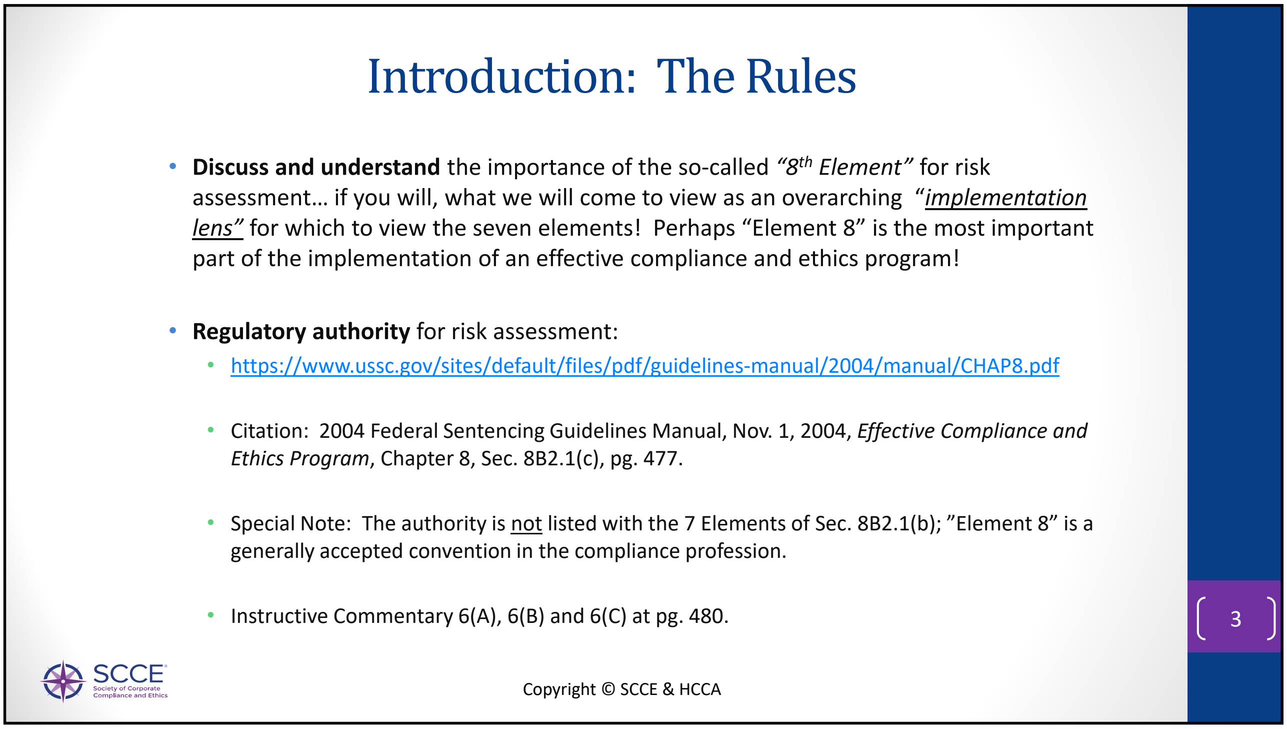
Element 8(a)

Jeffrey Driver, CHC, CHRC, CHPC, CCEP-I, JD
Instructor, Edson College, Arizona State University
Principal & Chief Consultant, Soteria Risk Works, LLC



Content & Learning Objectives

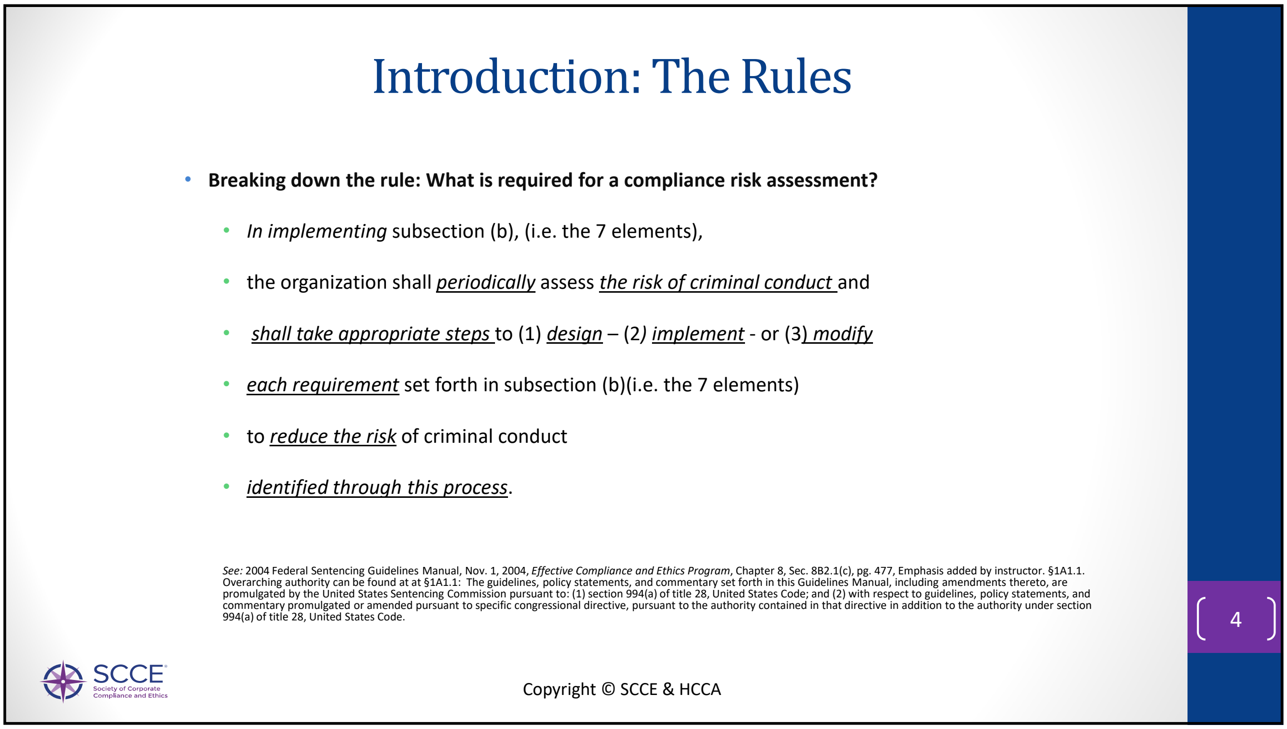
- Section 1: Introduction to the rules and continuous vs. periodic risk assessment
- Section 2: Methods of risk identification for compliance issues
- Section 3: Risk assessment criteria
- Section 4: Consideration of internal controls
- Section 5: Design and implementation of risk response



Introduction: The Rules

- **Discuss and understand** the importance of the so-called *"8th Element"* for risk assessment… if you will, what we will come to view as an overarching *"implementation lens"* for which to view the seven elements! Perhaps "Element 8" is the most important part of the implementation of an effective compliance and ethics program!

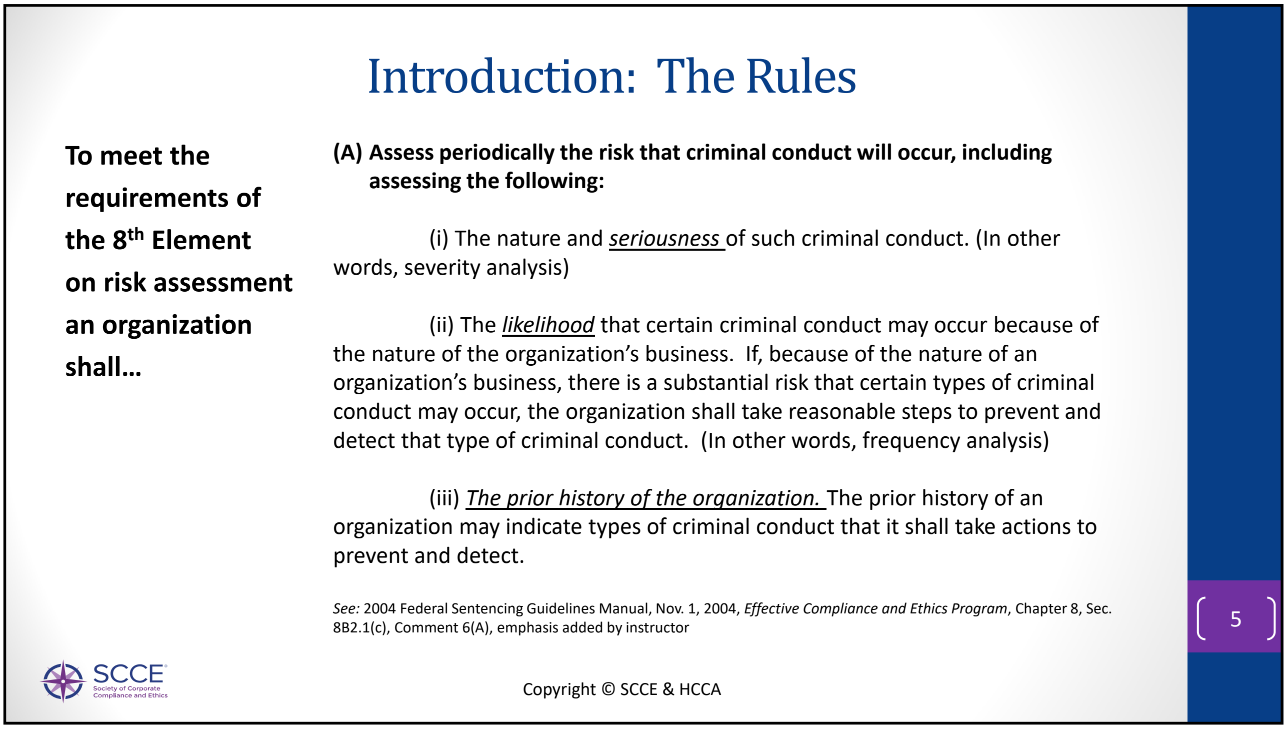
- **Regulatory authority** for risk assessment:
  - https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2004/manual/CHAP8.pdf
  - Citation: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1(c), pg. 477.
  - Special Note: The authority is not listed with the 7 Elements of Sec. 8B2.1(b); "Element 8" is a generally accepted convention in the compliance profession.
  - Instructive Commentary 6(A), 6(B) and 6(C) at pg. 480.



Introduction: The Rules

- **Breaking down the rule: What is required for a compliance risk assessment?**
  - *In implementing* subsection (b), (i.e. the 7 elements),
  - the organization shall *periodically* assess *the risk of criminal conduct* and
  - *shall take appropriate steps* to (1) *design* – (2*) implement* - or (3*) modify*
  - *each requirement* set forth in subsection (b)(i.e. the 7 elements)
  - to *reduce the risk* of criminal conduct
  - *identified through this process*.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1(c), pg. 477, Emphasis 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.



Introduction: The Rules

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

(A) Assess periodically the risk that criminal conduct will occur, including assessing the following:

(i) The nature and *seriousness* of such criminal conduct. (In other words, severity analysis)

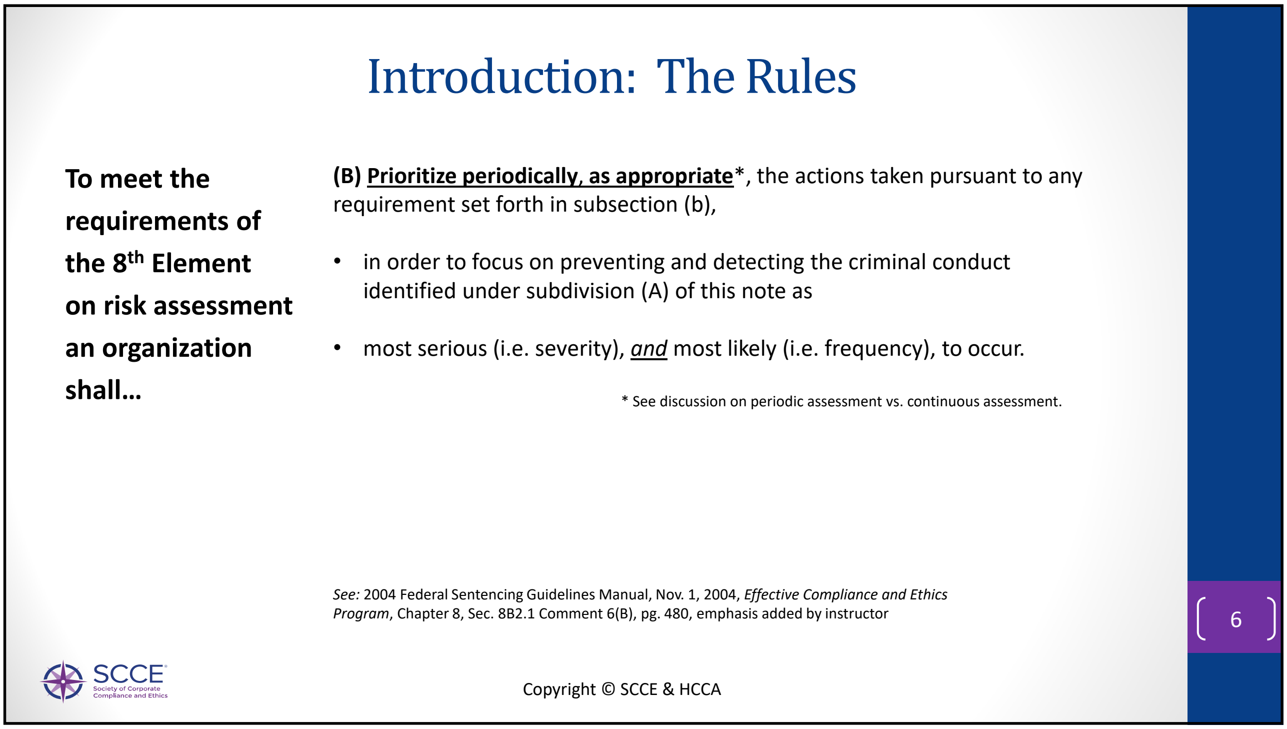
(ii) The *likelihood* that certain criminal conduct may occur because of the nature of the organization's business. If, because of the nature of an organization's business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct. (In other words, frequency analysis)

(iii) *The prior history of the organization.* The prior history of an organization may indicate types of criminal conduct that it shall take actions to prevent and detect.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1(c), Comment 6(A), emphasis added by instructor

5

5



Introduction: The Rules

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

(B) Prioritize periodically, as appropriate*, the actions taken pursuant to any requirement set forth in subsection (b),

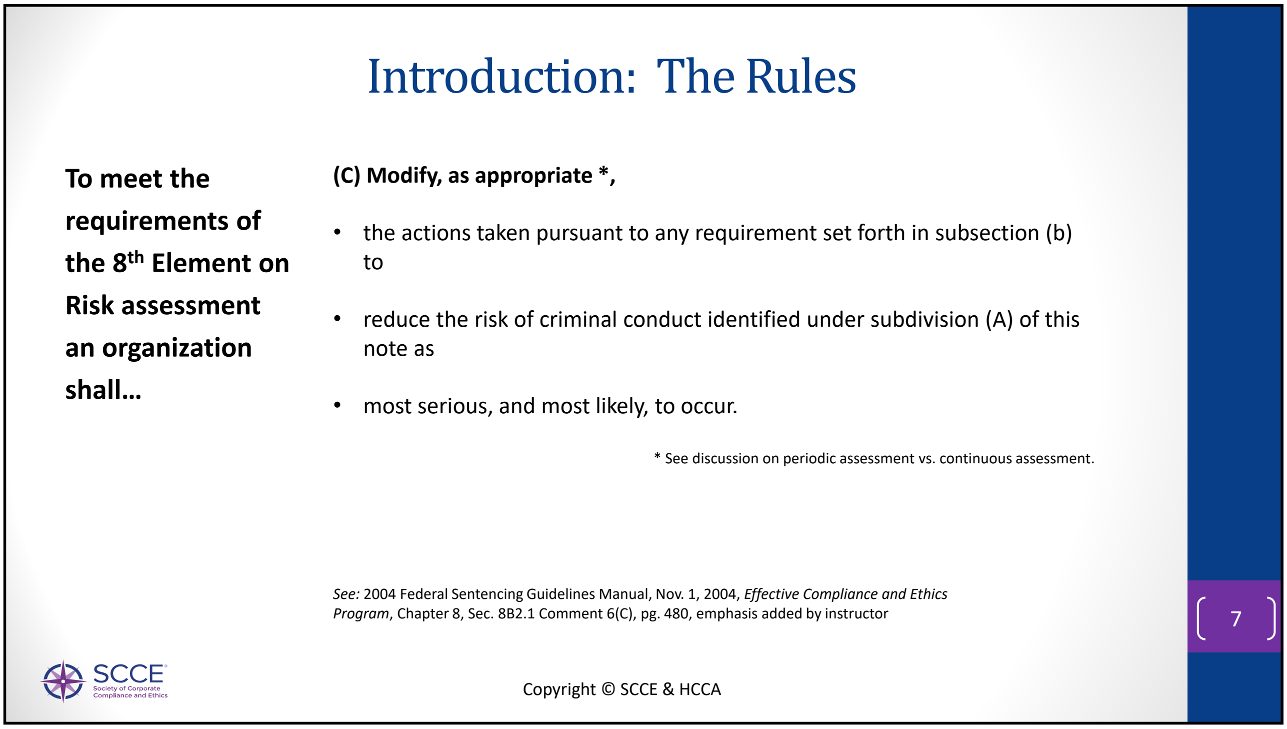
- in order to focus on preventing and detecting the criminal conduct identified under subdivision (A) of this note as
- most serious (i.e. severity), *and* most likely (i.e. frequency), to occur.

* See discussion on periodic assessment vs. continuous assessment.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1 Comment 6(B), pg. 480, emphasis added by instructor

6

6



Introduction: The Rules

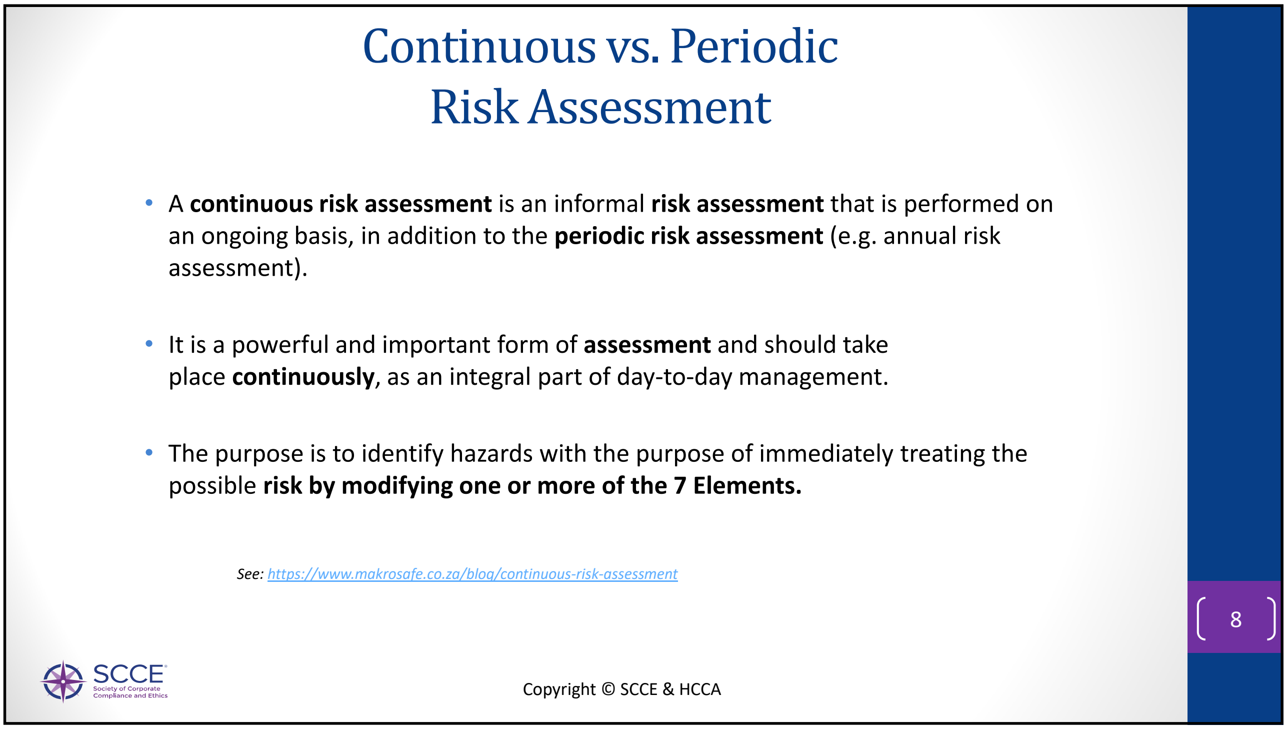
To meet the requirements of the 8th Element on Risk assessment an organization shall…

(C) Modify, as appropriate *,

- the actions taken pursuant to any requirement set forth in subsection (b) to
- reduce the risk of criminal conduct identified under subdivision (A) of this note as
- most serious, and most likely, to occur.

* See discussion on periodic assessment vs. continuous assessment.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1 Comment 6(C), pg. 480, emphasis added by instructor



Continuous vs. Periodic Risk Assessment

- A **continuous risk assessment** is an informal **risk assessment** that is performed on an ongoing basis, in addition to the **periodic risk assessment** (e.g. annual risk assessment).
- It is a powerful and important form of **assessment** and should take place **continuously**, as an integral part of day-to-day management.
- The purpose is to identify hazards with the purpose of immediately treating the possible **risk by modifying one or more of the 7 Elements.**

See: https://www.makrosafe.co.za/blog/continuous-risk-assessment

Continuous vs. Periodic Risk Assessment

- **A continuous risk assessment** does not need to be sophisticated or complicated, though there should be some formality around both continuous and periodic risk assessment policies and procedures.
- **A continuous risk assessment** should aim to create compliance hazard awareness through risk identification. A compliance hot-line, monitoring, and concurrent auditing are a few good methods to identify risk through a **continuous risk assessment.**
- **In most cases, it will be a good start for employees and supervisors to simply look and see what is happening in the workplace**. By simply observing what is happening and how staff is dealing with challenges that could pose a risk, the employee or supervisor should get a first-hand indication of possible risks and report them for compliance management.
- **Organizational monitoring** through checklists, like inspection checklists, pre-use checklists or critical parts and paths checklists (FMEA or Process Mapping) can also play an important role in identifying and registering possible risk immediately.

SCCE Society of Corporate Compliance and Ethics

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 Society of Corporate Compliance and Ethics
HCCA Health Care Compliance Association

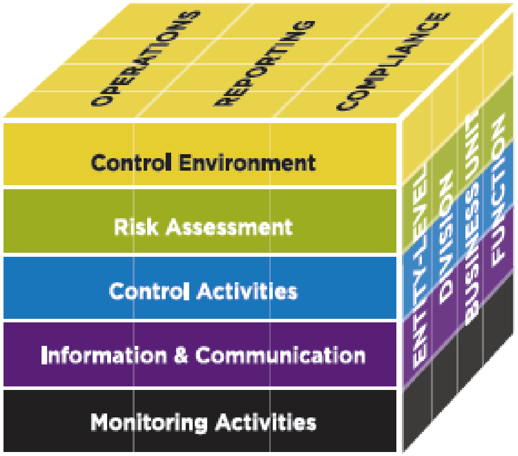
November 11, 2020

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

SCCE Society of Corporate Compliance and Ethics

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



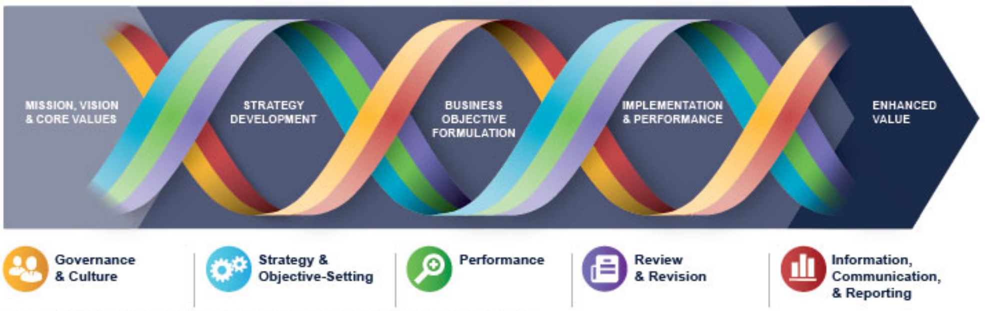
Source: COSO Internal Control Framework ©2013

SCCE Society of Corporate Compliance and Ethics

11

11

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

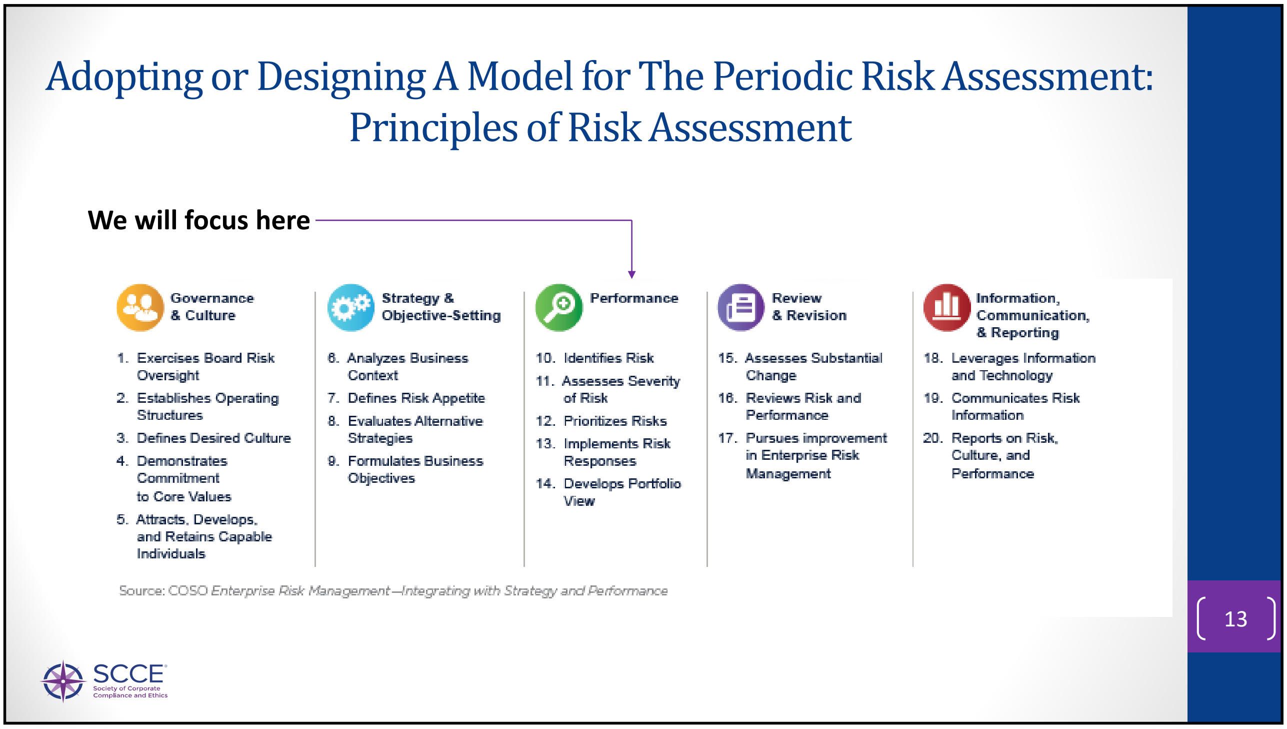

MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

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

SCCE Society of Corporate Compliance and Ethics

12

12



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

We will focus here → Performance

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

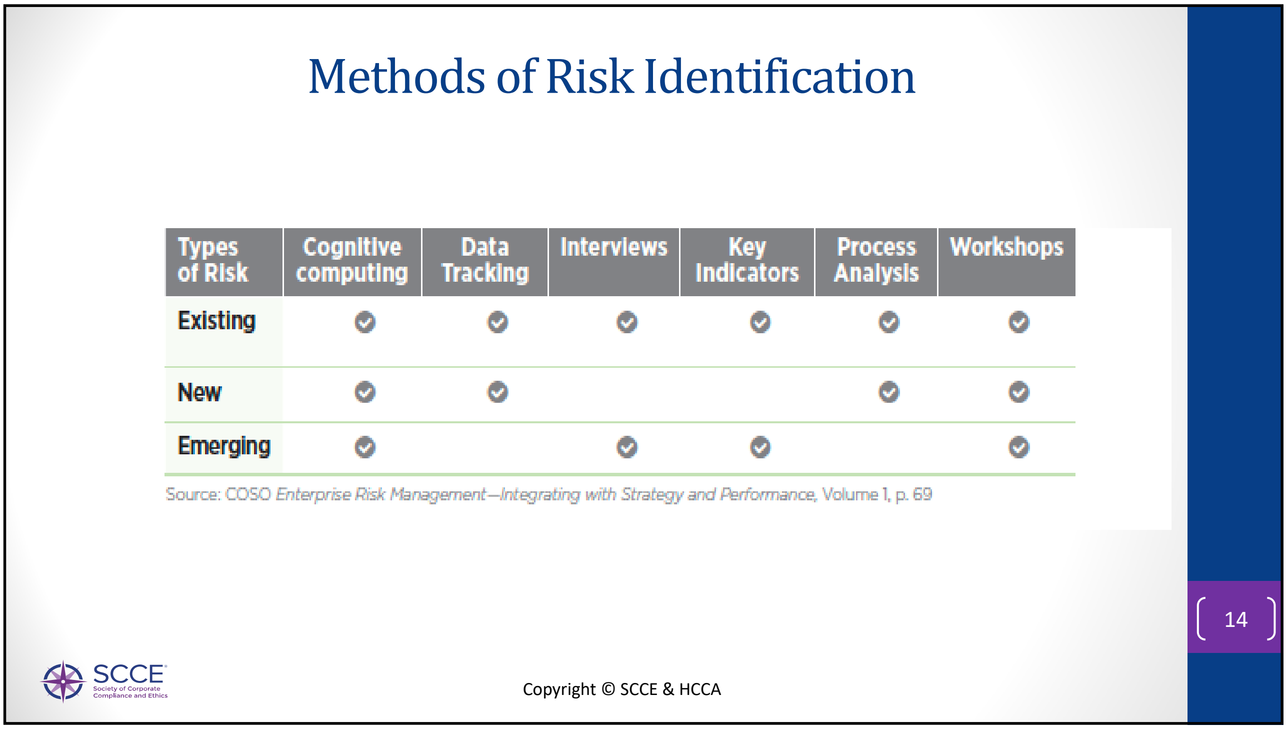
Review & Revision

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*

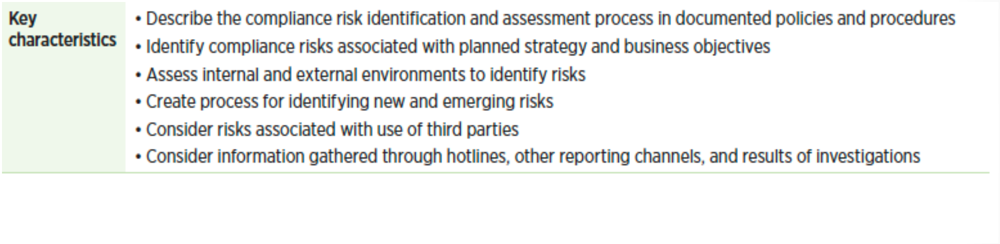


Methods of Risk Identification

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



Key characteristics	• Describe the compliance risk identification and assessment process in documented policies and procedures • Identify compliance risks associated with planned strategy and business objectives • Assess internal and external environments to identify risks • Create process for identifying new and emerging risks • Consider risks associated with use of third parties • Consider information gathered through hotlines, other reporting channels, and results of investigations

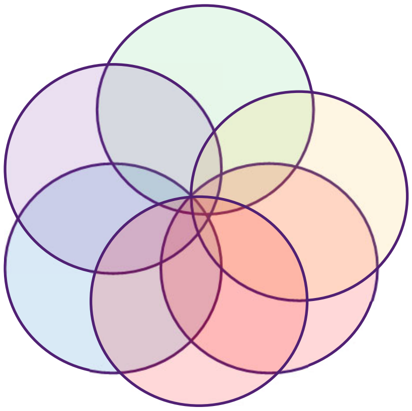
See: *https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf*

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.

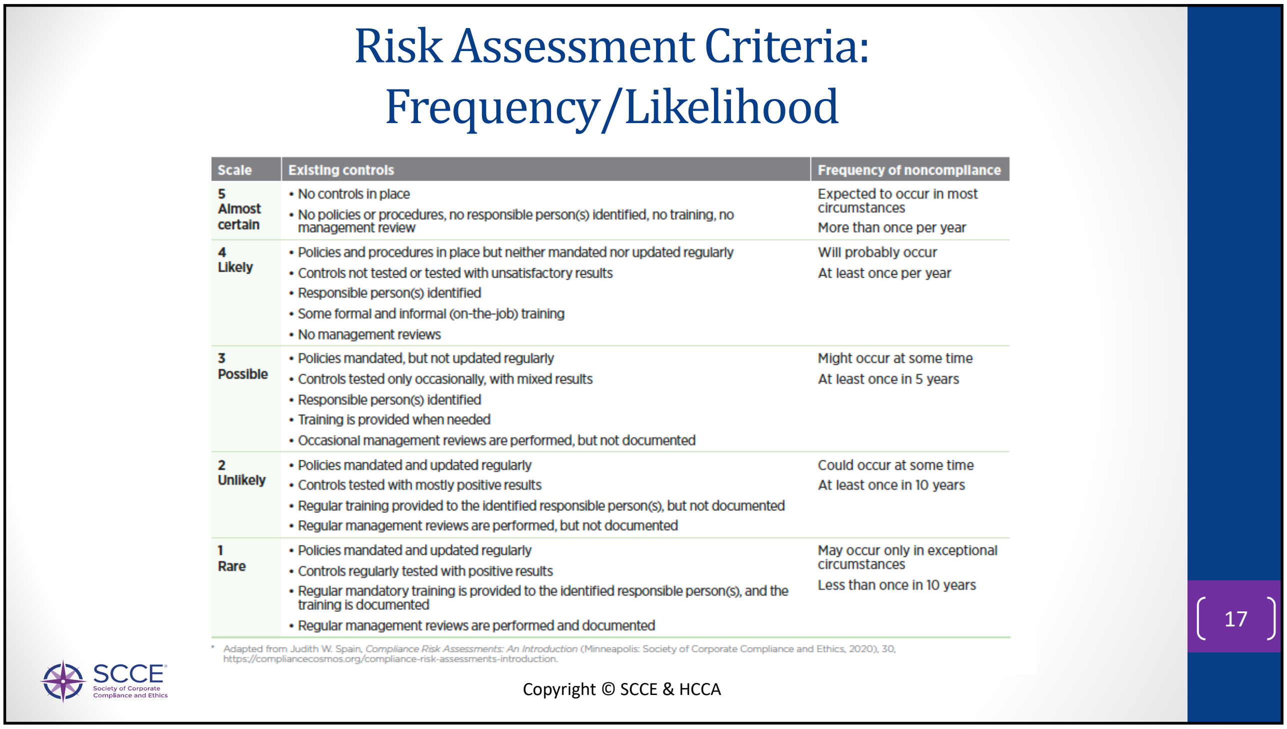


Reputation: Effect of media coverage, damage to image/brand, diminution in reputation with EE's, future EE's, business partners, vendors, and customers.

Health & Safety: EE, customer, others.

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

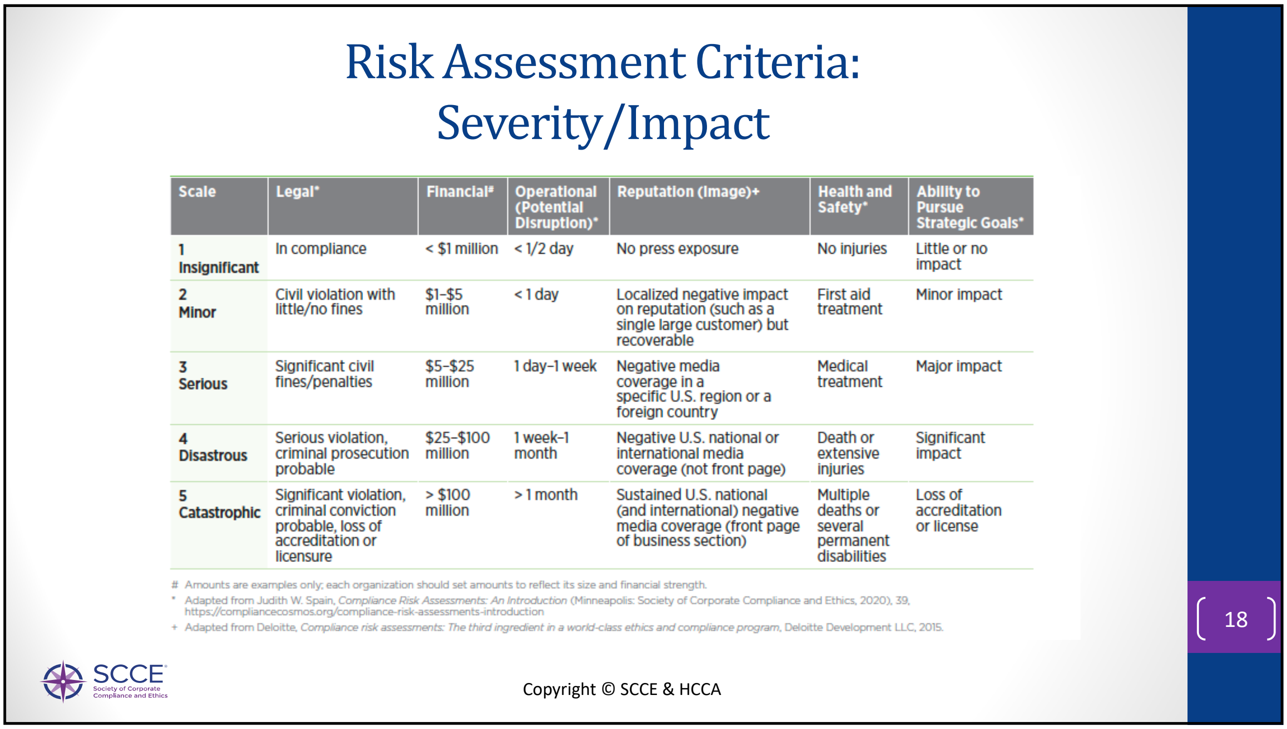
See: *https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf*



Risk Assessment Criteria: Frequency/Likelihood

Scale	Existing controls	Frequency of noncompliance
5 Almost certain	• No controls in place • No policies or procedures, no responsible person(s) identified, no training, no management review	Expected to occur in most circumstances More than once per year
4 Likely	• Policies and procedures in place but neither mandated nor updated regularly • Controls not tested or tested with unsatisfactory results • Responsible person(s) identified • Some formal and informal (on-the-job) training • No management reviews	Will probably occur At least once per year
3 Possible	• Policies mandated, but not updated regularly • Controls tested only occasionally, with mixed results • Responsible person(s) identified • Training is provided when needed • Occasional management reviews are performed, but not documented	Might occur at some time At least once in 5 years
2 Unlikely	• Policies mandated and updated regularly • Controls tested with mostly positive results • Regular training provided to the identified responsible person(s), but not documented • Regular management reviews are performed, but not documented	Could occur at some time At least once in 10 years
1 Rare	• Policies mandated and updated regularly • Controls regularly tested with positive results • Regular mandatory training is provided to the identified responsible person(s), and the training is documented • Regular management reviews are performed and documented	May occur only in exceptional circumstances Less than once in 10 years

* Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 30, https://compliancecosmos.org/compliance-risk-assessments-introduction.



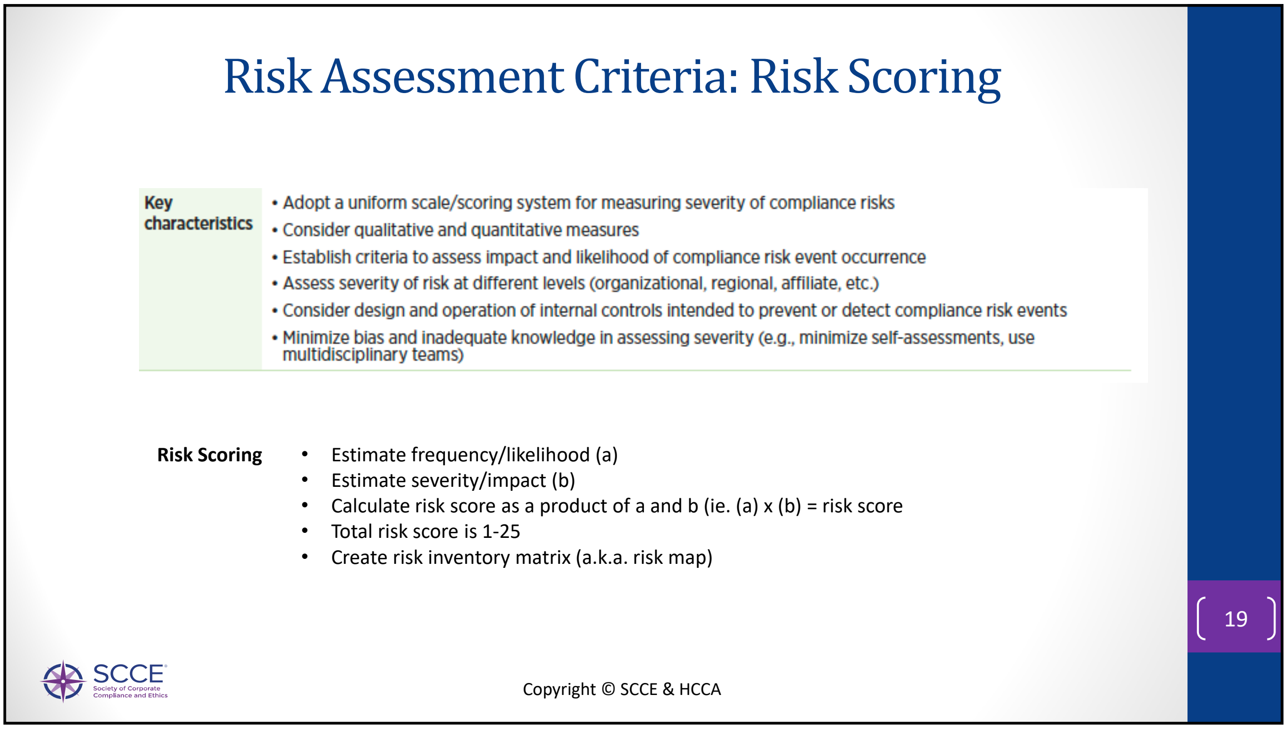
Risk Assessment Criteria: Severity/Impact

Scale	Legal*	Financial#	Operational (Potential Disruption)*	Reputation (Image)+	Health and Safety*	Ability to Pursue Strategic Goals*
1 Insignificant	In compliance	< $1 million	< 1/2 day	No press exposure	No injuries	Little or no impact
2 Minor	Civil violation with little/no fines	$1–$5 million	< 1 day	Localized negative impact on reputation (such as a single large customer) but recoverable	First aid treatment	Minor impact
3 Serious	Significant civil fines/penalties	$5–$25 million	1 day–1 week	Negative media coverage in a specific U.S. region or a foreign country	Medical treatment	Major impact
4 Disastrous	Serious violation, criminal prosecution probable	$25–$100 million	1 week–1 month	Negative U.S. national or international media coverage (not front page)	Death or extensive injuries	Significant impact
5 Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or licensure	> $100 million	> 1 month	Sustained U.S. national (and international) negative media coverage (front page of business section)	Multiple deaths or several permanent disabilities	Loss of accreditation or license

Amounts are examples only; each organization should set amounts to reflect its size and financial strength.

* Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 39, https://compliancecosmos.org/compliance-risk-assessments-introduction

+ Adapted from Deloitte, *Compliance risk assessments: The third ingredient in a world-class ethics and compliance program*, Deloitte Development LLC, 2015.

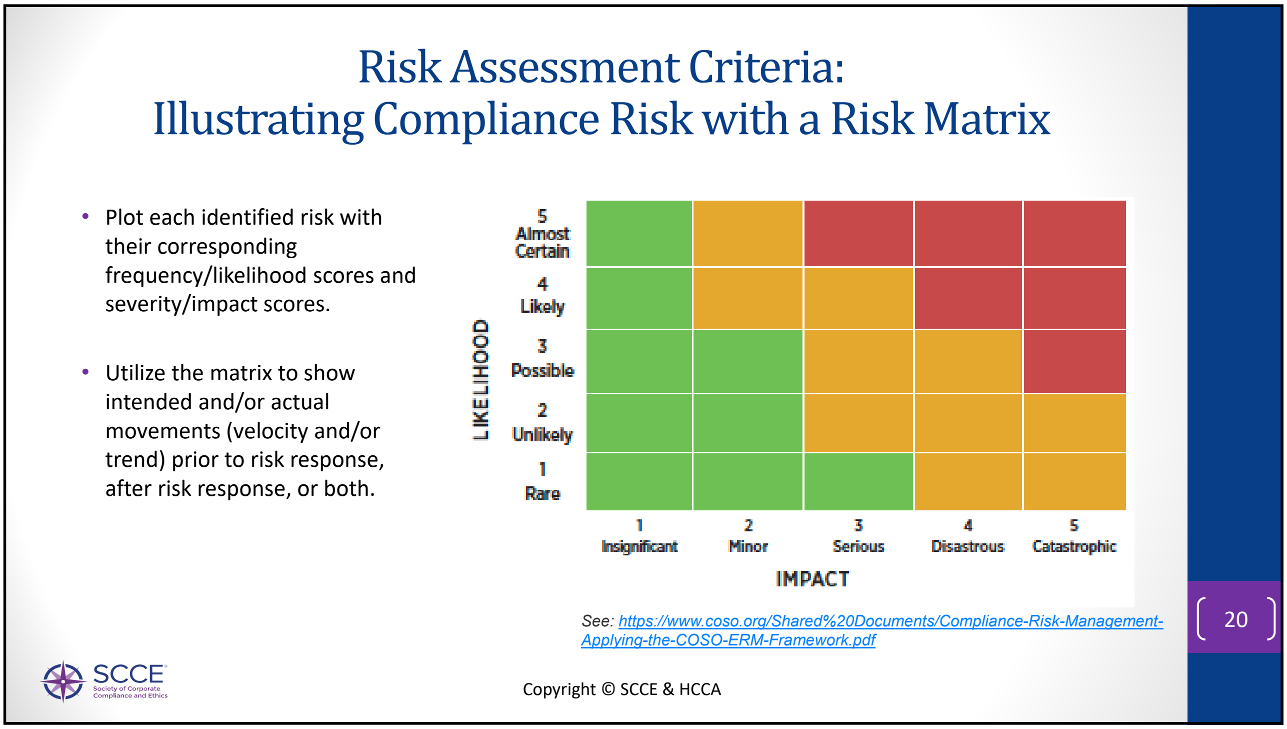


Risk Assessment Criteria: Risk Scoring

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 event occurrence • Assess severity of risk at different levels (organizational, regional, affiliate, etc.) • Consider design and operation of internal controls intended to prevent or detect compliance risk events • Minimize bias and inadequate knowledge in assessing severity (e.g., minimize self-assessments, use multidisciplinary teams)

Risk Scoring

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



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 (velocity and/or trend) 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

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

Consideration of Internal Controls: The Crucial Step of Prioritization

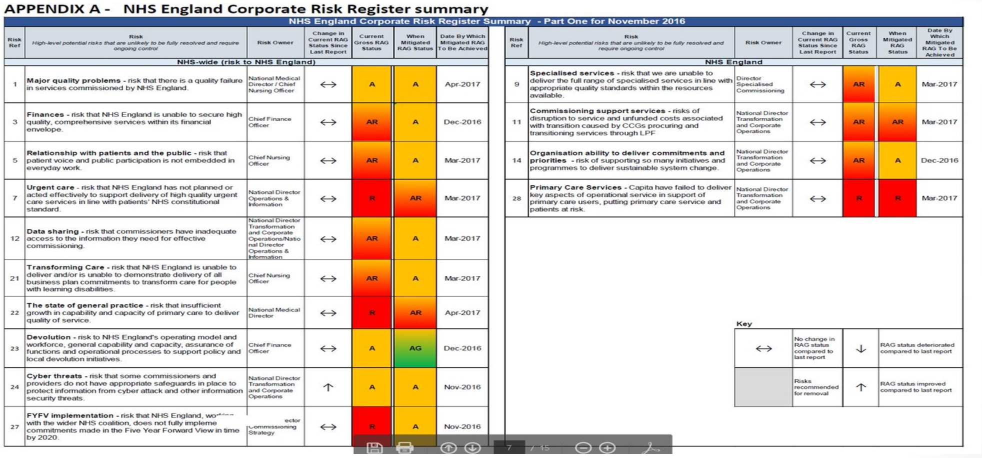
Key characteristics

- Prioritize compliance risks based on assessed level of risk relative to meeting of business objectives
- Use objective scoring based on assessment
- Consider use of other assessment criteria (trend, velocity, etc.) in prioritizing compliance risks
- Consider possible effects of planned changes in strategy and operations
- Develop risk-based action plans for mitigation (risk responses, implemented in next step)

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

Consideration of Internal Controls: The Crucial Step of Prioritization

An Example of a Risk Register from the Twitter-sphere



APPENDIX A - NHS England Corporate Risk Register summary

NHS England Corporate Risk Register Summary - Part One for November 2016

Risk Ref	Risk *High-level potential risks that are unlikely to be fully resolved and require ongoing control*	Risk Owner	Change in Current RAG Status Since Last Report	Current Gross RAG Status	When Mitigated RAG Status	Date By Which Mitigated RAG To Be Achieved
	NHS-wide (risk to NHS England)					
1	**Major quality problems** - risk that there is a quality failure in services commissioned by NHS England.	National Medical Director / Chief Nursing Officer	↔	A	A	Apr-2017
3	**Finances** - risk that NHS England is unable to secure high quality, comprehensive services within its financial envelope.	Chief Finance Officer	↔	AR	A	Dec-2016
5	**Relationship with patients and the public** - risk that patient voice and public participation is not embedded in everyday work.	Chief Nursing Officer	↔	AR	A	Mar-2017
7	**Urgent care** - risk that NHS England has not planned or acted effectively to support delivery of high quality urgent care services in line with patients' NHS constitutional standard.	National Director Operations & Information	↔	R	AR	Mar-2017
12	**Data sharing** - risk that commissioners have inadequate access to the information they need for effective commissioning.	National Director Transformation and Corporate Operations/National Director Operations & Information	↔	AR	A	Mar-2017
21	**Transforming Care** - risk that NHS England is unable to deliver and/or is unable to demonstrate delivery of all business plan commitments to transform care for people with learning disabilities.	Chief Nursing Officer	↔	AR	A	Mar-2017
22	**The state of general practice** - risk that insufficient growth in capability and capacity of primary care to deliver quality of service.	National Medical Director	↔	R	AR	Apr-2017
23	**Devolution** - risk to NHS England's operating model and workforce, general capability and capacity, assurance of functions and operational processes to support policy and local devolution initiatives.	Chief Finance Officer	↔	A	AG	Dec-2016
24	**Cyber threats** - risk that some commissioners and providers do not have appropriate safeguards in place to protect information from cyber attack and other information security threats.	National Director Transformation and Corporate Operations	↑	A	A	Nov-2016
27	**FYFV implementation** - risk that NHS England, wo with the wider NHS coalition, does not fully impleme commitments made in the Five Year Forward View in time by 2020.	ector Commissioning Strategy	↔	R	A	Nov-2016

Risk Ref	Risk *High-level potential risks that are unlikely to be fully resolved and require ongoing control*	Risk Owner	Change in Current RAG Status Since Last Report	Current Gross RAG Status	When Mitigated RAG Status	Date By Which Mitigated RAG To Be Achieved
	NHS England					
9	**Specialised services** - risk that we are unable to deliver the full range of specialised services in line with appropriate quality standards within the resources available.	Director Specialised Commissioning	↔	AR	A	Mar-2017
11	**Commissioning support services** - risks of disruption to service and unfunded costs associated with transition caused by CCGs procuring and transitioning services through LPF	National Director Transformation and Corporate Operations	↔	AR	AR	Mar-2017
14	**Organisation ability to deliver commitments and priorities** - risk of supporting so many initiatives and programmes to deliver sustainable system change.	National Director Transformation and Corporate Operations	↔	AR	A	Dec-2016
28	**Primary Care Services** - Capita have failed to deliver key aspects of operational service in support of primary care users, putting primary care service and patients at risk.	National Director Transformation and Corporate Operations	↔	R	R	Mar-2017

Key

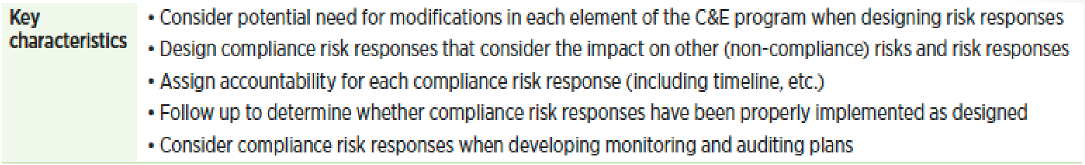
↔	No change in RAG status compared to last report	↓	RAG status deteriorated compared to last report
▨	Risks recommended for removal	↑	RAG status improved compared to last report

Consideration of Internal Controls: Risk Response to Identified Priority Risks

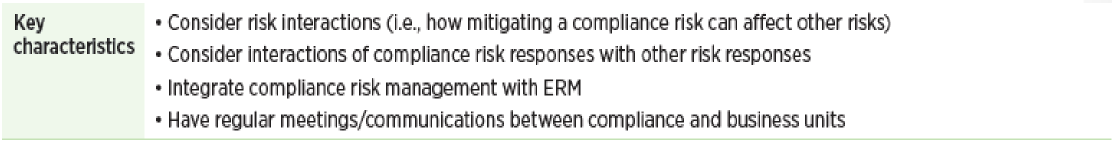
- Effective risk mitigation of a compliance risk involves consideration of all 7 elements of a compliance and ethics program! Consider each element for possible modification!
- Consider a combination of preventative and detective controls.
- Ask what is the driver of the risk; e.g. frequency/likelihood driving severity/impact → preventive controls. High impact but low frequency → detective controls more suitable.
- Consider training, monitoring, and auditing responses, as well as redesigning work procedures and reducing or eliminating failure points in a process.

23

Consideration of Internal Controls: Implementation & Portfolio View of Risk



Key characteristics	• Consider potential need for modifications in each element of the C&E program when designing risk responses • Design compliance risk responses that consider the impact on other (non-compliance) risks and risk responses • Assign accountability for each compliance risk response (including timeline, etc.) • Follow up to determine whether compliance risk responses have been properly implemented as designed • Consider compliance risk responses when developing monitoring and auditing plans



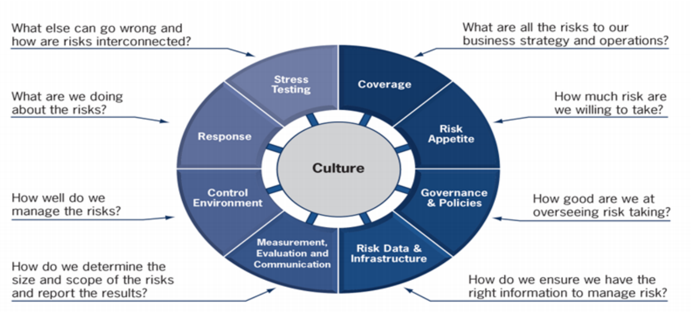
Key characteristics	• Consider risk interactions (i.e., how mitigating a compliance risk can affect other risks) • Consider interactions of compliance risk responses with other risk responses • Integrate compliance risk management with ERM • Have regular meetings/communications between compliance and business units

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

24

Consideration of Internal Controls: An ERM Portfolio View of Risk

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?
What are we doing about the risks?
How much risk are we willing to take?
How well do we manage the risks?
How good are we at overseeing risk taking?
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?
Stress Testing
Coverage
Risk Appetite
Governance & Policies
Risk Data & Infrastructure
Measurement, Evaluation and Communication
Control Environment
Response
Culture

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

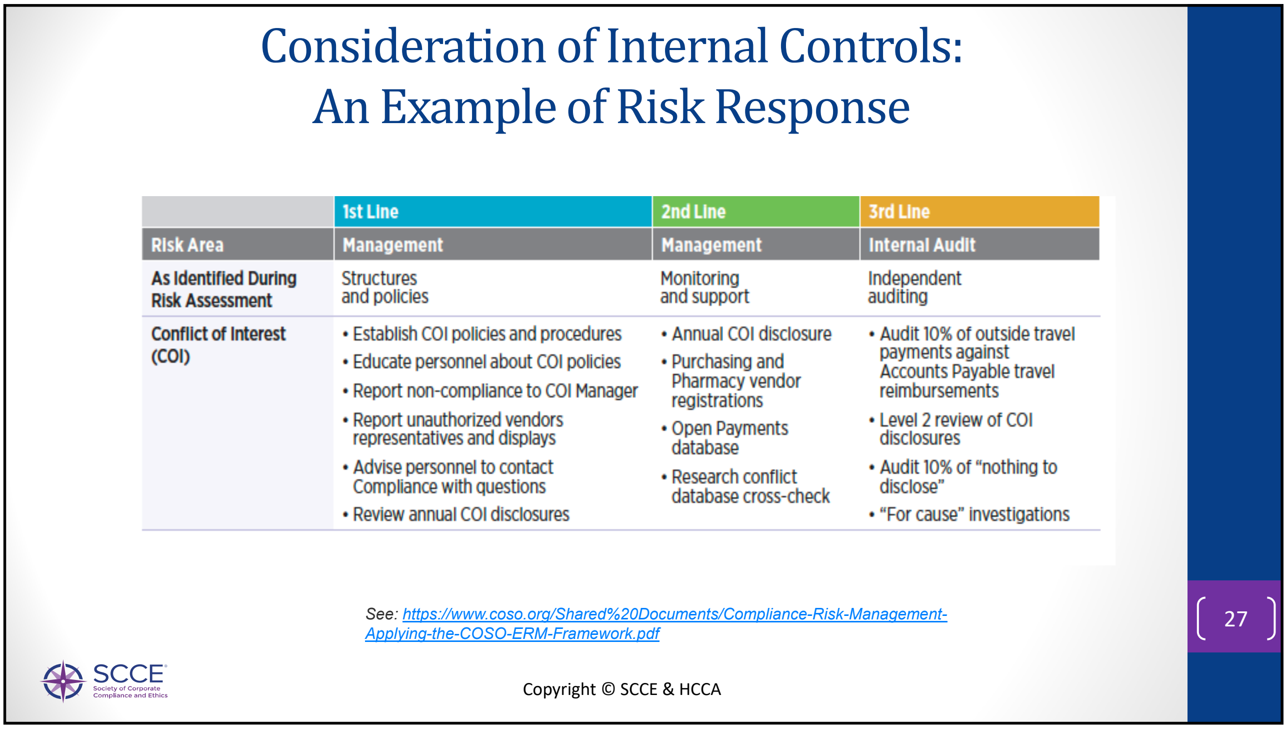
https://www.rmahq.org/erm-framework/

25

Consideration of Internal Controls and Risk Response: A Designer's Approach by Simon Mawer, Blue Wren & Company

SCOPE	DISCOVER	DEFINE	DEVELOP	DELIVER	SCALE
Envision the future, build the team, and plan the journey.	*Build empathy with people and explore the system.*	*Frame the problem and identify design principles.*	*Co-create, prototype, and test many ideas.*	*Pilot promising concepts in the real world.*	*Design for scale, launch, and refine.*
Mindset: Founder	**Mindset: Beginner**	**Mindset: Analyst**	**Mindset: Child**	**Mindset: Scientist**	**Mindset: Operator**
Goal ‣ Engage the team ‣ Secure a mandate	**Goal** ‣ Understand the system ‣ Understand user journeys	**Goal** ‣ Identify unmet needs ‣ Define the challenge	**Goal** ‣ 10+ alternatives ‣ Alpha tests with users	**Goal** ‣ Phased pilots ‣ Business design	**Goal** ‣ Scale and integrate ‣ Design org. systems
Activities ‣ Vision: goals and values ‣ Sense of urgency ‣ Project Charter ‣ Mgt. support. ‣ Build the winning team ‣ Team Charter ‣ Comms. plan	**Activities** ‣ Build empathy ‣ Learn from users, experts, research ‣ Map the system ‣ Map user journeys ‣ Stakeholder analyses	**Activities** ‣ Synthesize learning ‣ Define ideal process ‣ Define frictions ‣ Define PoV ‣ User feedback ‣ Broaden support	**Activities** ‣ Generate ideas ‣ Create concepts ‣ Think small ‣ Rapid prototypes ‣ Design principles	**Activities** ‣ Capture baseline ‣ Live testing ‣ Phased pilots ‣ Refine and validate ‣ Business model canvas ‣ Build rollout plan	**Activities** ‣ Design organization ‣ Training ‣ Monitoring and metrics ‣ Engagement strategy ‣ Implement and refine ‣ Storytelling!
Key Milestones ‣ Sign-off ‣ Core Team Kick-Off	**Key Milestones** ‣ Learning snapshot	**Key Milestones** ‣ Synthesis Review	**Key Milestones** ‣ Co-design sessions ‣ Concept review	**Key Milestones** ‣ Solution Review ‣ Approval	**Key Milestones** ‣ Solution Review

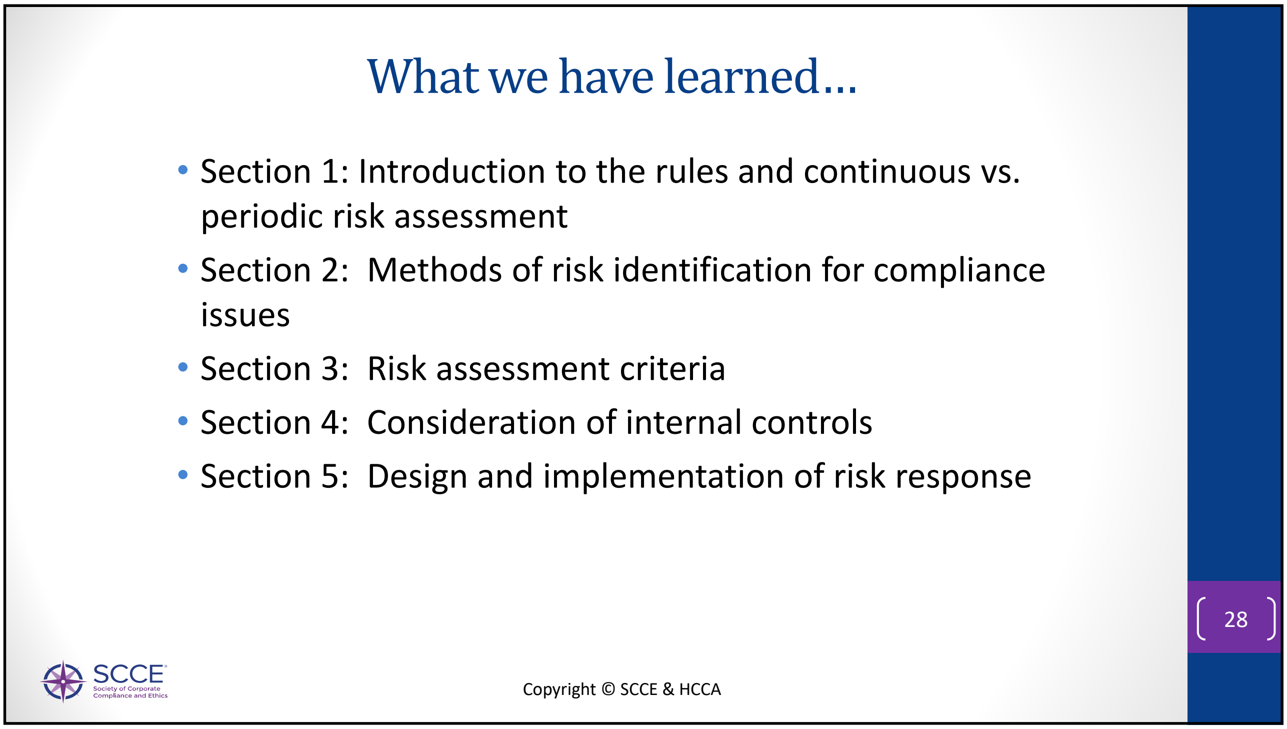
26



Consideration of Internal Controls: An Example of Risk Response

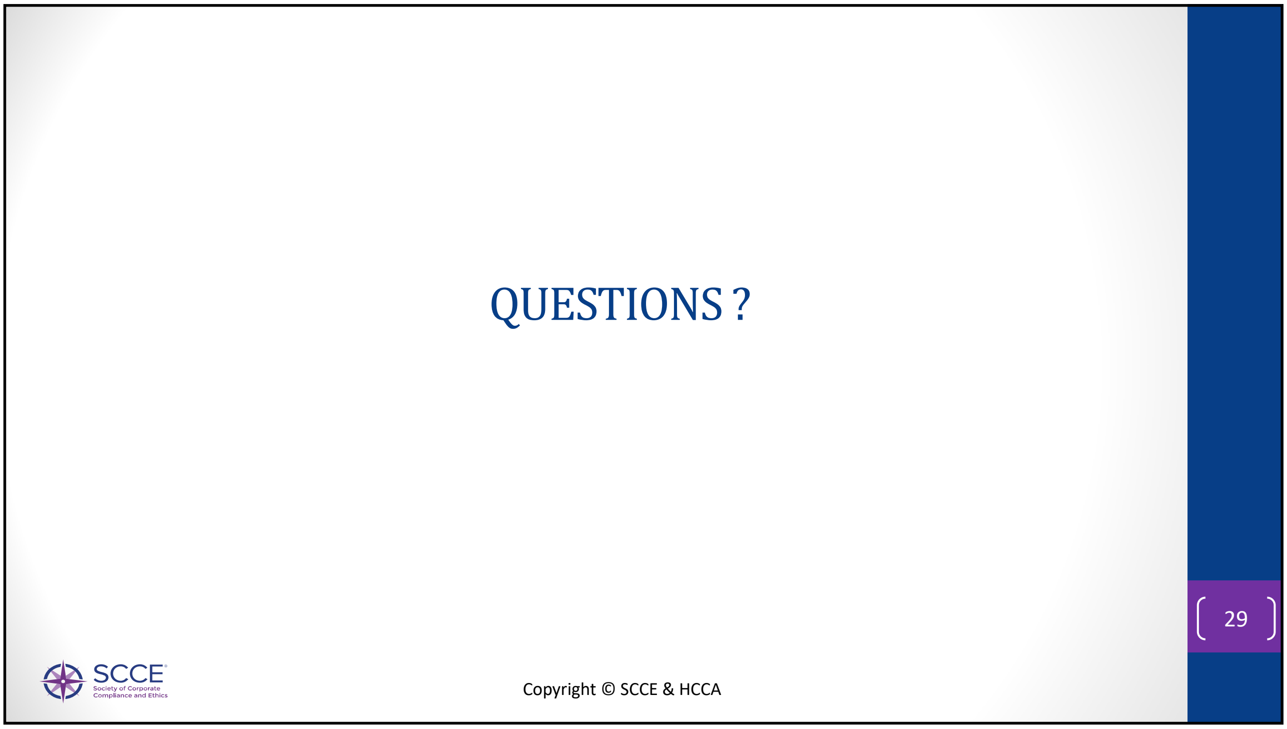
	1st Line	2nd Line	3rd Line
Risk Area	**Management**	**Management**	**Internal Audit**
As Identified During Risk Assessment	Structures and policies	Monitoring and support	Independent auditing
Conflict of Interest (COI)	• Establish COI policies and procedures • Educate personnel about COI policies • Report 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



What we have learned…

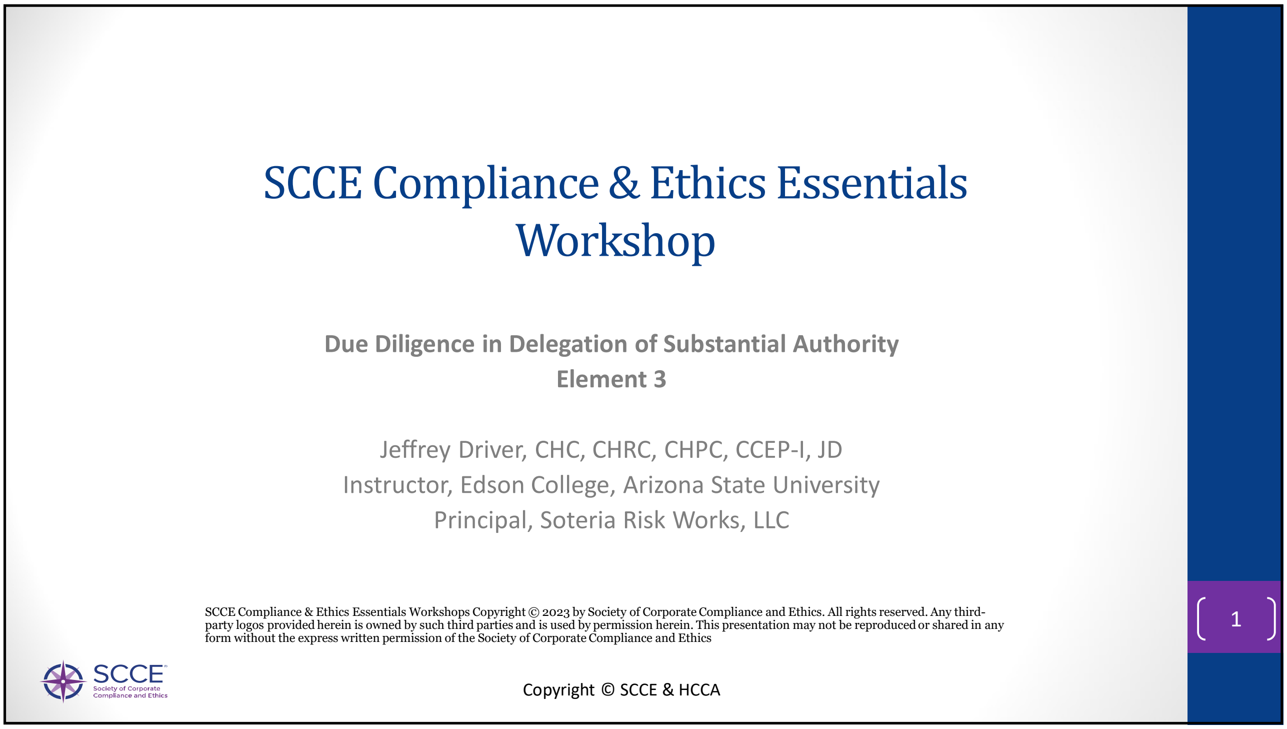
- Section 1: Introduction to the rules and continuous vs. periodic risk assessment
- Section 2: Methods of risk identification for compliance issues
- Section 3: Risk assessment criteria
- Section 4: Consideration of internal controls
- Section 5: Design and implementation of risk response



QUESTIONS ?

29

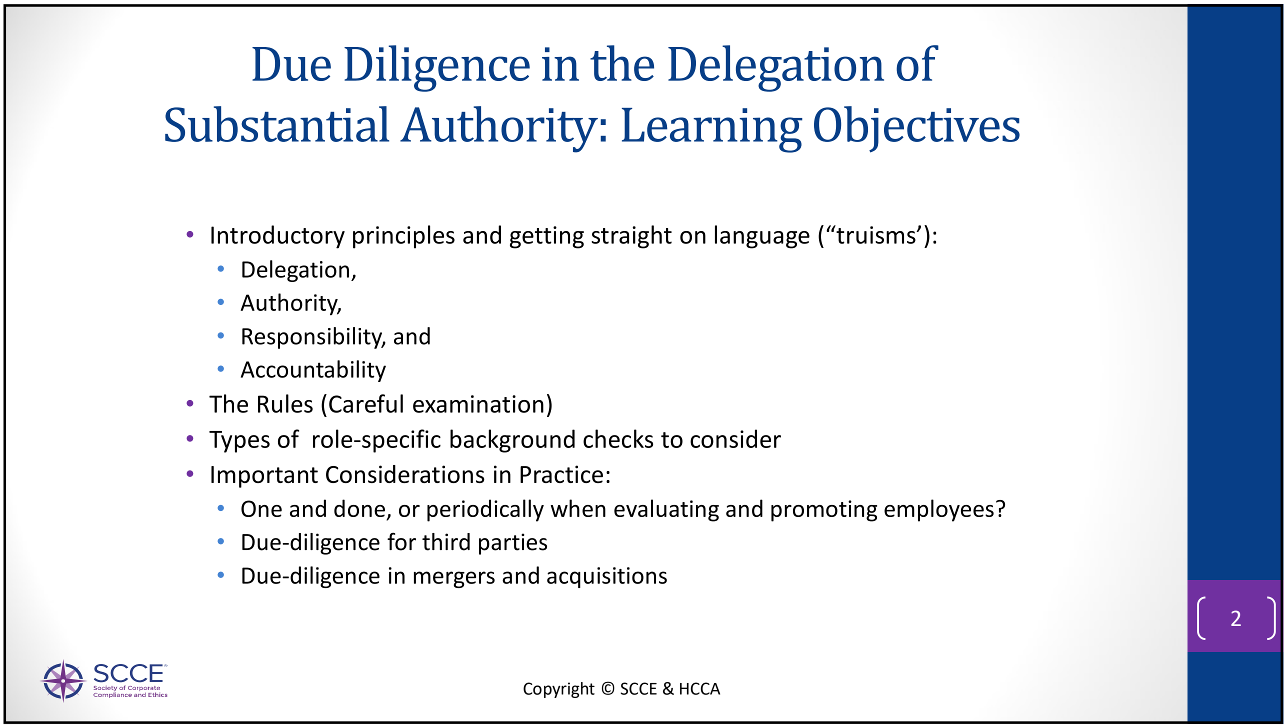
29



SCCE Compliance & Ethics Essentials Workshop

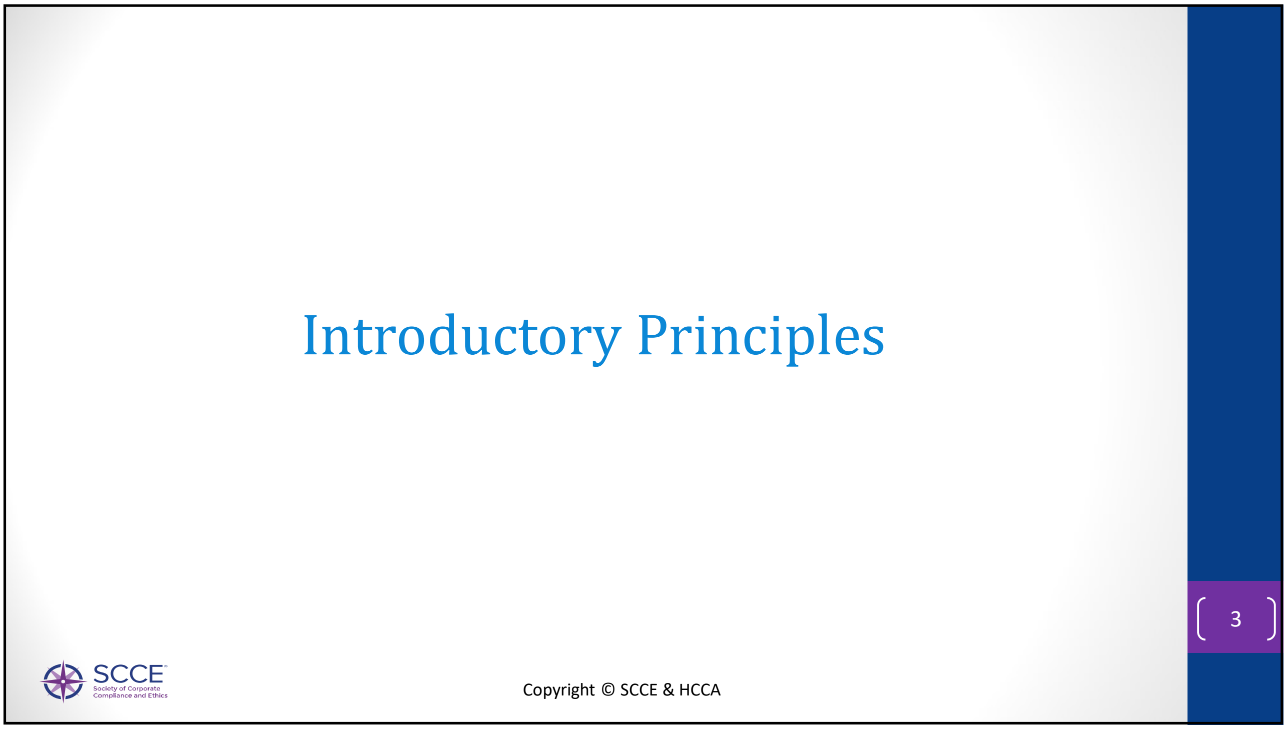
Due Diligence in Delegation of Substantial Authority
Element 3

Jeffrey Driver, CHC, CHRC, CHPC, CCEP-I, JD
Instructor, Edson College, Arizona State University
Principal, Soteria Risk Works, LLC

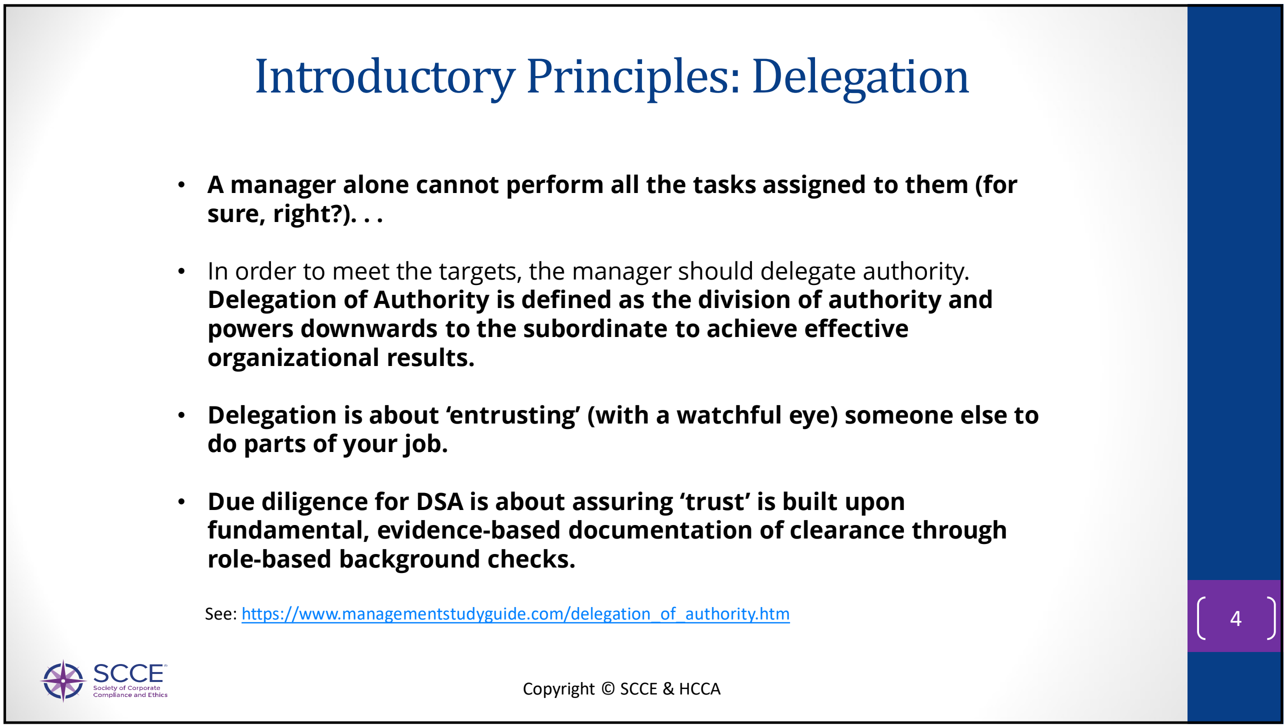


Due Diligence in the Delegation of Substantial Authority: Learning Objectives

- 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

- **A manager alone cannot perform all the tasks assigned to them (for sure, right?). . .**
- In order to meet the targets, the manager should delegate authority. **Delegation of Authority is defined as the division of authority and powers downwards to the subordinate to achieve effective organizational results.**
- **Delegation is about '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.**

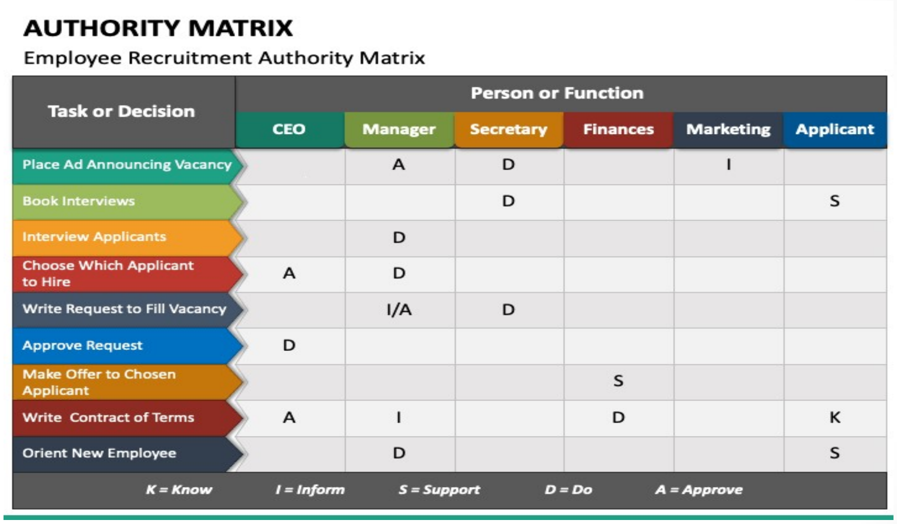
See: https://www.managementstudyguide.com/delegation_of_authority.htm

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)**. All people who have the authority should know what is the scope of their authority is and they shouldn't misutilize it. We can also audit compliance with a clearly defined authority matrix.
- **The 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 (next slide)**.
- **Delegating the authority to someone else doesn't imply escaping from accountability.** Accountability still rest with the person having the utmost authority.

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

Example of Recruitment Authority Matrix – What's missing?



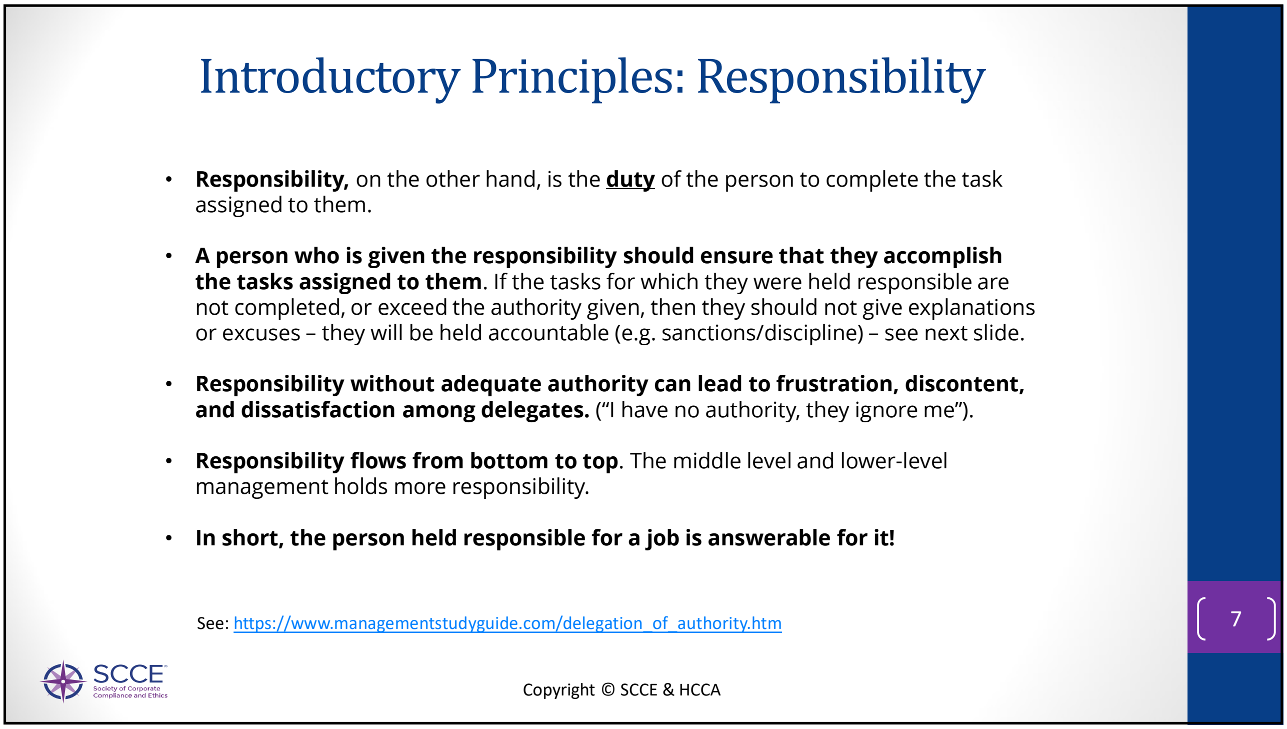
AUTHORITY MATRIX

Employee Recruitment Authority Matrix

Task or Decision	Person or Function					
	CEO	Manager	Secretary	Finances	Marketing	Applicant
Place Ad Announcing Vacancy		A	D		I	
Book Interviews			D			S
Interview Applicants		D				
Choose Which Applicant to Hire	A	D				
Write Request to Fill Vacancy		I/A	D			
Approve Request	D					
Make Offer to Chosen Applicant				S		
Write Contract of Terms	A	I		D		K
Orient New Employee		D				S

K = Know *I = Inform* *S = Support* *D = Do* *A = Approve*

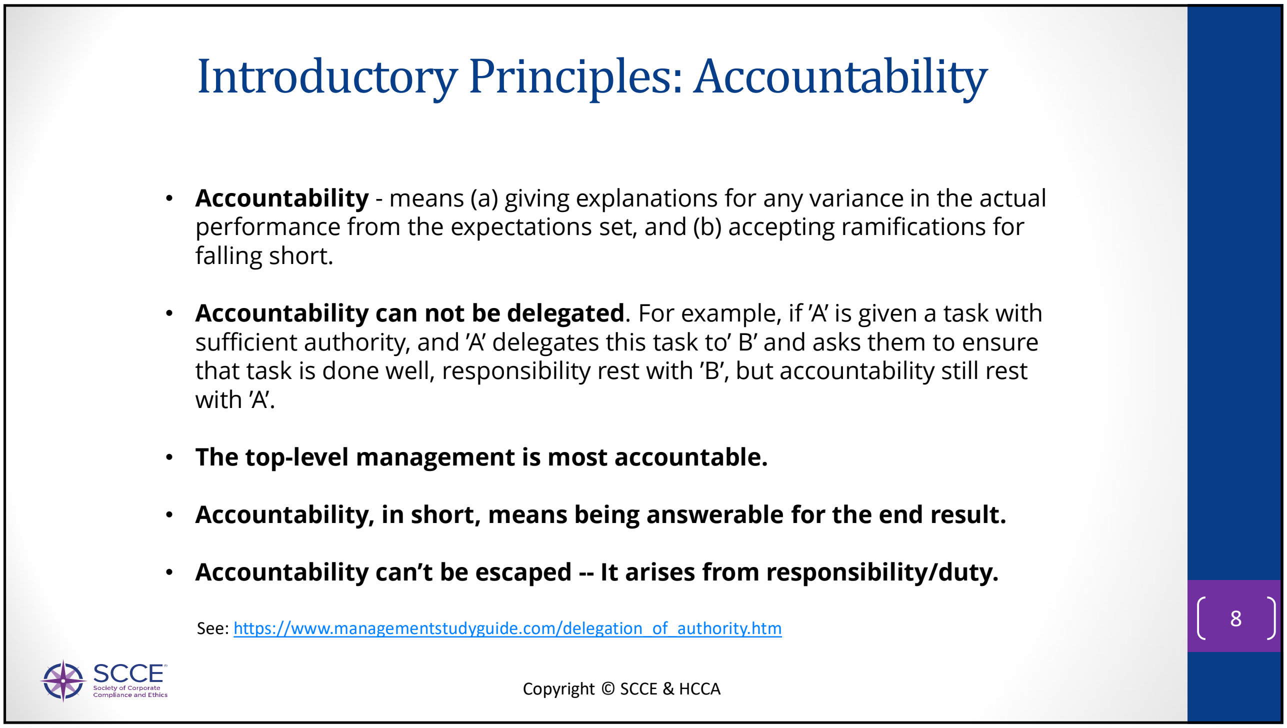
Found at Sketch Bubble



Introductory Principles: Responsibility

- **Responsibility,** on the other hand, is the **duty** of the person to complete the task assigned to them.
- **A person who is given the responsibility should ensure that they accomplish the tasks assigned to them**. If the tasks for which they were held responsible are not completed, or exceed the authority given, then they should not give explanations or excuses – they will be held accountable (e.g. sanctions/discipline) – see next slide.
- **Responsibility without adequate authority can lead to frustration, discontent, and dissatisfaction among delegates.** ("I have no authority, they ignore me").
- **Responsibility flows from bottom to top**. The middle level and lower-level management holds more responsibility.
- **In short, the person held responsible for a job is answerable for it!**

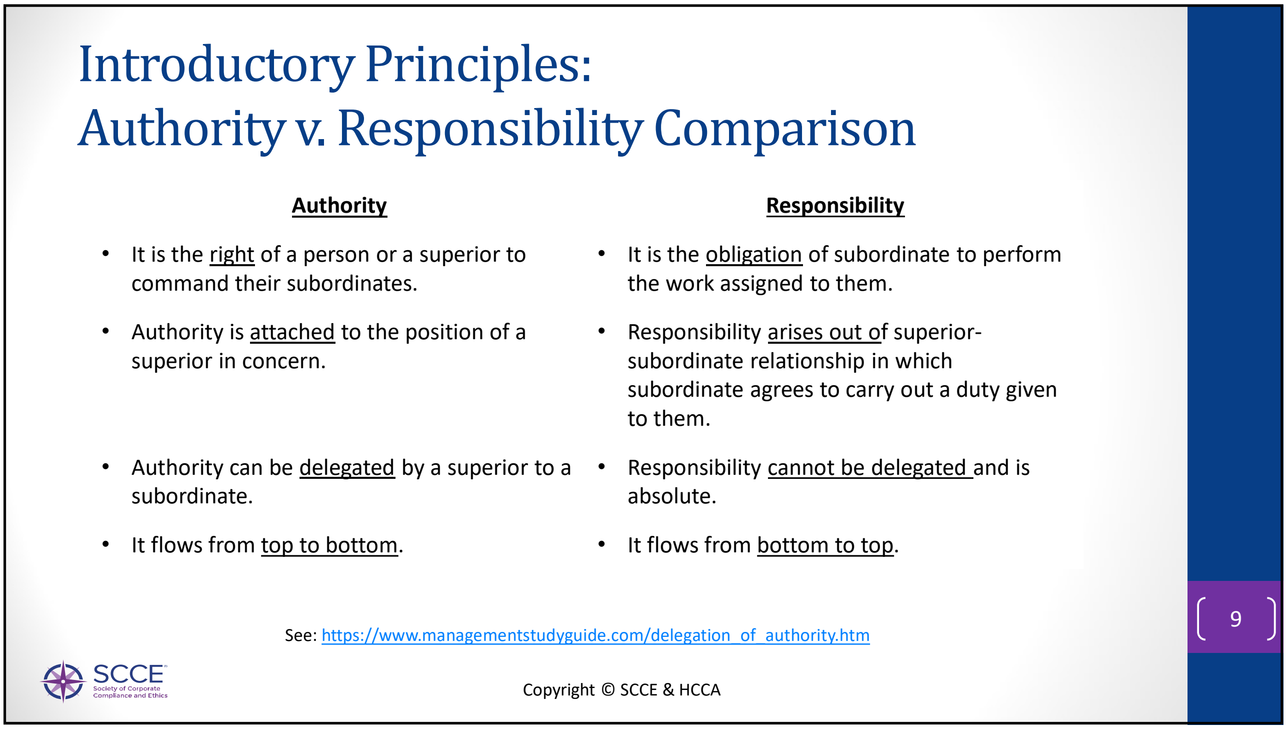
See: https://www.managementstudyguide.com/delegation_of_authority.htm



Introductory Principles: Accountability

- **Accountability** - means (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 'A' is given a task with sufficient authority, and 'A' delegates this task to' B' and asks them to ensure that task is done well, responsibility rest with 'B', but accountability still rest with 'A'.
- **The top-level management is most accountable.**
- **Accountability, in short, means being answerable for the end result.**
- **Accountability can't be escaped -- It arises from responsibility/duty.**

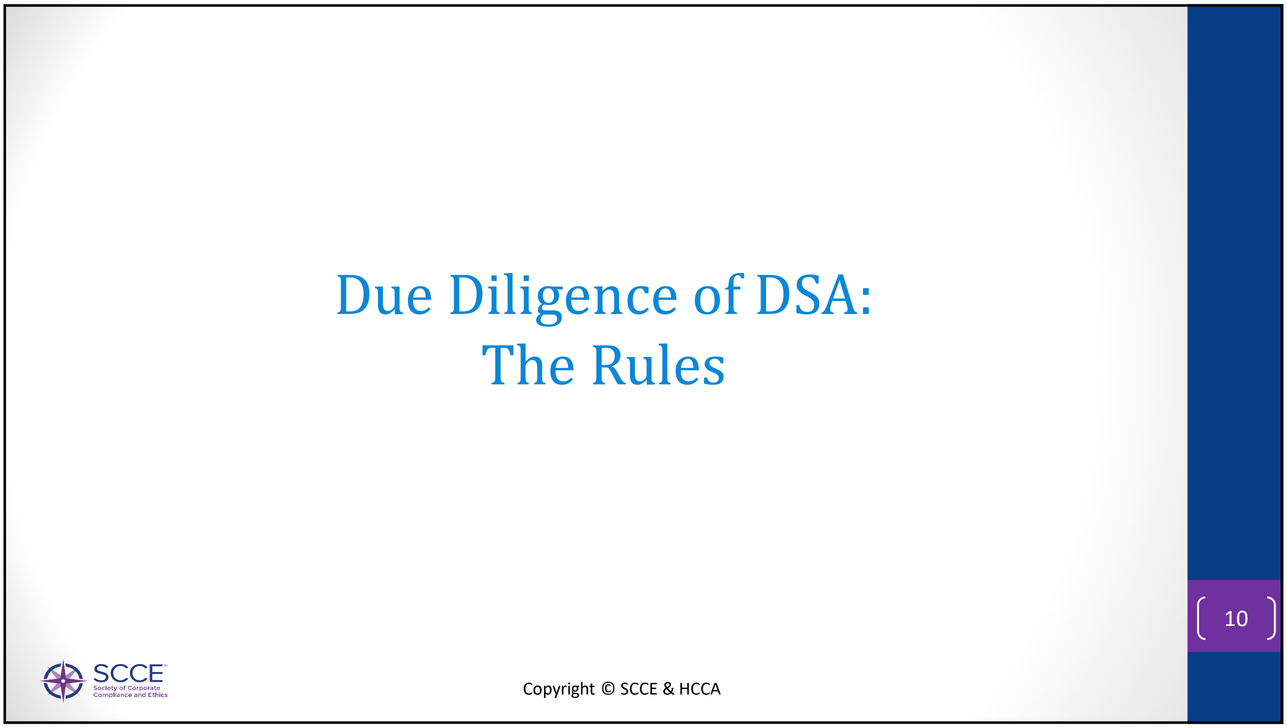
See: https://www.managementstudyguide.com/delegation_of_authority.htm



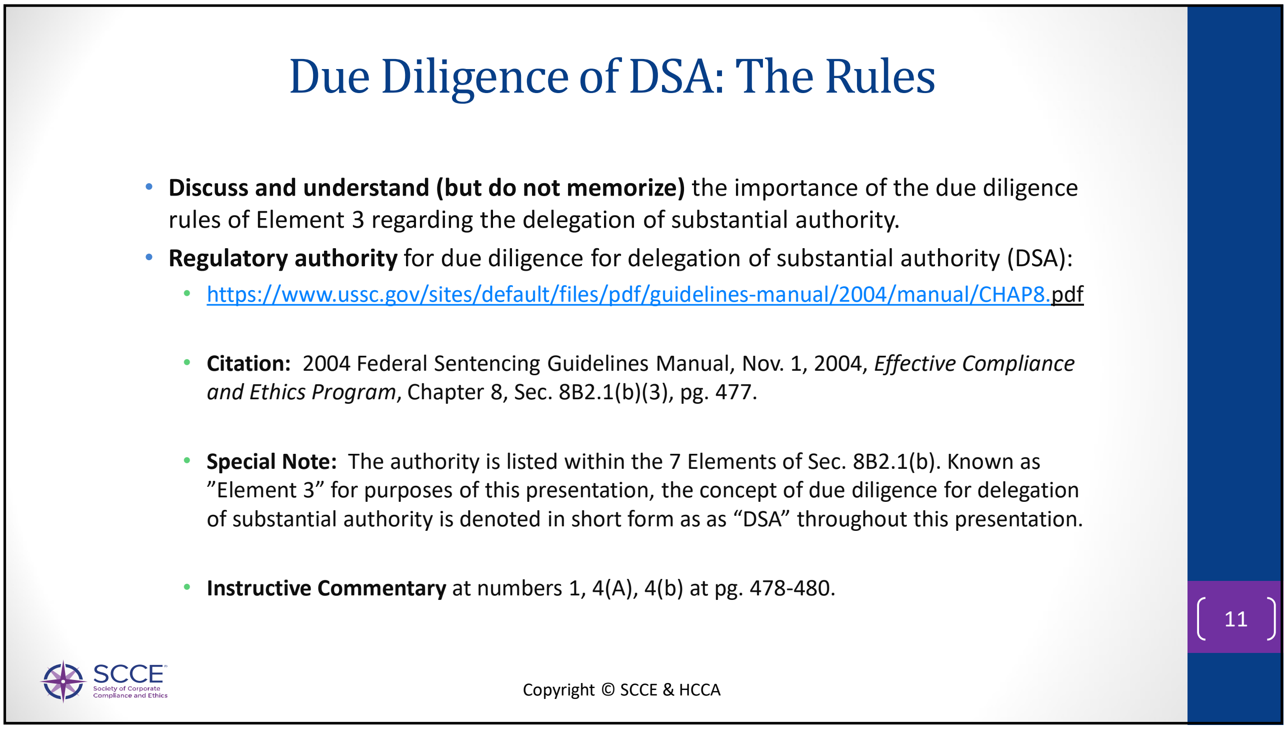
Introductory Principles: Authority v. Responsibility Comparison

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 in concern.	• Responsibility arises out of 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 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

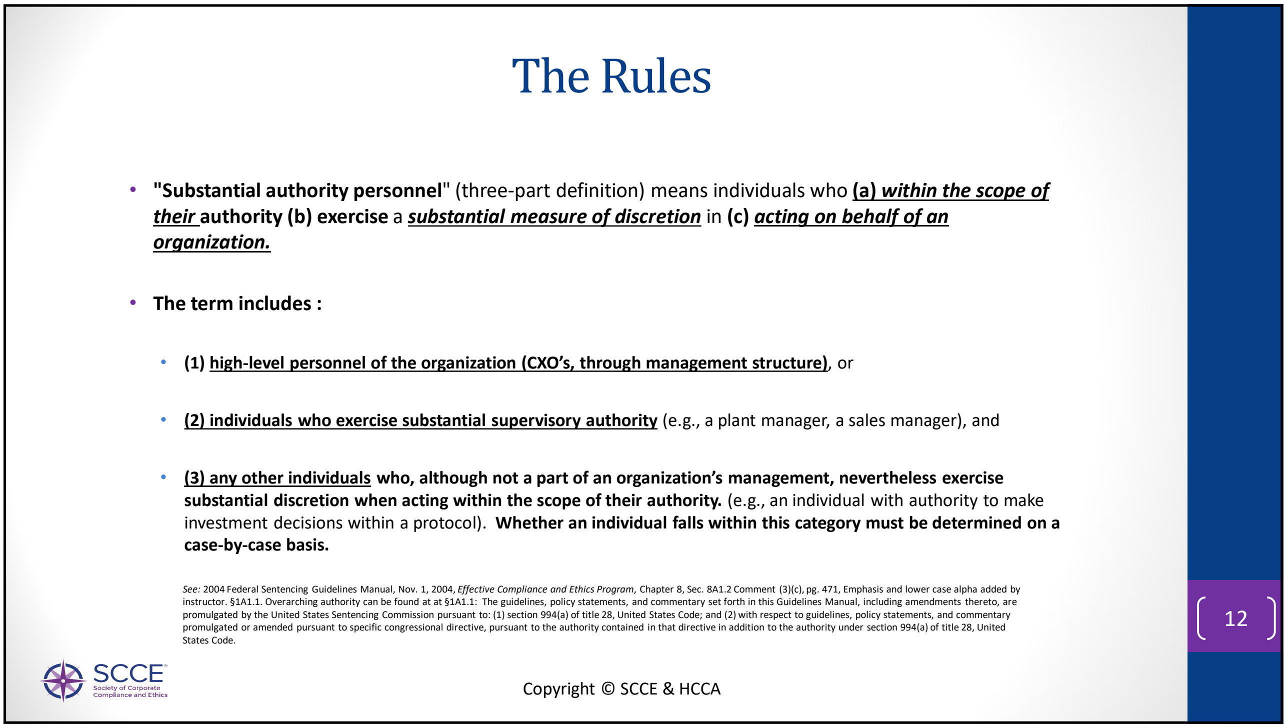


Due Diligence of DSA: The Rules



Due Diligence of DSA: The Rules

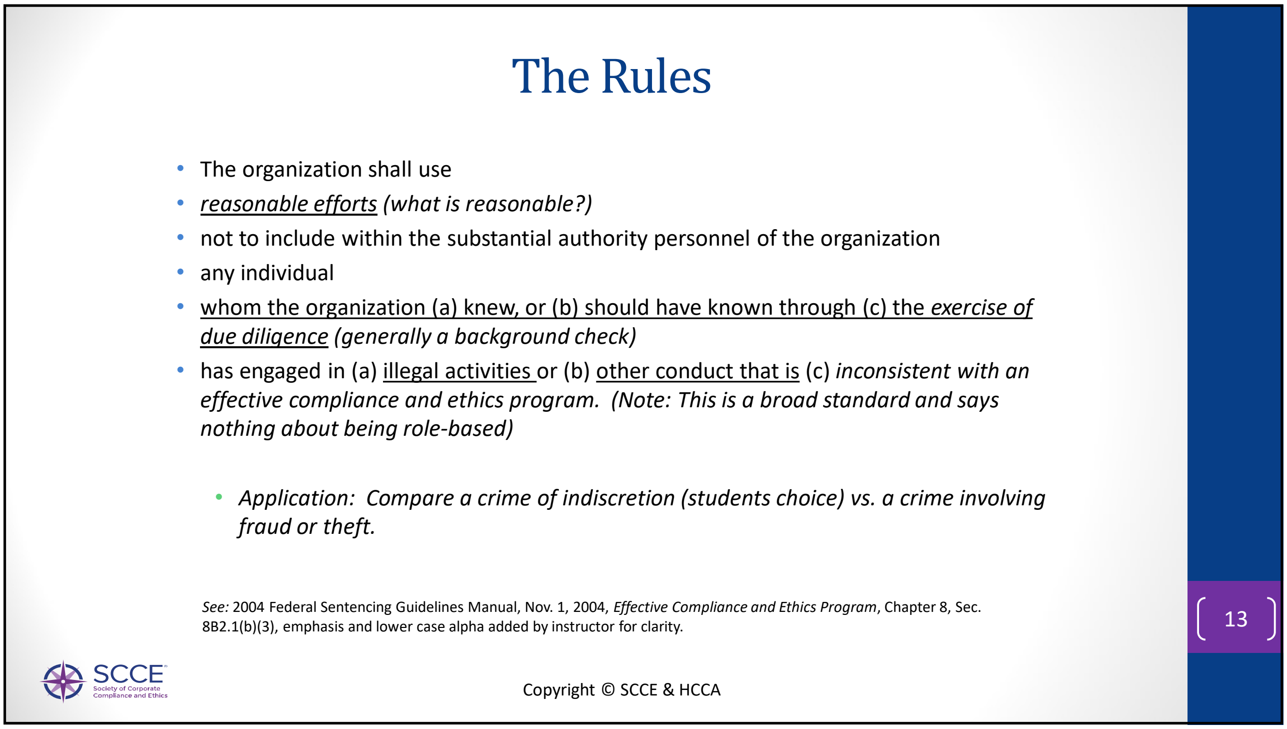
- **Discuss and understand (but do not memorize)** the importance of the due diligence rules of Element 3 regarding the delegation of substantial authority.
- **Regulatory authority** for due diligence for delegation of substantial authority (DSA):
  - https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2004/manual/CHAP8.pdf
  - **Citation:** 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1(b)(3), pg. 477.
  - **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.
  - **Instructive Commentary** at numbers 1, 4(A), 4(b) at pg. 478-480.



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, through 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

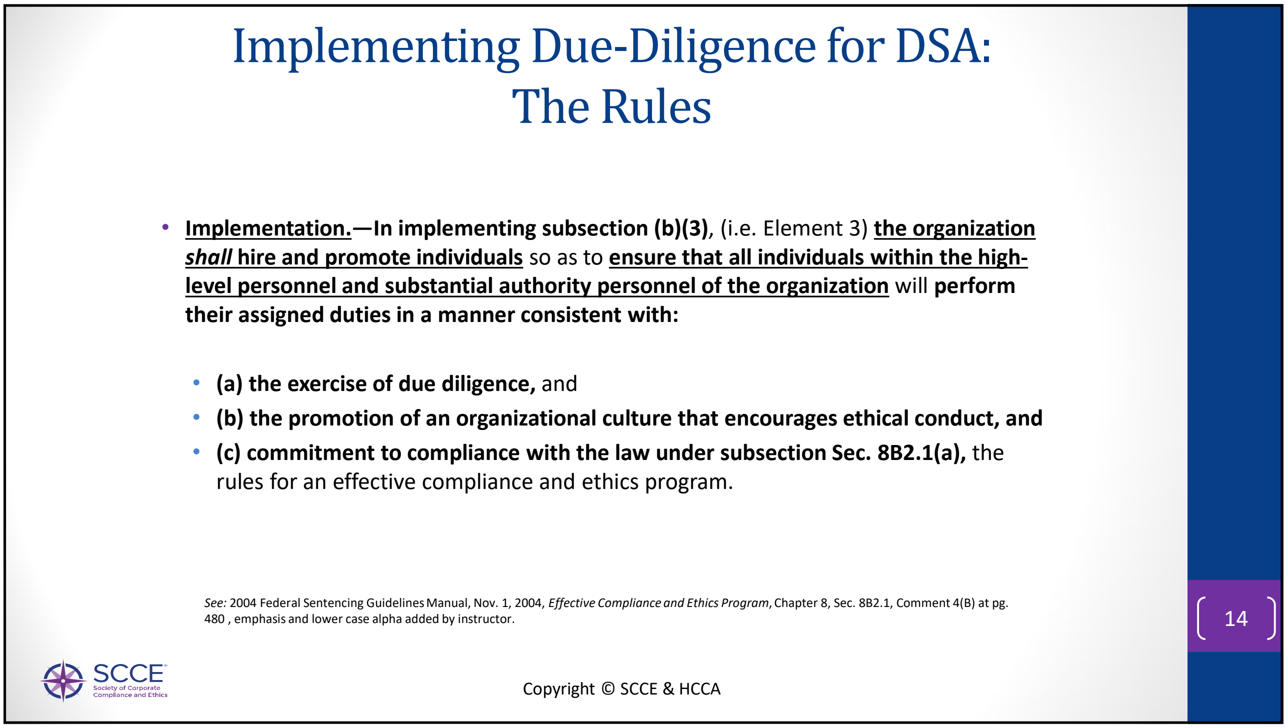
- The organization shall use
- *reasonable efforts (what is reasonable?)*
- not to include within the substantial authority personnel of the organization
- any individual
- whom the organization (a) knew, or (b) should have known through (c) the *exercise of due diligence (generally a background check)*
- 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)*
  - *Application: Compare a crime of indiscretion (students choice) vs. a crime involving fraud or theft.*

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1(b)(3), emphasis and lower case alpha added by instructor for clarity.

SCCE Society of Corporate Compliance and Ethics

13

13



Implementing Due-Diligence for DSA: The Rules

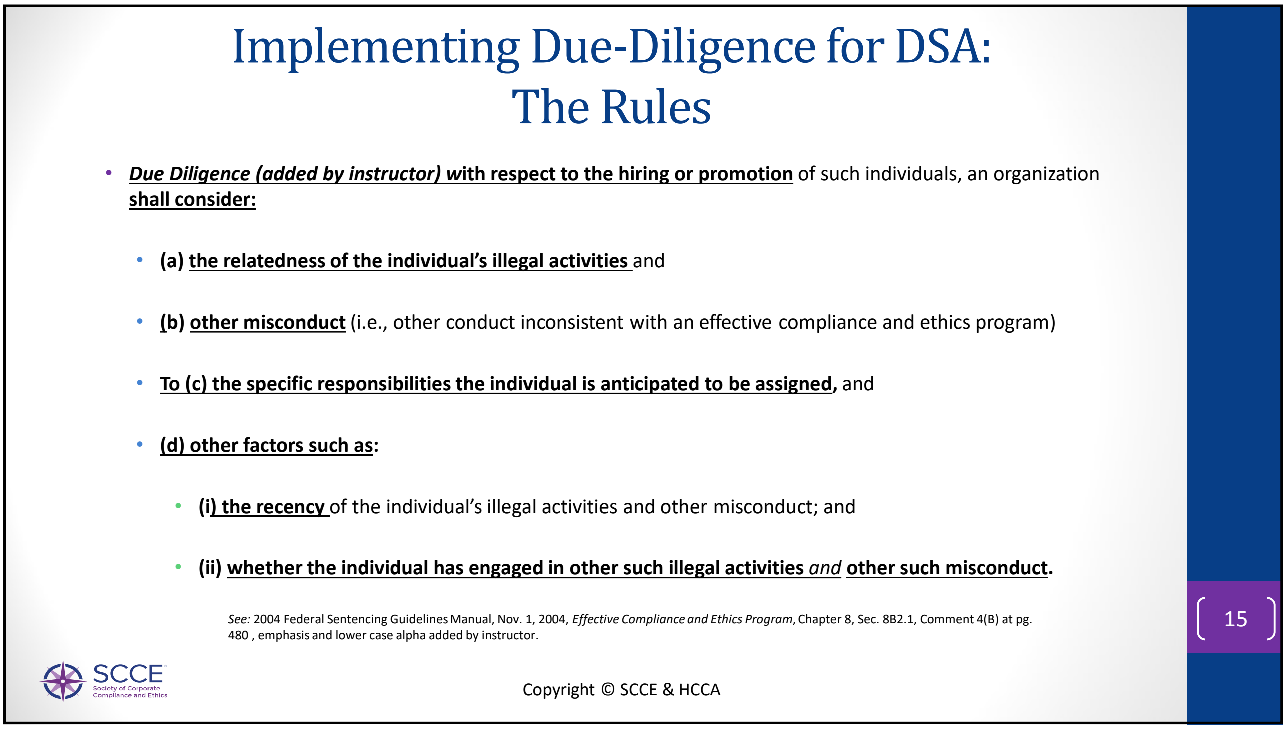
- **Implementation.—In implementing subsection (b)(3)**, (i.e. Element 3) **the organization *shall* hire and promote individuals** so as to **ensure that all individuals within the high-level personnel and substantial authority personnel of the organization** will **perform their assigned duties in 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.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1, Comment 4(B) at pg. 480 , emphasis and lower case alpha added by instructor.

SCCE Society of Corporate Compliance and Ethics

14

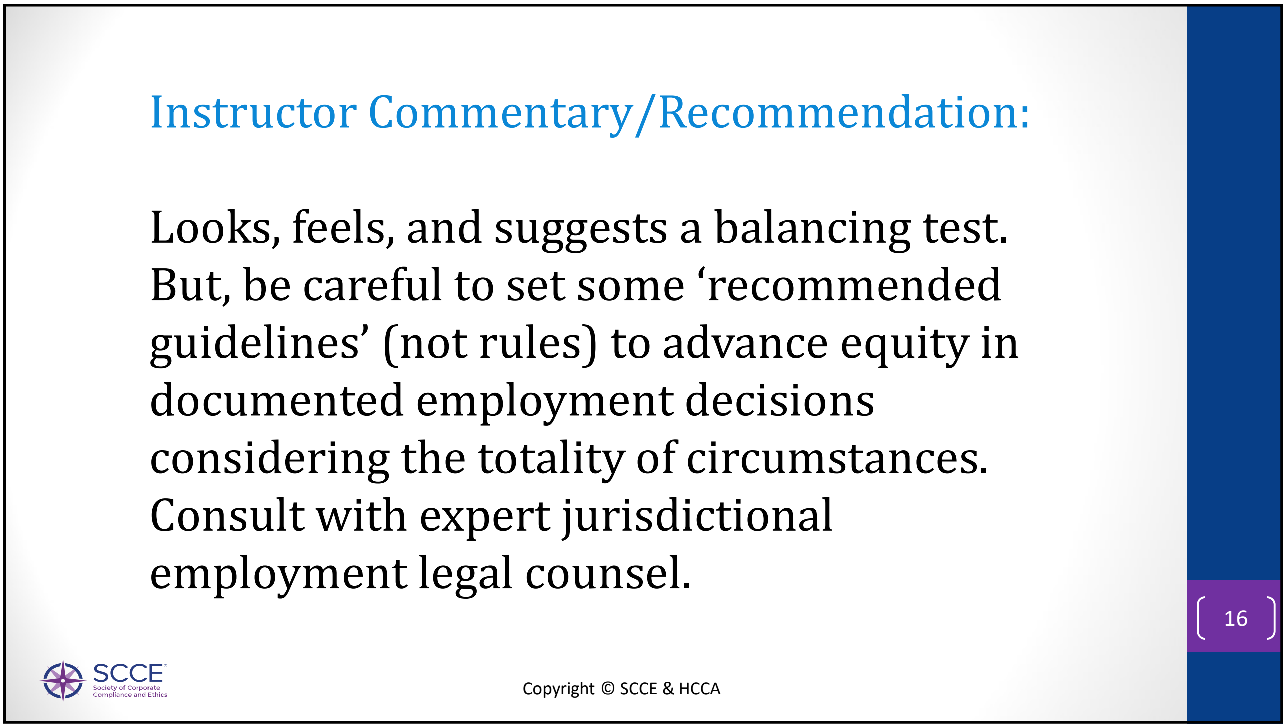
14



Implementing Due-Diligence for DSA: The Rules

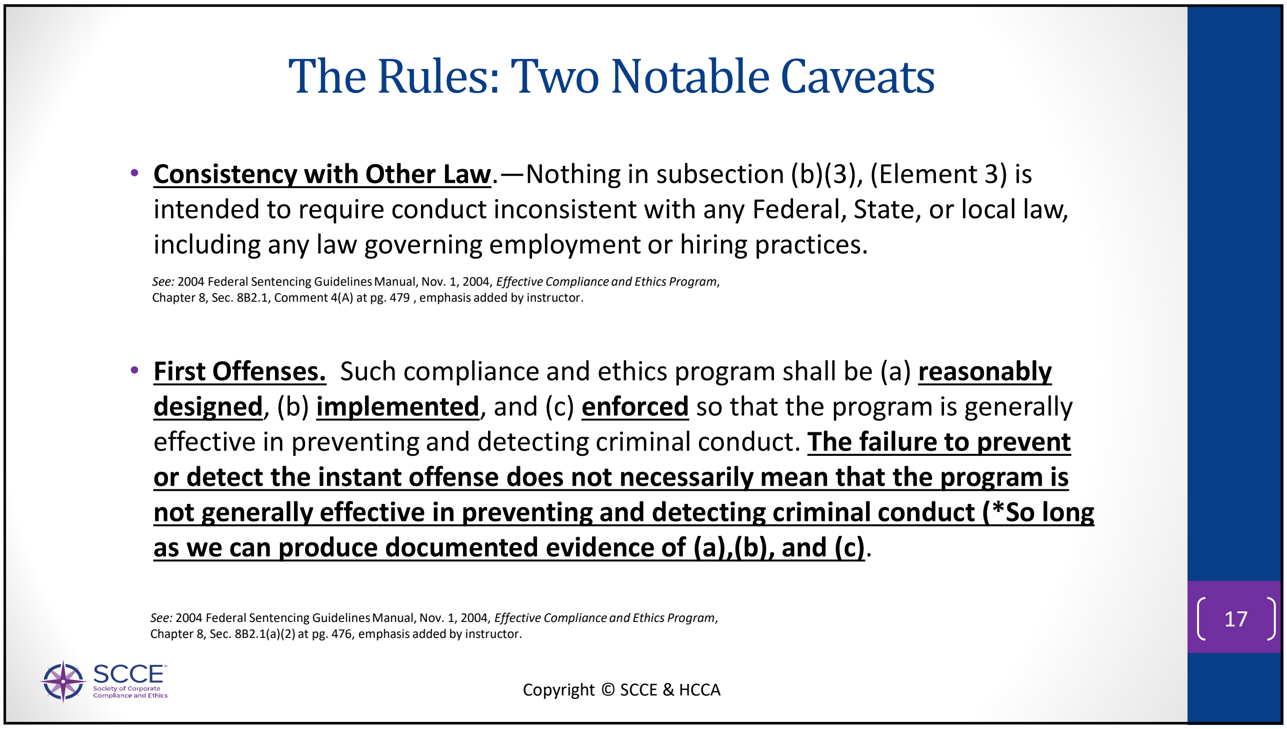
- ***Due Diligence (added by instructor)* with respect to the hiring or promotion** of such individuals, an organization **shall consider:**
  - **(a) the relatedness of the individual's illegal activities** and
  - **(b) other misconduct** (i.e., other conduct inconsistent with an effective compliance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

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1, Comment 4(B) at pg. 480 , emphasis and lower case alpha added by instructor.



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.

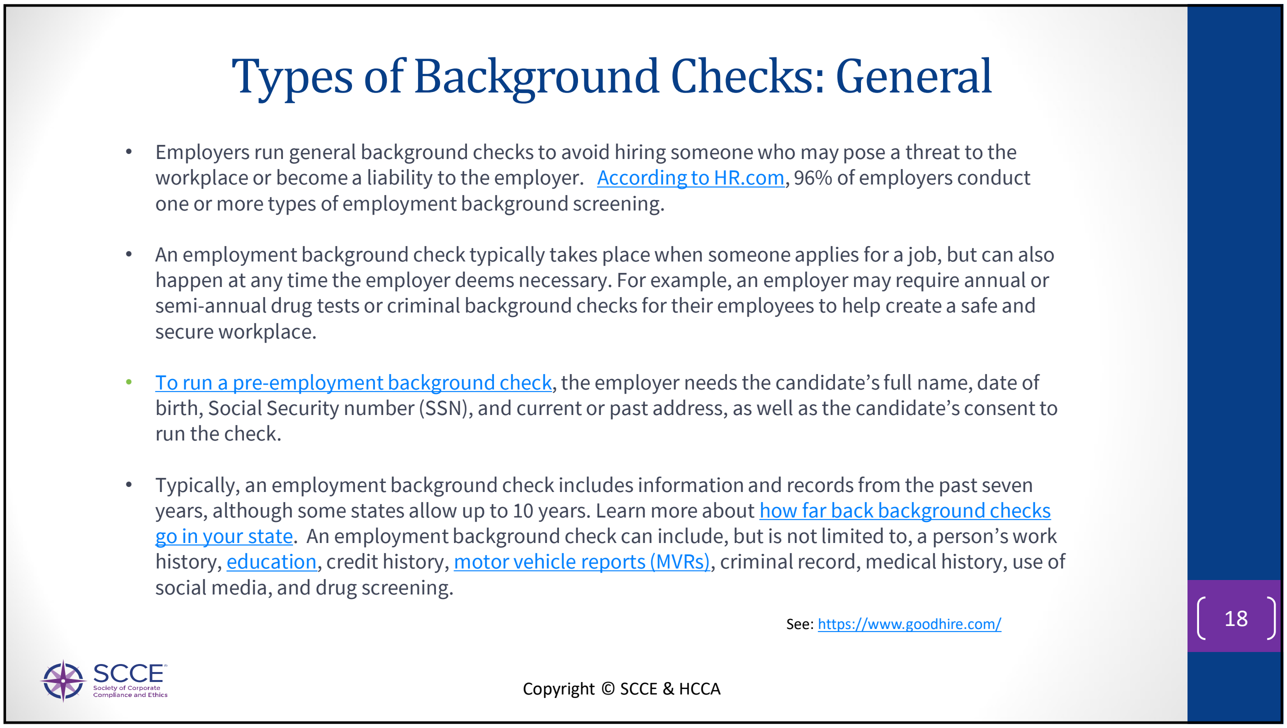
See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1, Comment 4(A) at pg. 479 , emphasis added by instructor.

- **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)**.

See: 2004 Federal Sentencing Guidelines Manual, Nov. 1, 2004, *Effective Compliance and Ethics Program*, Chapter 8, Sec. 8B2.1(a)(2) at pg. 476, emphasis added by instructor.

17

SCCE Society of Corporate Compliance and Ethics



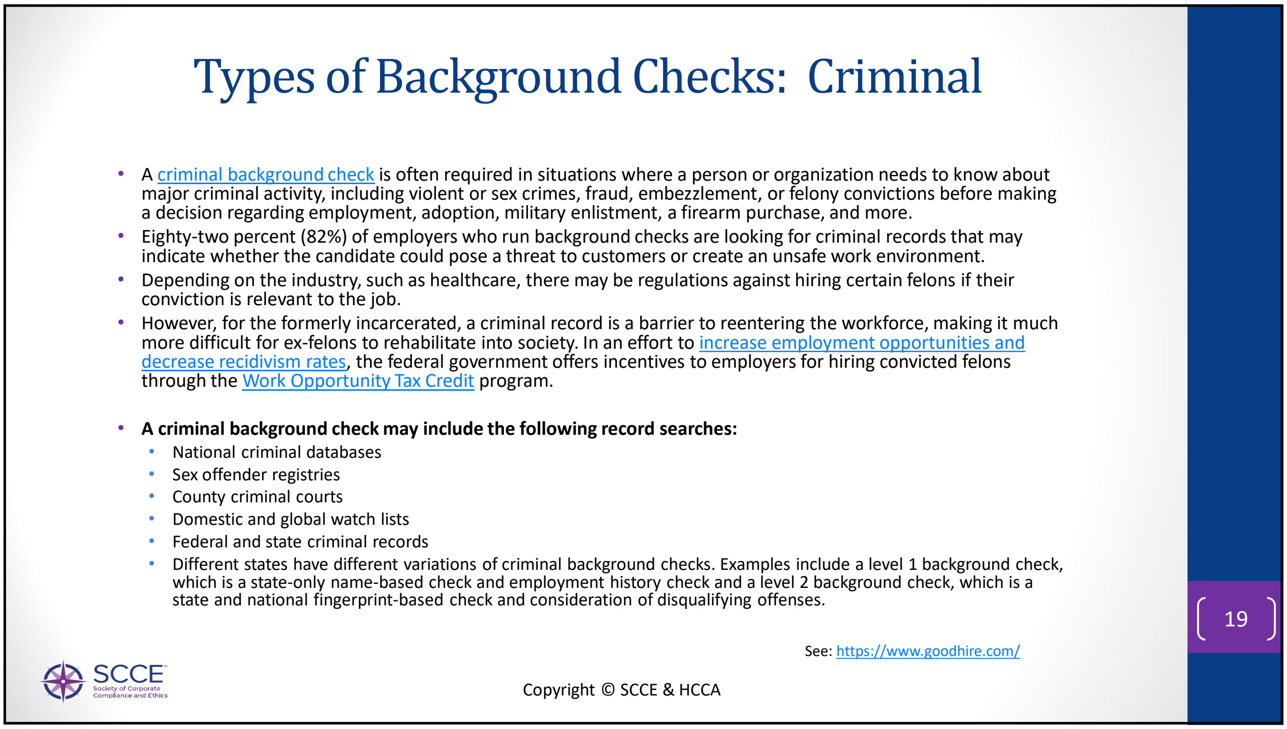
Types of Background Checks: General

- 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.

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

18

SCCE Society of Corporate Compliance and Ethics

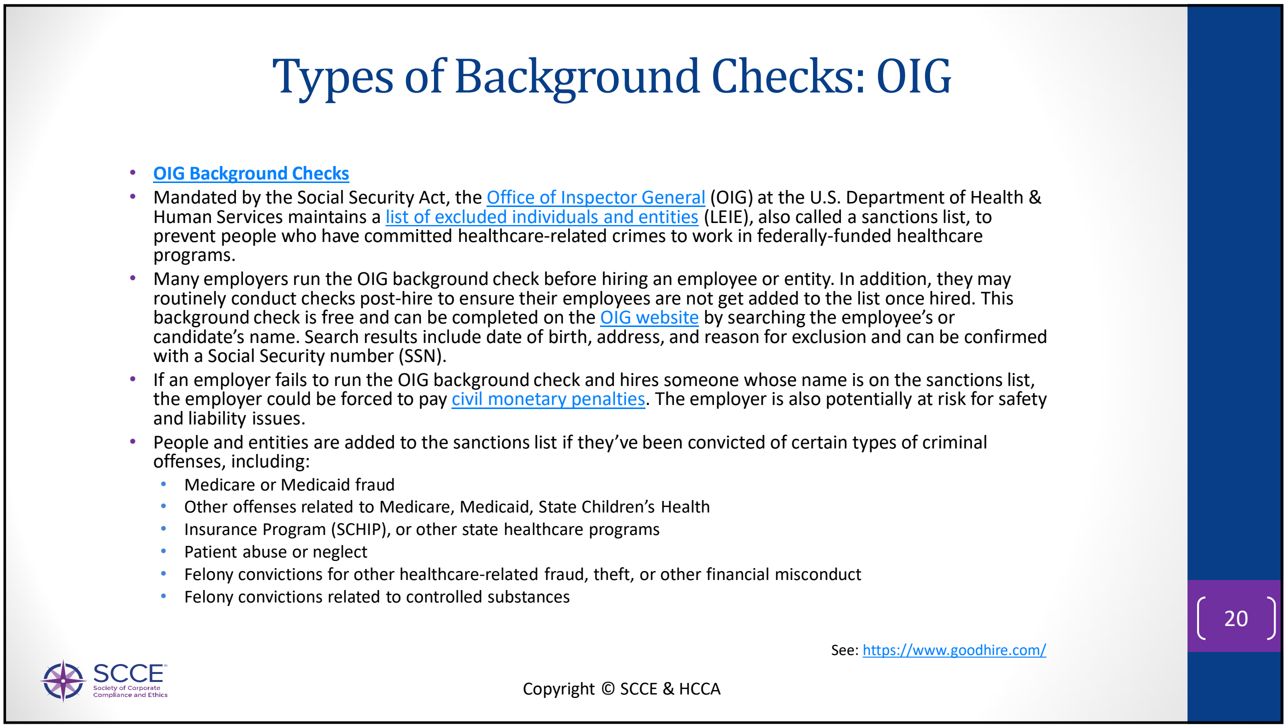


Types of Background Checks: Criminal

- 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.

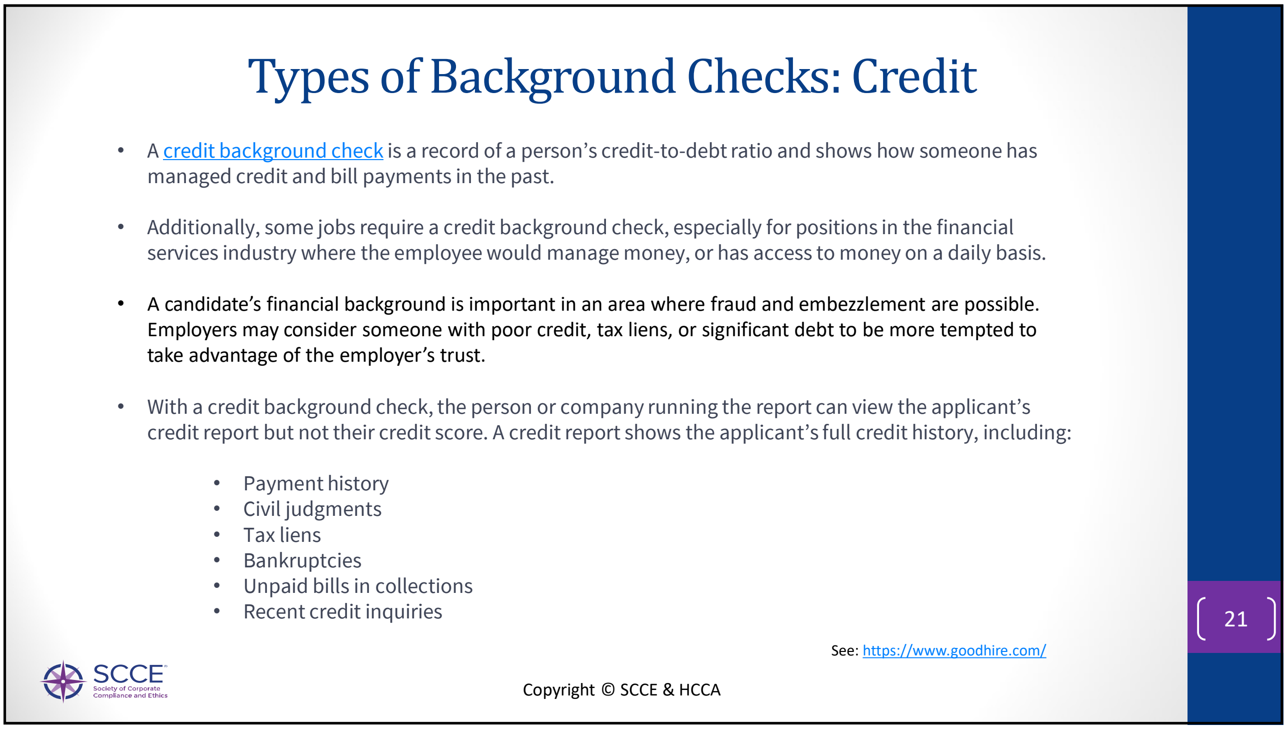
See: https://www.goodhire.com/



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

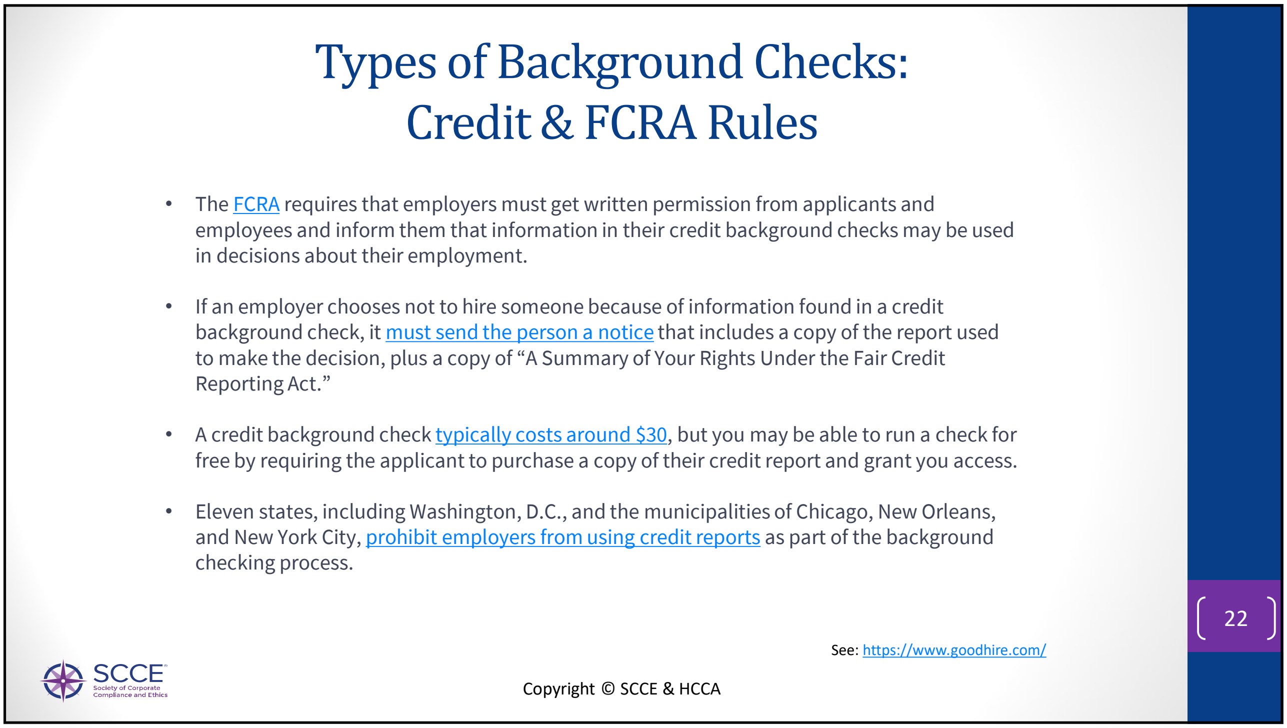
See: https://www.goodhire.com/



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

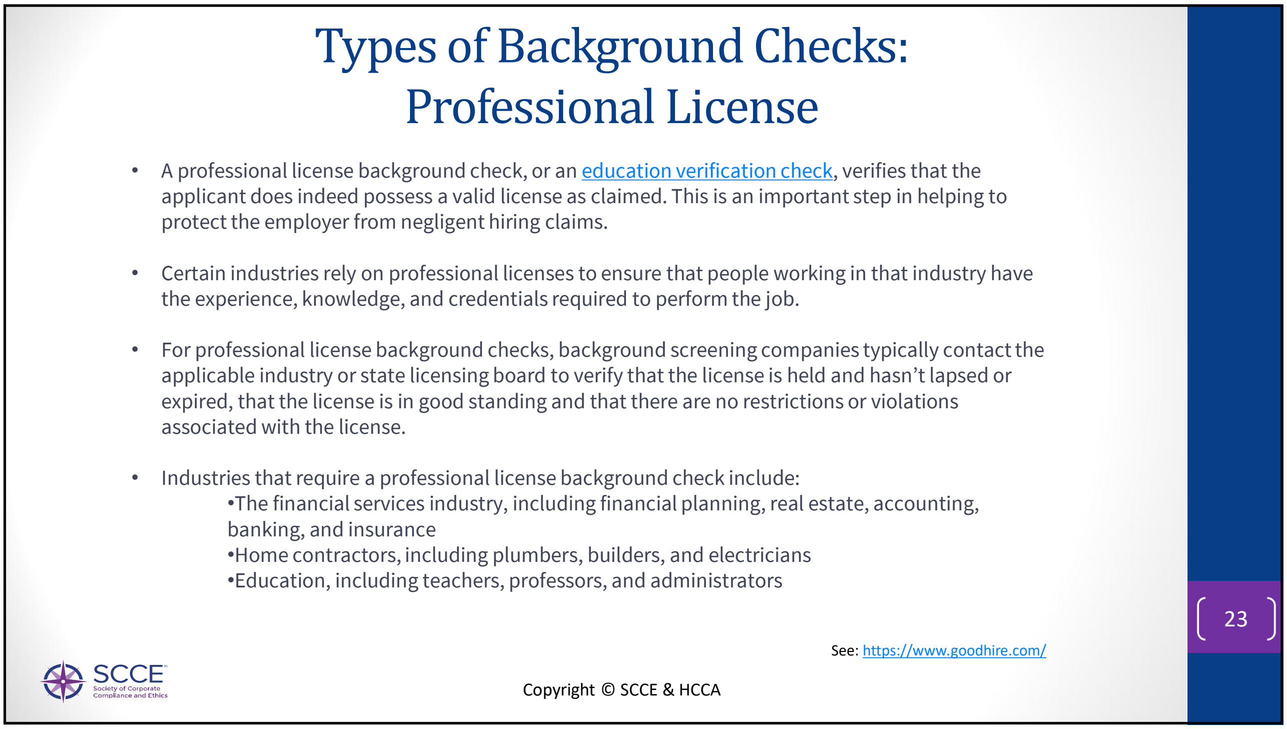
See: https://www.goodhire.com/



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

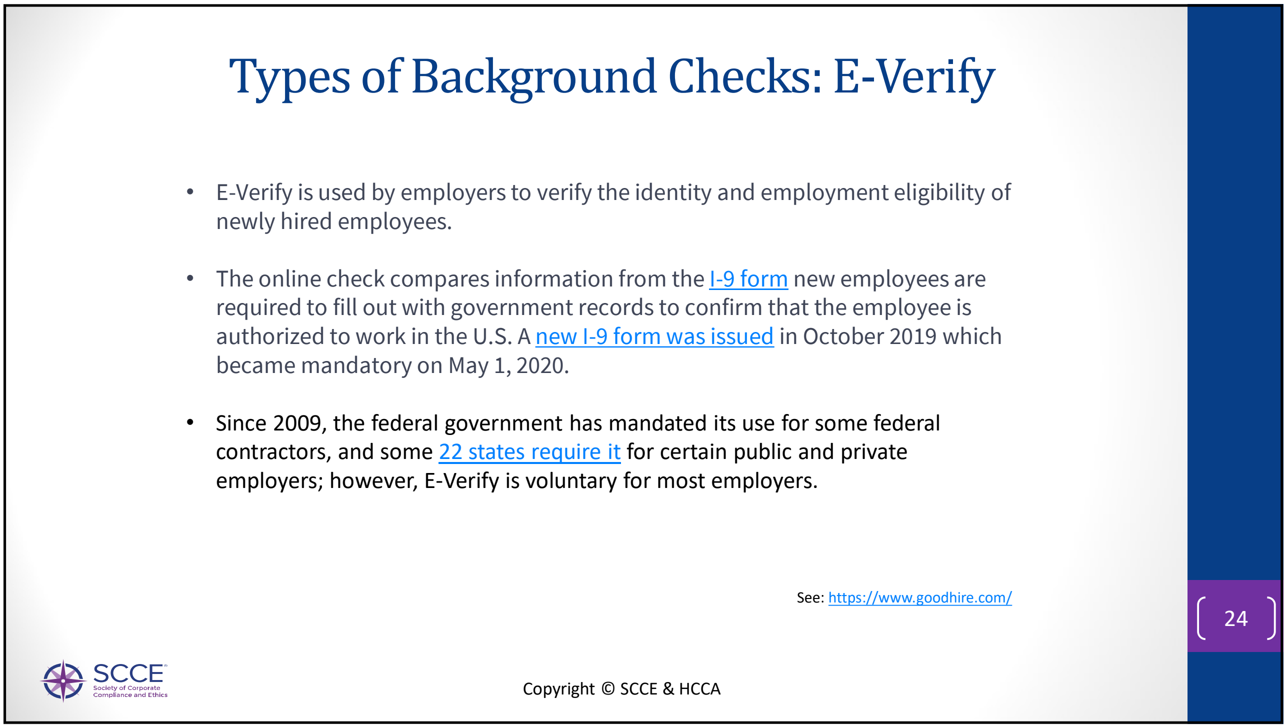
- A professional license background check, or an education verification check, verifies that the applicant does indeed possess a valid license as claimed. This is an important step in helping to protect the employer from negligent hiring claims.

- 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

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



Types of Background Checks: E-Verify

- E-Verify is used by employers to verify the identity and employment eligibility of newly hired employees.

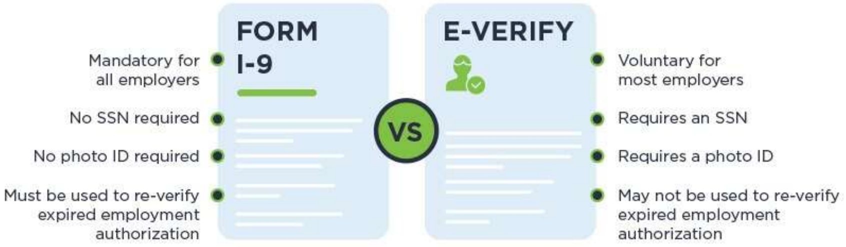
- The online check compares information from the I-9 form new employees are required to fill out with government records to confirm that the employee is authorized to work in the U.S. A new I-9 form was issued in October 2019 which became mandatory on May 1, 2020.

- Since 2009, the federal government has mandated its use for some federal contractors, and some 22 states require it for certain public and private employers; however, E-Verify is voluntary for most employers.

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

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:



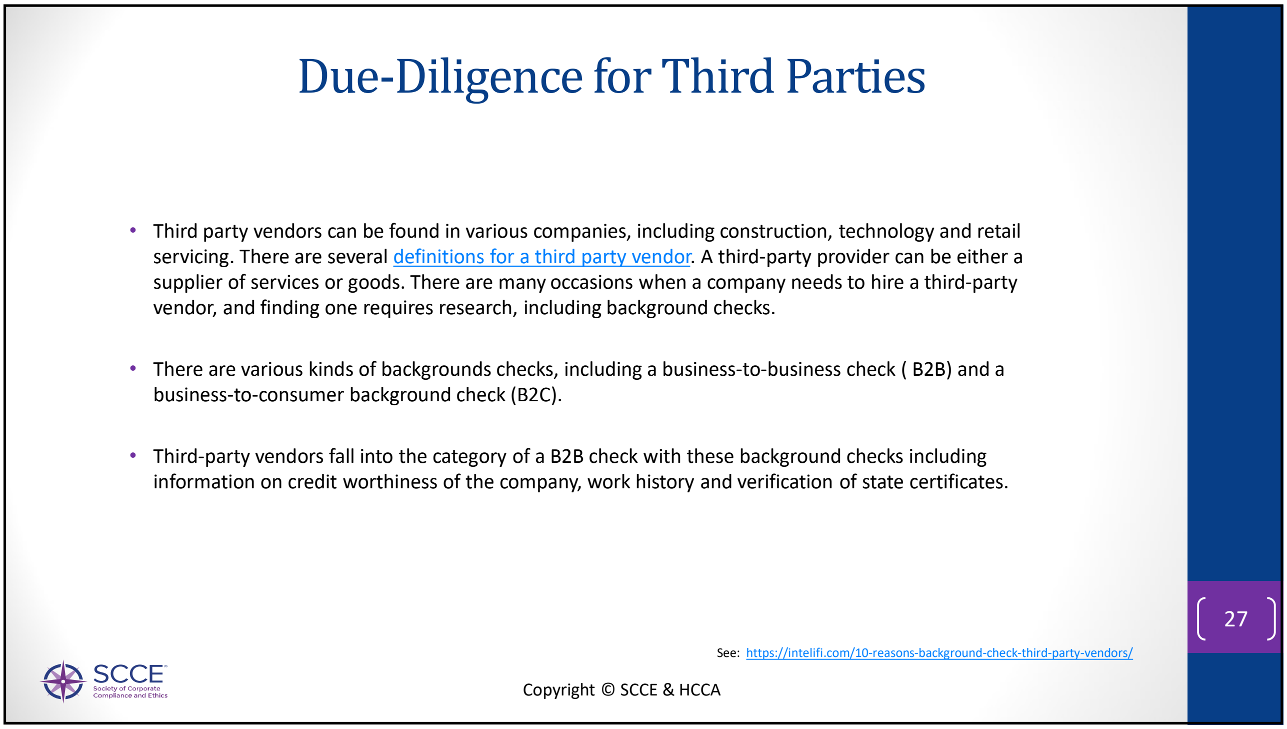
FORM I-9	E-VERIFY
Mandatory for all employers	Voluntary for most employers
No SSN required	Requires an SSN
No photo ID required	Requires a photo ID
Must be used to re-verify expired employment authorization	May not be used to re-verify expired employment authorization

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/



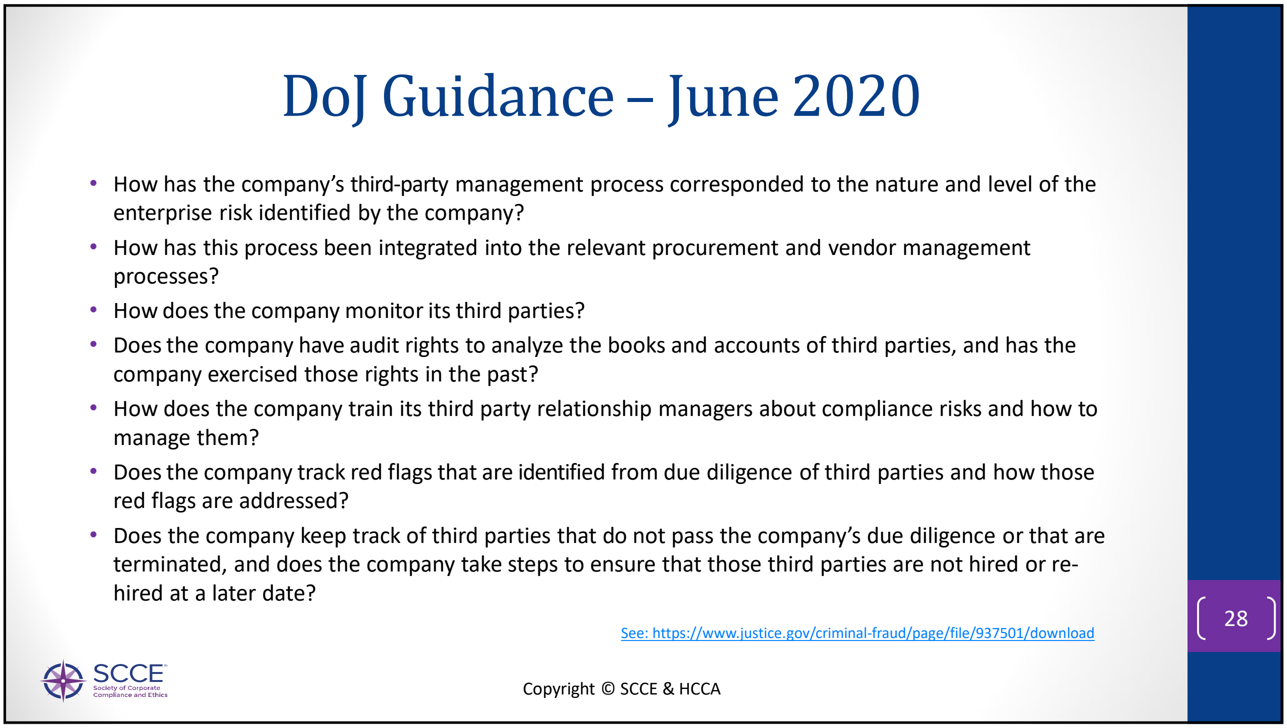
Due-Diligence for Third Parties

- 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.

27

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

27



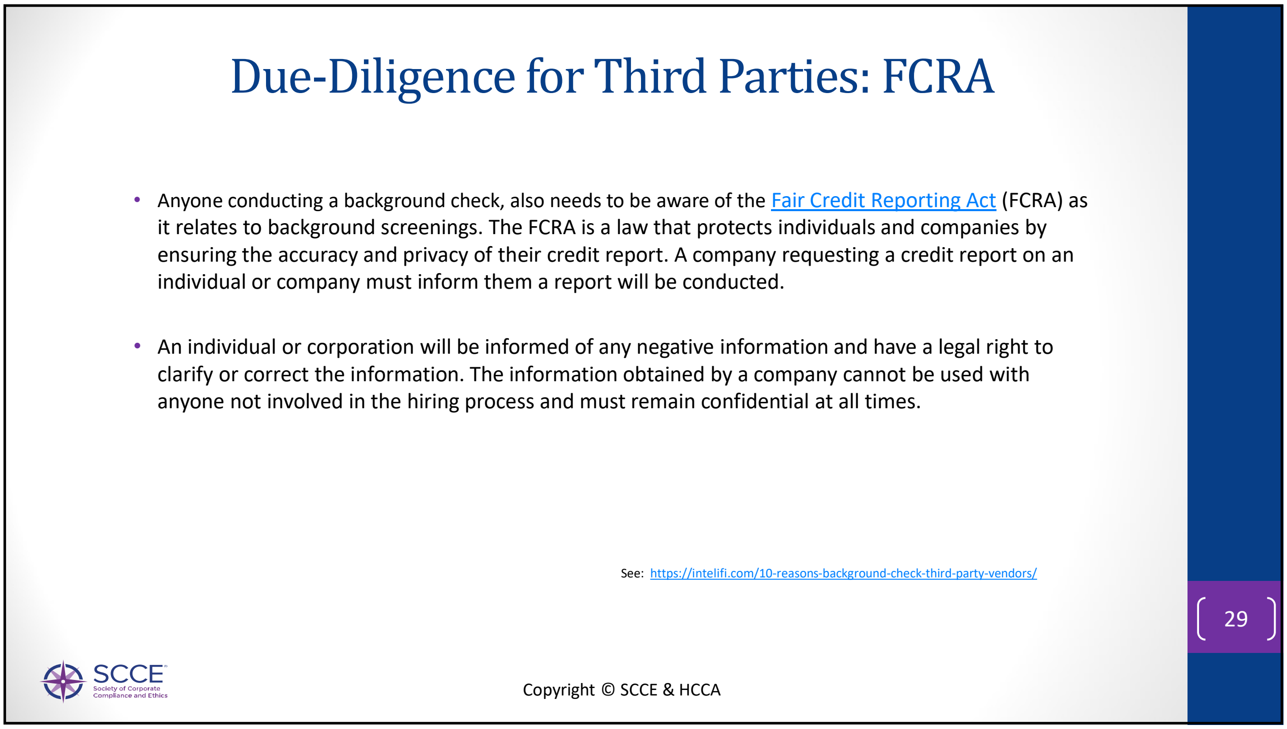
DoJ Guidance – June 2020

- 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?

28

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

28



Due-Diligence for Third Parties: FCRA

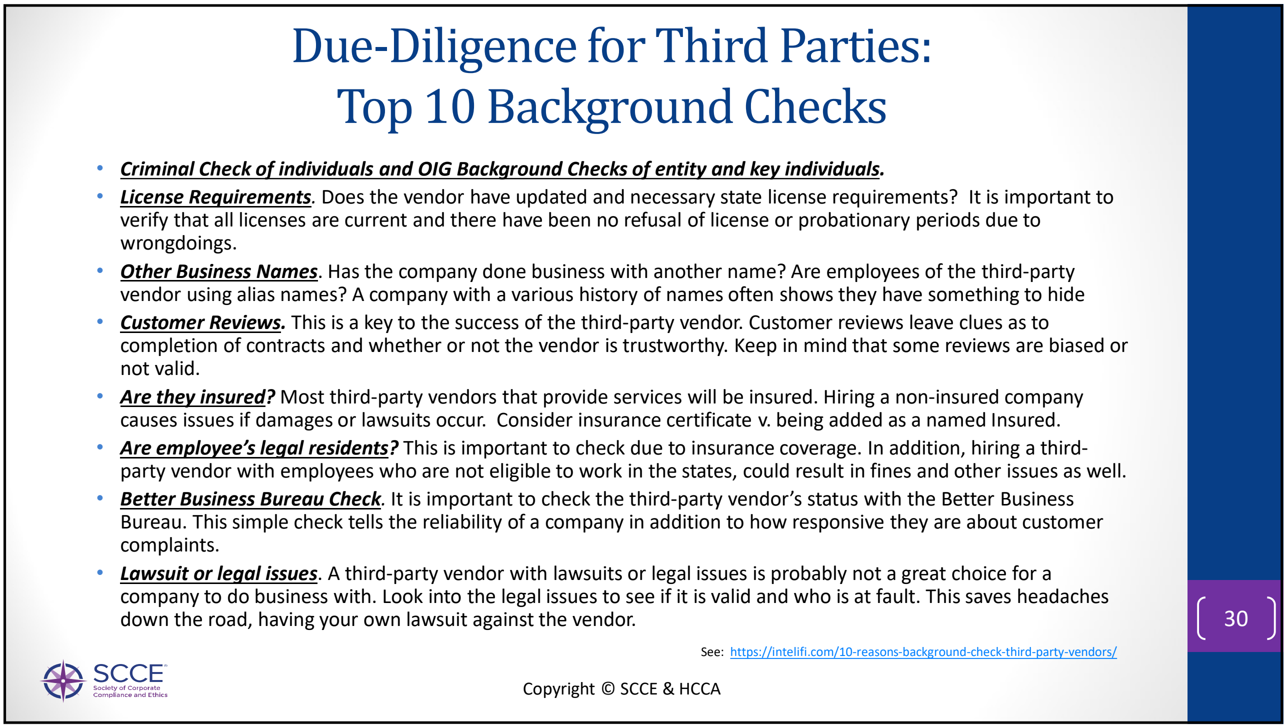
- Anyone conducting a background check, also needs to be aware of the Fair Credit Reporting Act (FCRA) as it relates to background screenings. The FCRA is a law that protects individuals and companies by ensuring the accuracy and privacy of their credit report. A company requesting a credit report on 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/

29

SCCE Society of Corporate Compliance and Ethics

29



Due-Diligence for Third Parties: Top 10 Background Checks

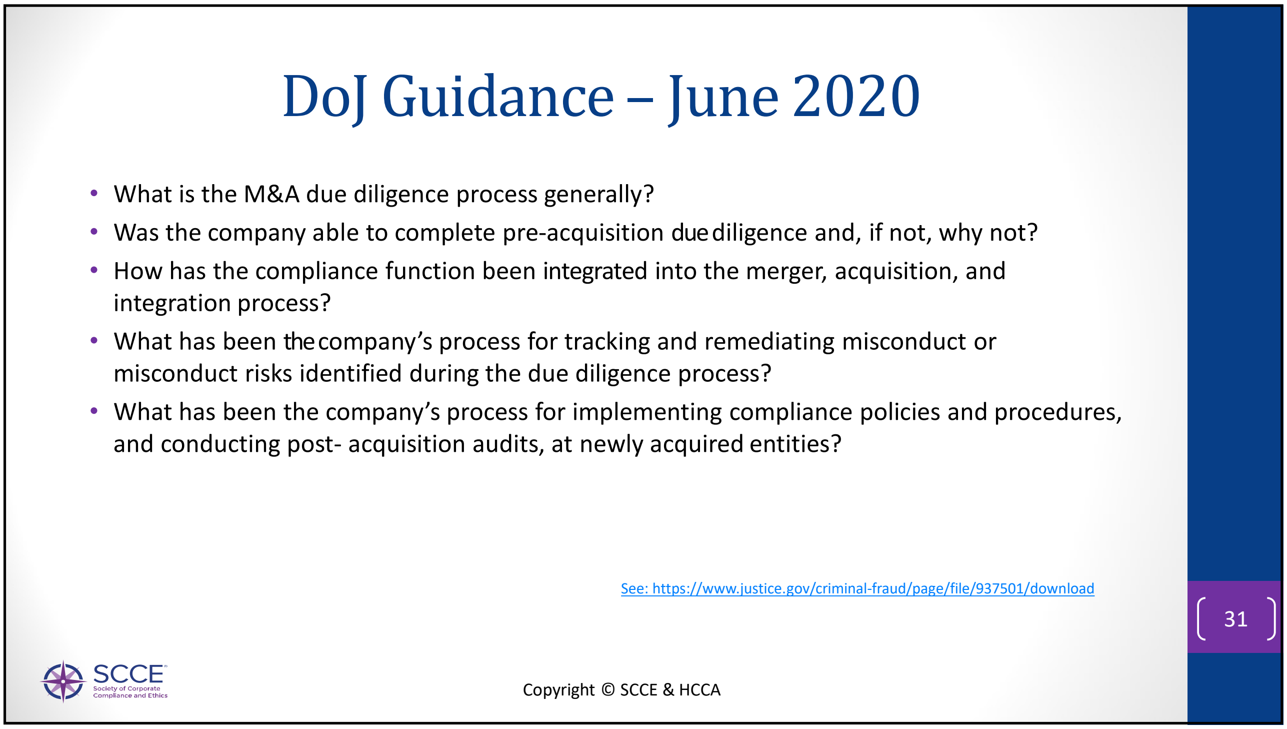
- ***Criminal Check of individuals and OIG Background Checks of entity and key individuals.***
- ***License Requirements***. Does the vendor have updated and necessary state license requirements? It is important to verify that all licenses are current and there have been no refusal of license or probationary 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/

30

SCCE Society of Corporate Compliance and Ethics

30



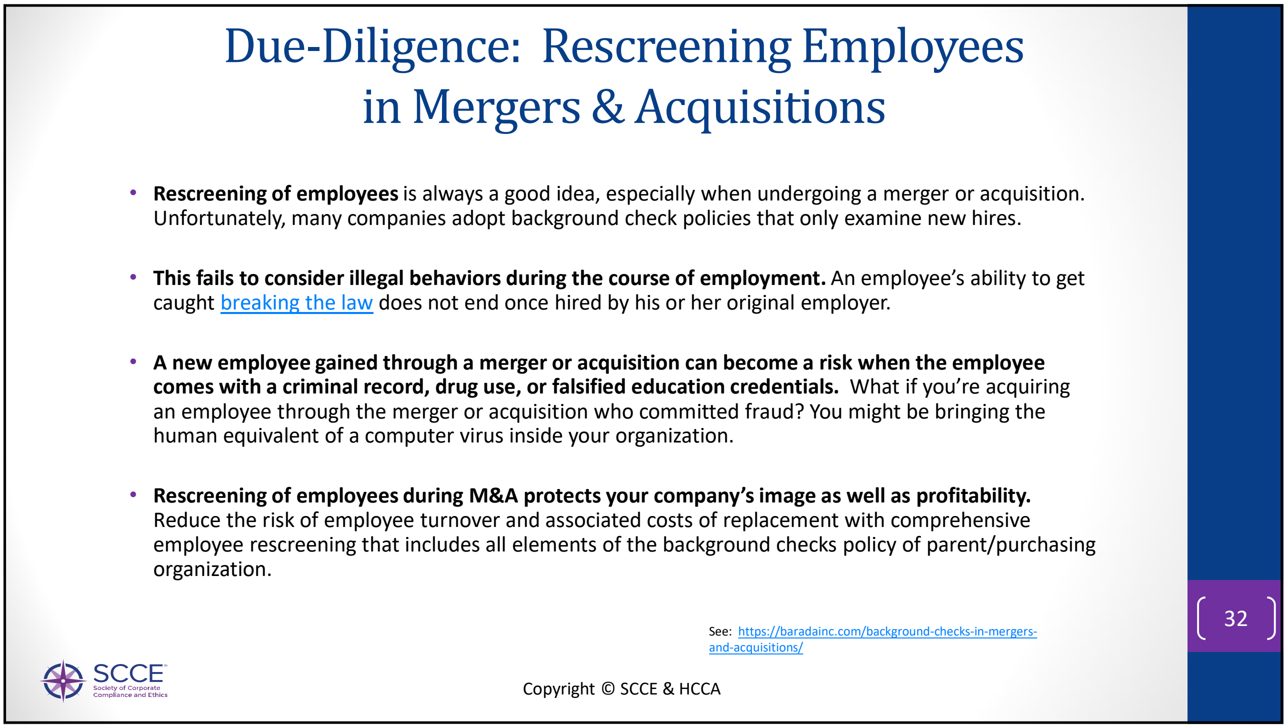
DoJ Guidance – June 2020

- 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

31

31



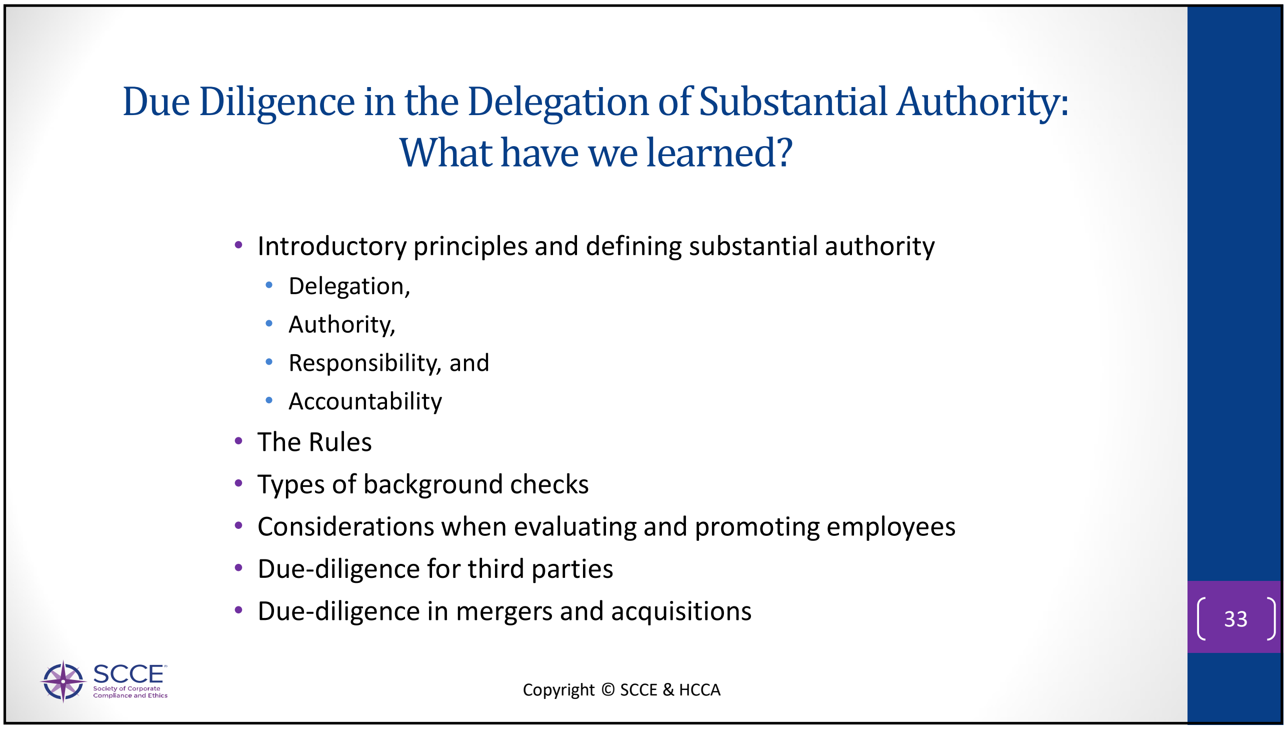
Due-Diligence: Rescreening Employees in Mergers & Acquisitions

- **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/

32

32

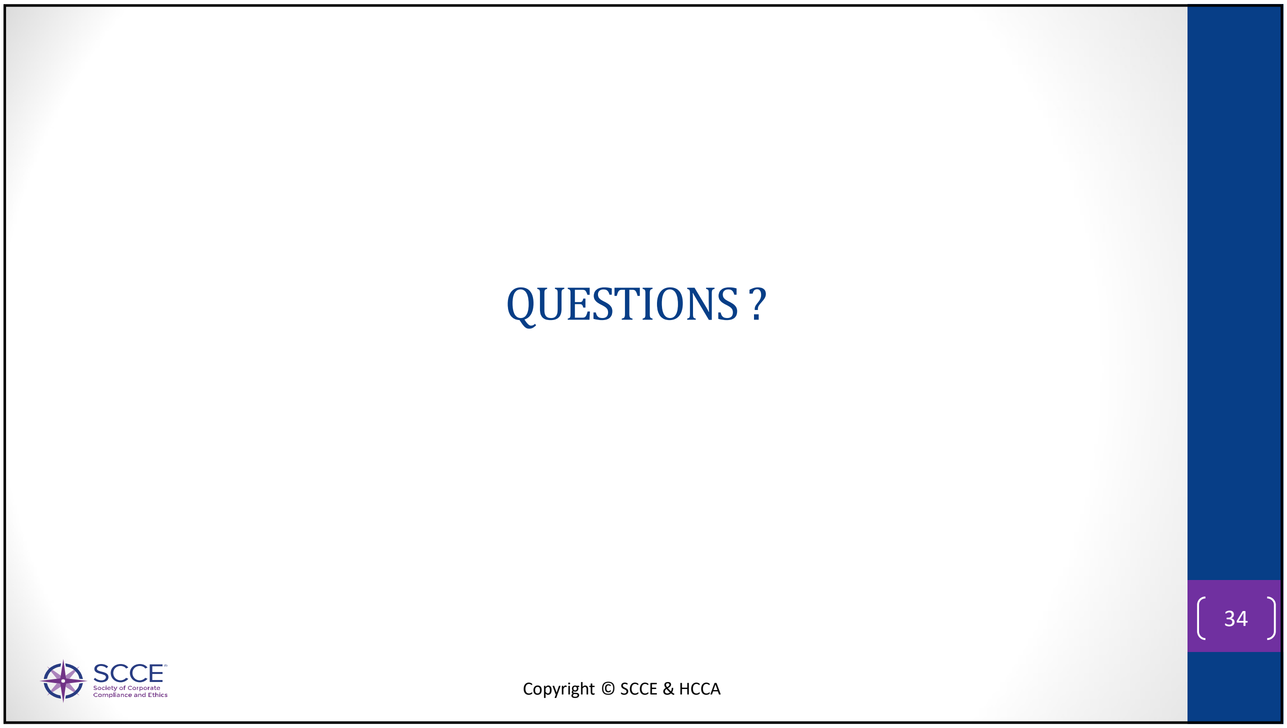


Due Diligence in the Delegation of Substantial Authority: What have we learned?

- 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

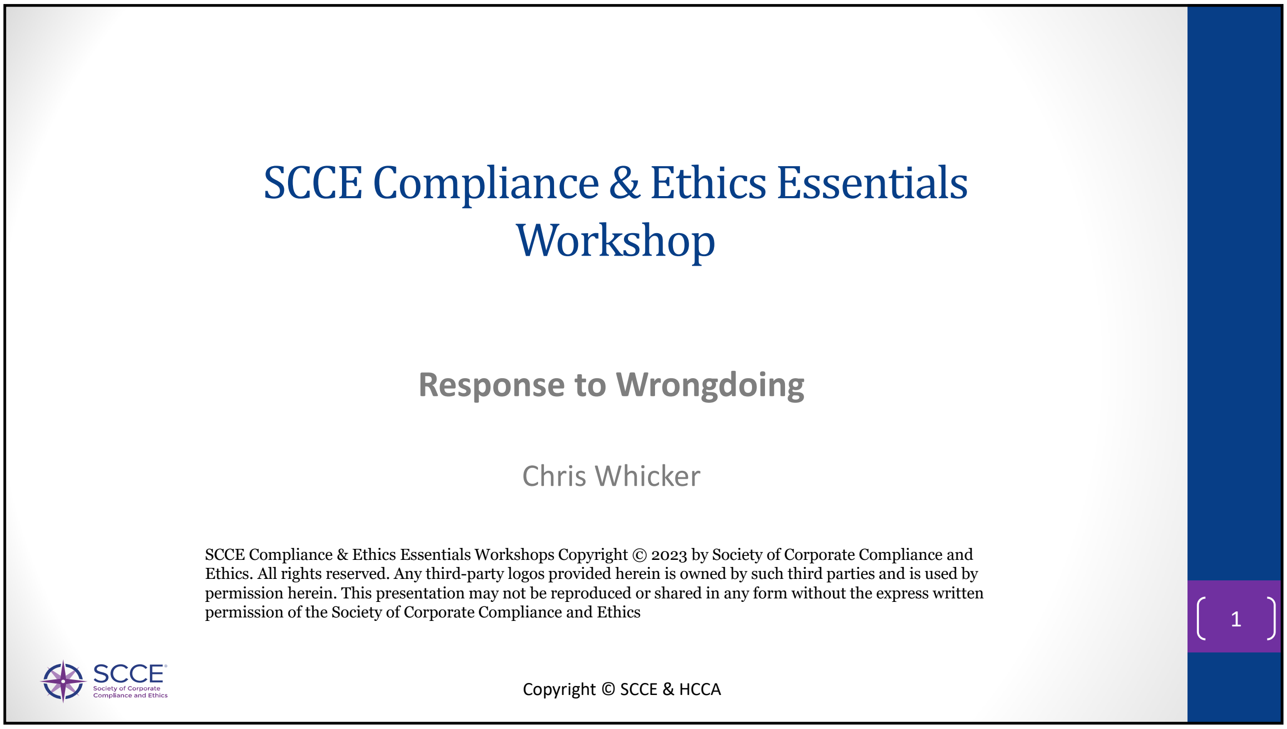
33



QUESTIONS ?

34

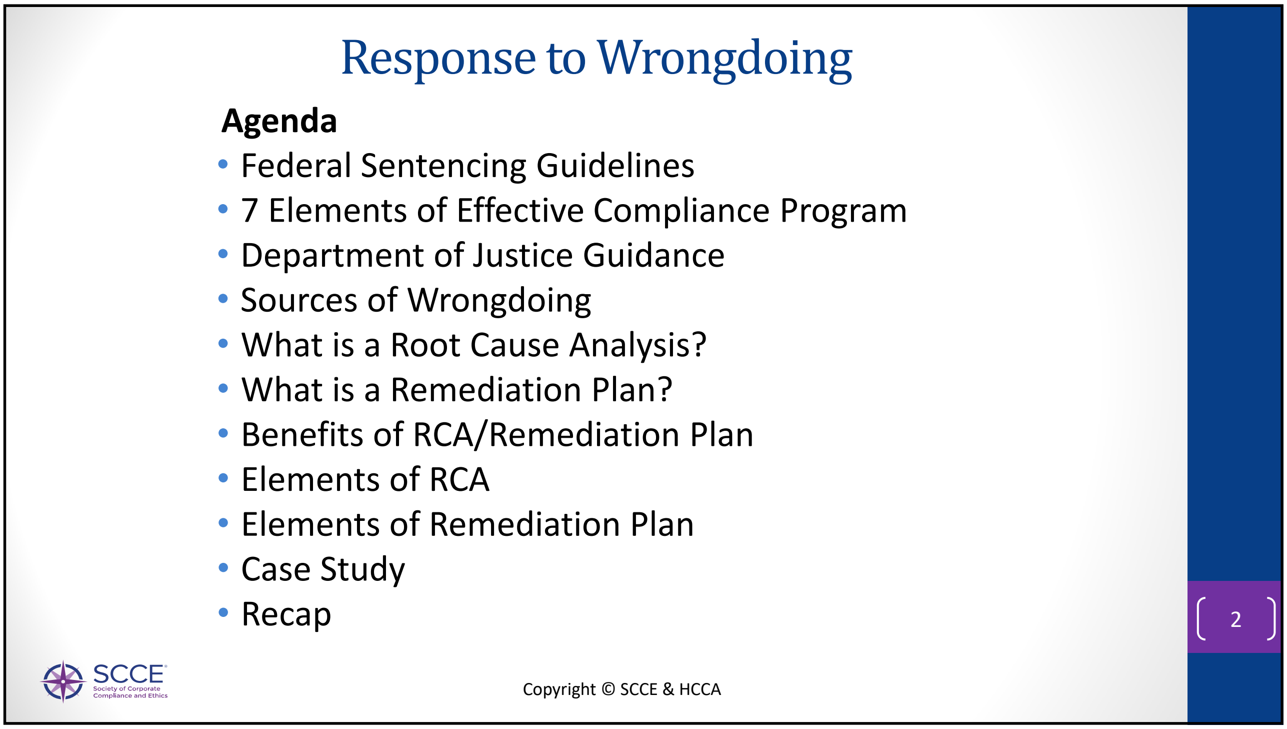
34



SCCE Compliance & Ethics Essentials Workshop

Response to Wrongdoing

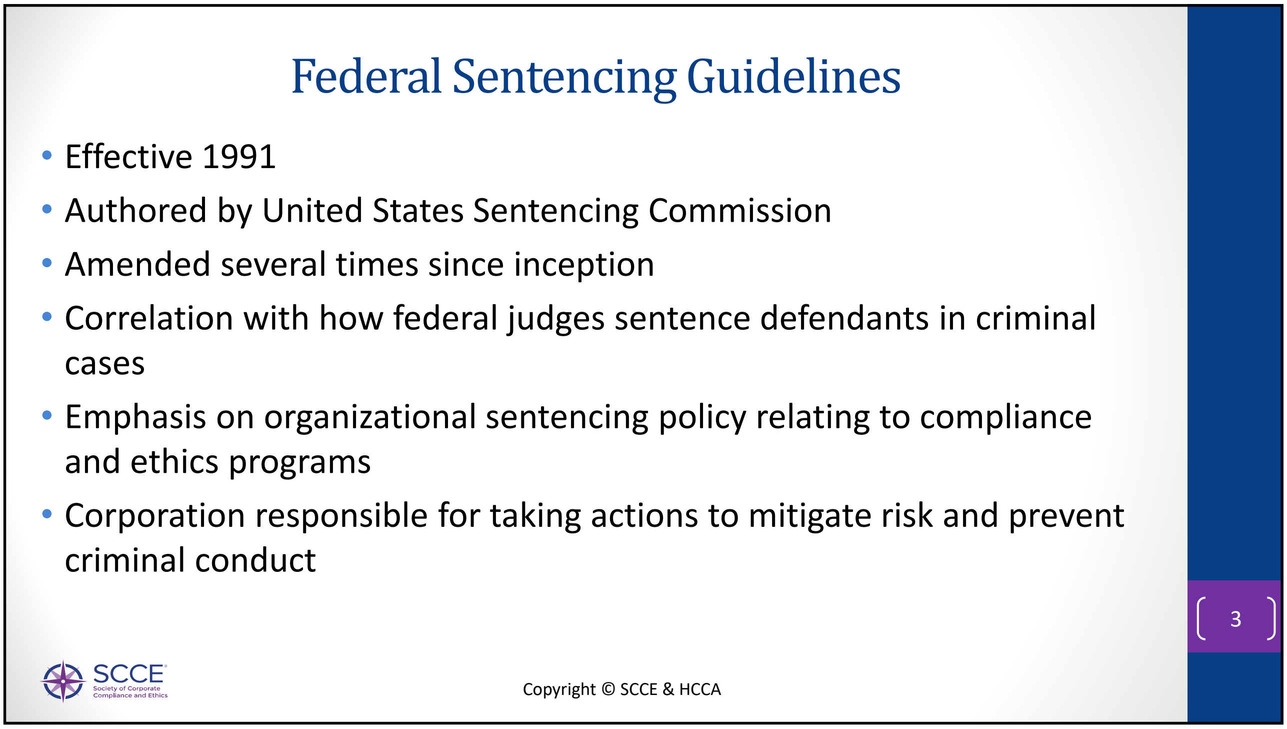
Chris Whicker



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



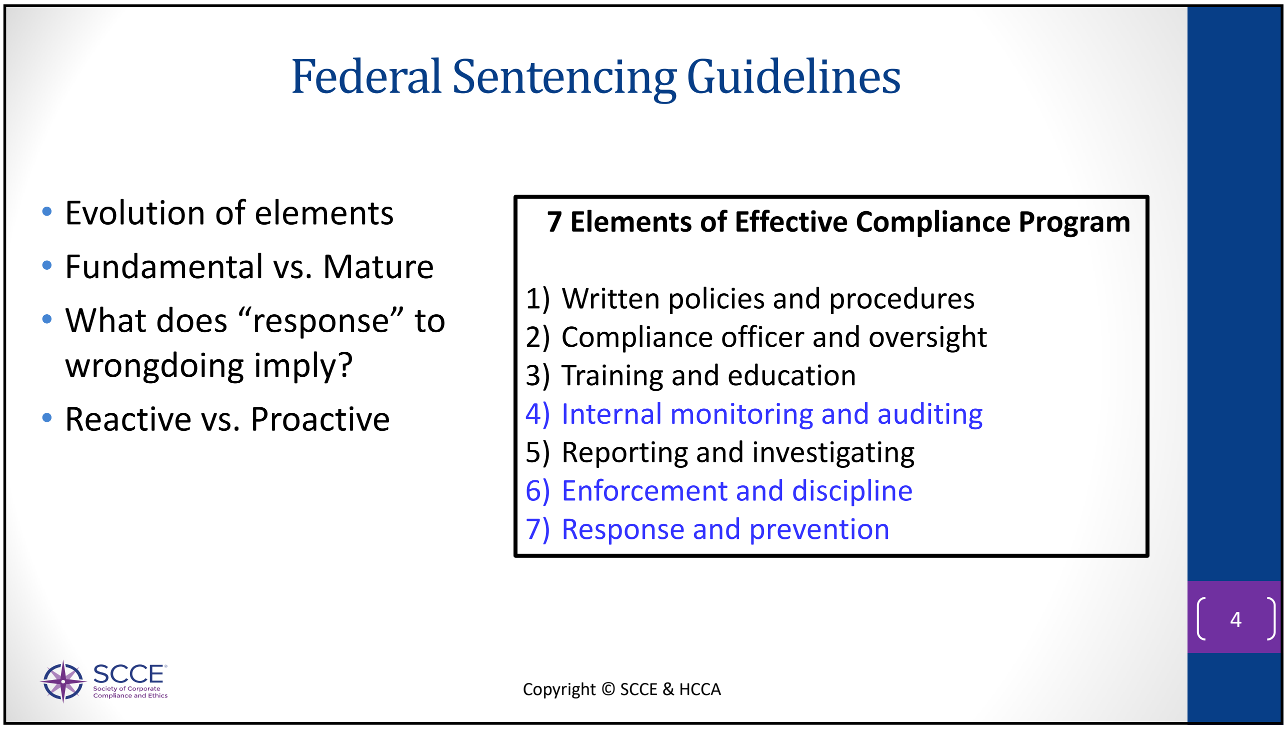
Federal Sentencing Guidelines

- 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

SCCE Society of Corporate Compliance and Ethics

3



Federal Sentencing Guidelines

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

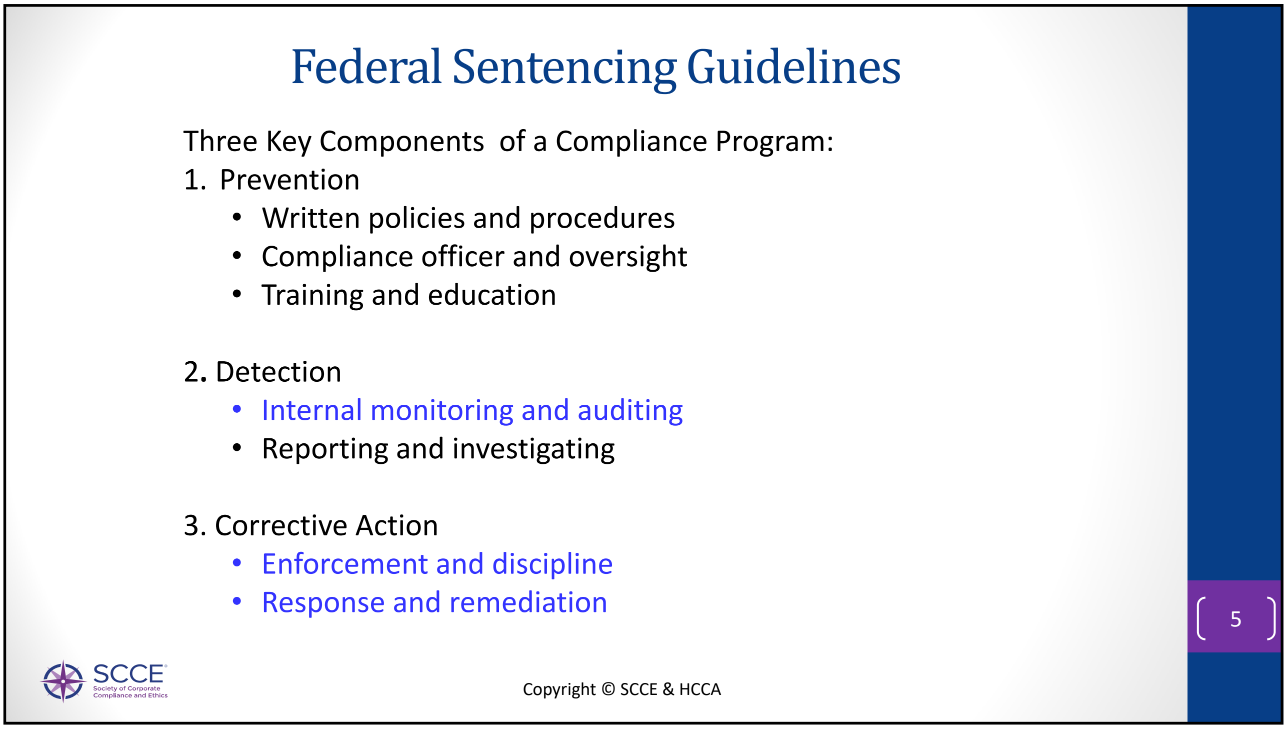
7 Elements of Effective Compliance Program

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

SCCE Society of Corporate Compliance and Ethics

4



Federal Sentencing Guidelines

Three Key Components of a Compliance Program:

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

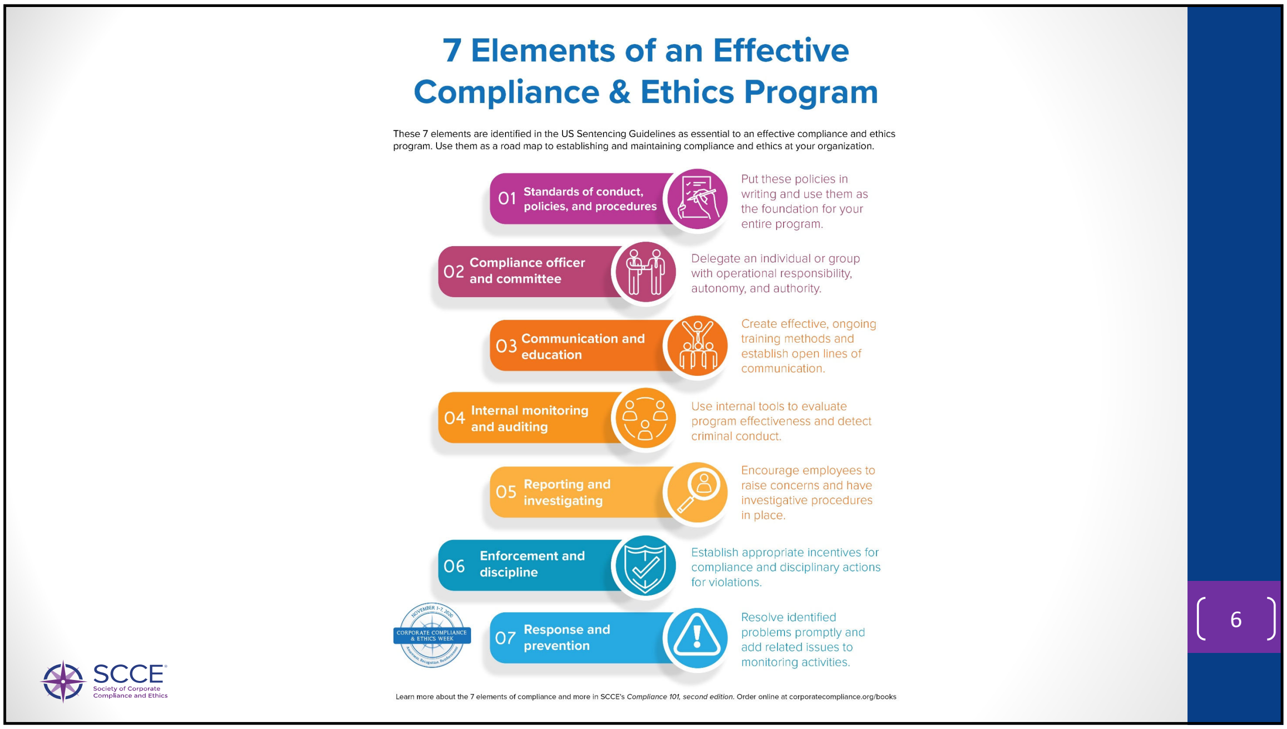
2. Detection
   - Internal monitoring and auditing
   - Reporting and investigating

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

5

SCCE Society of Corporate Compliance and Ethics

5



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.

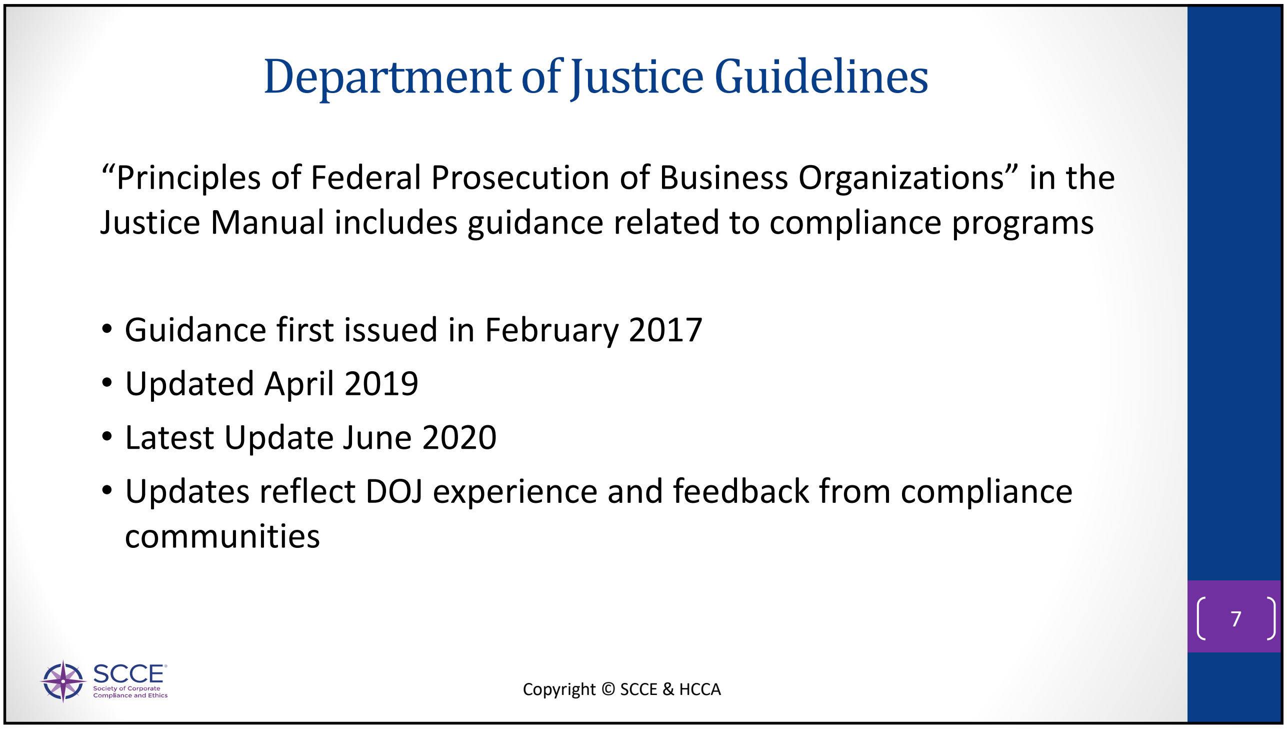
NOVEMBER 1–7, 2020
CORPORATE COMPLIANCE & ETHICS WEEK
Awareness, Recognition, Reinforcement

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

6

SCCE Society of Corporate Compliance and Ethics

6



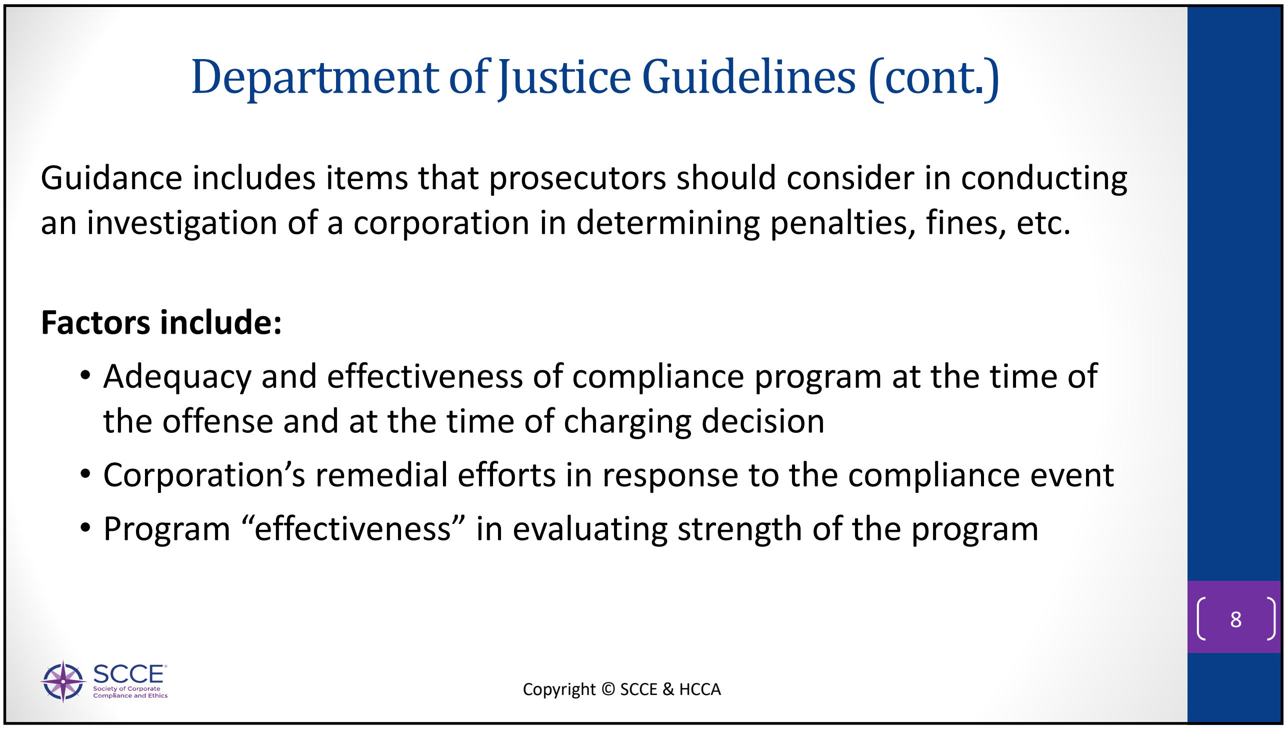
Department of Justice Guidelines

“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 June 2020
- Updates reflect DOJ experience and feedback from compliance communities

7

7



Department of Justice Guidelines (cont.)

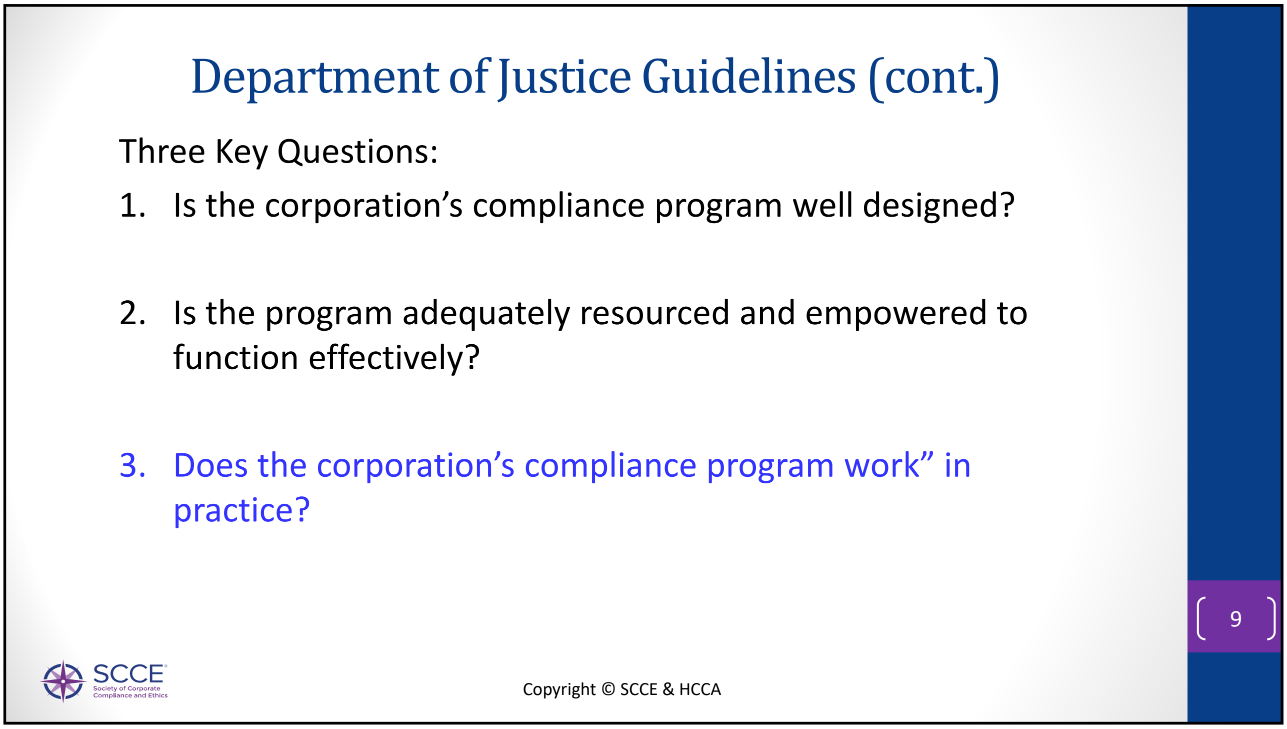
Guidance includes items that prosecutors should consider in conducting an investigation of a corporation in determining penalties, fines, etc.

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

8



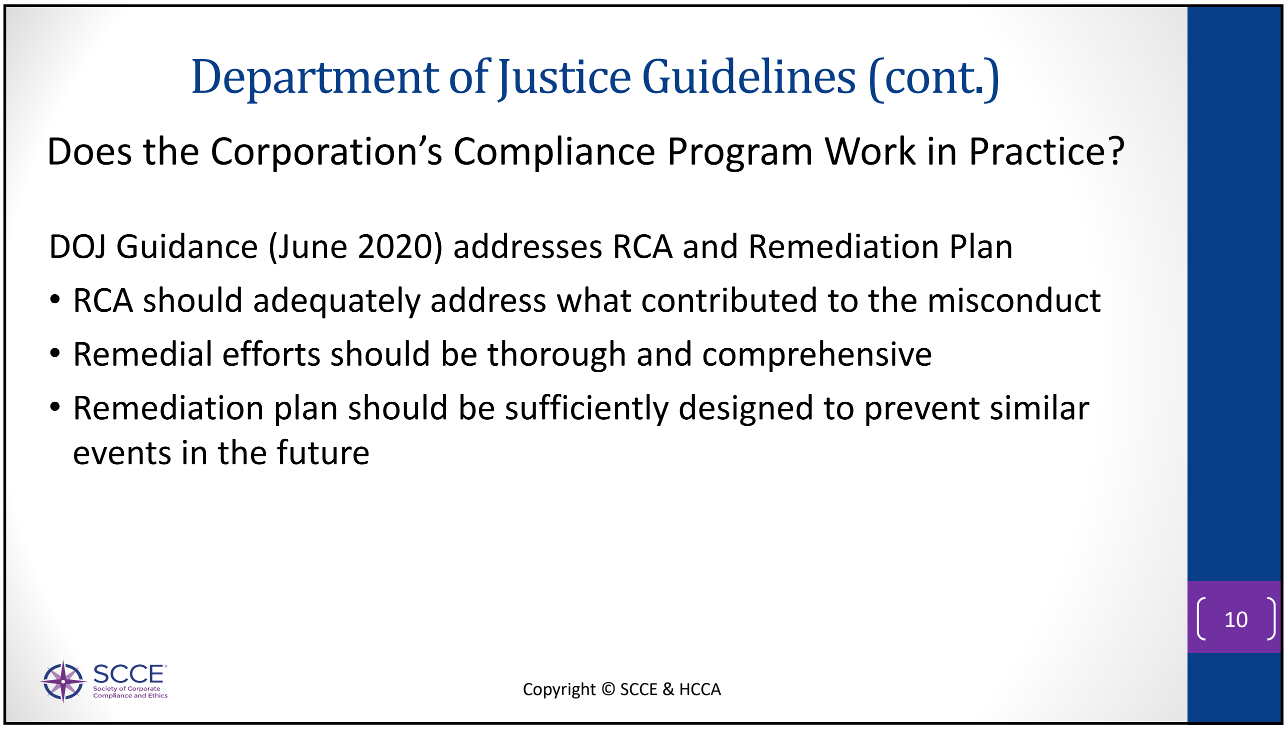
Department of Justice Guidelines (cont.)

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?

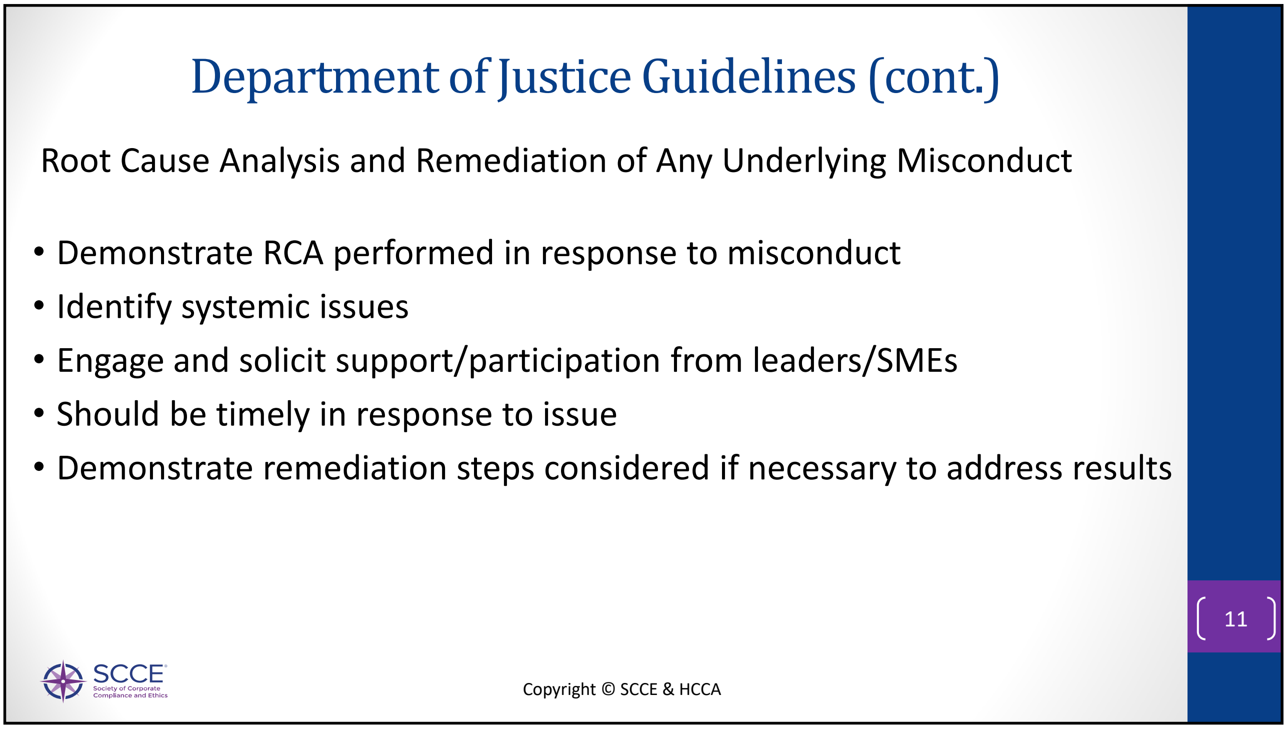


Department of Justice Guidelines (cont.)

Does the Corporation’s Compliance Program Work in Practice?

DOJ Guidance (June 2020) addresses RCA and Remediation Plan

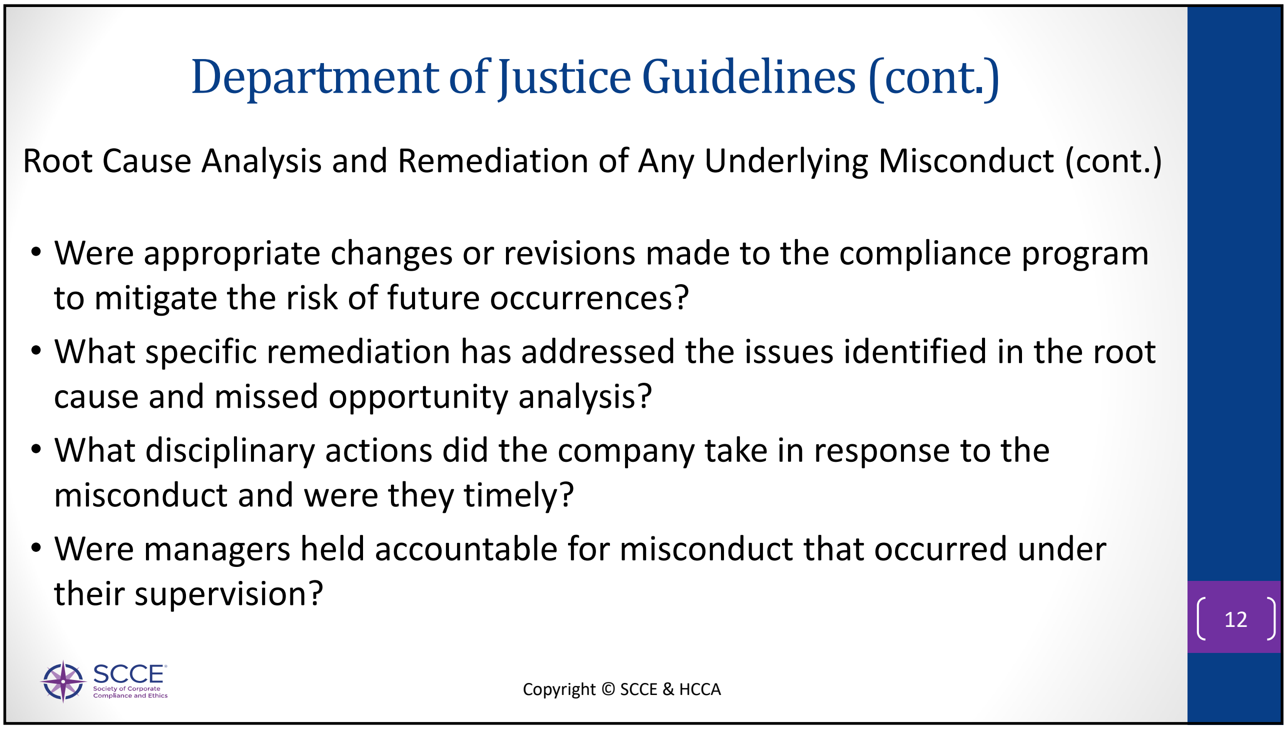
- RCA should adequately address what contributed to the misconduct
- Remedial efforts should be thorough and comprehensive
- Remediation plan should be sufficiently designed to prevent similar events in the future



Department of Justice Guidelines (cont.)

Root Cause Analysis and Remediation of Any Underlying Misconduct

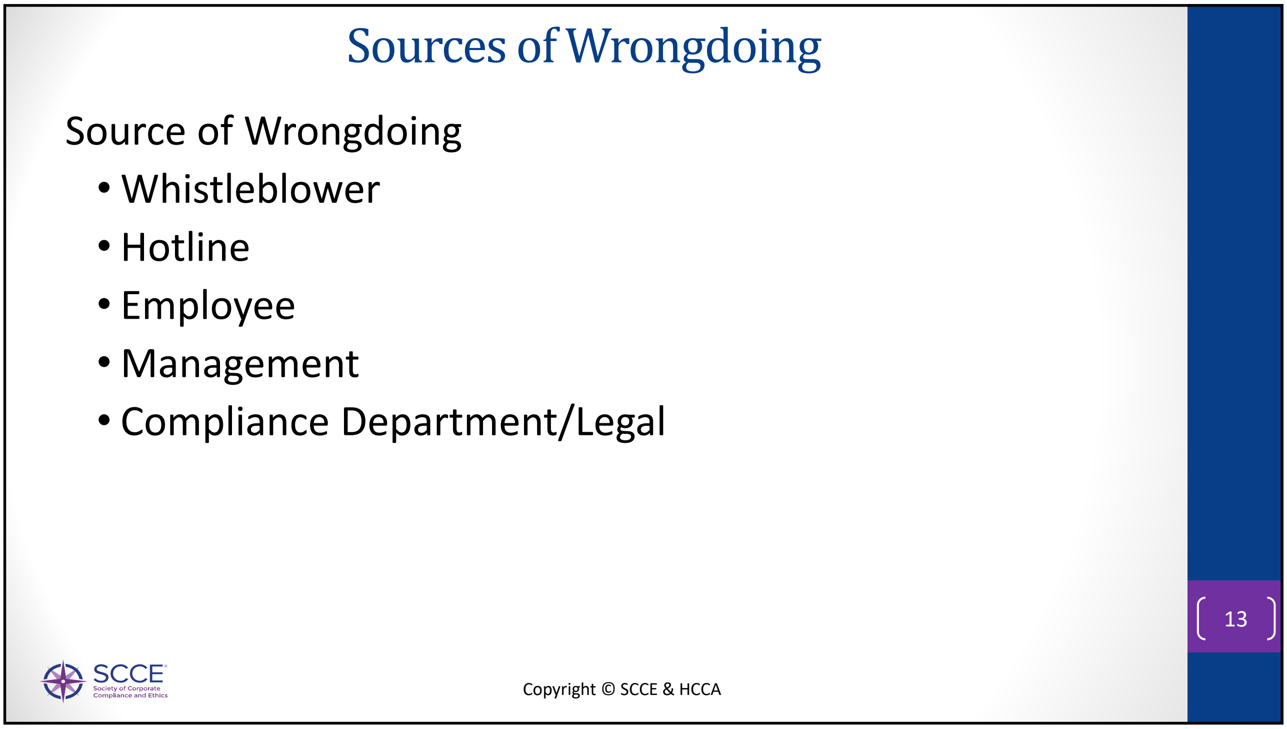
- Demonstrate RCA performed in response to misconduct
- Identify systemic issues
- Engage and solicit support/participation from leaders/SMEs
- Should be timely in response to issue
- Demonstrate remediation steps considered if necessary to address results



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?



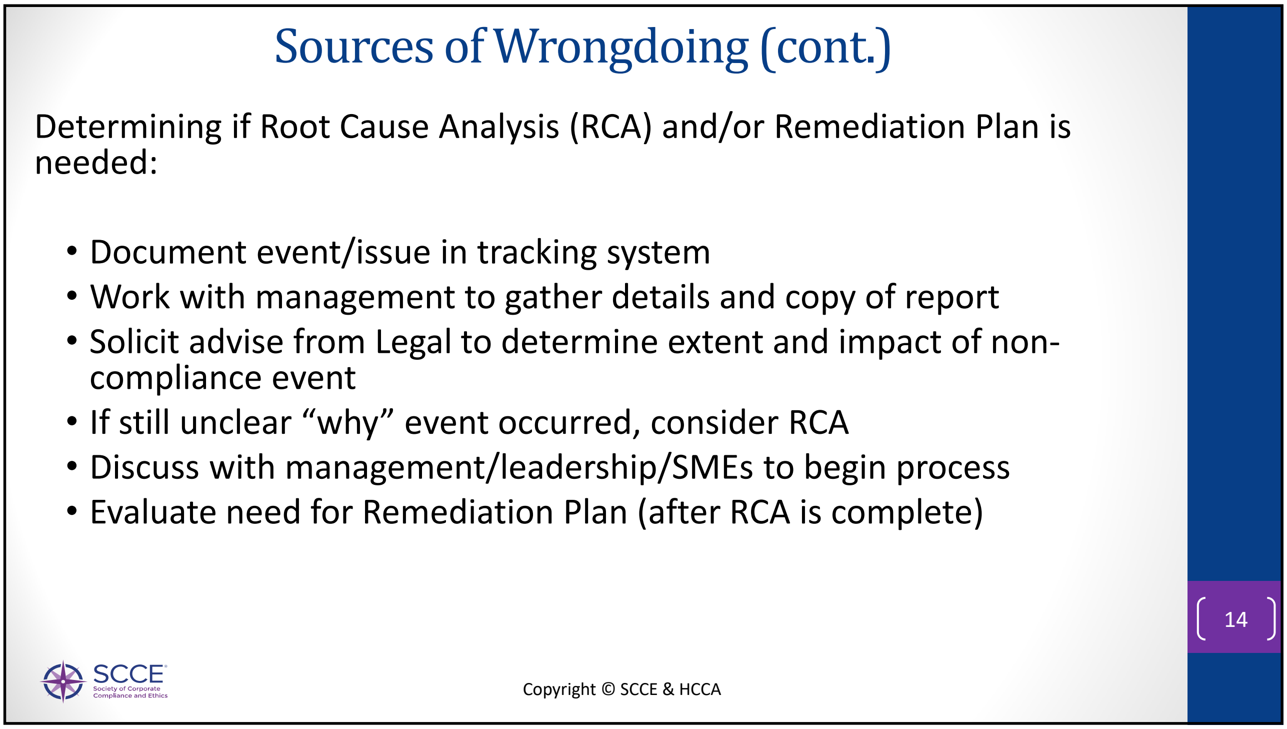
Sources of Wrongdoing

Source of Wrongdoing

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

13

SCCE Society of Corporate Compliance and Ethics



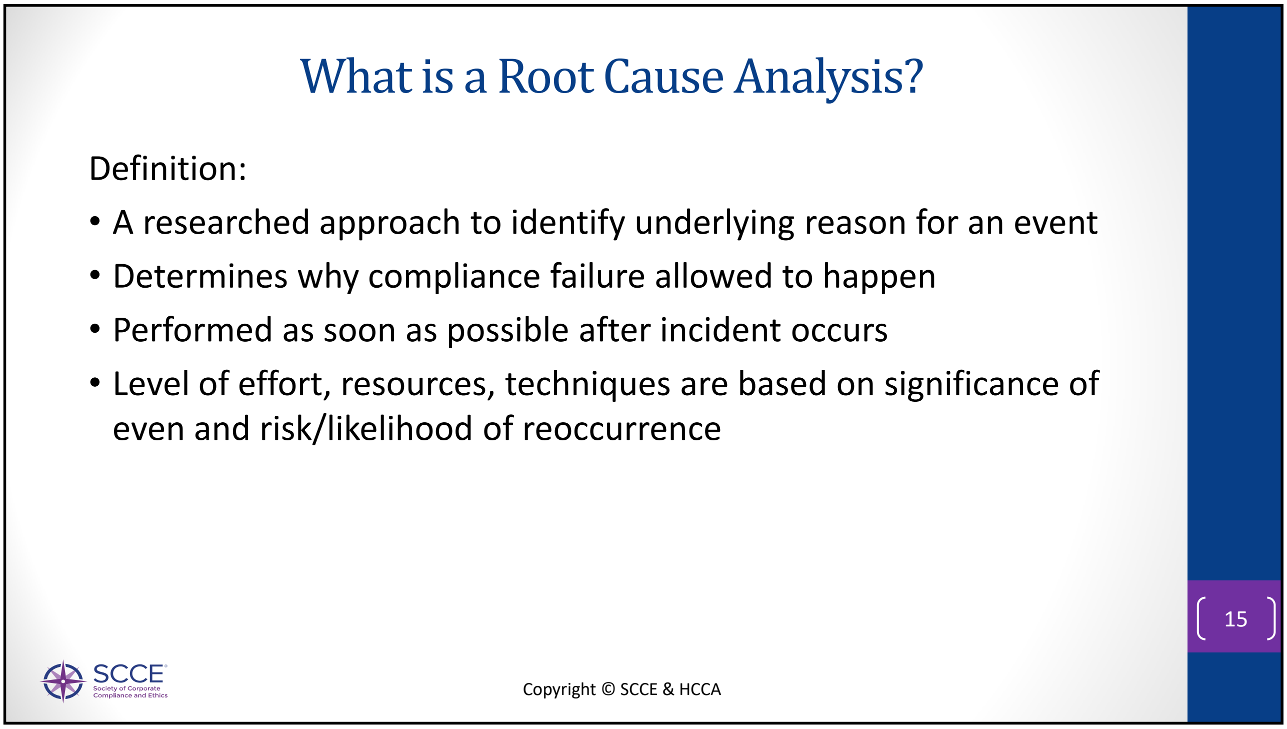
Sources of Wrongdoing (cont.)

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)

14

SCCE Society of Corporate Compliance and Ethics



What is a Root Cause Analysis?

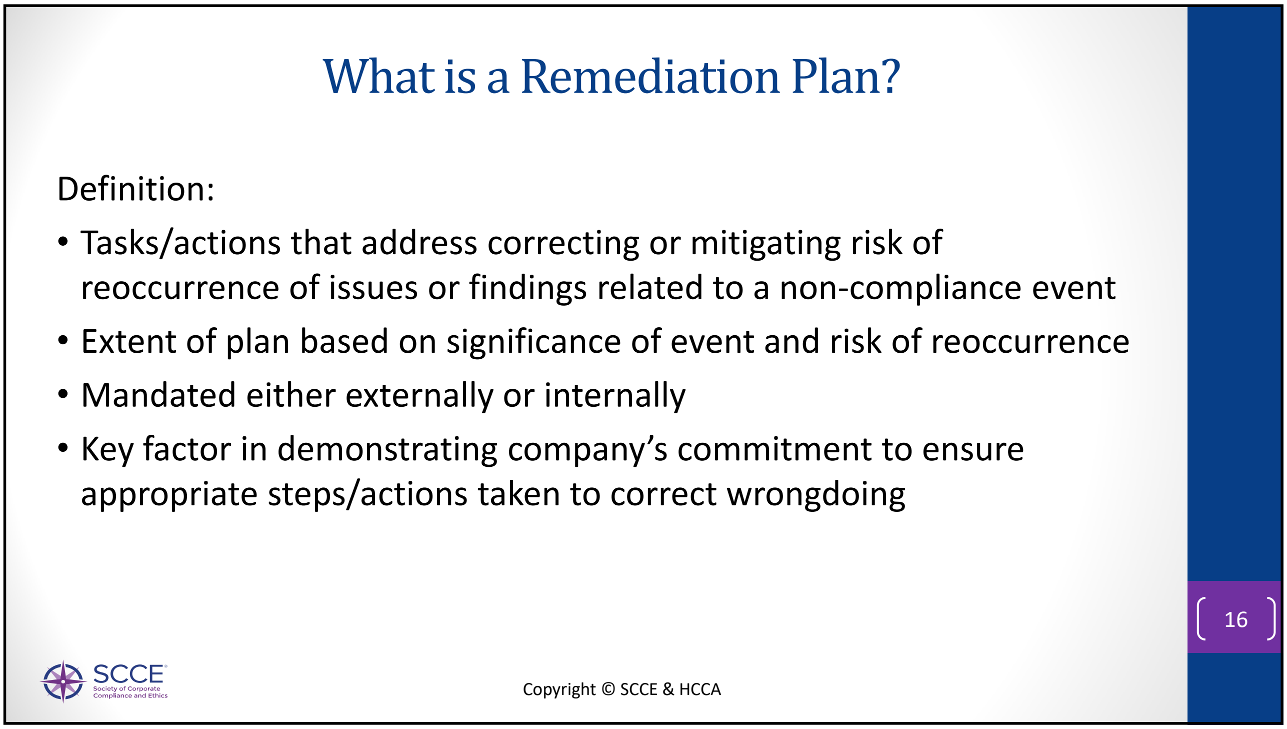
Definition:

- 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

SCCE Society of Corporate Compliance and Ethics

15



What is a Remediation Plan?

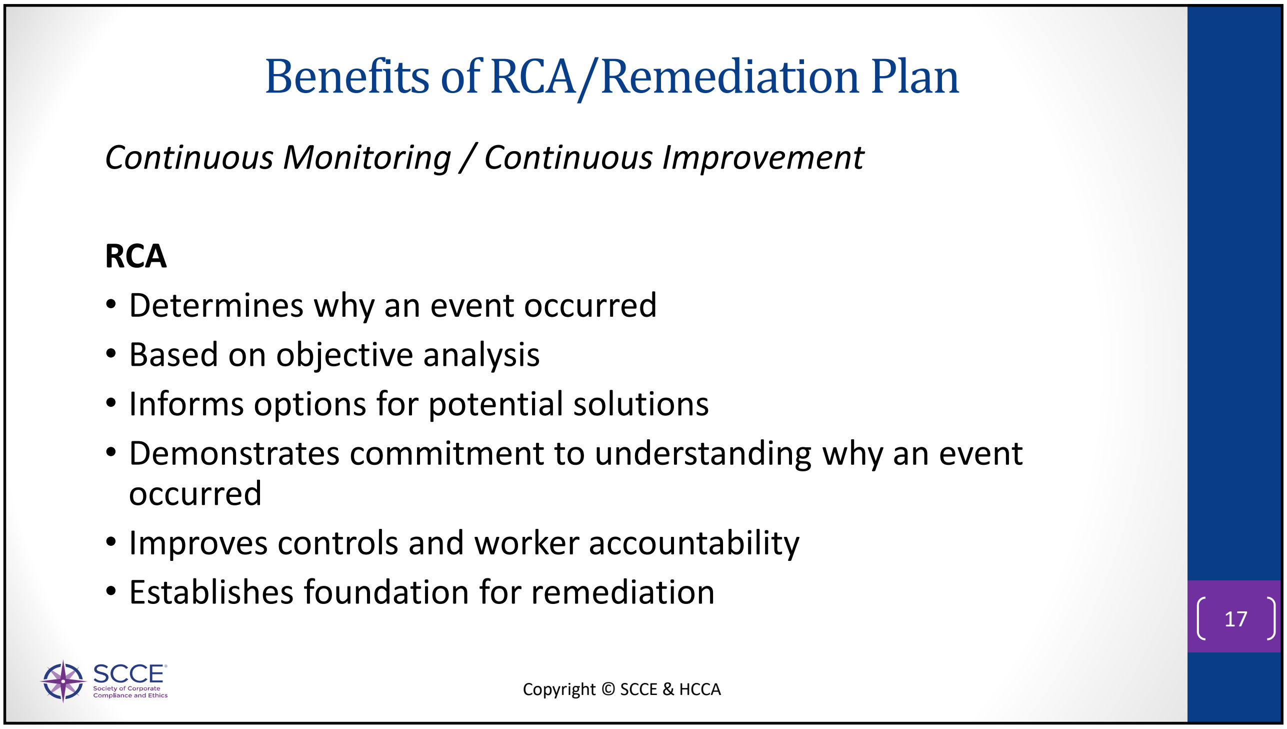
Definition:

- 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

SCCE Society of Corporate Compliance and Ethics

16

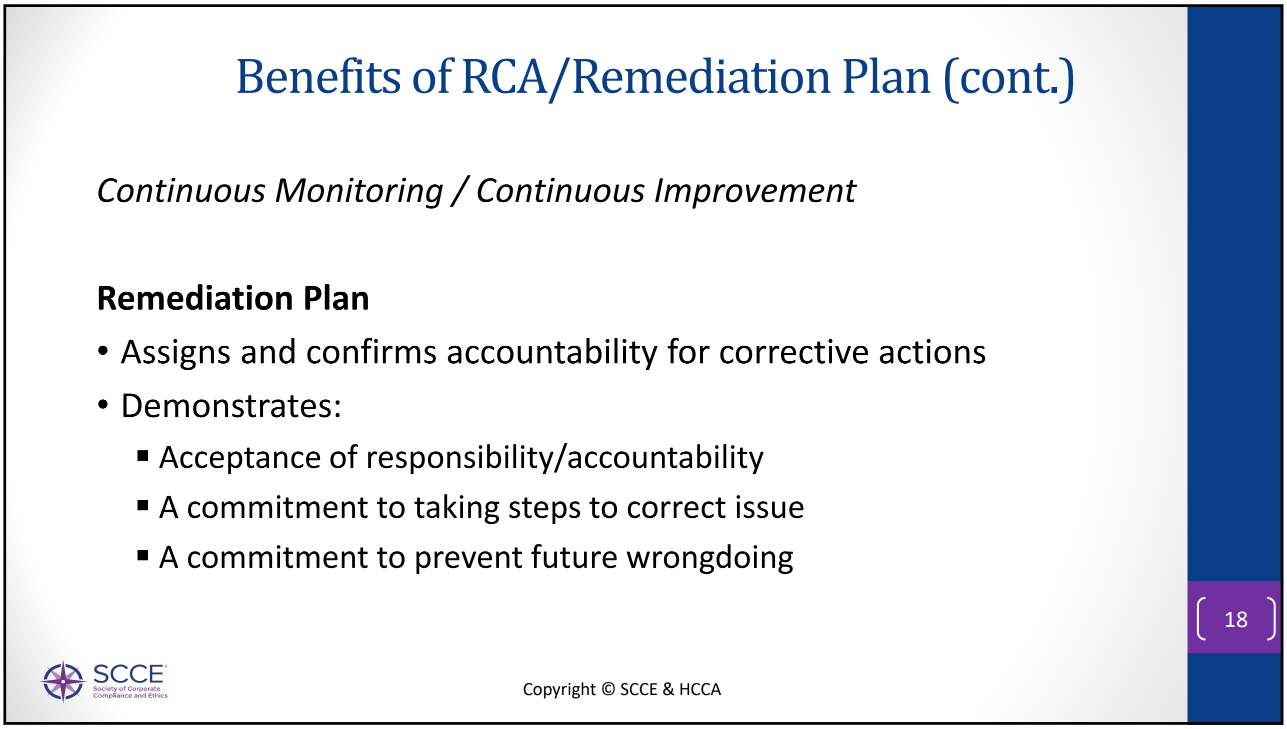


Benefits of RCA/Remediation Plan

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

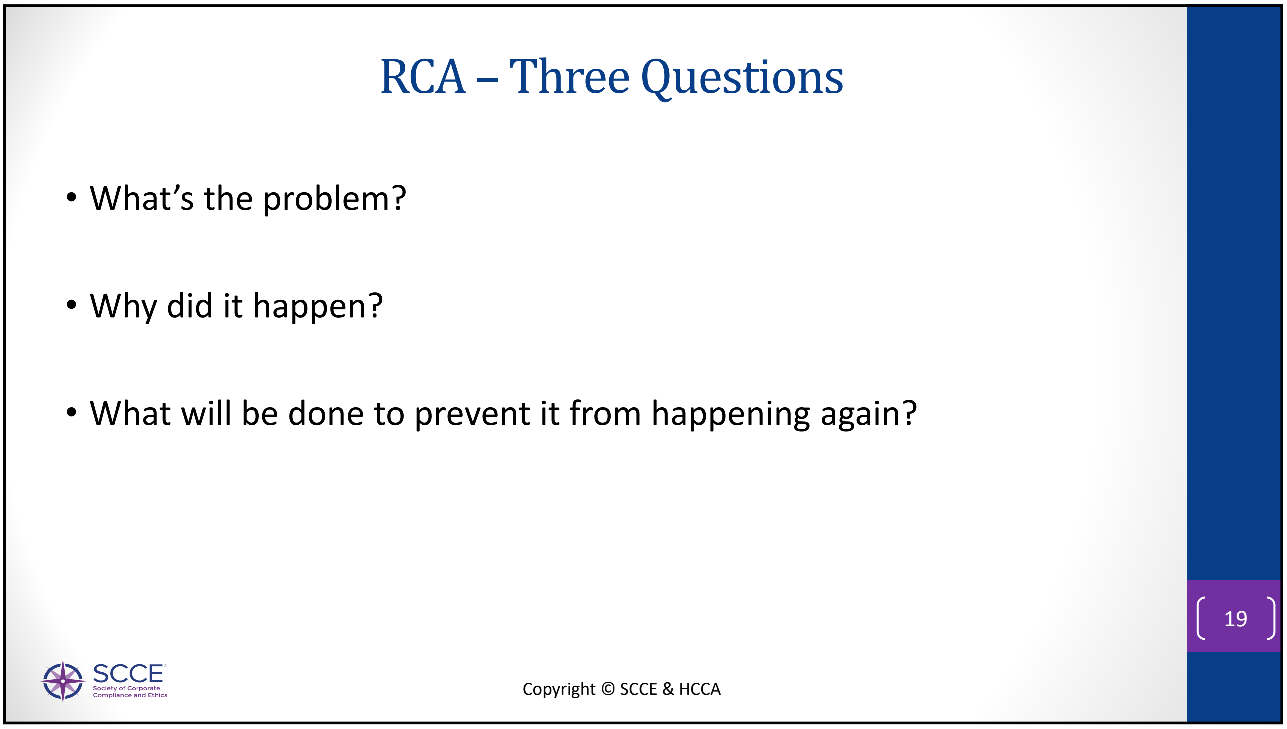


Benefits of RCA/Remediation Plan (cont.)

Continuous Monitoring / Continuous Improvement

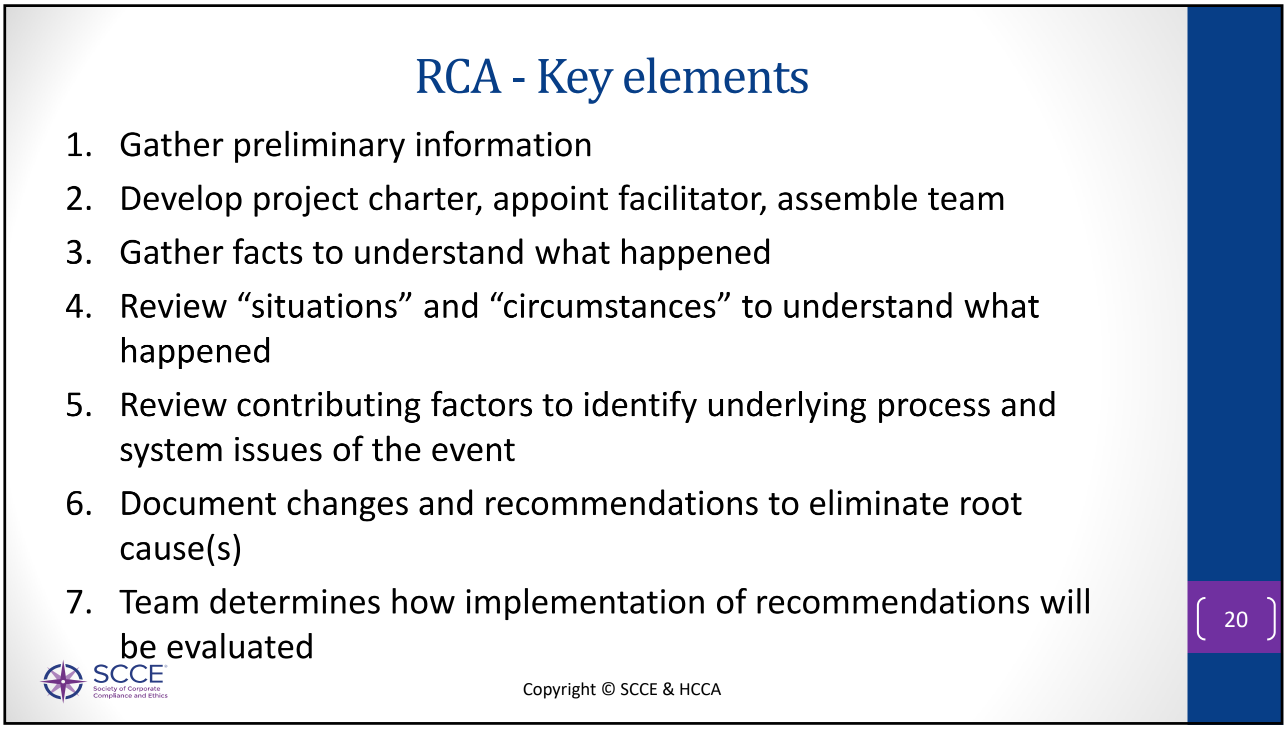
Remediation Plan

- 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



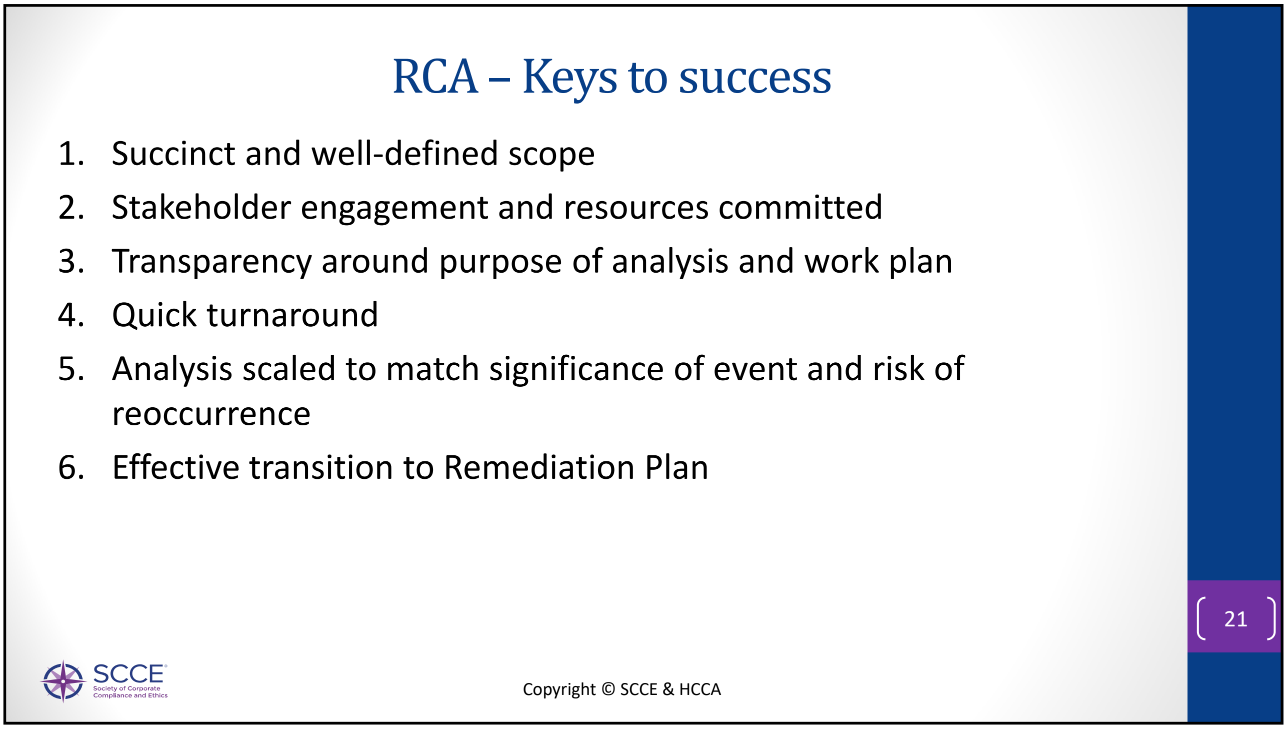
RCA – Three Questions

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



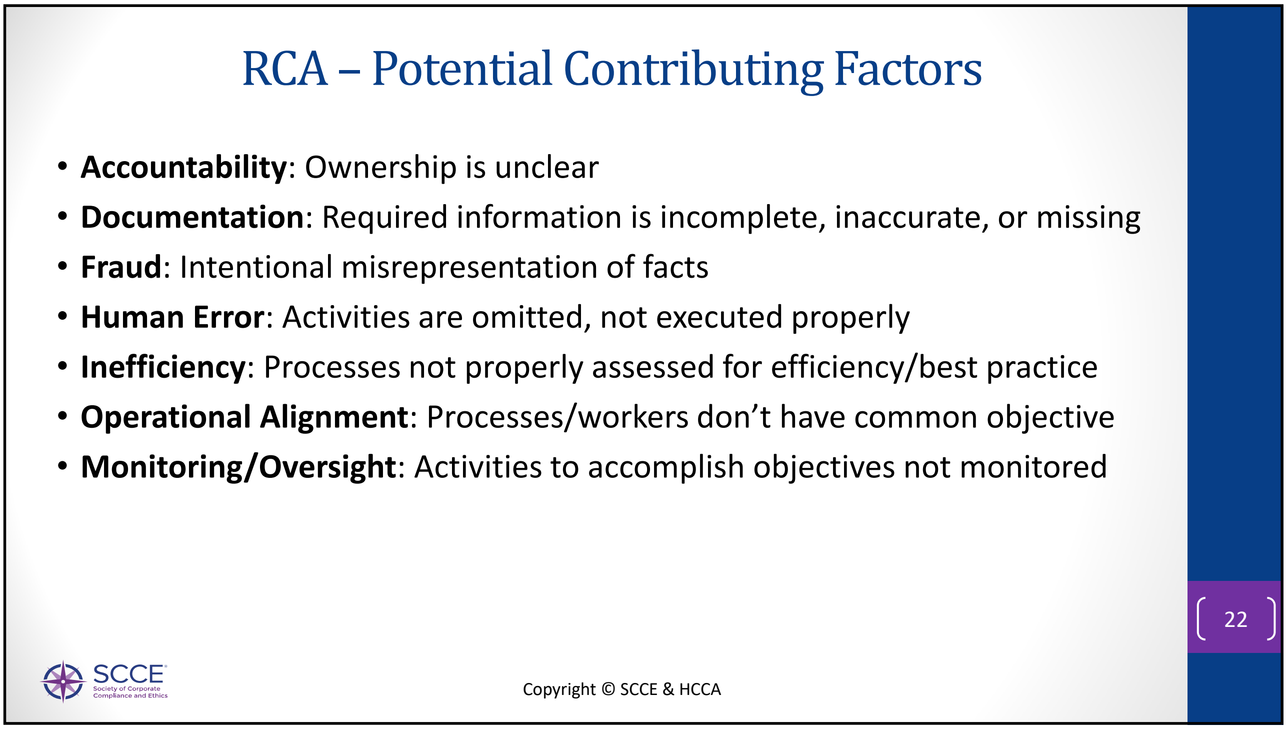
RCA - Key elements

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



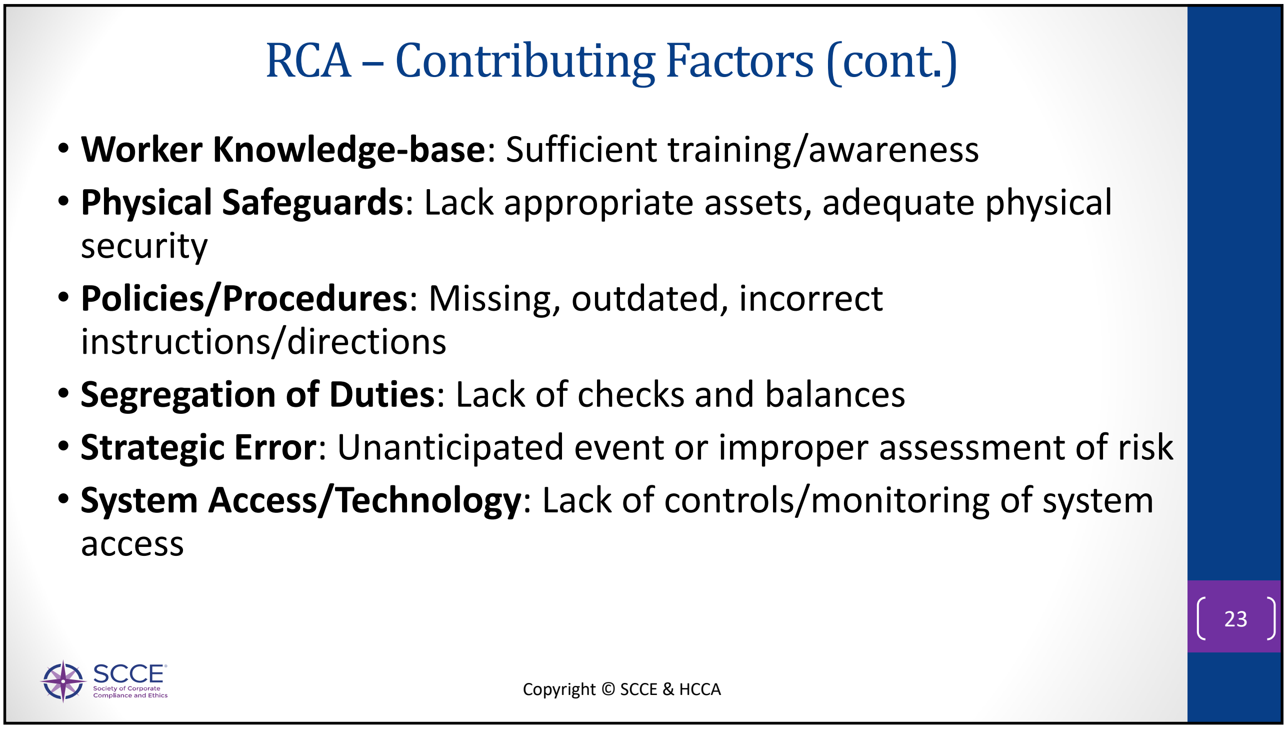
RCA – Keys to success

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



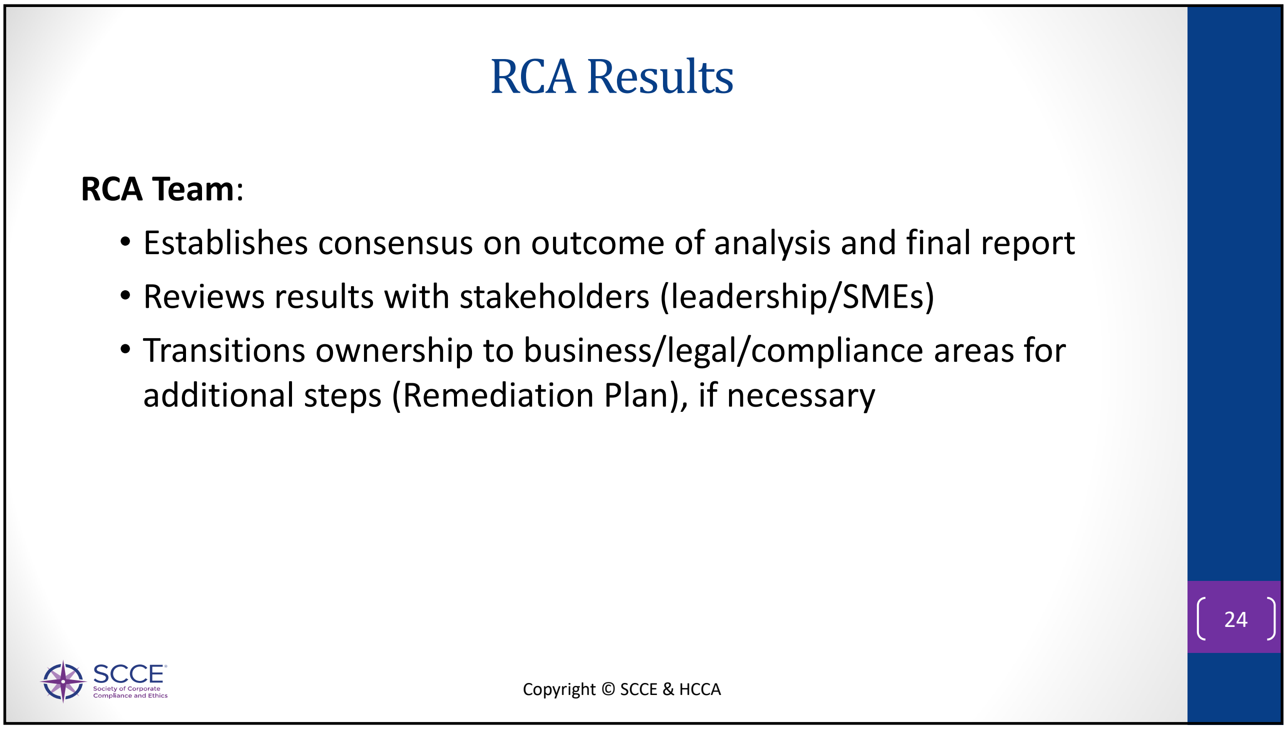
RCA – Potential Contributing Factors

- **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



RCA – Contributing Factors (cont.)

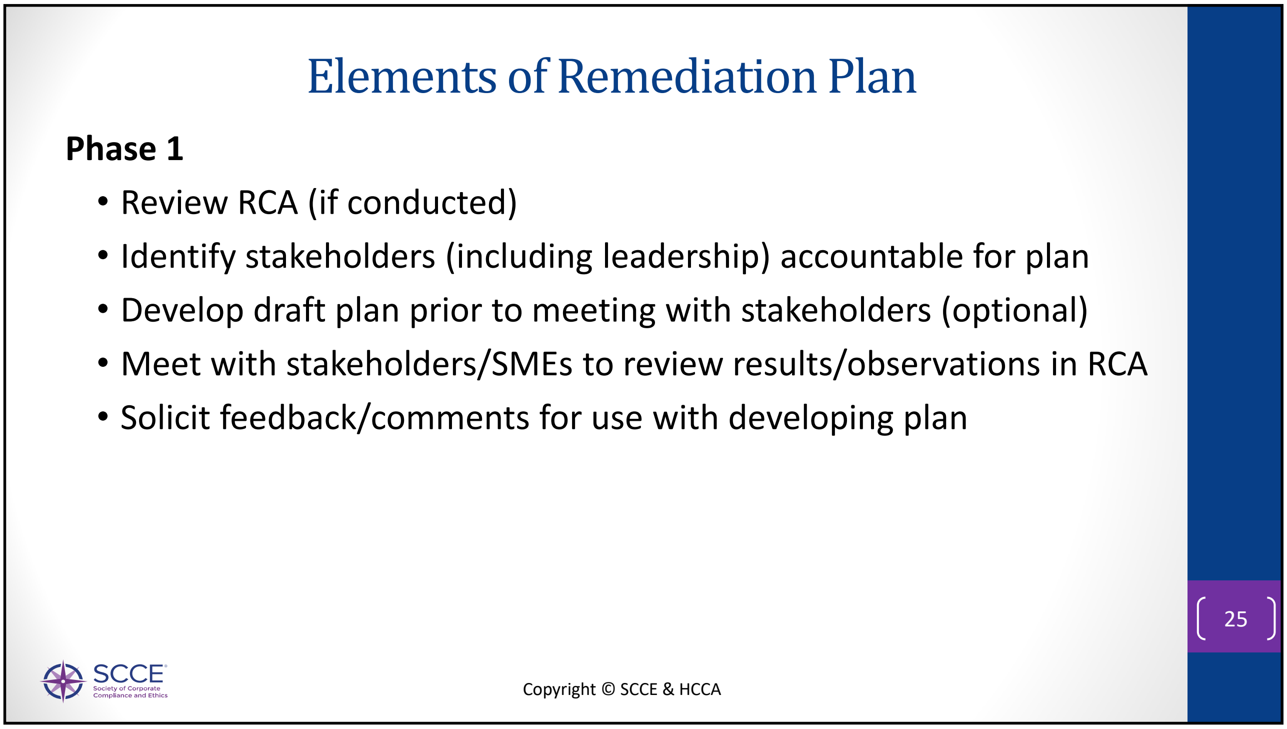
- **Worker Knowledge-base**: Sufficient training/awareness
- **Physical Safeguards**: Lack appropriate assets, adequate physical security
- **Policies/Procedures**: Missing, outdated, incorrect instructions/directions
- **Segregation of Duties**: Lack of checks and balances
- **Strategic Error**: Unanticipated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



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

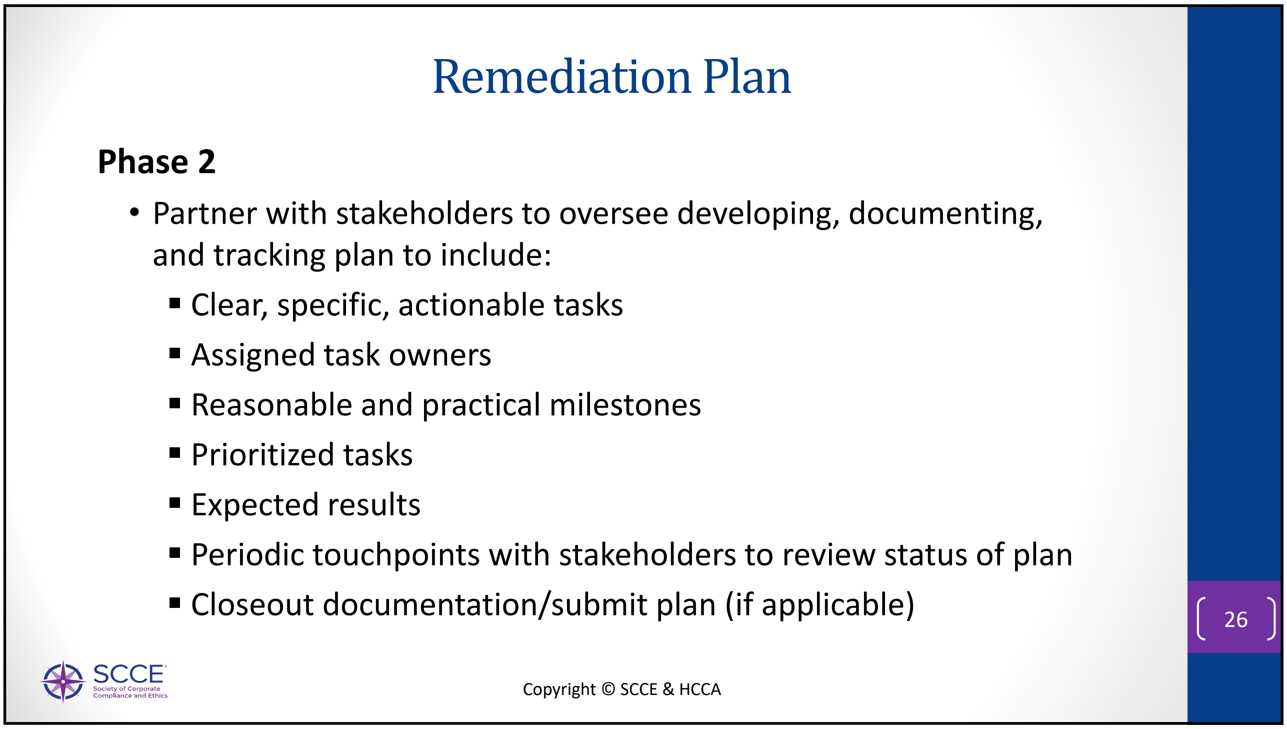


Elements of Remediation Plan

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

25



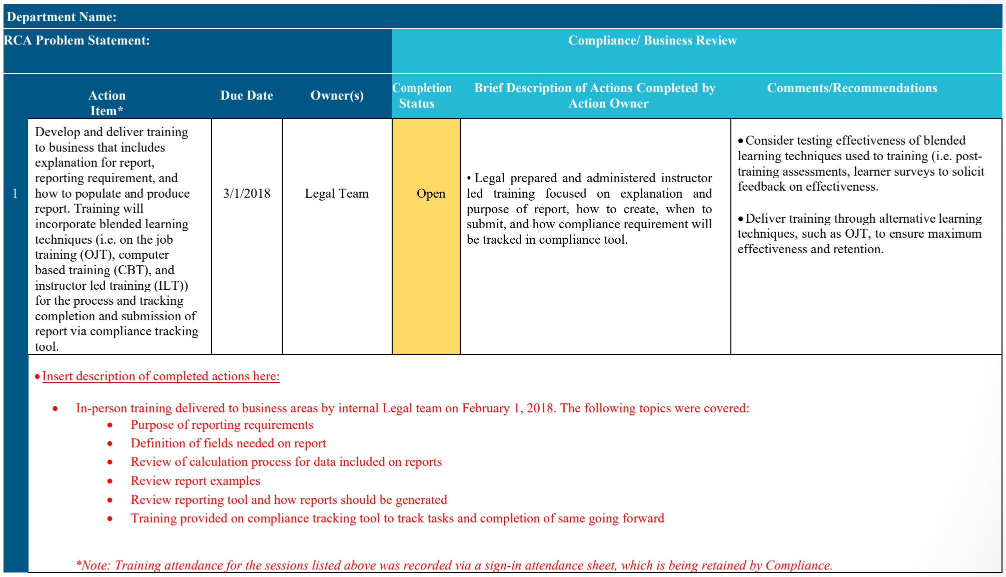
Remediation Plan

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)

26

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:

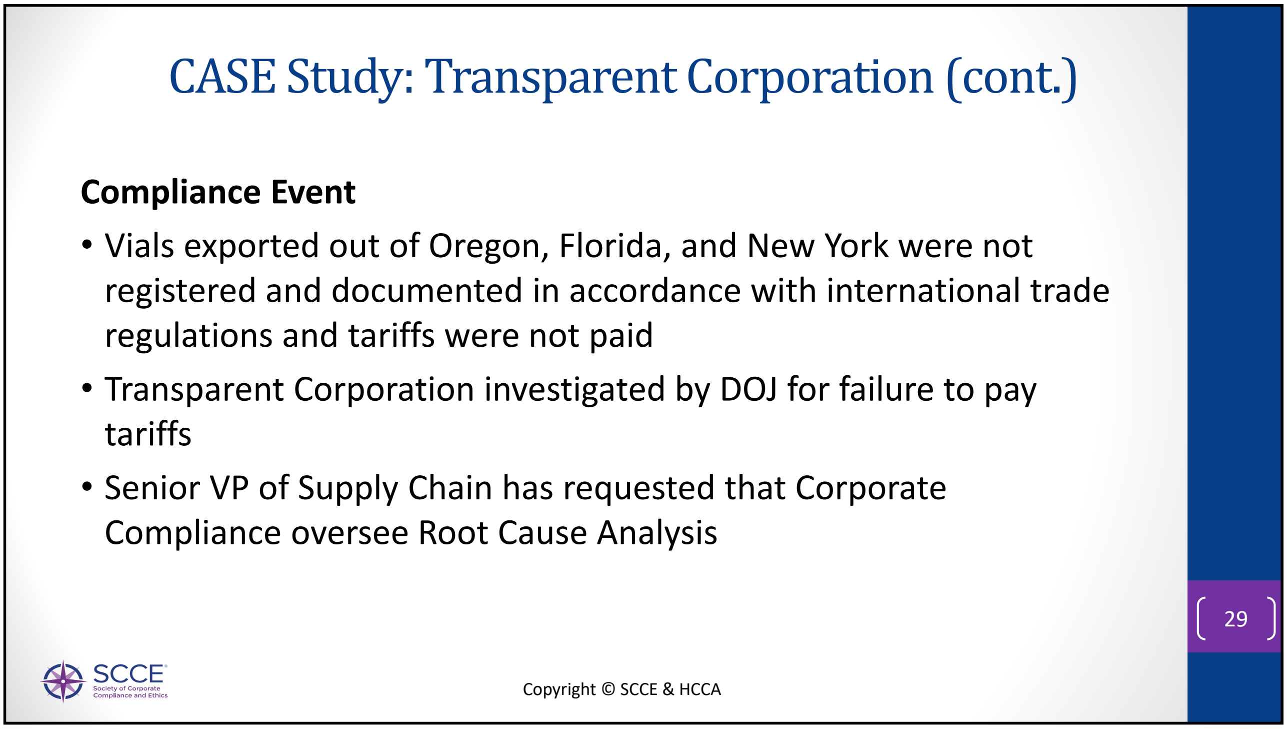
- In-person training delivered to business areas by internal Legal team on February 1, 2018. The following topics were covered:
  - Purpose of reporting requirements
  - Definition of fields needed on report
  - Review of calculation process for data included on reports
  - Review report examples
  - 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.*

CASE Study: Transparent Corporation

Background

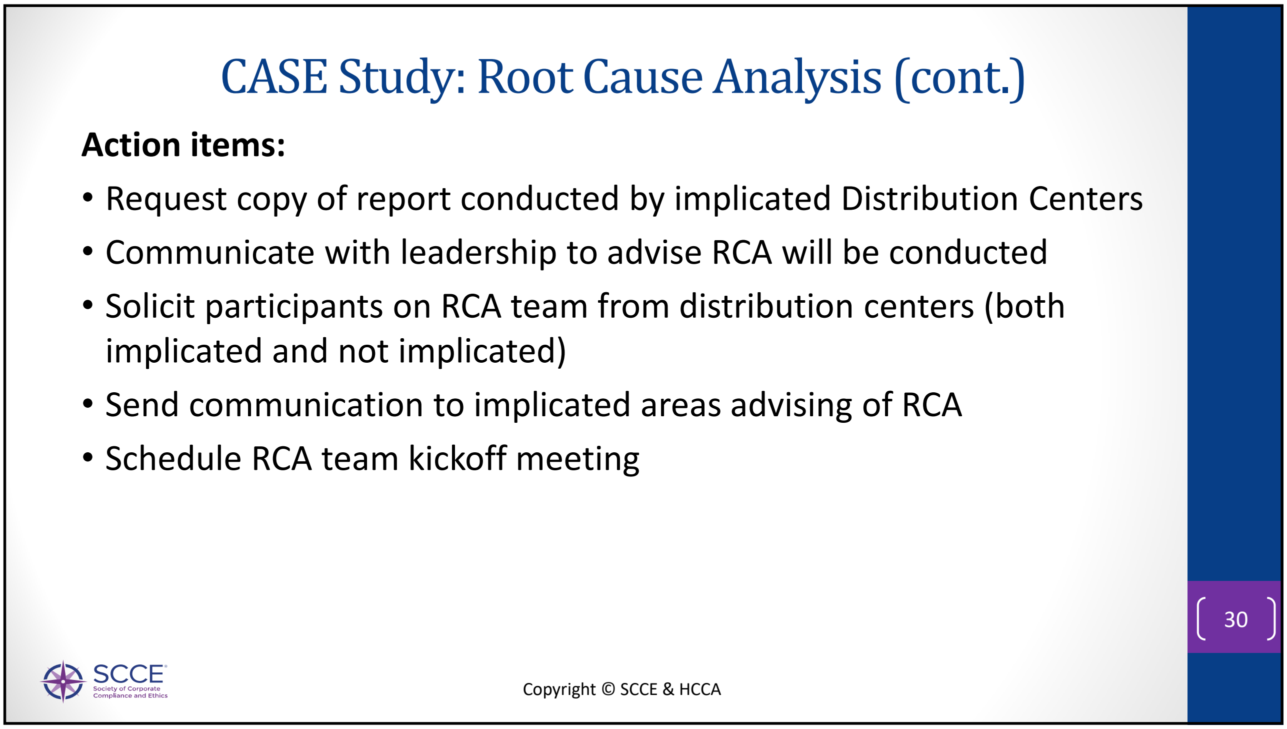
- Manufactures vials used for distributing vaccine for highly contagious disease
- Worldwide distribution of vials number <60 million
- Distribution Centers located in New York, North Carolina, Florida, Texas, California, and Oregon
- Distribution Centers managed by team of region directors who report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



CASE Study: Transparent Corporation (cont.)

Compliance Event

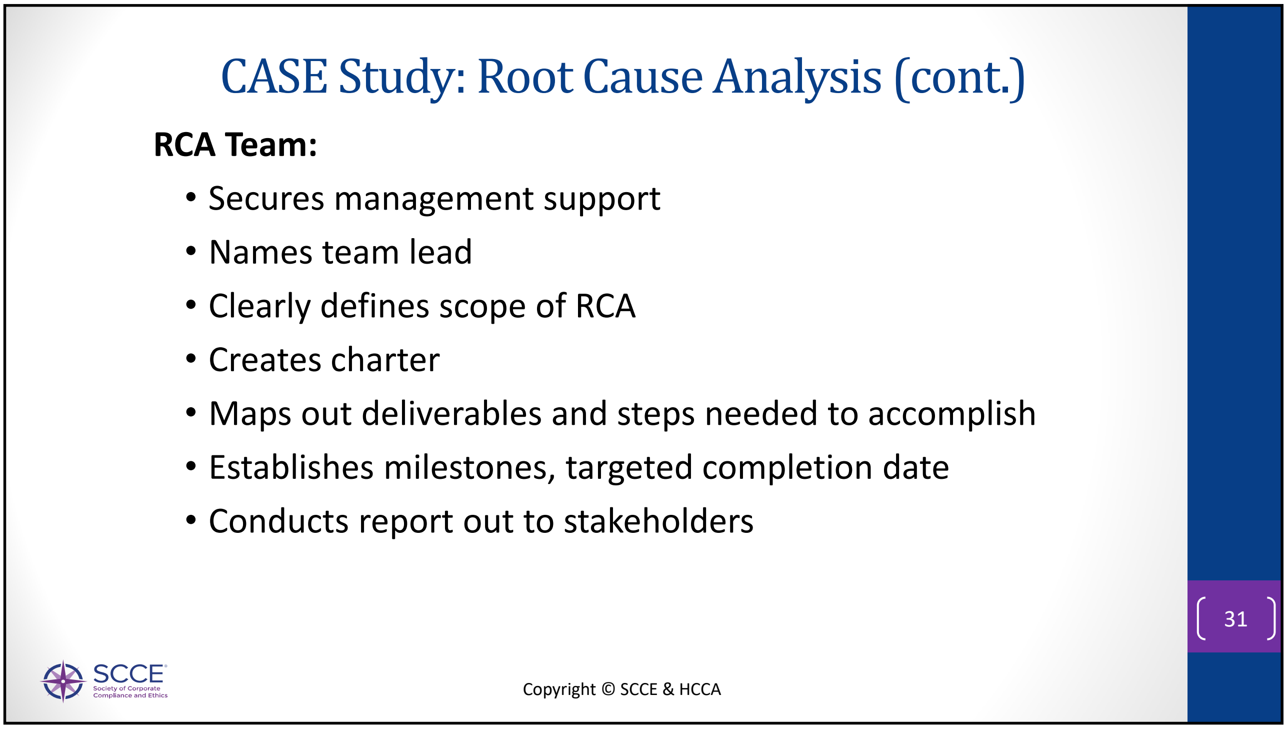
- Vials exported out of Oregon, Florida, and New York were not registered and documented in accordance with international trade regulations and tariffs were not paid
- Transparent Corporation investigated by DOJ for failure to pay tariffs
- Senior VP of Supply Chain has requested that Corporate Compliance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



CASE Study: Root Cause Analysis (cont.)

Action items:

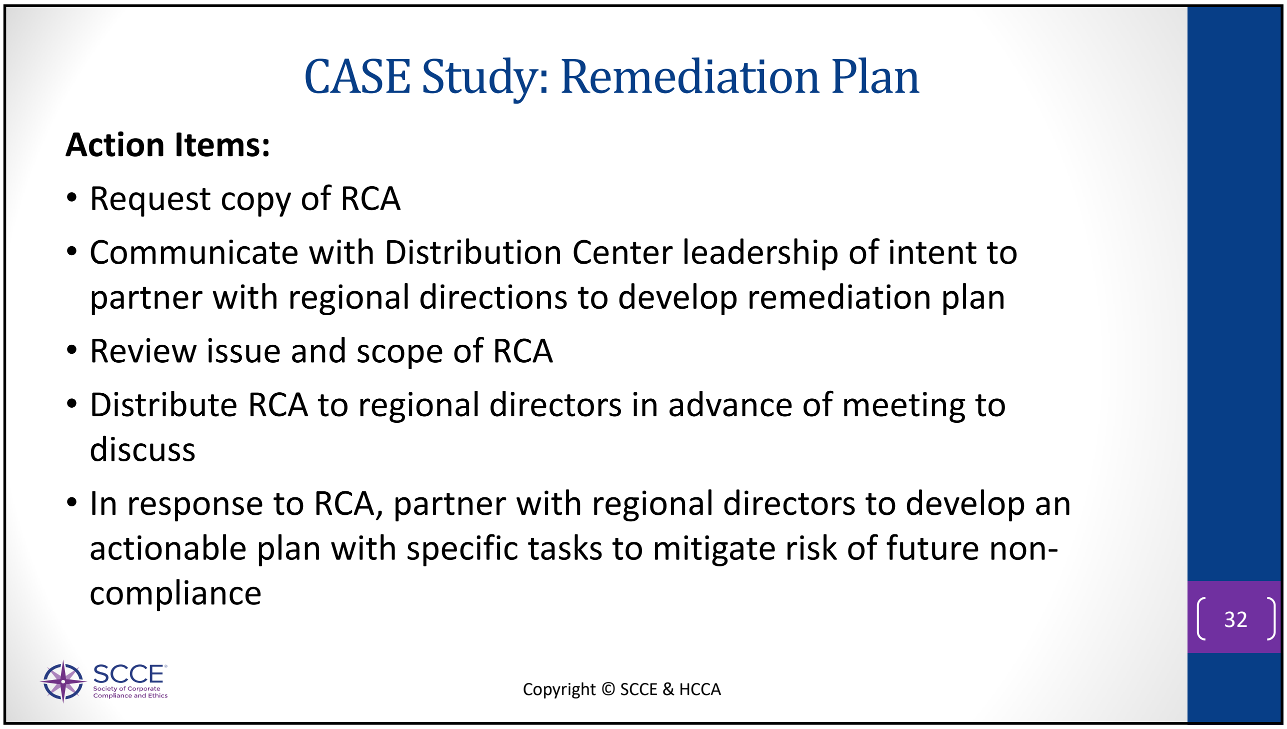
- Request copy of report conducted by implicated Distribution Centers
- Communicate with leadership to advise RCA will be conducted
- Solicit participants on RCA team from distribution centers (both implicated and not implicated)
- Send communication to implicated areas advising of RCA
- Schedule RCA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



CASE Study: Root Cause Analysis (cont.)

RCA Team:

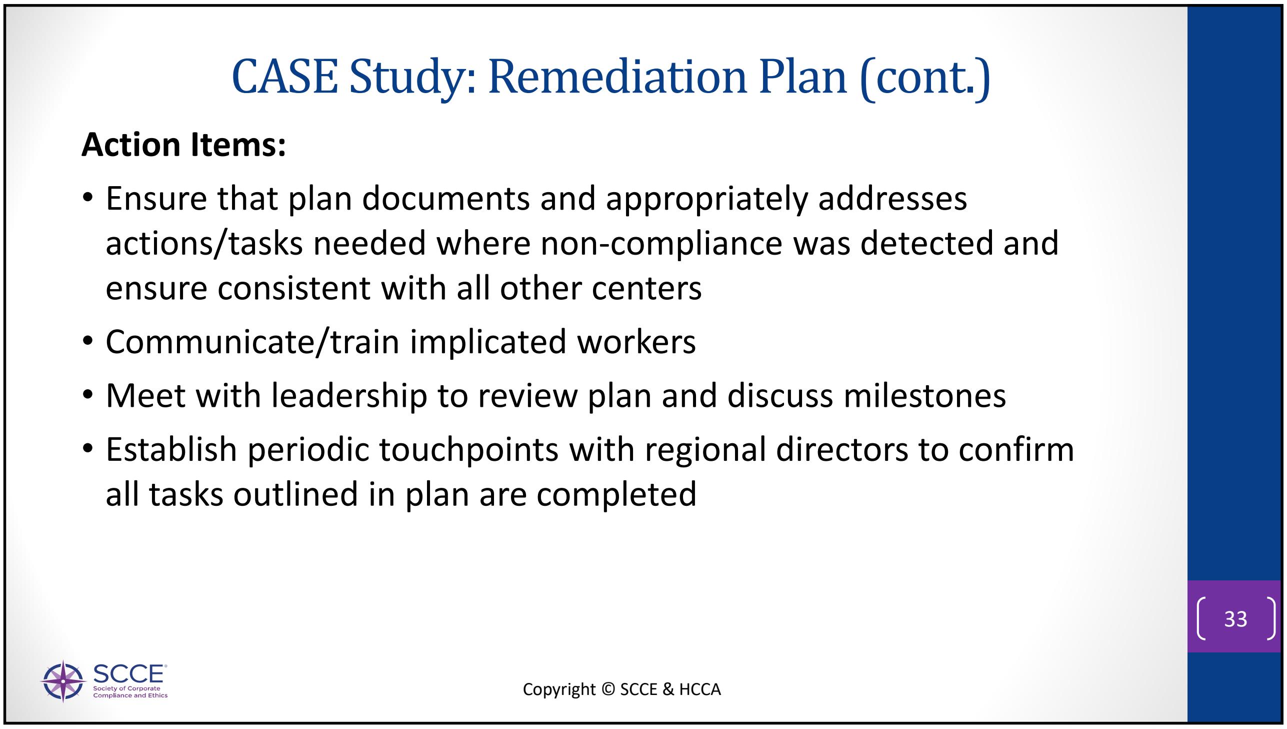
- Secures management support
- Names team lead
- Clearly defines scope of RCA
- Creates charter
- Maps out deliverables and steps needed to accomplish
- Establishes milestones, targeted completion date
- Conducts report out to stakeholders



CASE Study: Remediation Plan

Action Items:

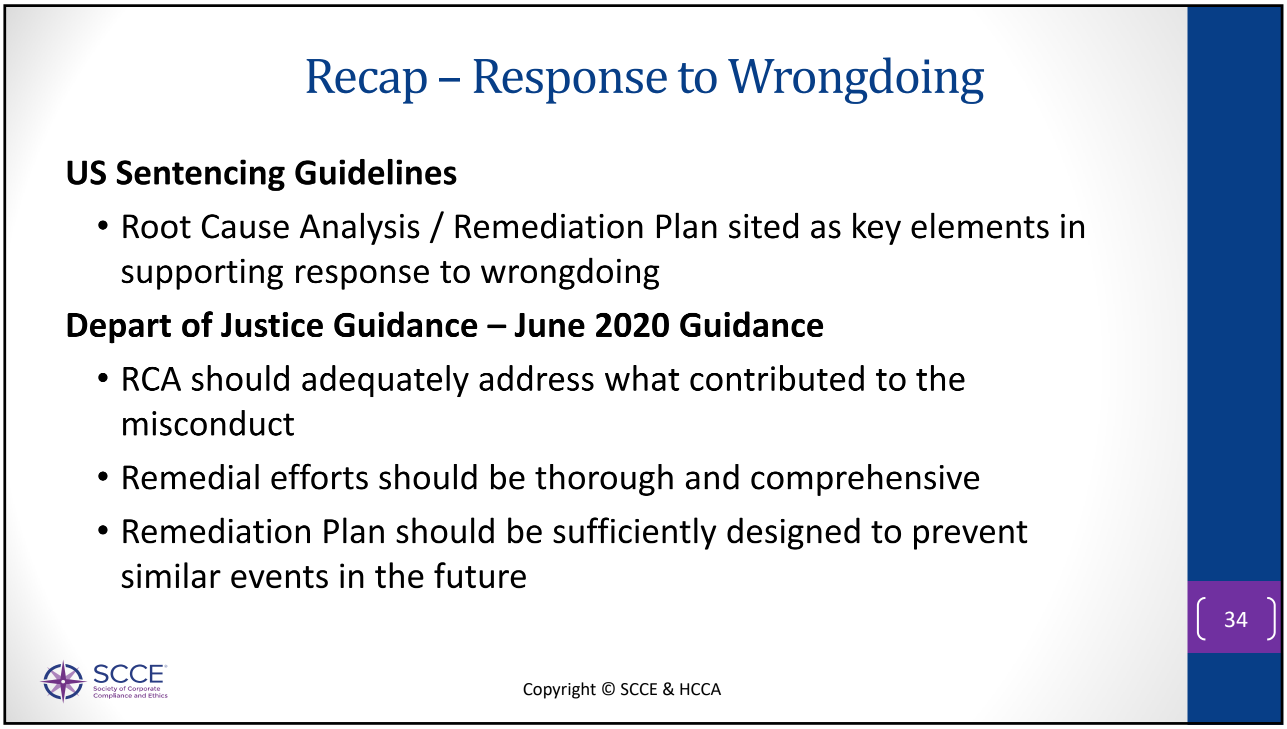
- Request copy of RCA
- Communicate with Distribution Center leadership of intent to partner with regional directions to develop remediation plan
- Review issue and scope of RCA
- Distribute RCA to regional directors in advance of meeting to discuss
- In response to RCA, partner with regional directors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



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



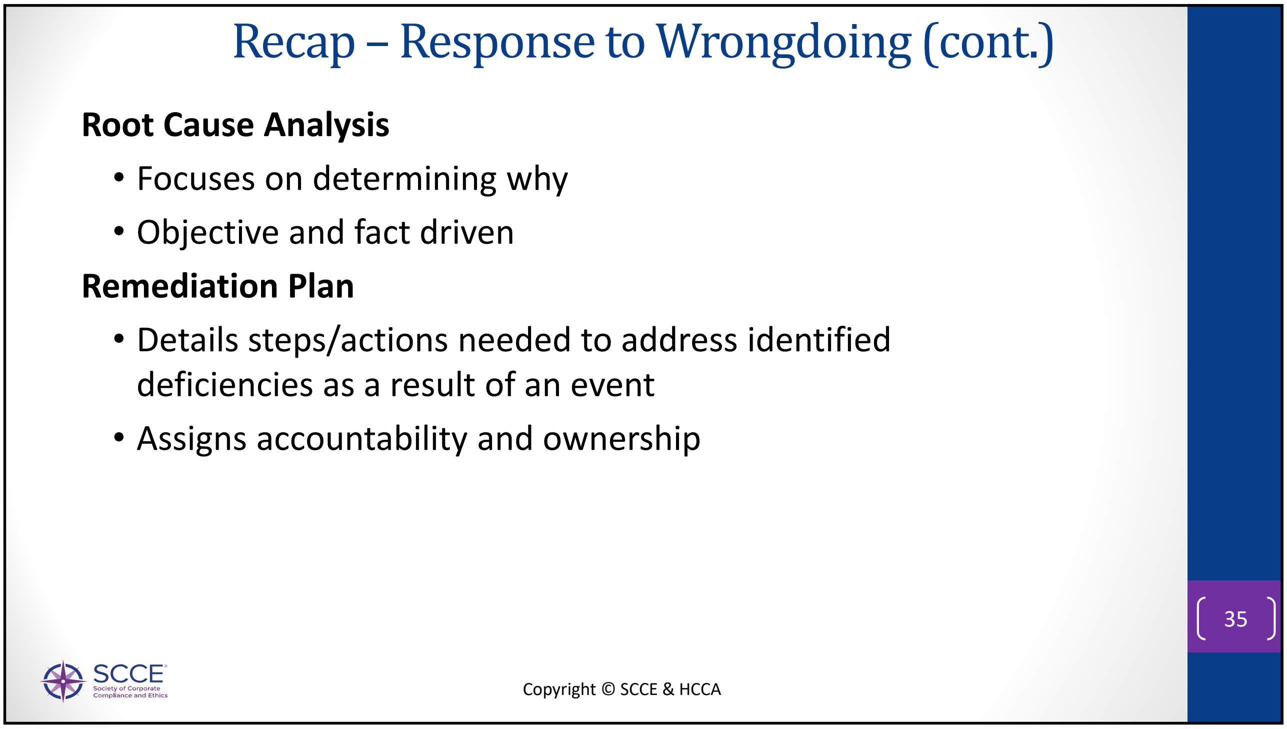
Recap – Response to Wrongdoing

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



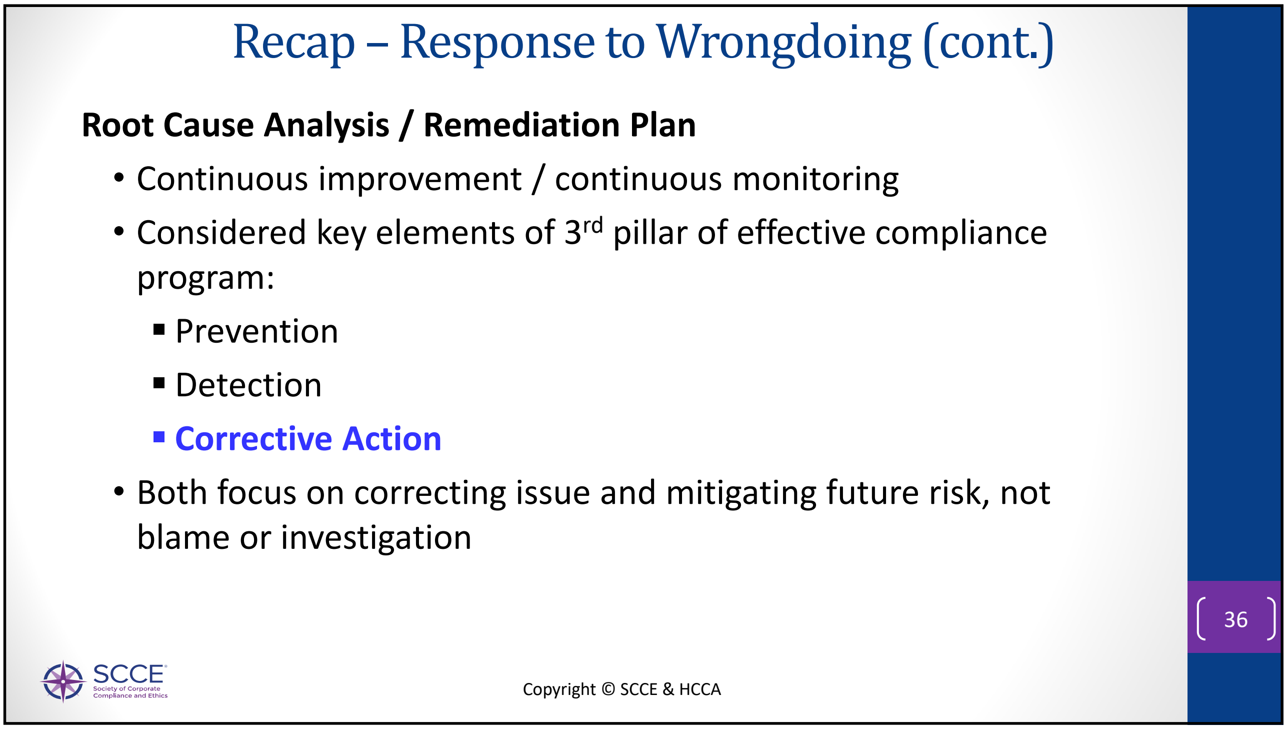
Recap – Response to Wrongdoing (cont.)

Root Cause Analysis

- Focuses on determining why
- Objective and fact driven

Remediation Plan

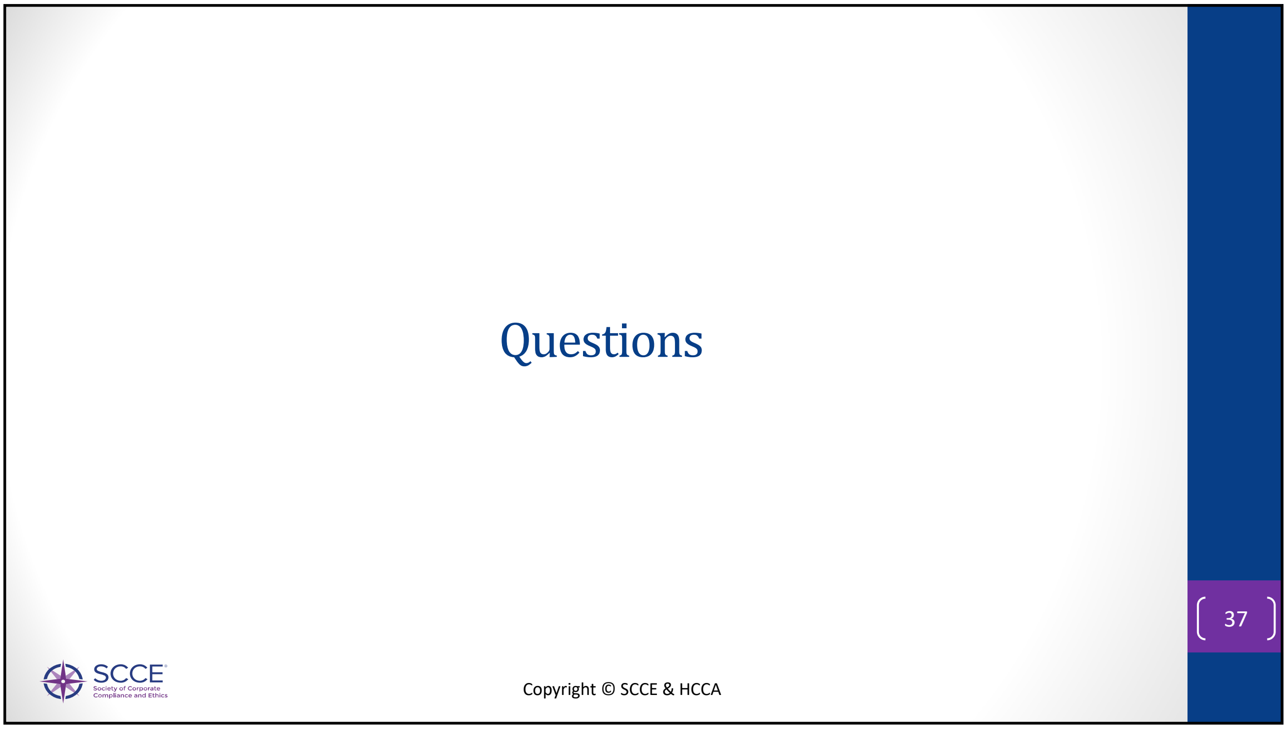
- Details steps/actions needed to address identified deficiencies as a result of an event
- Assigns accountability and ownership



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



Questions

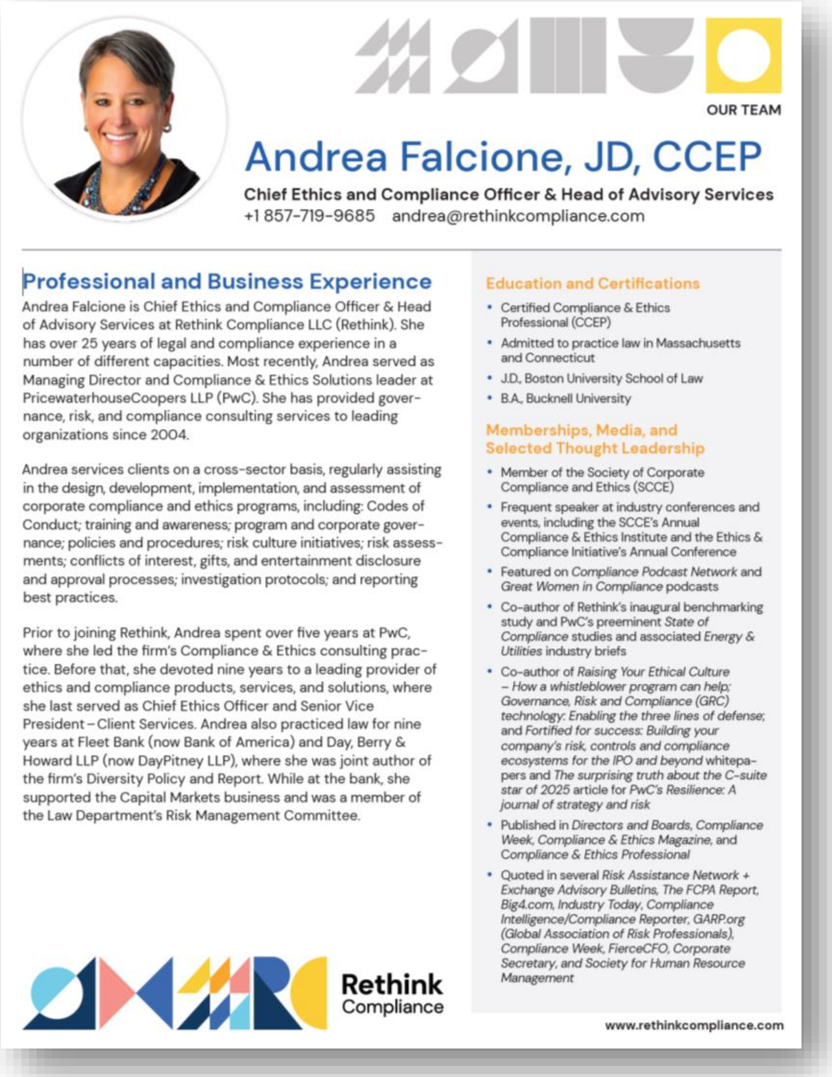
SCCE Compliance & Ethics Essentials Workshop

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

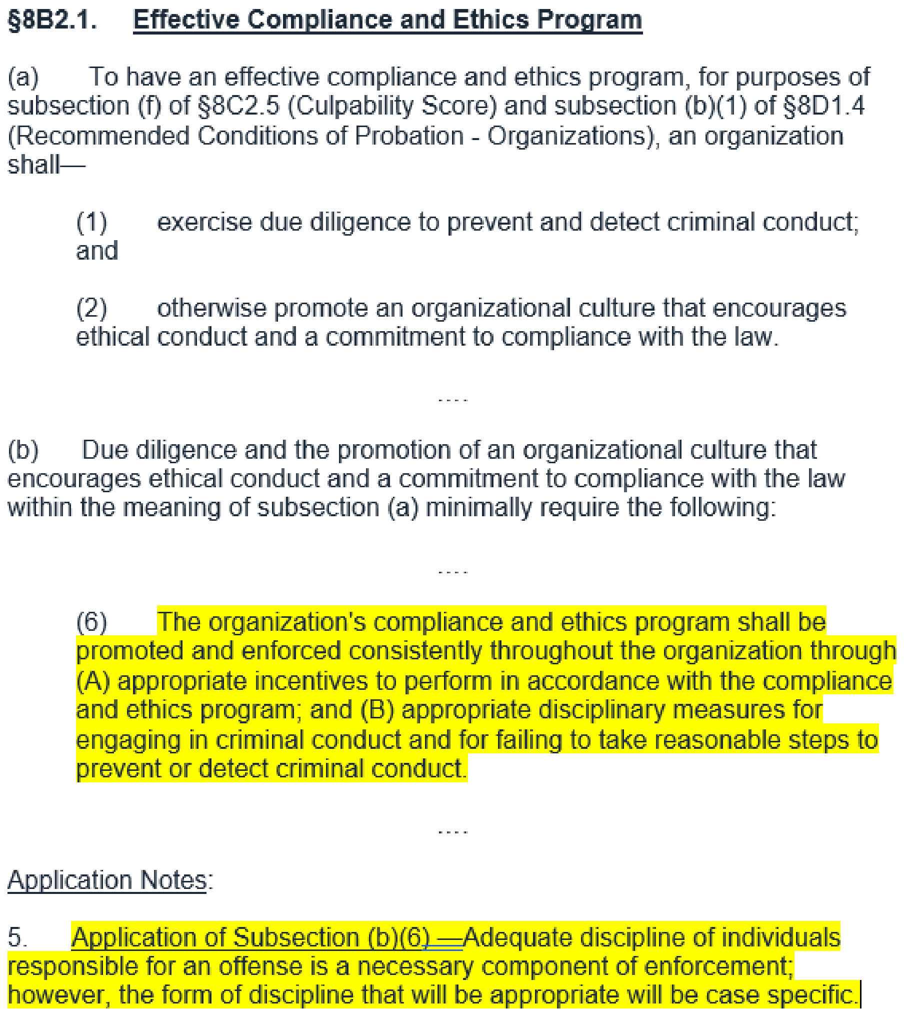
____

- Reference material

5 minutes

INCENTIVES AND ENFORCEMENT (ELEMENT NO. 4)

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!”

So, what can you do?

This Photo by Unknown Author is licensed under CC BY-SA-NC

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 …

S
M
A
R
T
Specific
Measurable
Attainable
Relevant
Time Based

This Photo by Unknown Author is licensed under CC BY-SA

SCCE Society of Corporate Compliance and Ethics

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

SCCE® Society of Corporate Compliance and Ethics

Other considerations

- Benefits of 360º 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

This Photo by Unknown Author is licensed under CC BY

The good, the bad, and the ugly

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

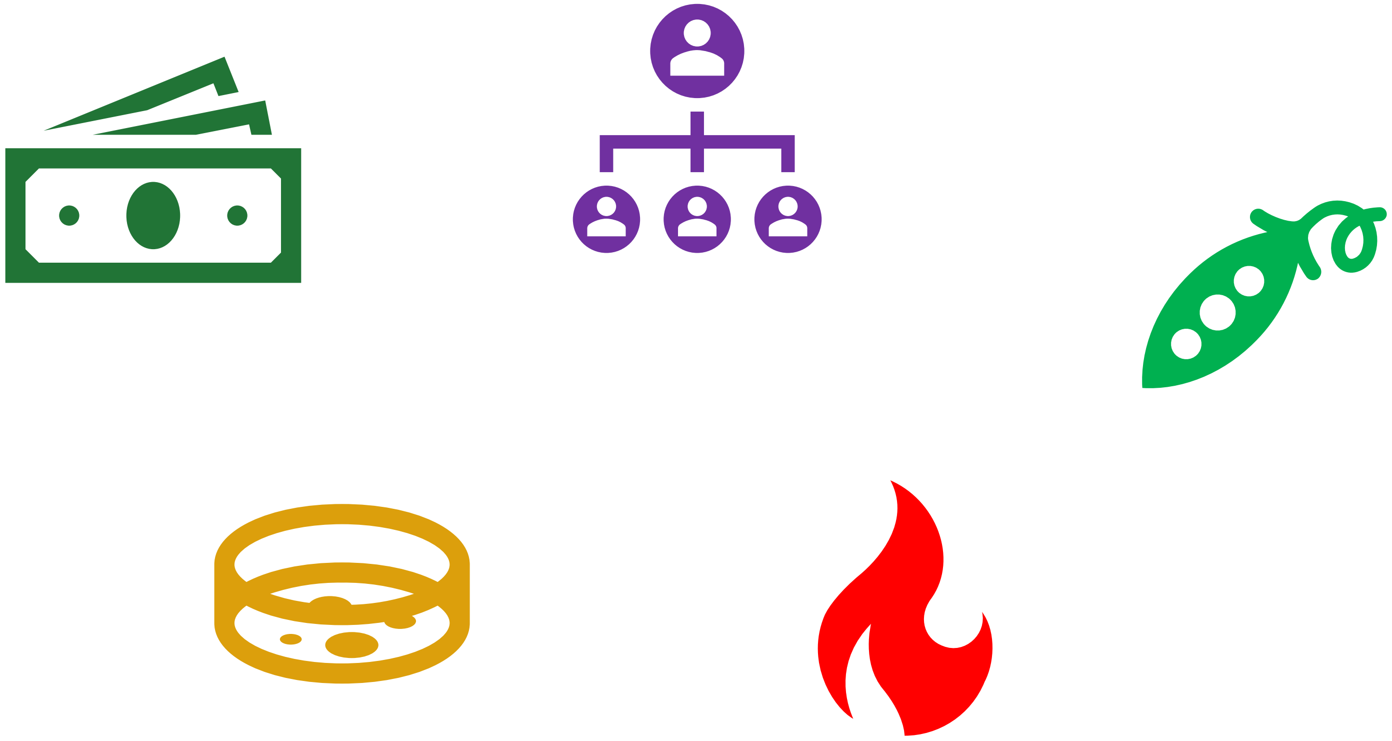
- Celebrations of compliance and ethics successes

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

This Photo by Unknown Author is licensed under CC BY-NC

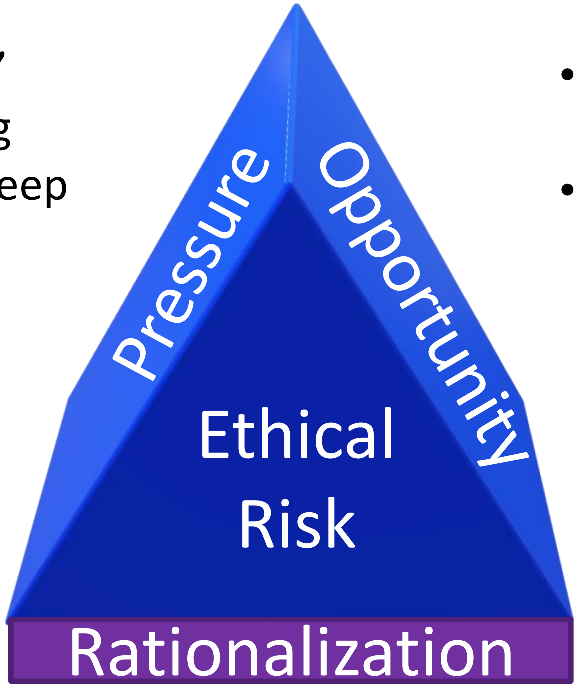
A cautionary tale….

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."



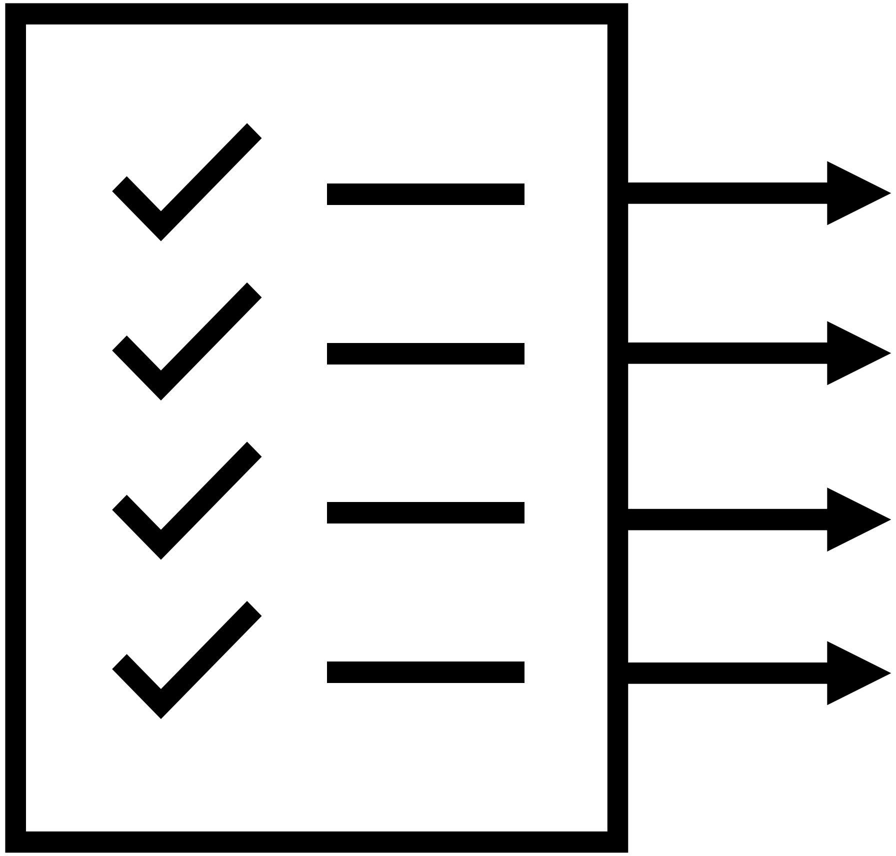
- Weak or circumventable internal controls
- Management's tacit approval / corrupt culture
- Poor oversight and lack of monitoring

- "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

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

SCCE
Society of Corporate Compliance and Ethics

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

This Photo by Unknown Author is licensed under CC BY-SA

Fairly applied

This Photo by Unknown Author is licensed under CC BY-NC-ND

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

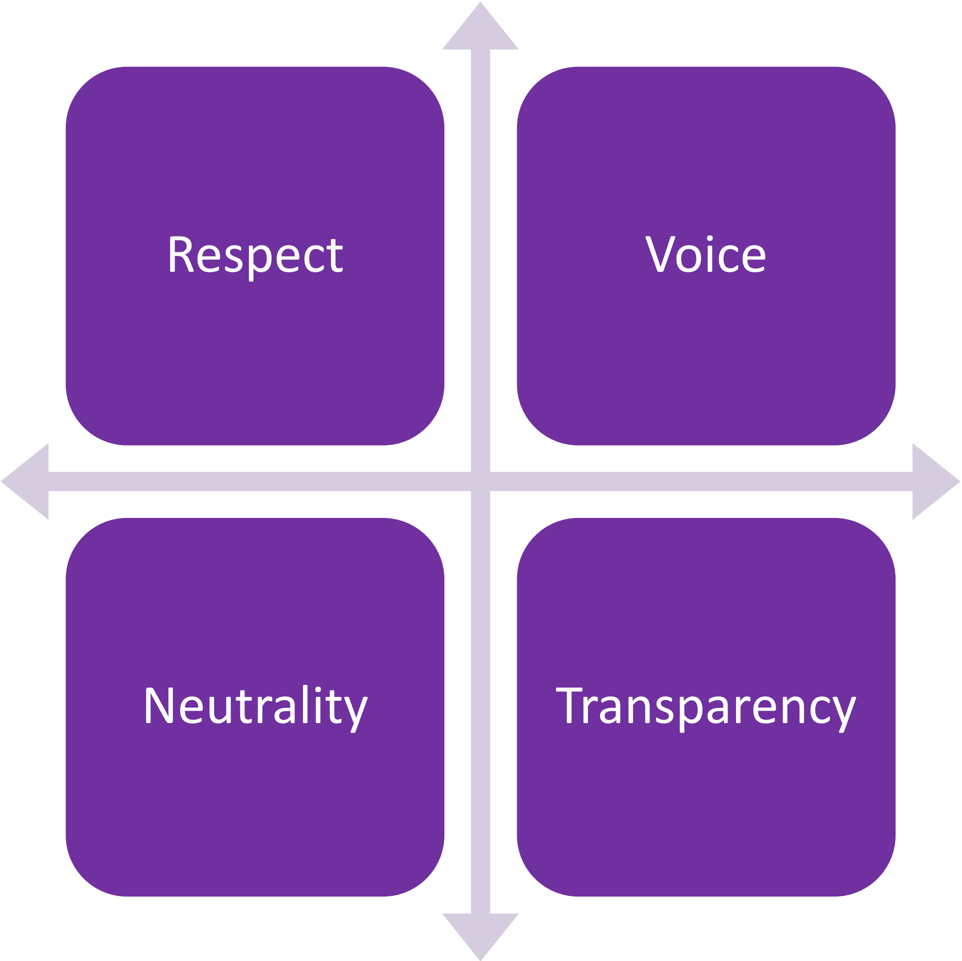
Wells Fargo to Claw Back $75 Million over Incentive Pay Scandal

Let’s start with the easy part …

Microsoft Word
7 - 2003 Documer

Now the hard part …

Procedural Justice



Respect

Voice

Neutrality

Transparency

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

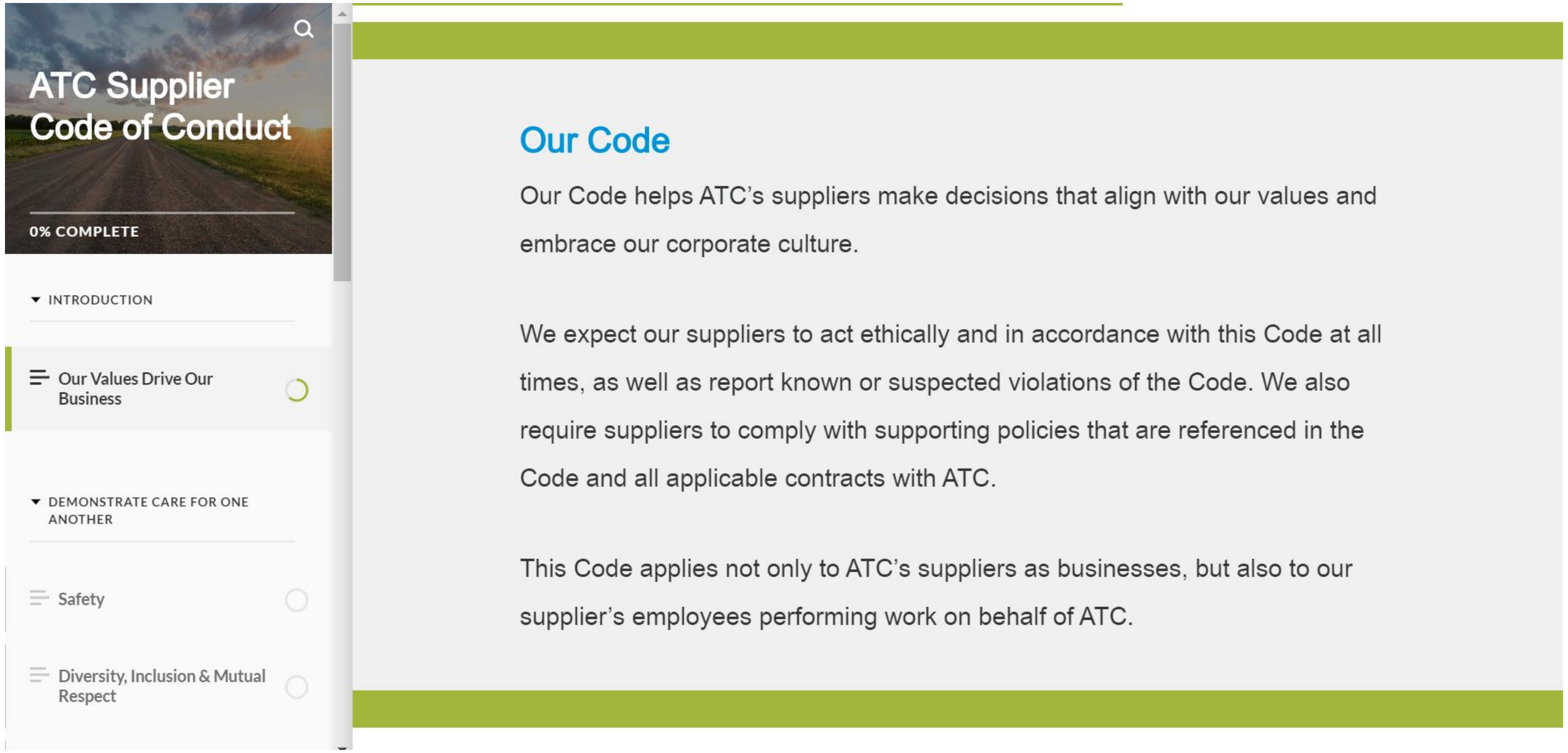
- Guess what? They matter, too!

- 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

0% COMPLETE

INTRODUCTION

Our Values Drive Our Business

DEMONSTRATE CARE FOR ONE ANOTHER

Safety

Diversity, Inclusion & Mutual Respect

Our Code

Our Code helps ATC's suppliers make decisions that align with our values and embrace our corporate culture.

We expect our suppliers to act ethically and in accordance with this Code at all times, as well as report known or suspected violations of the Code. We also require suppliers to comply with supporting policies that are referenced in the Code and all applicable contracts with ATC.

This Code applies not only to ATC's suppliers as businesses, but also to our supplier's employees performing work on behalf of ATC.

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."

This Photo by Unknown Author is licensed under CC BY-SA

"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."

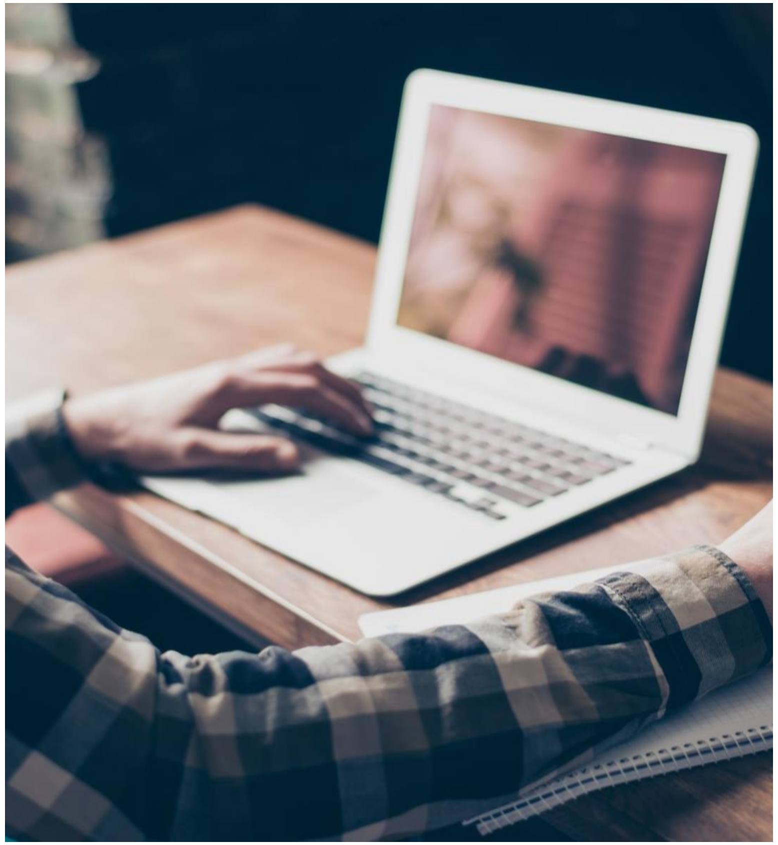
UnitedHealth Group

This Photo by Unknown Author is licensed under CC BY-SA-NC

Accountability, continued

Contractual provisions

Training



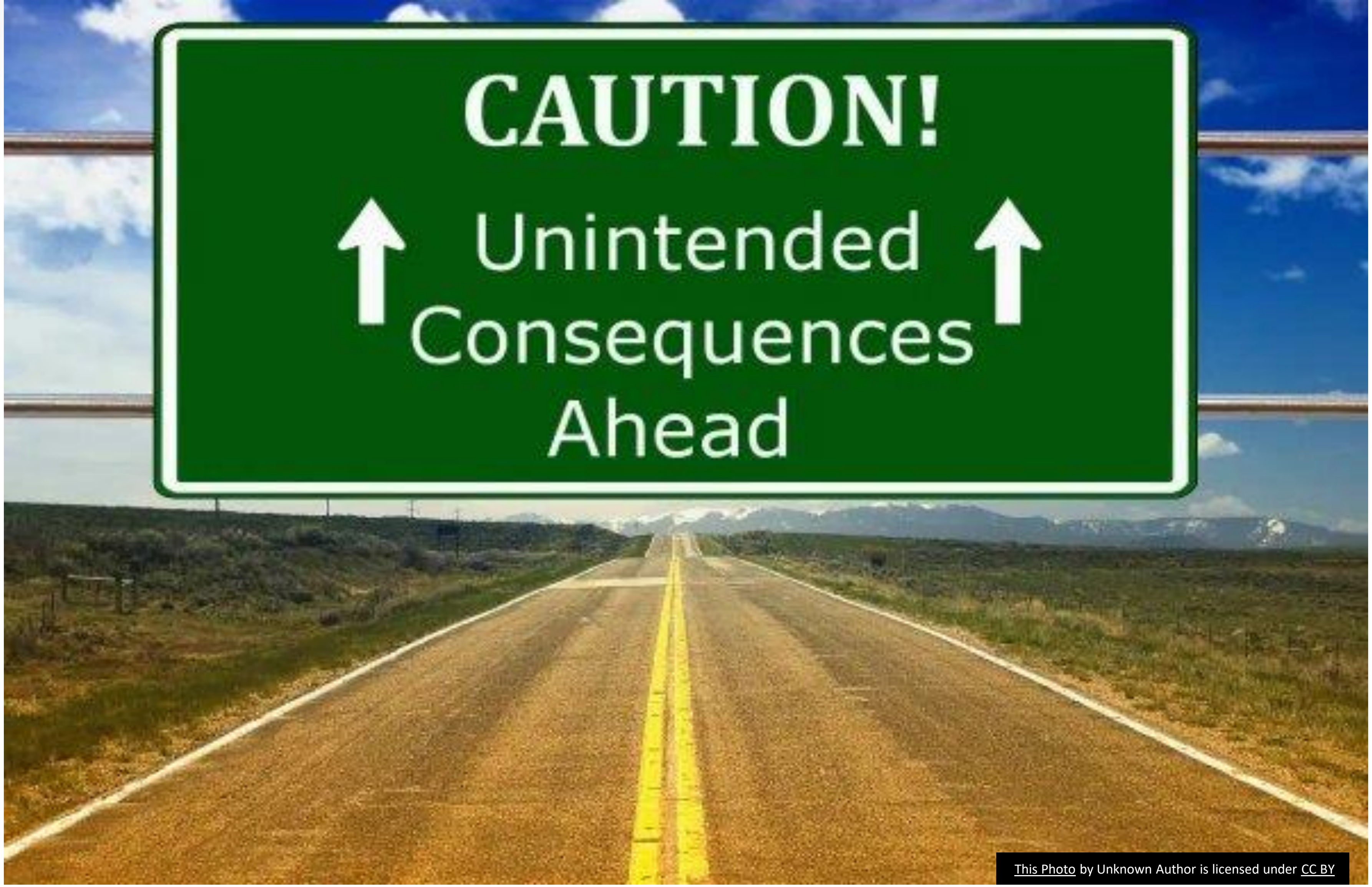
SCCE Society of Corporate Compliance and Ethics

How can we know?

Monitor

Audit

This Photo by Unknown Author is licensed under CC BY-NC



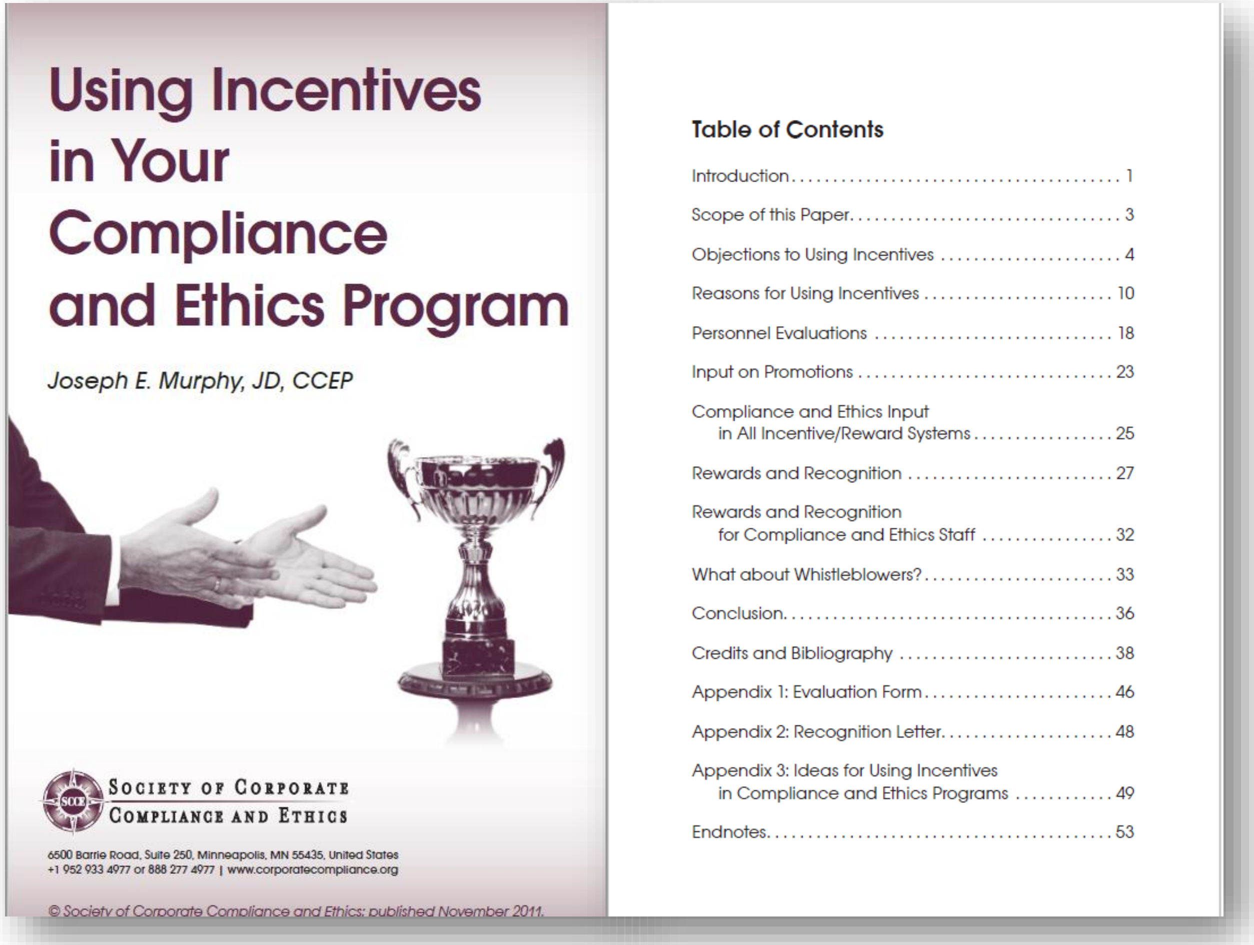
This Photo by Unknown Author is licensed under CC BY

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

THANK YOU!

SCCE
Society of Corporate Compliance and Ethics

Reference material



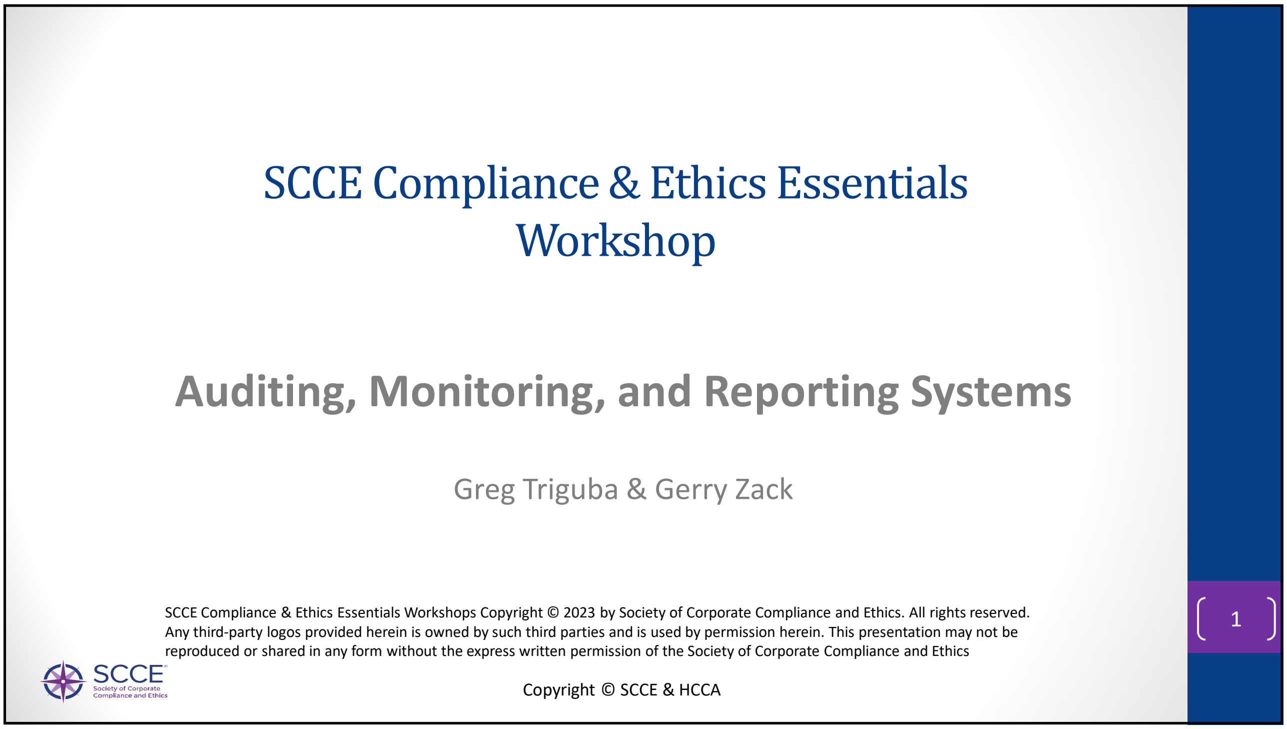
Using Incentives in Your Compliance and Ethics Program

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

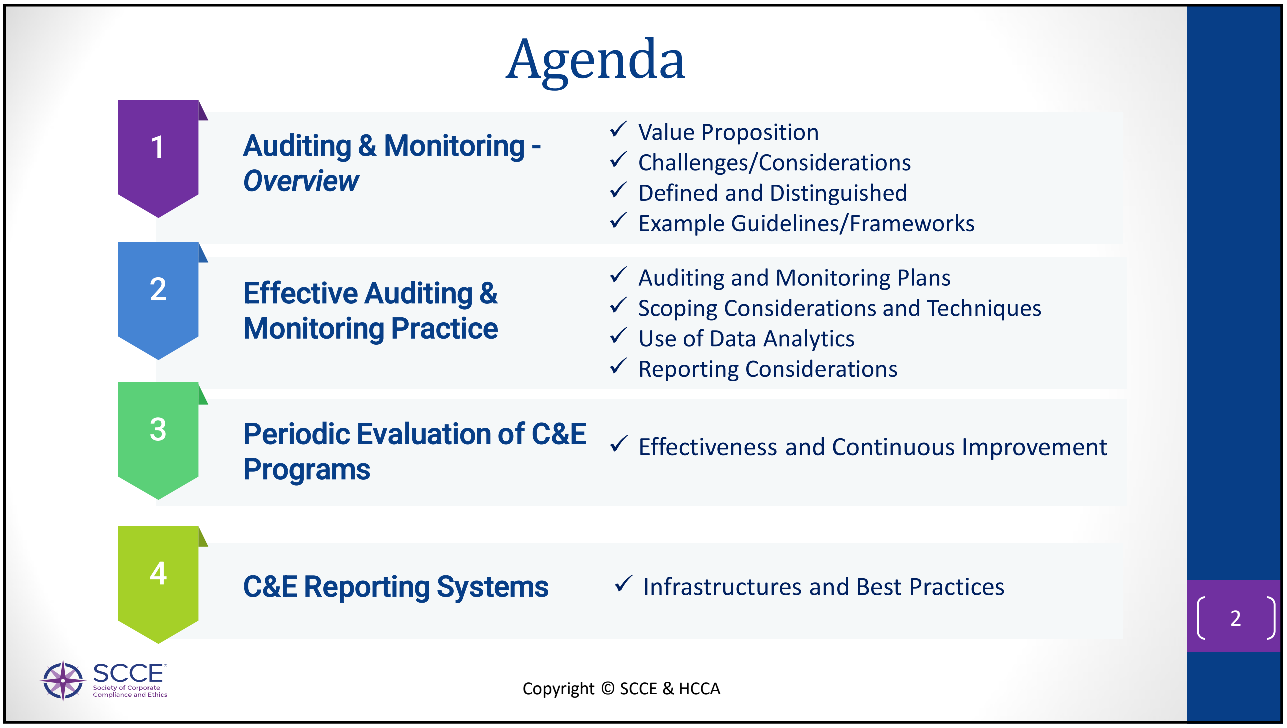
Table of Contents



SCCE Compliance & Ethics Essentials Workshop

Auditing, Monitoring, and Reporting Systems

Greg Triguba & Gerry Zack



Agenda

1 **Auditing & Monitoring - *Overview***

- ✓ Value Proposition
- ✓ Challenges/Considerations
- ✓ Defined and Distinguished
- ✓ Example Guidelines/Frameworks

2 **Effective Auditing & Monitoring Practice**

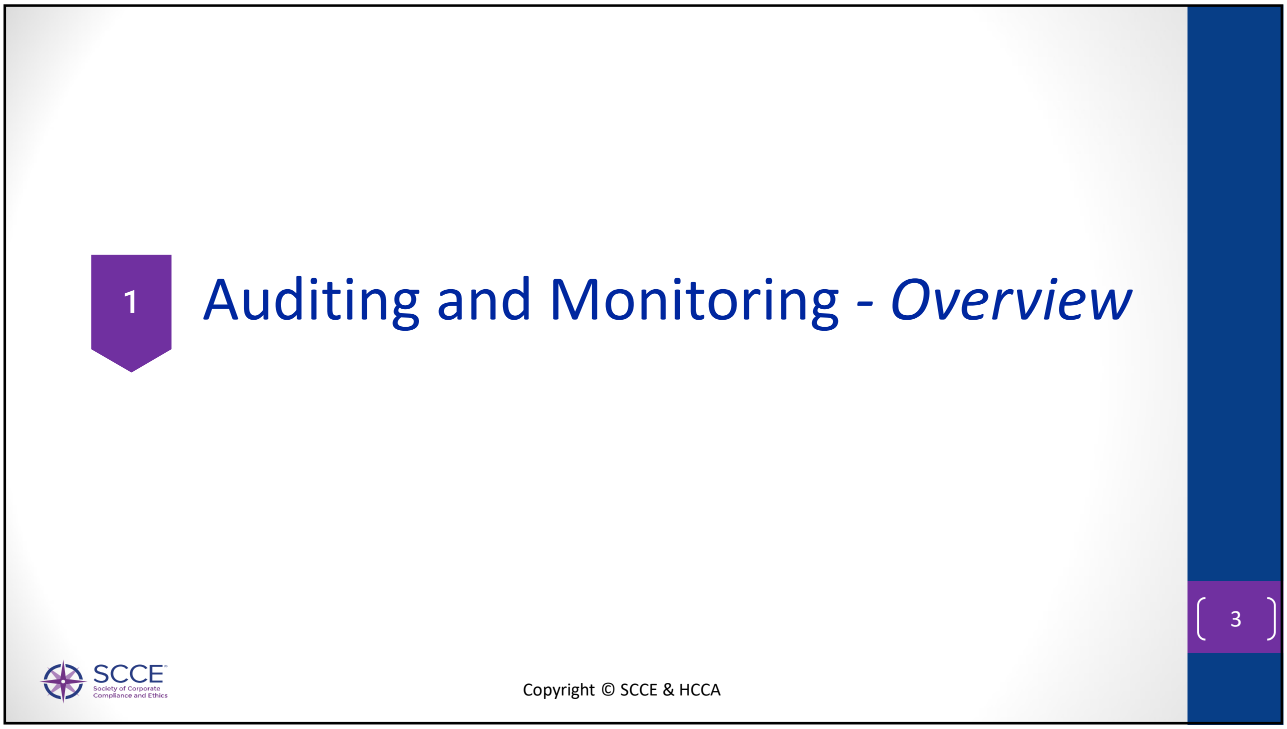
- ✓ Auditing and Monitoring Plans
- ✓ Scoping Considerations and Techniques
- ✓ Use of Data Analytics
- ✓ Reporting Considerations

3 **Periodic Evaluation of C&E Programs**

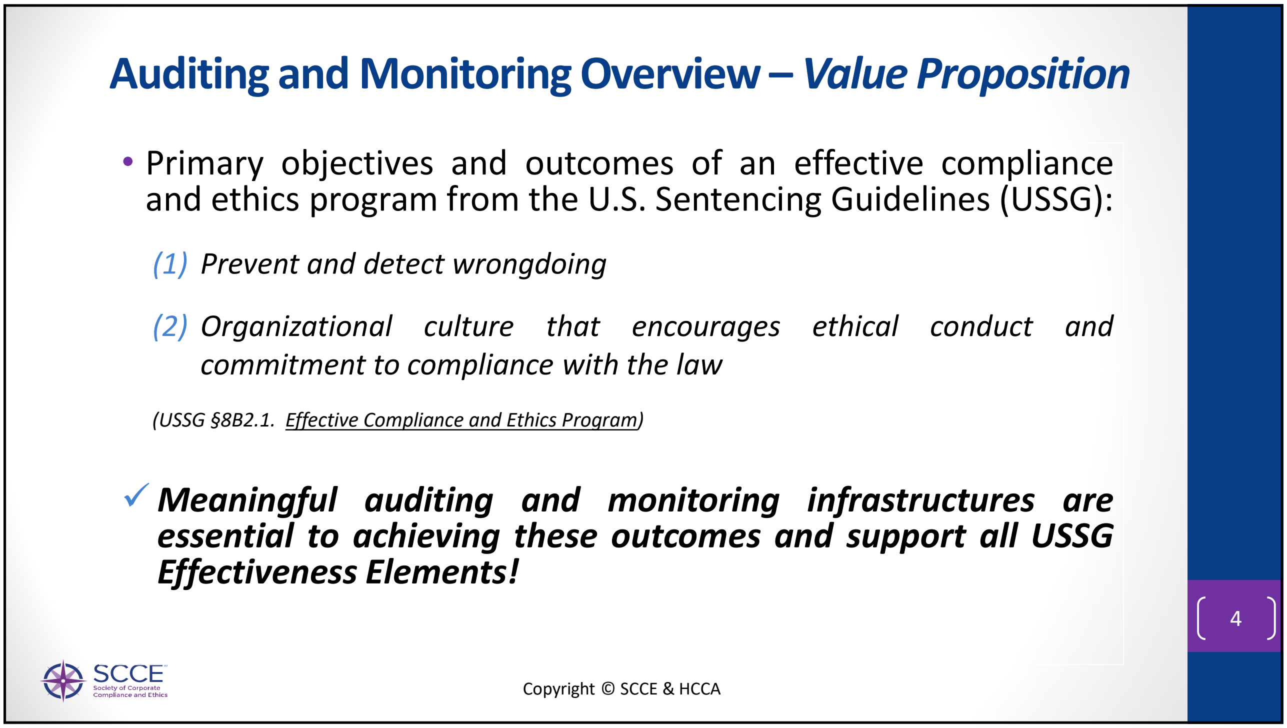
- ✓ Effectiveness and Continuous Improvement

4 **C&E Reporting Systems**

- ✓ Infrastructures and Best Practices



1 Auditing and Monitoring - *Overview*



Auditing and Monitoring Overview – *Value Proposition*

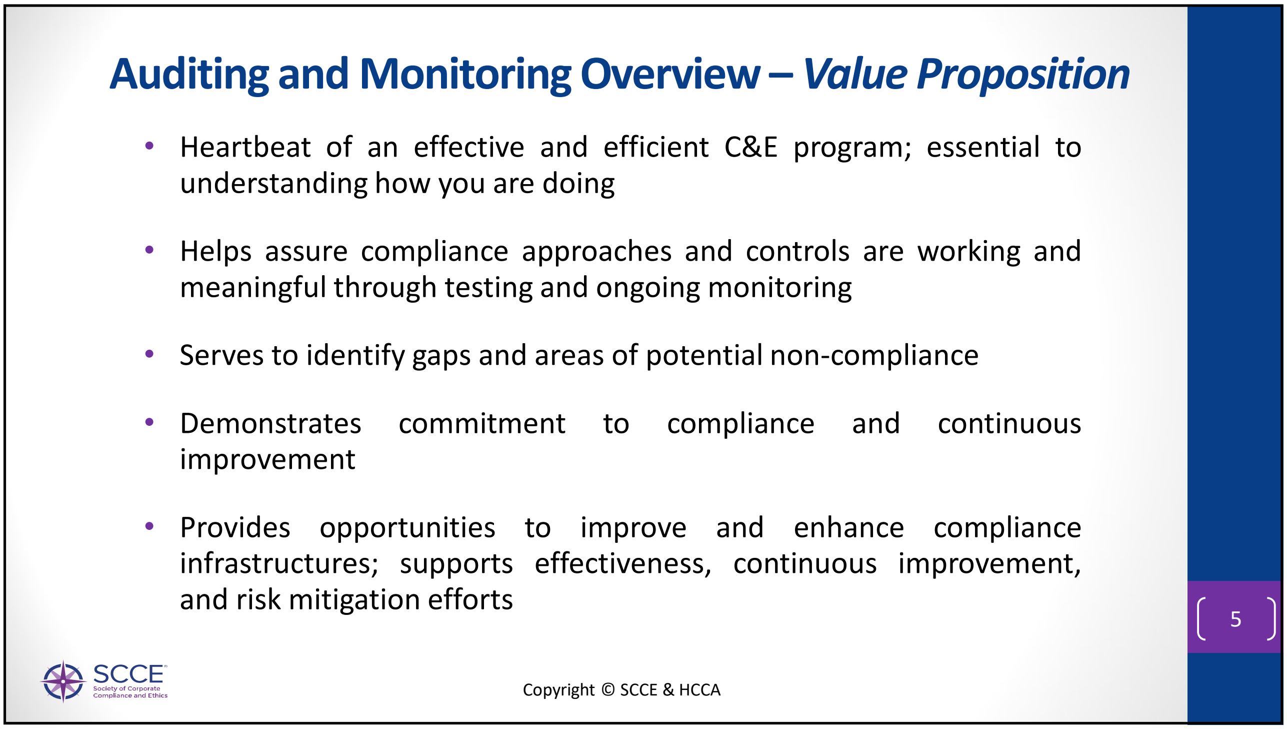
- Primary objectives and outcomes of an effective compliance and ethics program from the U.S. Sentencing Guidelines (USSG):

  (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 USSG Effectiveness Elements!***

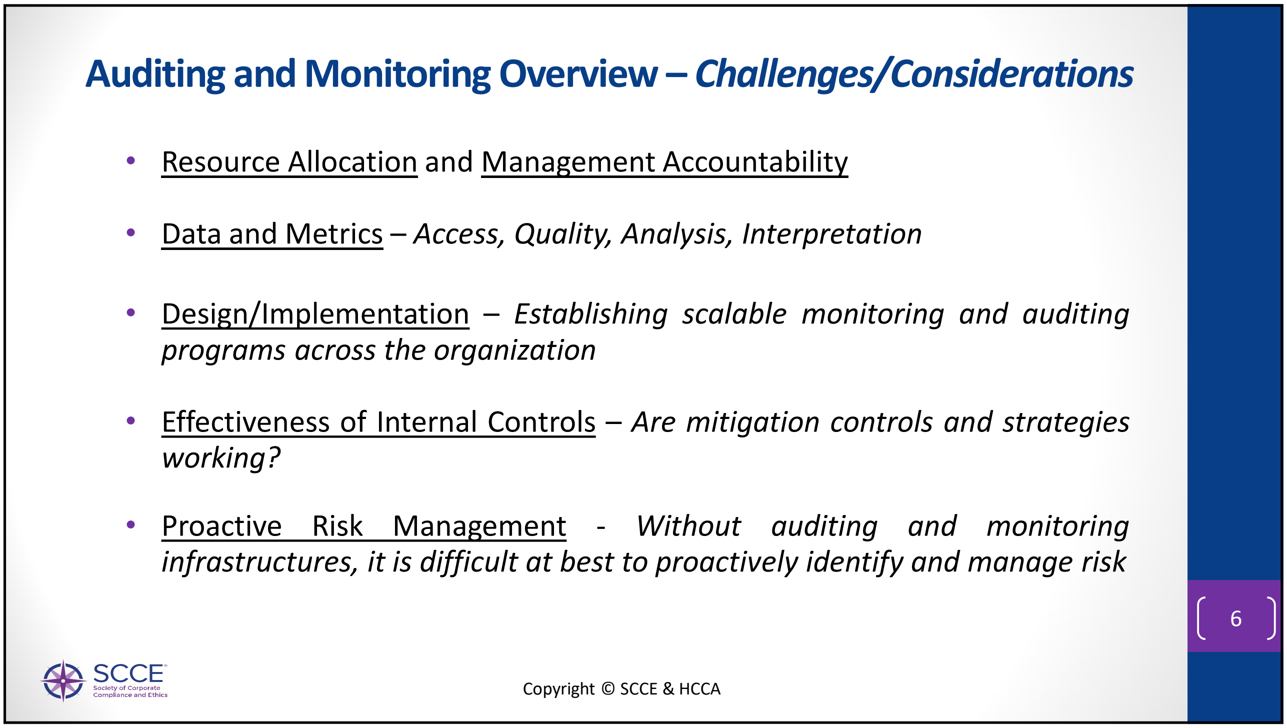


Auditing and Monitoring Overview – *Value Proposition*

- Heartbeat of an effective and efficient C&E program; essential to understanding how you are doing
- Helps assure compliance approaches and controls are working and meaningful through testing and ongoing monitoring
- Serves to identify gaps and areas of potential non-compliance
- Demonstrates commitment to compliance and continuous improvement
- Provides opportunities to improve and enhance compliance infrastructures; supports effectiveness, continuous improvement, and risk mitigation efforts

5

5

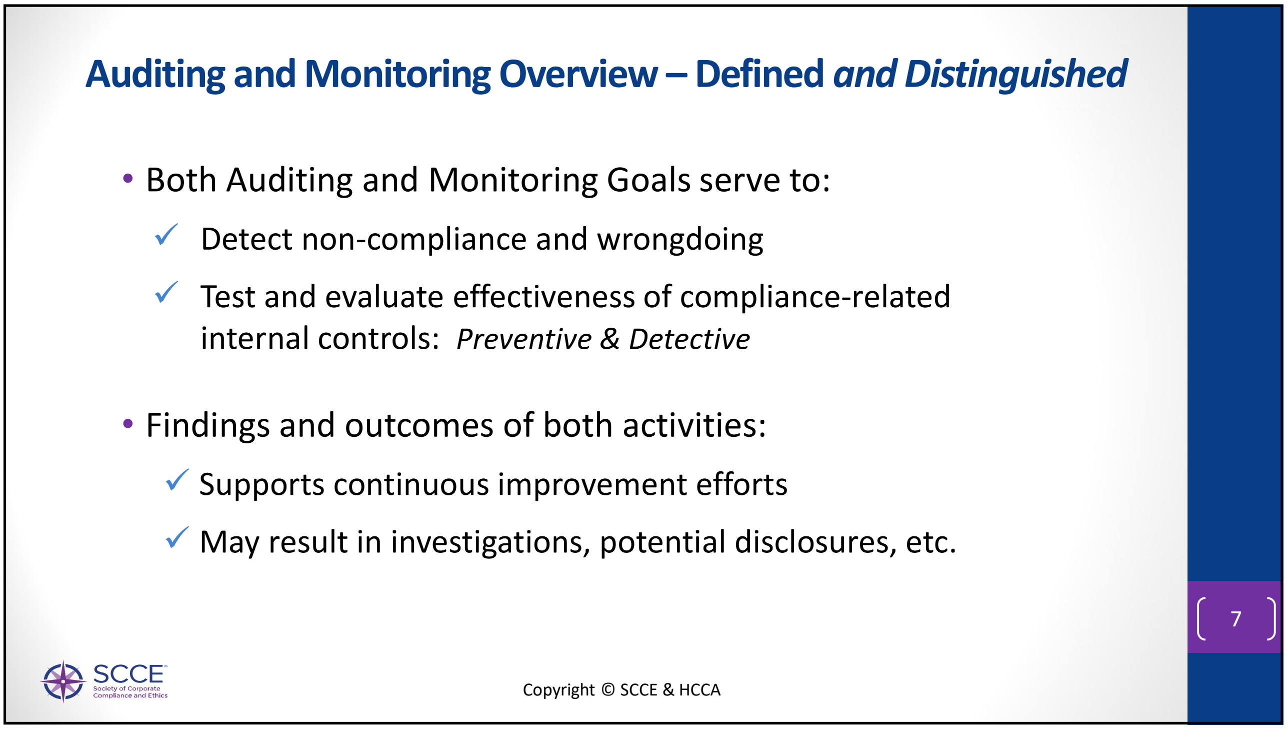


Auditing and Monitoring Overview – *Challenges/Considerations*

- 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 at best to proactively identify and manage risk*

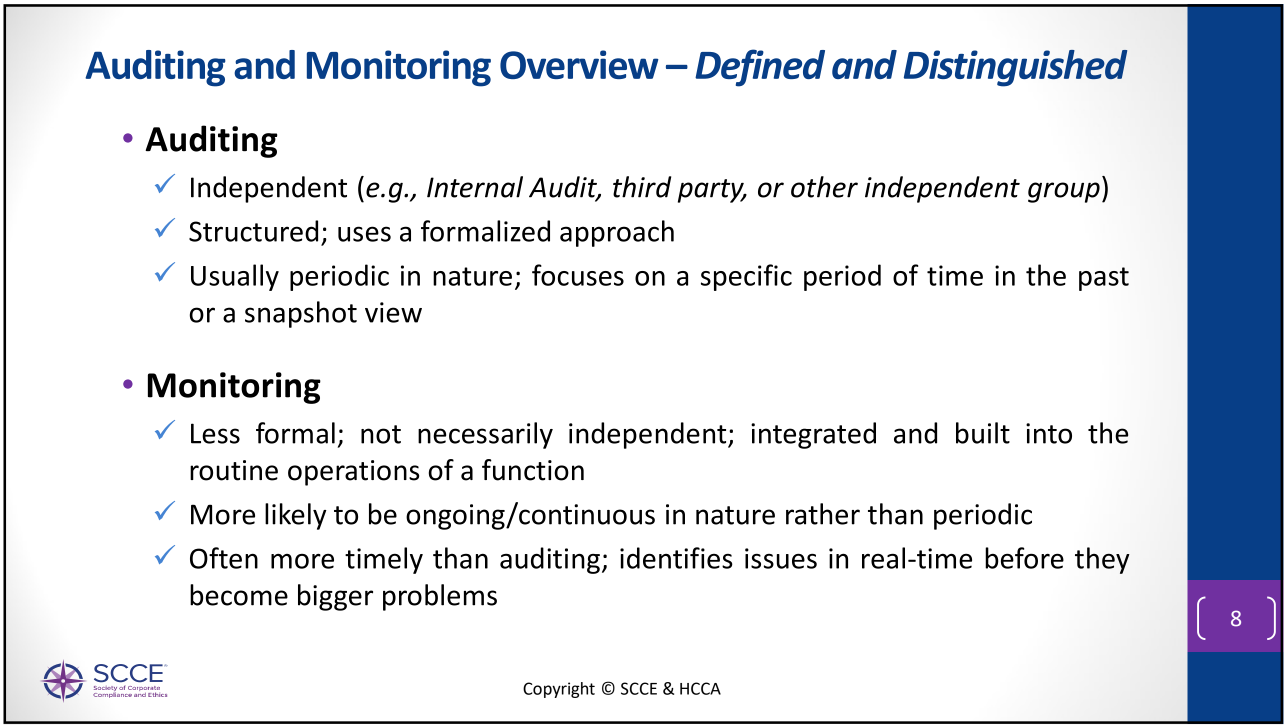
6

6



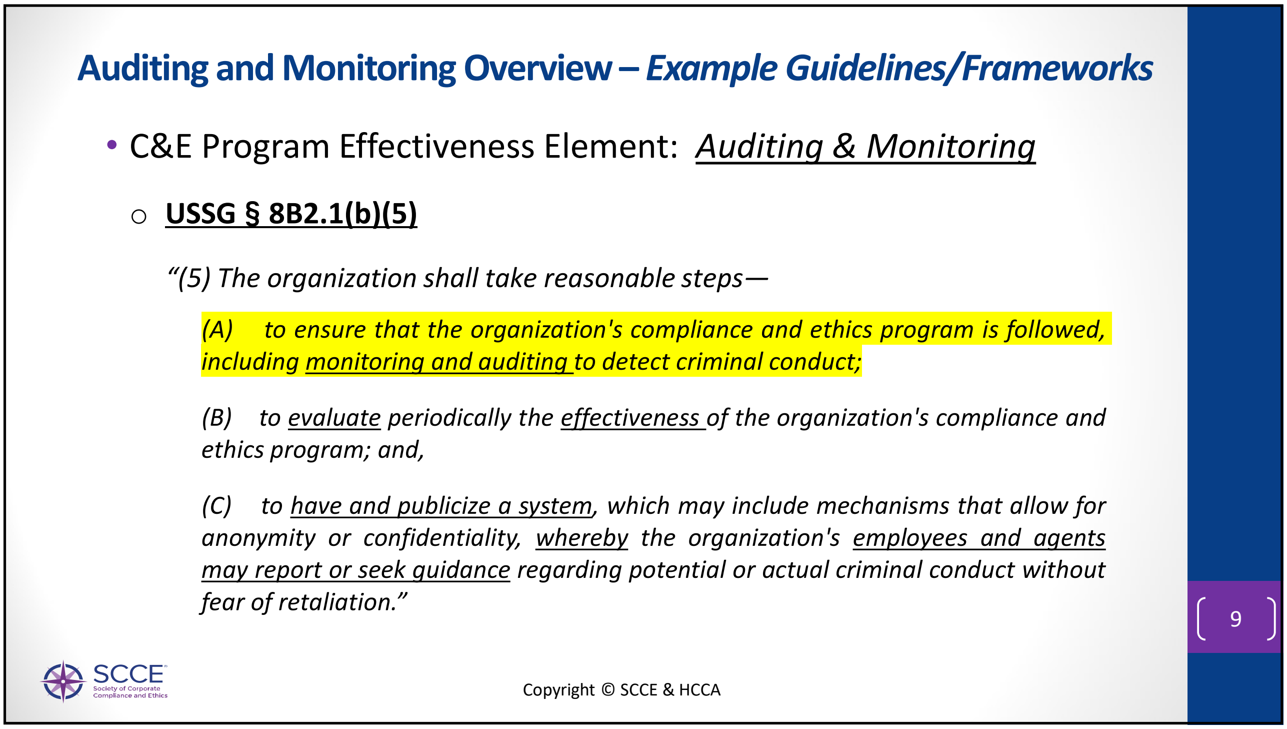
Auditing and Monitoring Overview – Defined *and Distinguished*

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



Auditing and Monitoring Overview – *Defined and Distinguished*

- **Auditing**
  - ✓ Independent (*e.g., Internal Audit, third party, or other independent group*)
  - ✓ 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
  - ✓ Often more timely than auditing; identifies issues in real-time before they become bigger problems



Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

- C&E Program Effectiveness Element: *Auditing & Monitoring*
  - **USSG § 8B2.1(b)(5)**

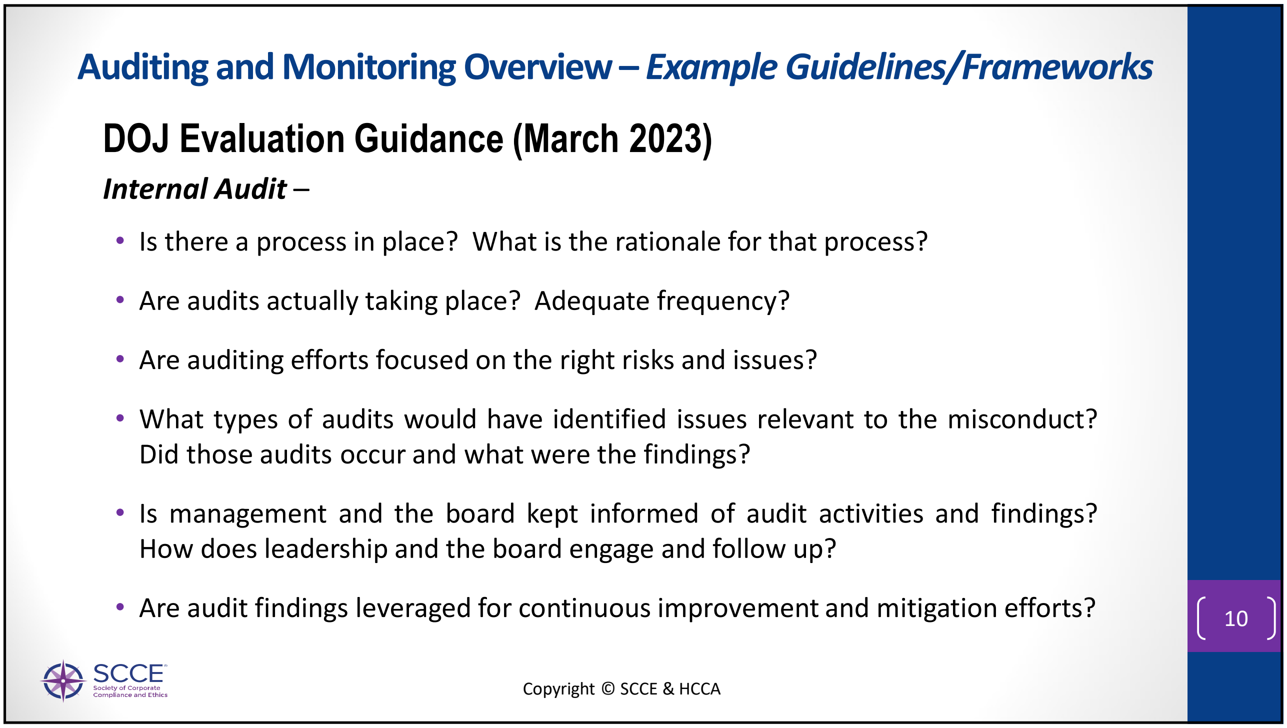
“(5) The organization shall take reasonable steps—

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

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and,

(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.”

SCCE Society of Corporate Compliance and Ethics



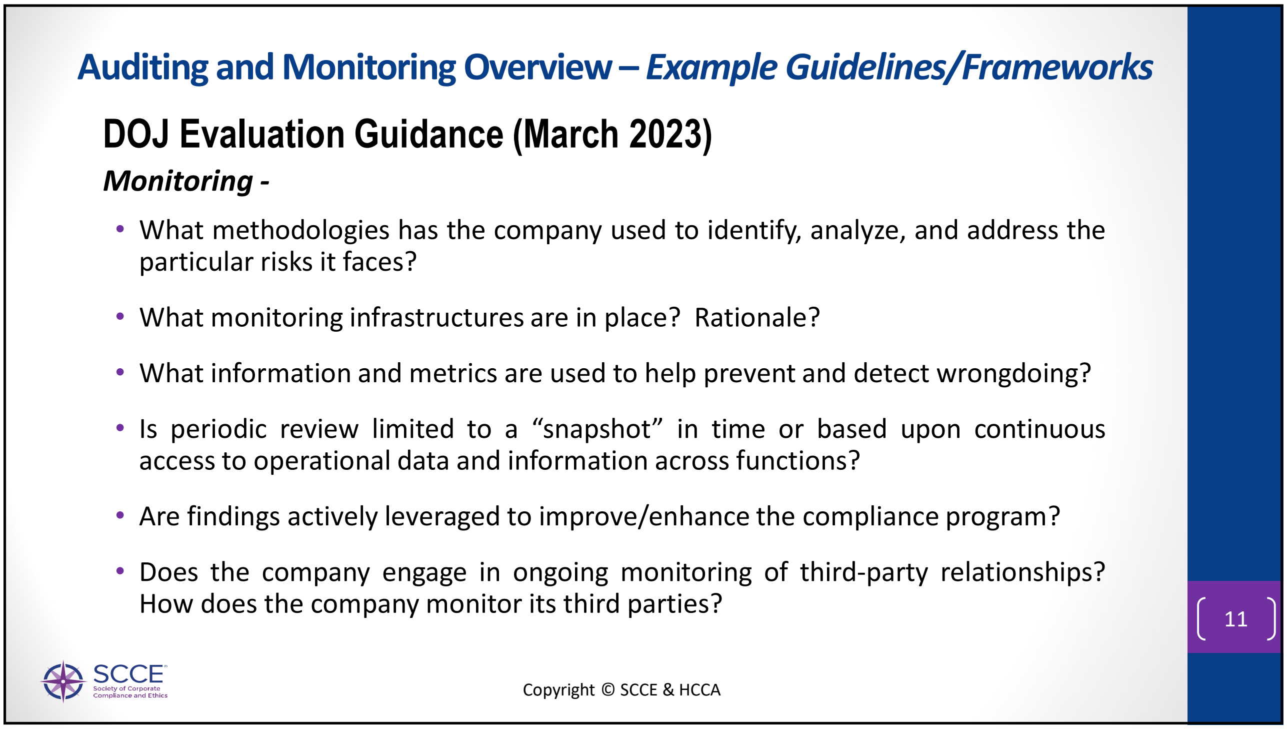
Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

DOJ Evaluation Guidance (March 2023)

Internal Audit –

- 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 the board engage and follow up?
- Are audit findings leveraged for continuous improvement and mitigation efforts?

SCCE Society of Corporate Compliance and Ethics



Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

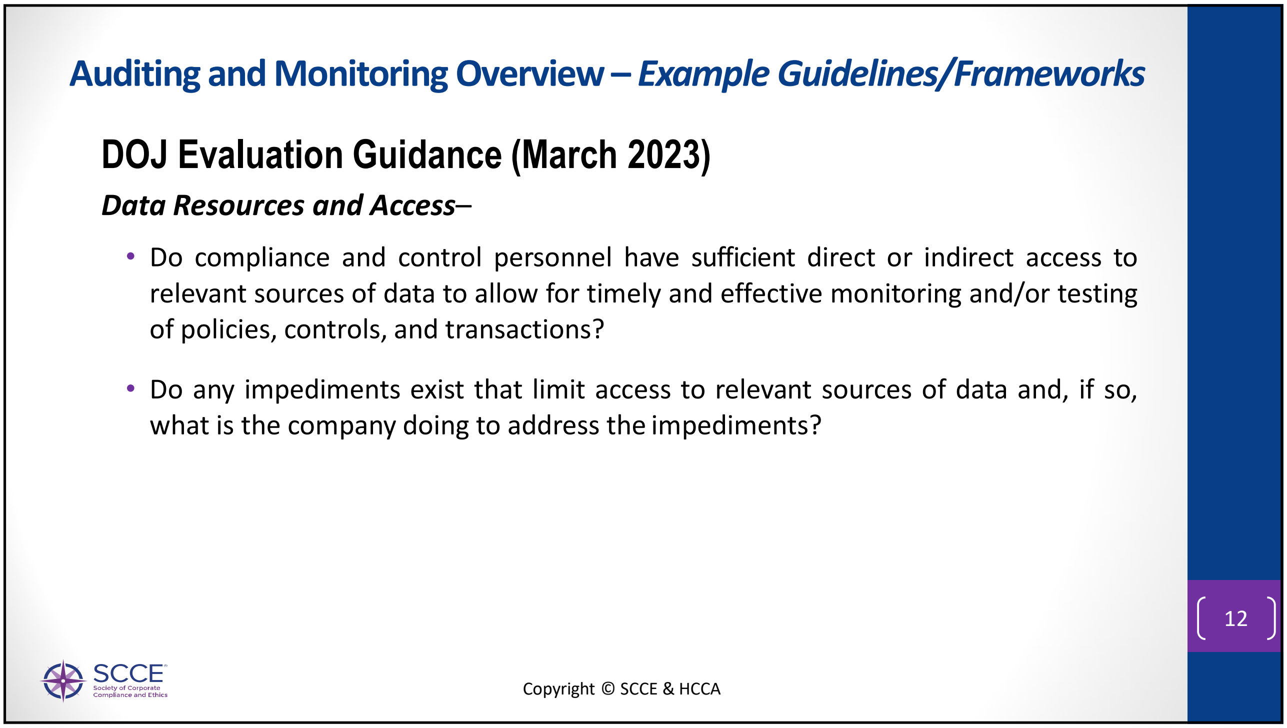
DOJ Evaluation Guidance (March 2023)

Monitoring -

- What methodologies has the company used to identify, analyze, and address the particular risks it faces?
- 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?

11

11



Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

DOJ Evaluation Guidance (March 2023)

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 access to relevant sources of data and, if so, what is the company doing to address the impediments?

12

12

Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

COSO – Internal Control

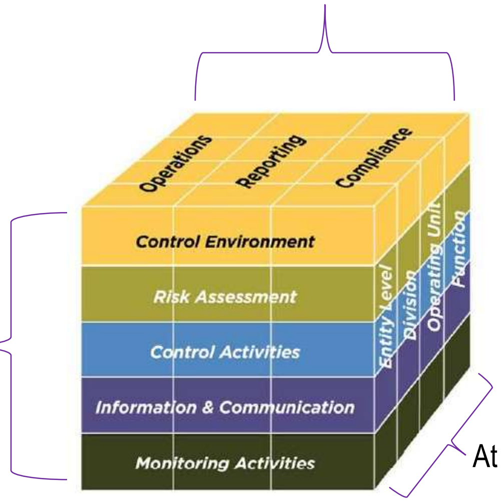
- COSO = Committee of Sponsoring Organizations of the Treadway Commission
- Published two widely-used frameworks
  - Internal Control
  - Enterprise Risk Management
- Internal Control framework defines monitoring as:
  - A process that assesses the quality of the internal control system's performance over time
- Compliance is one of three broad objectives associate with internal controls

SCCE Society of Corporate Compliance and Ethics

Example Framework – COSO Internal Control (2013)

Three Objectives

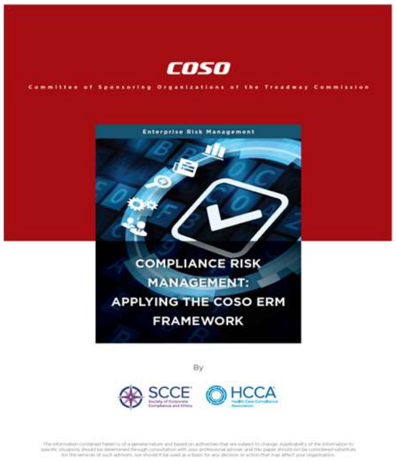
Five Components



At Various Org. Levels

SCCE Society of Corporate Compliance and Ethics

Auditing and Monitoring Overview – *Example 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

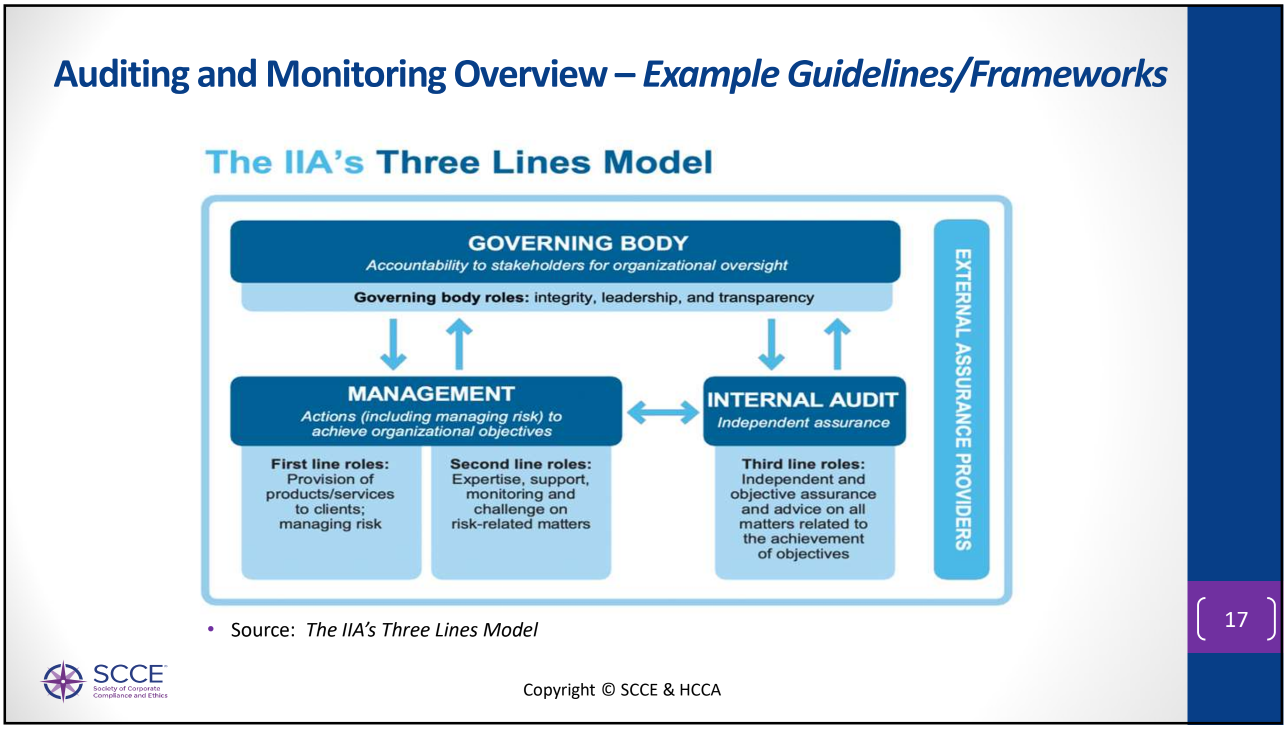
The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your professional adviser and this paper should not be considered substitute for the services 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/SitePages/Guidance.aspx

Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

Relationship to *The IIA's Three Lines Model* (2020)

- Formerly the "Three Lines of Defense" model, until 2020 revision
- Assists in identifying structures and processes that ensure the achievement of objectives and facilitate strong governance and risk management
  - Governing body
  - Management
  - Internal audit
  - External assurance
- Permits CCO (or CRO) to have a direct reporting line to the governing body (similar to Internal Audit)
- Identifies compliance-related responsibilities at:
  - Governing body
  - 1st line roles
  - 2nd line roles



Auditing and Monitoring Overview – *Example 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

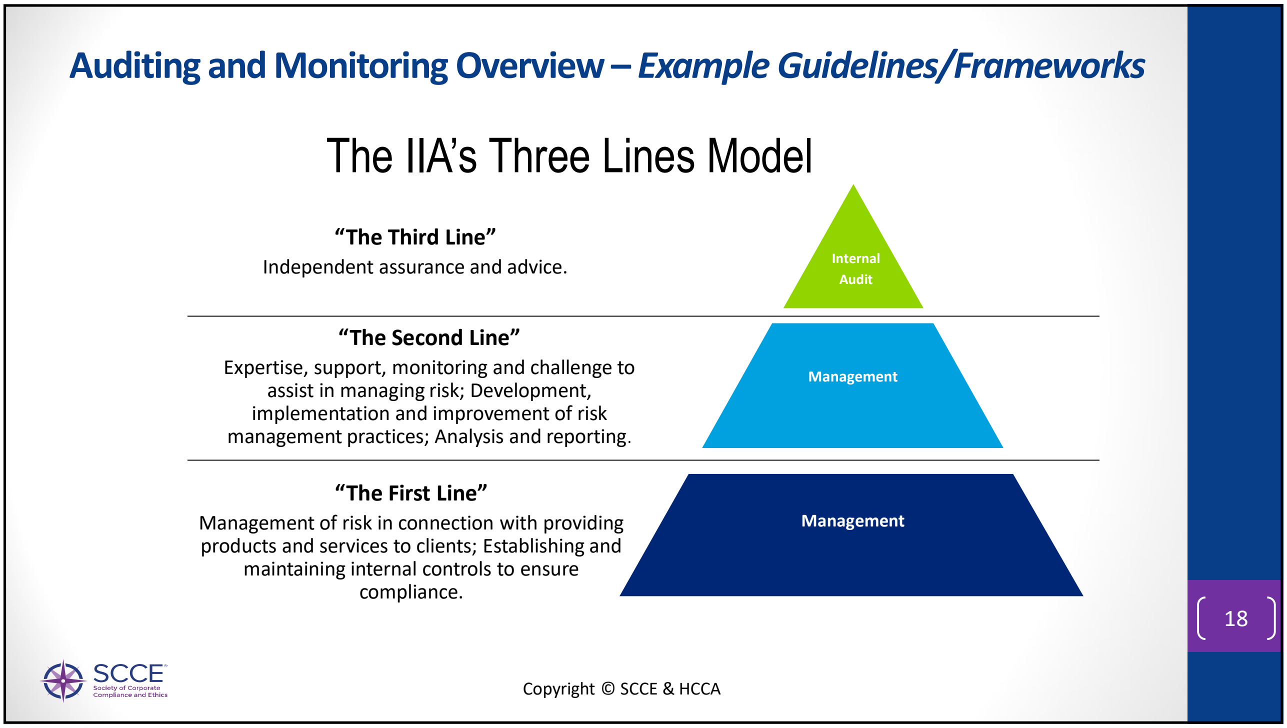
INTERNAL AUDIT

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 Lines Model*



Auditing and Monitoring Overview – *Example Guidelines/Frameworks*

The IIA's Three Lines Model

"The Third Line"

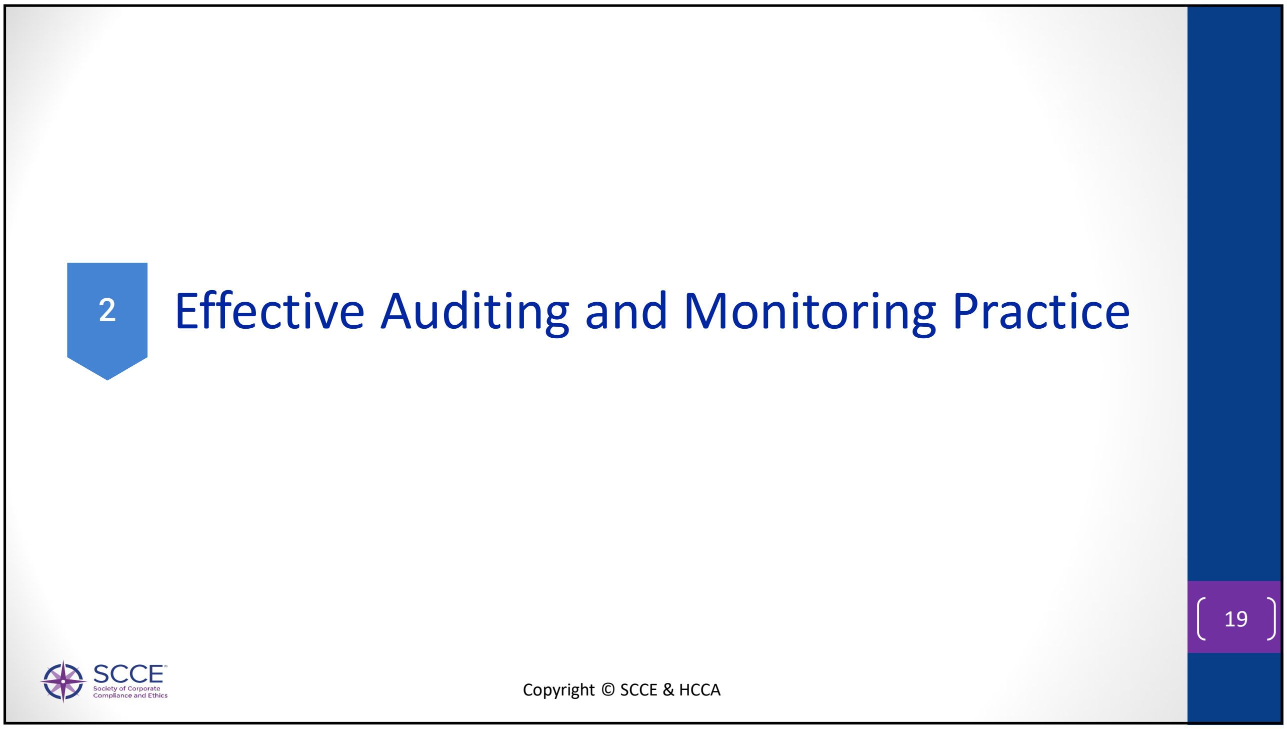
Independent assurance and advice.

"The Second Line"

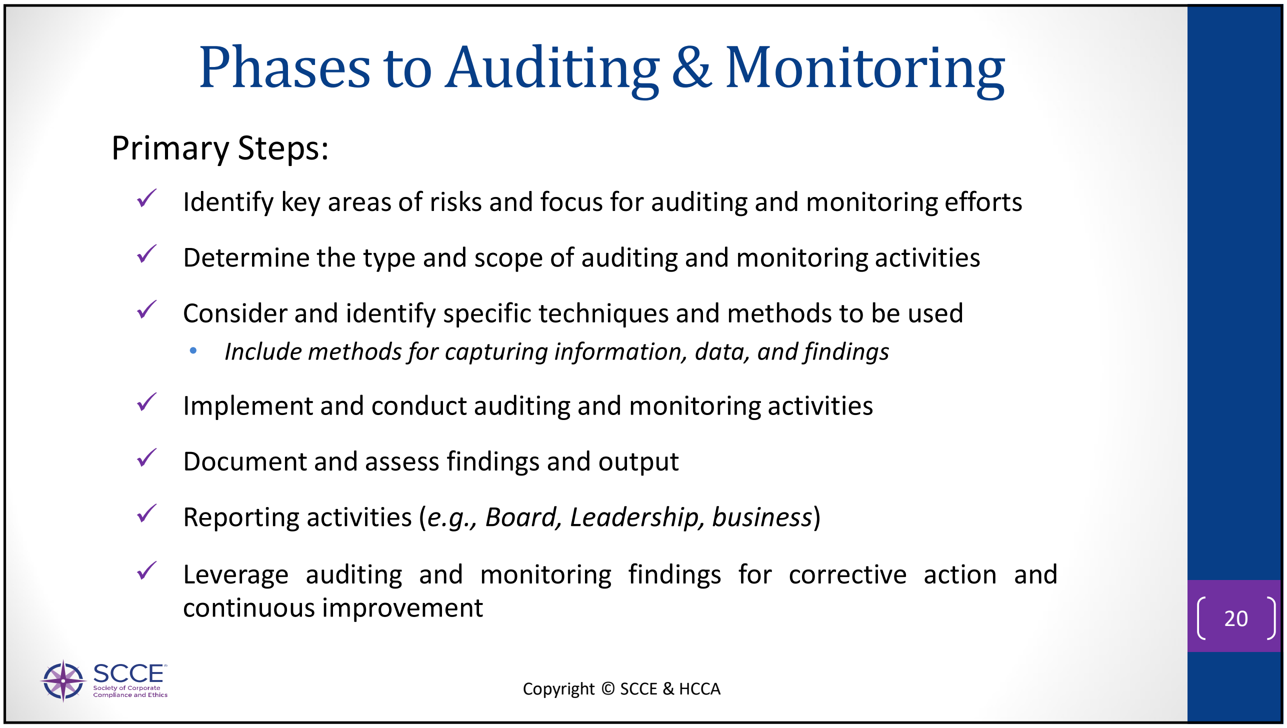
Expertise, support, monitoring and challenge to assist in managing risk; Development, implementation and improvement of risk management practices; Analysis and reporting.

"The First Line"

Management of risk in connection with providing products and services to clients; Establishing and maintaining internal controls to ensure compliance.



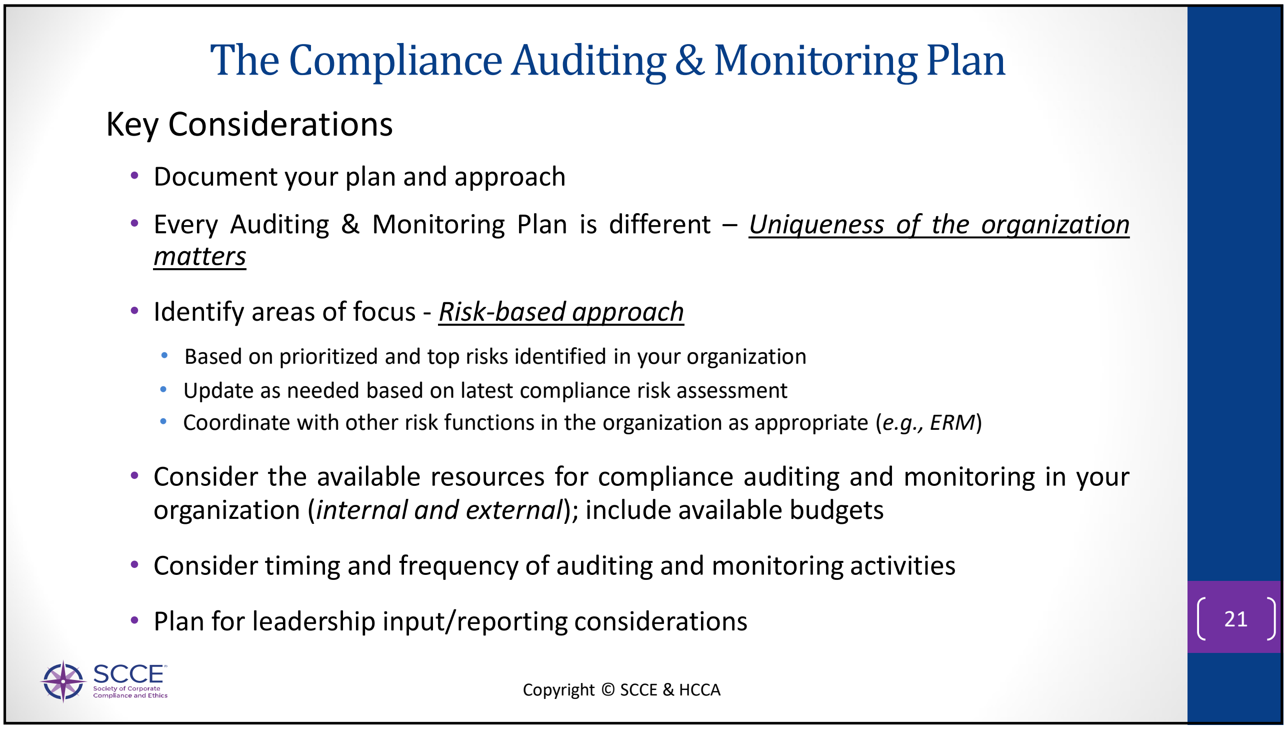
2 Effective Auditing and Monitoring Practice



Phases to Auditing & Monitoring

Primary Steps:

- ✓ Identify key areas of risks and focus for auditing and monitoring efforts
- ✓ Determine the type and scope of auditing and monitoring activities
- ✓ Consider and identify 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 and monitoring findings for corrective action and continuous improvement



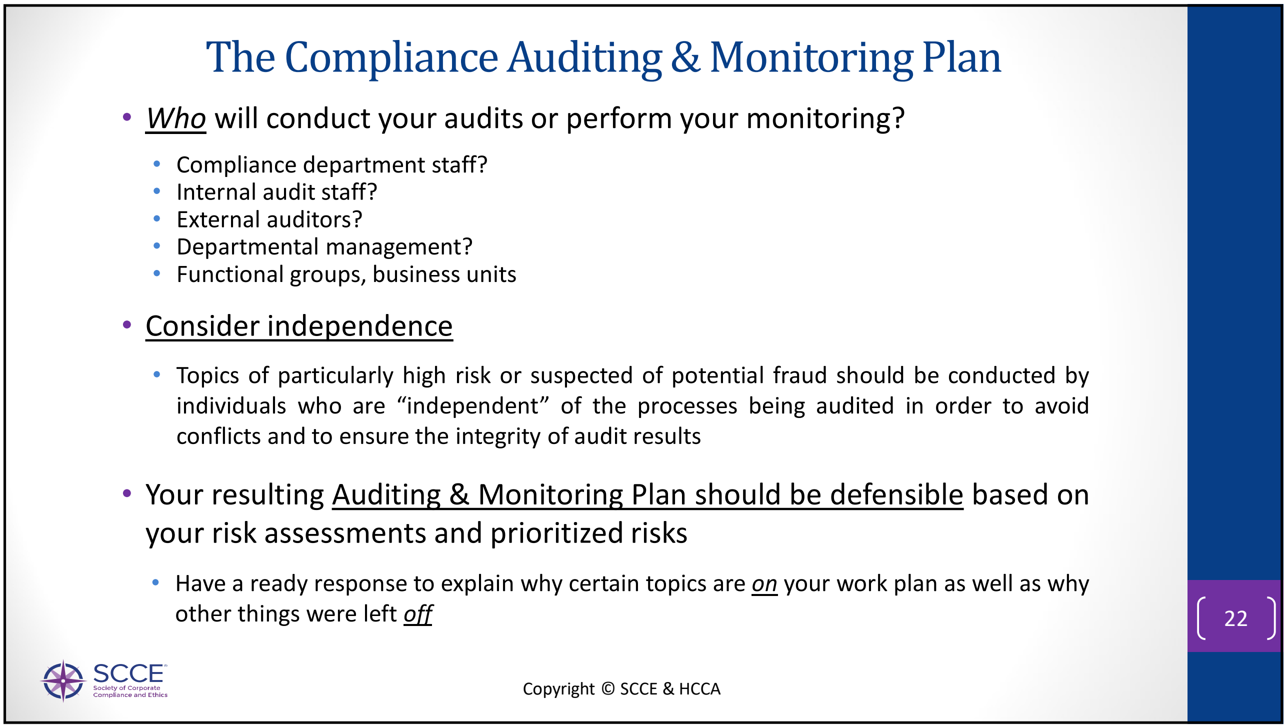
The Compliance Auditing & Monitoring Plan

Key Considerations

- Document your plan and approach
- Every Auditing & 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

21

21

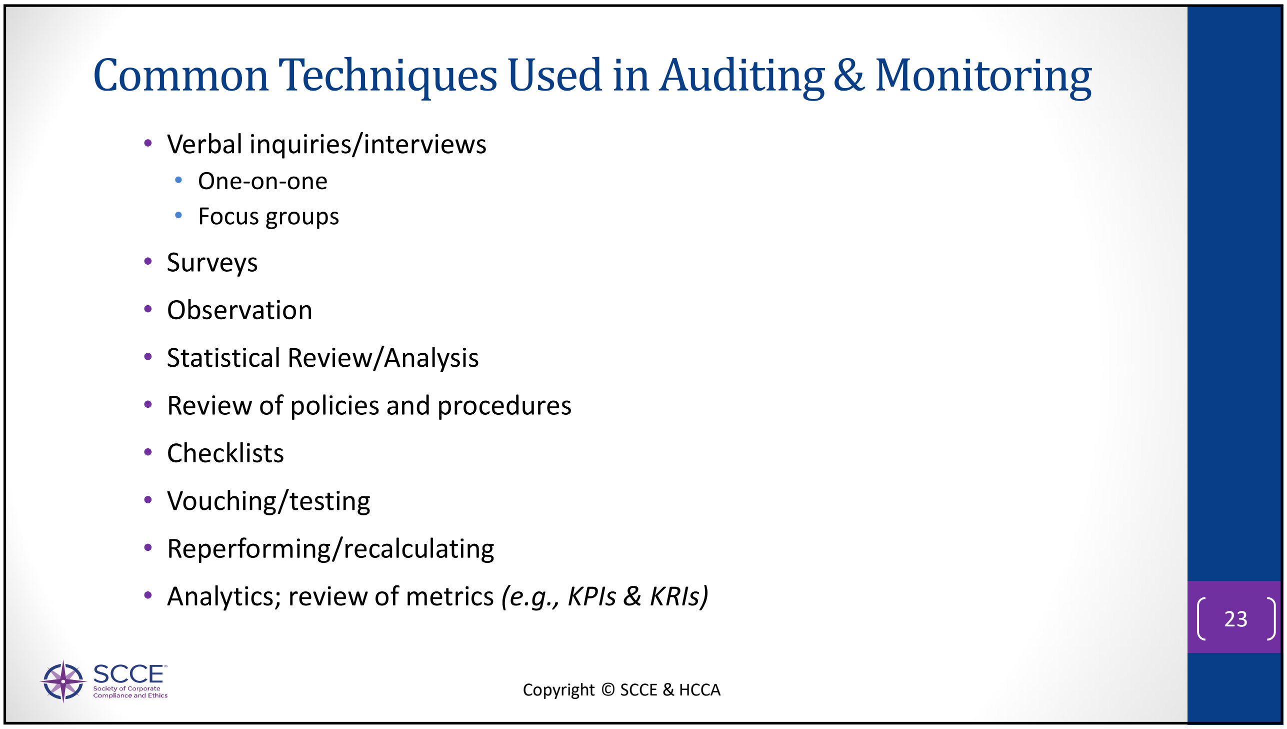


The Compliance Auditing & Monitoring Plan

- *Who* will conduct your audits or perform your monitoring?
  - Compliance department staff?
  - Internal audit staff?
  - External auditors?
  - Departmental management?
  - Functional groups, business units
- 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*

22

22

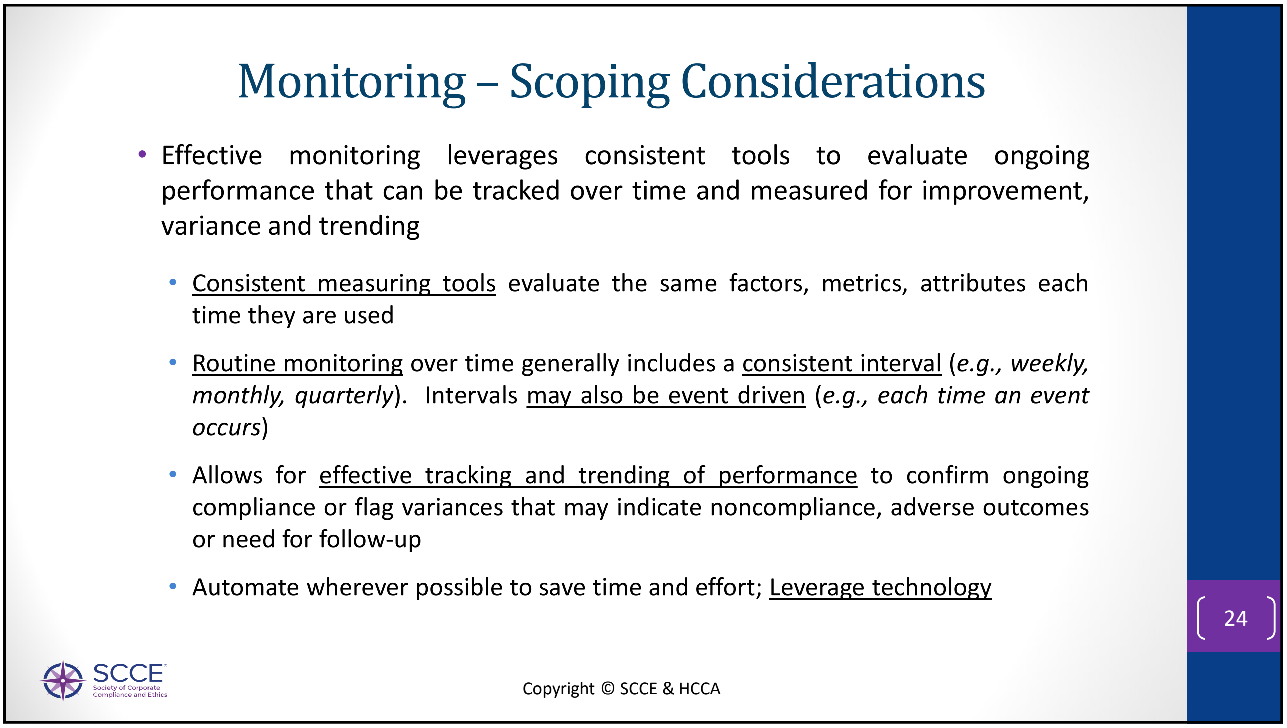


Common Techniques Used in Auditing & Monitoring

- Verbal inquiries/interviews
  - One-on-one
  - 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)*

23
SCCE
Society of Corporate Compliance and Ethics

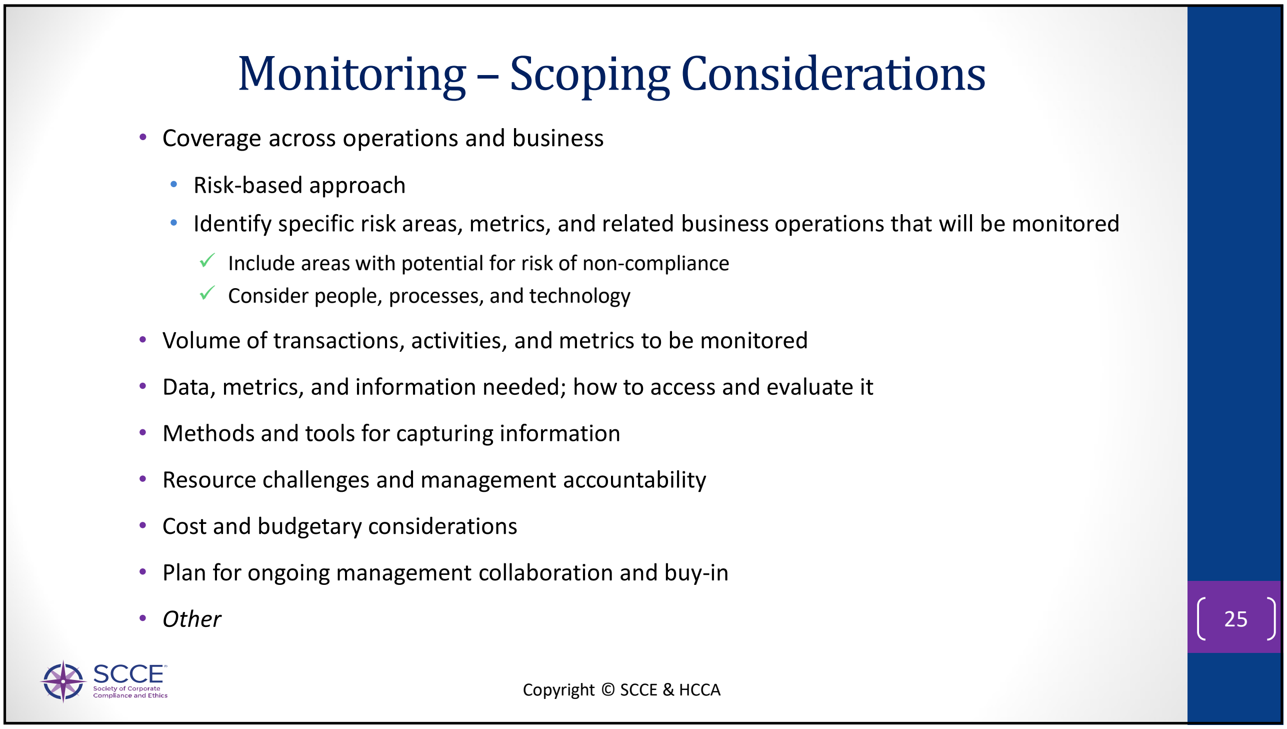
23



Monitoring – Scoping Considerations

- Effective monitoring leverages consistent tools to evaluate ongoing performance that can be tracked over time and measured for improvement, variance 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

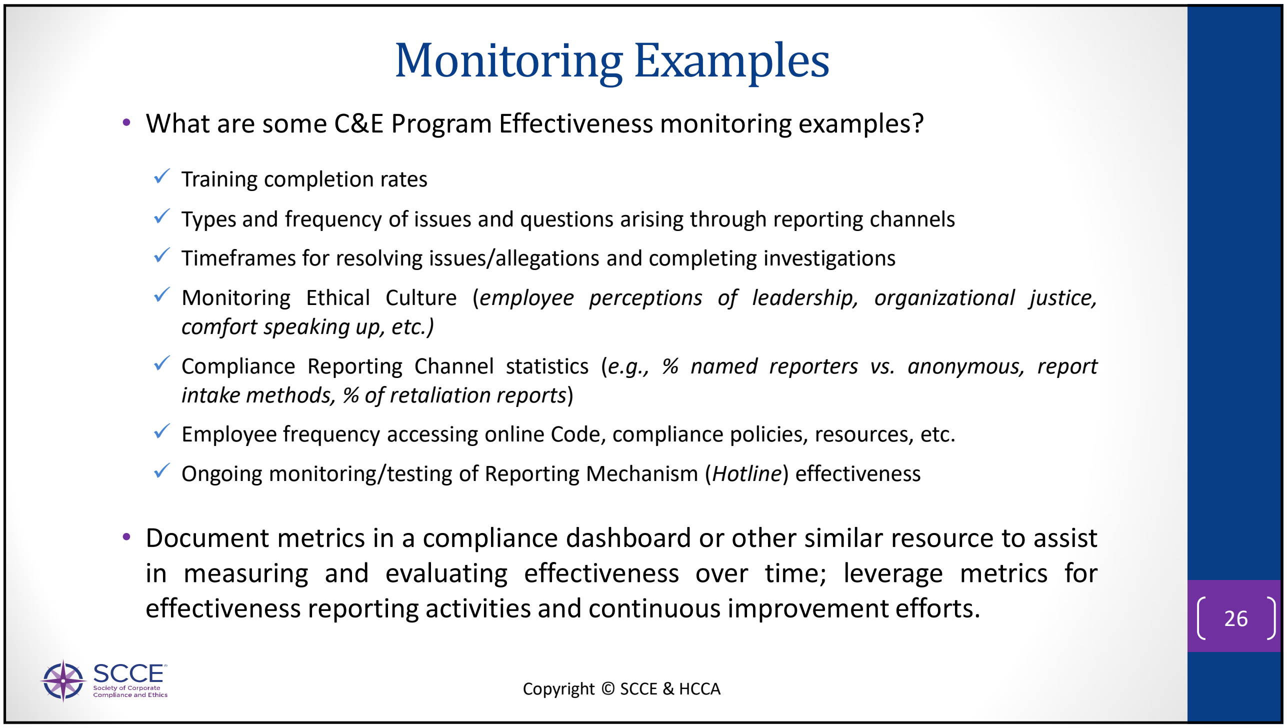
24



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
    - ✓ Consider people, processes, and technology
- Volume of transactions, activities, and metrics to be monitored
- 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 and buy-in
- *Other*

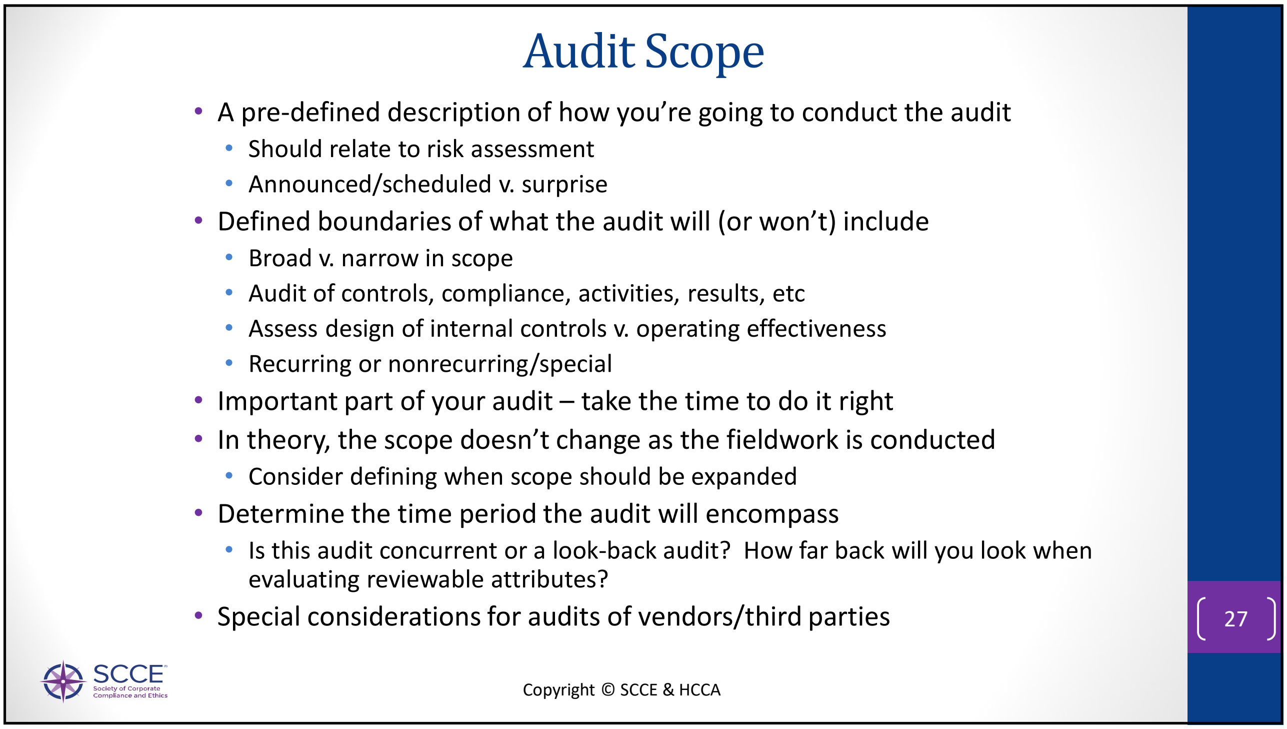
25



Monitoring Examples

- What are some C&E Program Effectiveness monitoring examples?
  - ✓ 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.

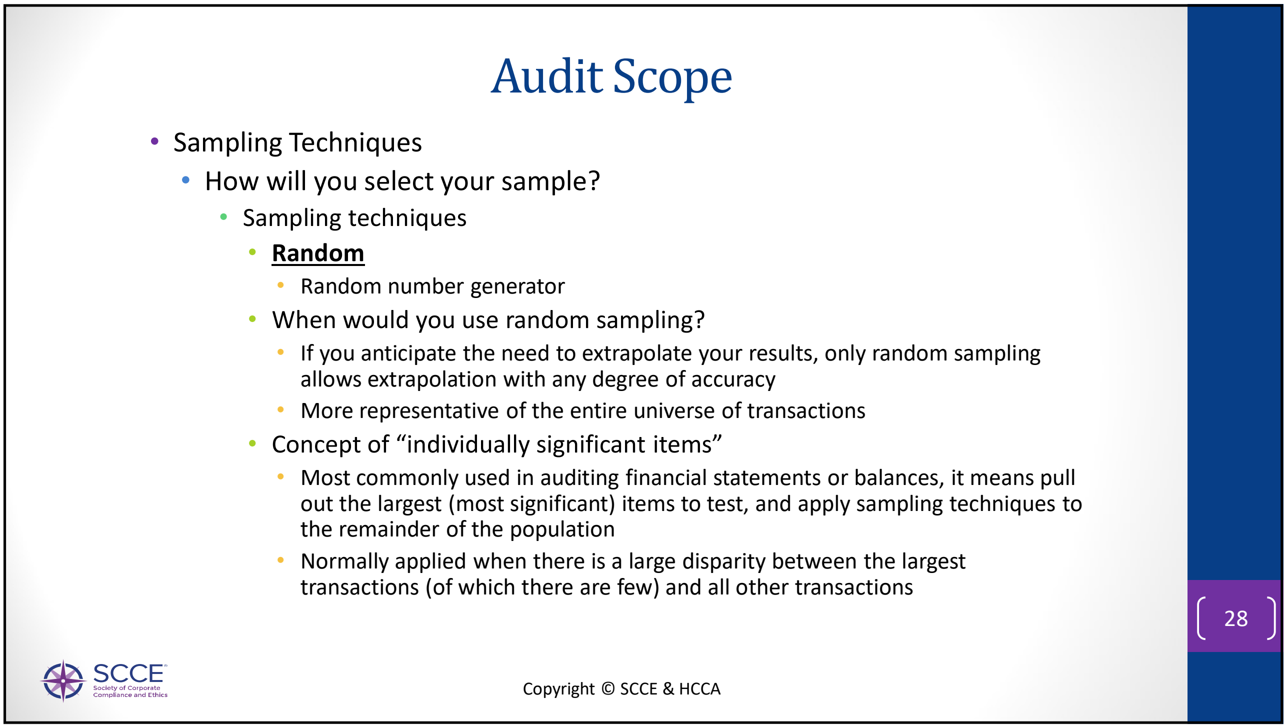
26



Audit Scope

- A pre-defined description of how you're going to conduct the audit
  - Should relate to risk assessment
  - Announced/scheduled v. surprise
- Defined boundaries of what the audit will (or won't) include
  - Broad v. narrow in scope
  - Audit of controls, compliance, activities, results, etc
  - Assess design of internal controls v. operating effectiveness
  - Recurring or nonrecurring/special
- Important part of your audit – take the time to do it right
- In theory, the scope doesn't change as the fieldwork is conducted
  - Consider defining when scope should be expanded
- Determine the time period the audit will encompass
  - Is this audit concurrent or a look-back audit? How far back will you look when evaluating reviewable attributes?
- Special considerations for audits of vendors/third parties

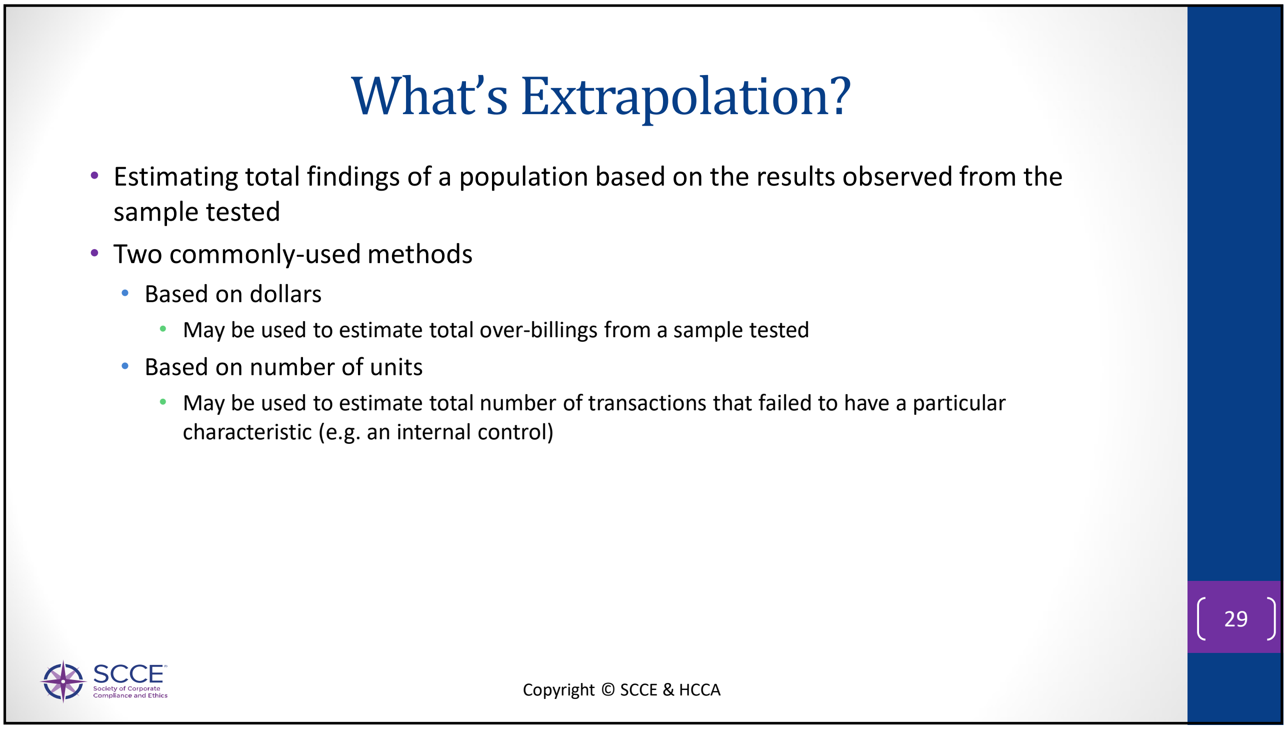
27



Audit Scope

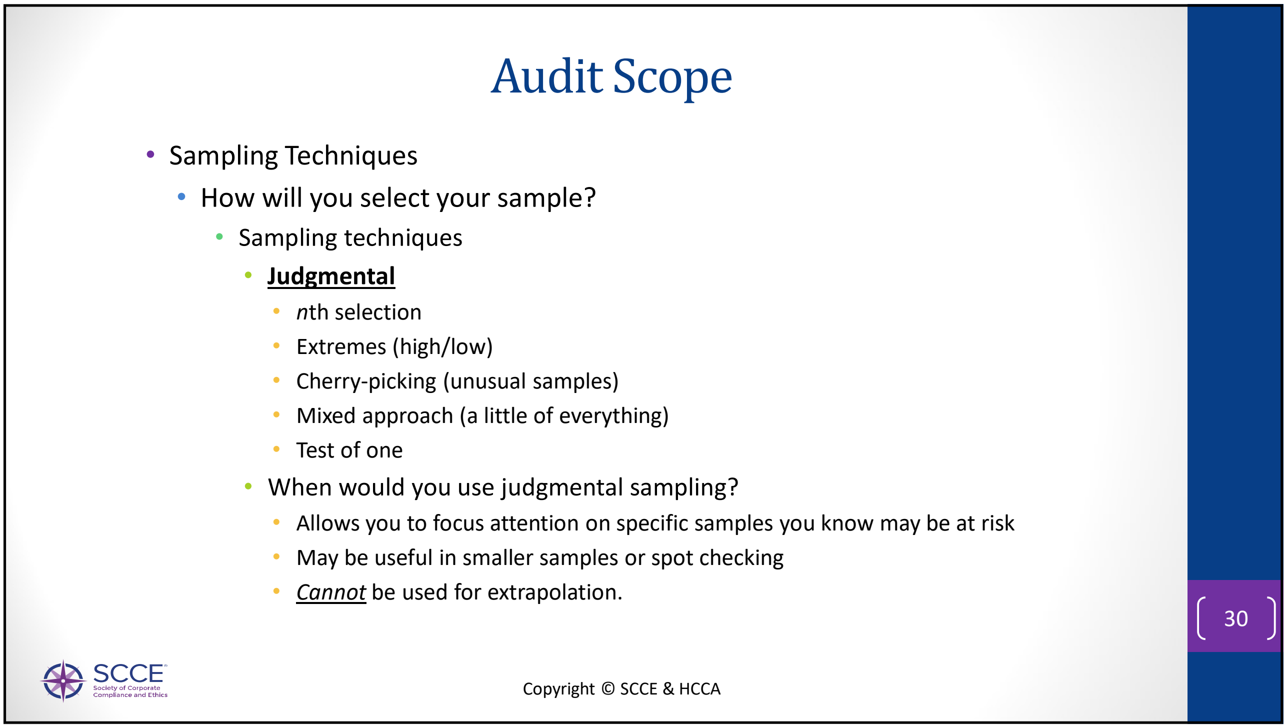
- Sampling Techniques
  - How will you select your sample?
    - Sampling techniques
      - **<u>Random</u>**
        - Random number generator
      - When would you use random sampling?
        - If you anticipate the need to extrapolate your results, only random sampling allows extrapolation with any degree of accuracy
        - More representative of the entire universe of transactions
      - Concept of "individually significant items"
        - Most commonly used in auditing financial statements or balances, it means pull out the largest (most significant) items to test, and apply sampling techniques to the remainder of the population
        - Normally applied when there is a large disparity between the largest transactions (of which there are few) and all other transactions

28



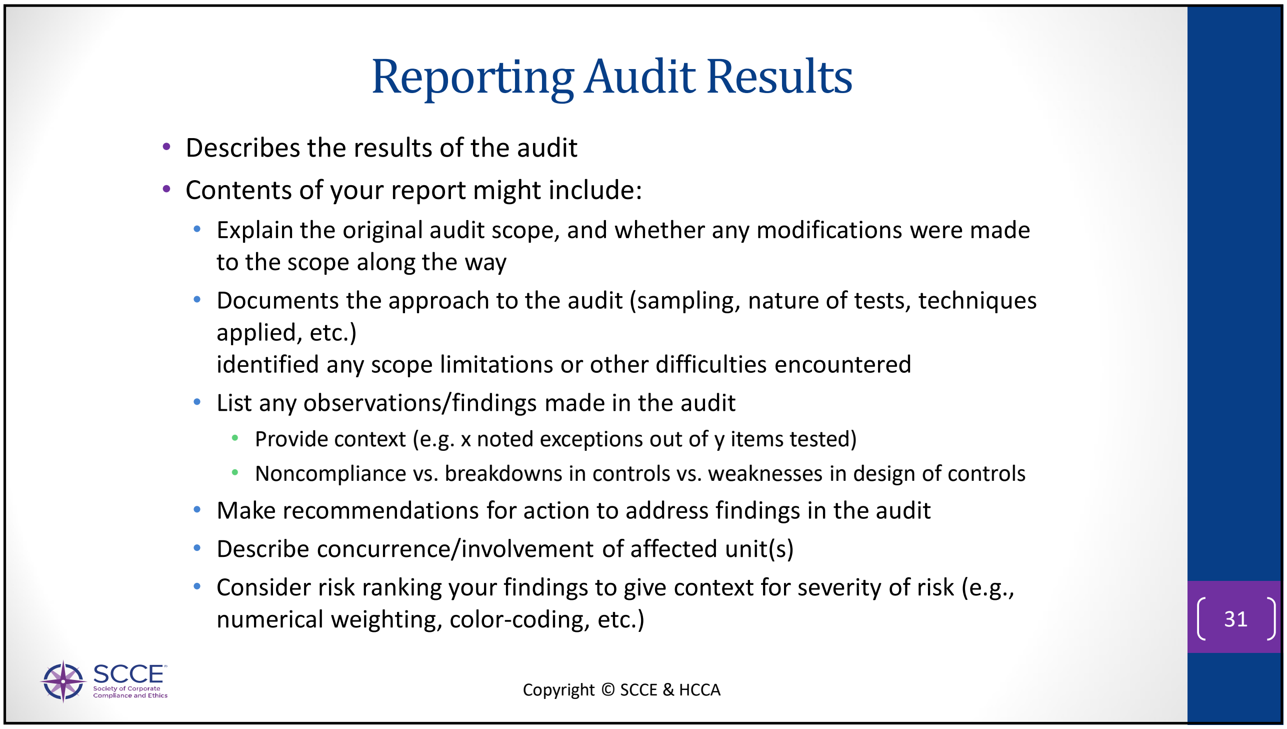
What’s Extrapolation?

- Estimating total findings of a population based on the results observed from the sample tested
- Two commonly-used methods
  - Based on dollars
    - May be used to estimate total over-billings from a sample tested
  - Based on number of units
    - May be used to estimate total number of transactions that failed to have a particular characteristic (e.g. an internal control)



Audit Scope

- Sampling Techniques
  - How will you select your sample?
    - Sampling techniques
      - **<u>Judgmental</u>**
        - *n*th selection
        - Extremes (high/low)
        - Cherry-picking (unusual samples)
        - Mixed approach (a little of everything)
        - Test of one
      - When would you use judgmental sampling?
        - Allows you to focus attention on specific samples you know may be at risk
        - May be useful in smaller samples or spot checking
        - *Cannot* be used for extrapolation.



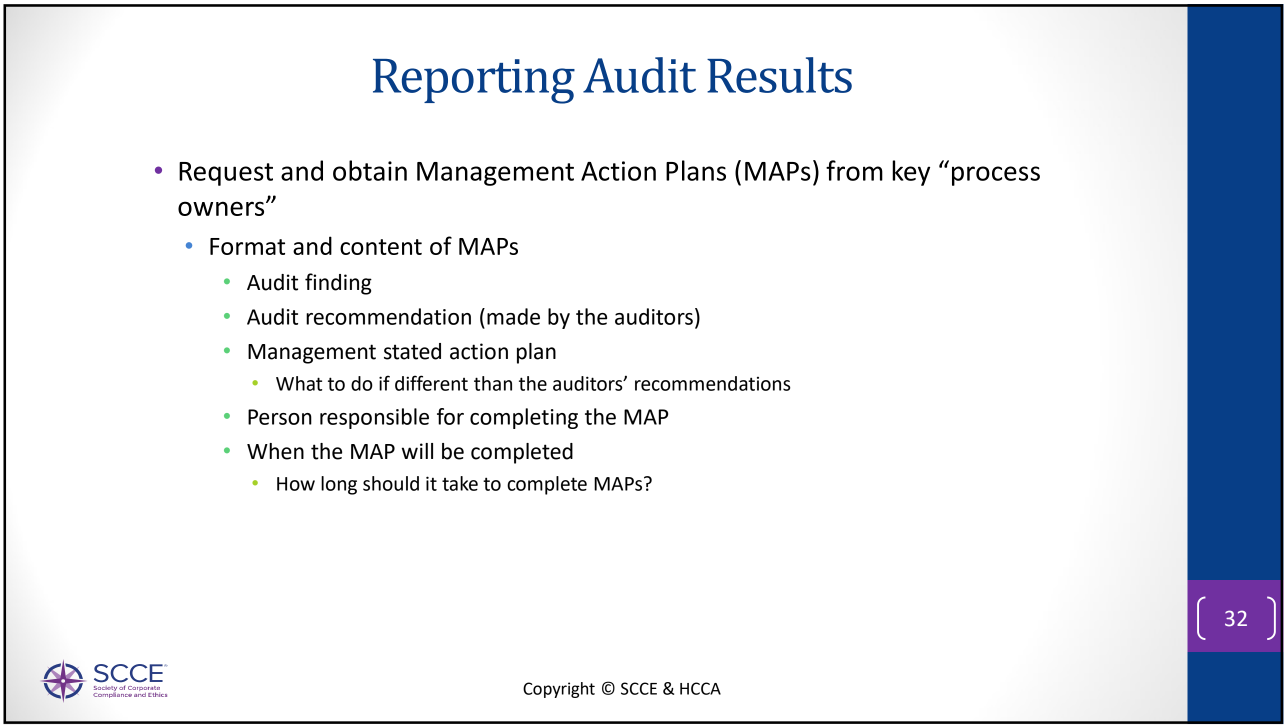
Reporting Audit Results

- Describes the results of the audit
- Contents of your report might include:
  - Explain the original audit scope, and whether any modifications were made to the scope along the way
  - Documents the approach to the audit (sampling, nature of tests, techniques applied, etc.)
    identified any scope limitations or other difficulties encountered
  - List any observations/findings made in the audit
    - Provide context (e.g. x noted exceptions out of y items tested)
    - Noncompliance vs. breakdowns in controls vs. weaknesses in design of controls
  - Make recommendations for action to address findings in the audit
  - Describe concurrence/involvement of affected unit(s)
  - Consider risk ranking your findings to give context for severity of risk (e.g., numerical weighting, color-coding, etc.)

31

SCCE Society of Corporate Compliance and Ethics

31



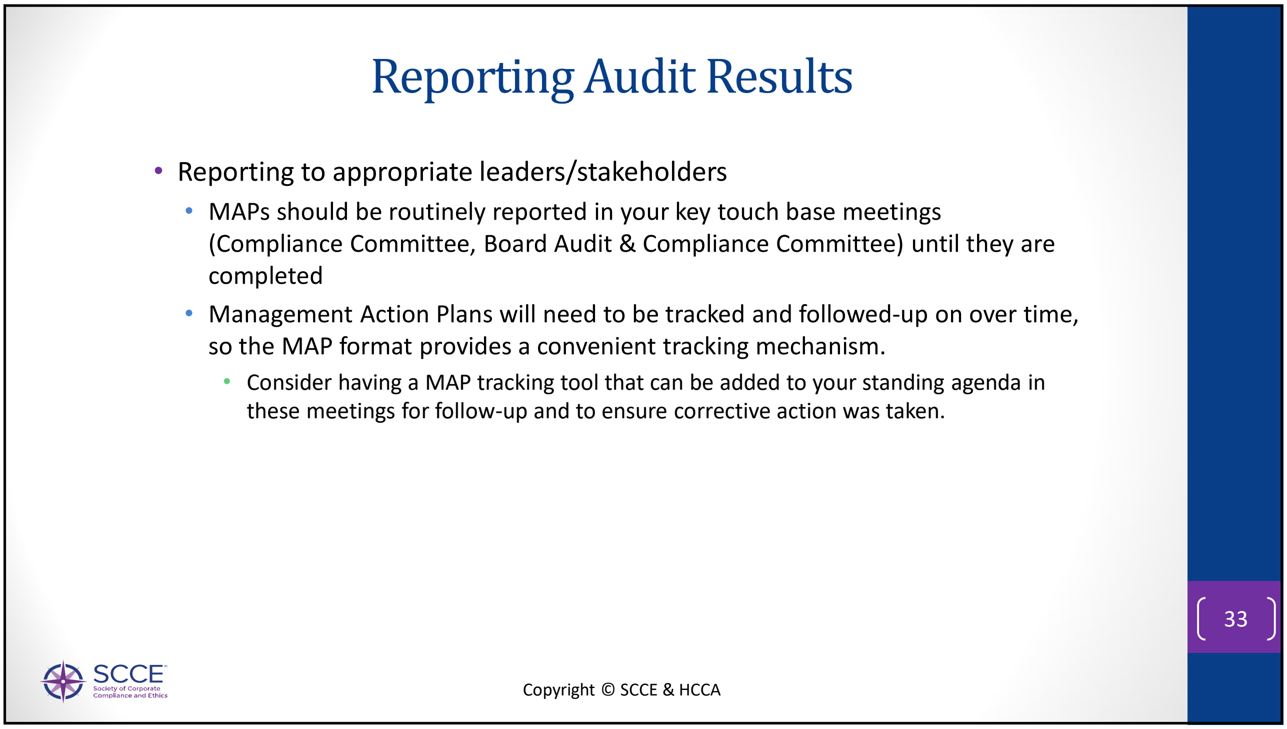
Reporting Audit Results

- Request and obtain Management Action Plans (MAPs) from key “process owners”
  - Format and content of MAPs
    - Audit finding
    - Audit recommendation (made by the auditors)
    - Management stated action plan
      - What to do if different than the auditors’ recommendations
    - Person responsible for completing the MAP
    - When the MAP will be completed
      - How long should it take to complete MAPs?

32

SCCE Society of Corporate Compliance and Ethics

32

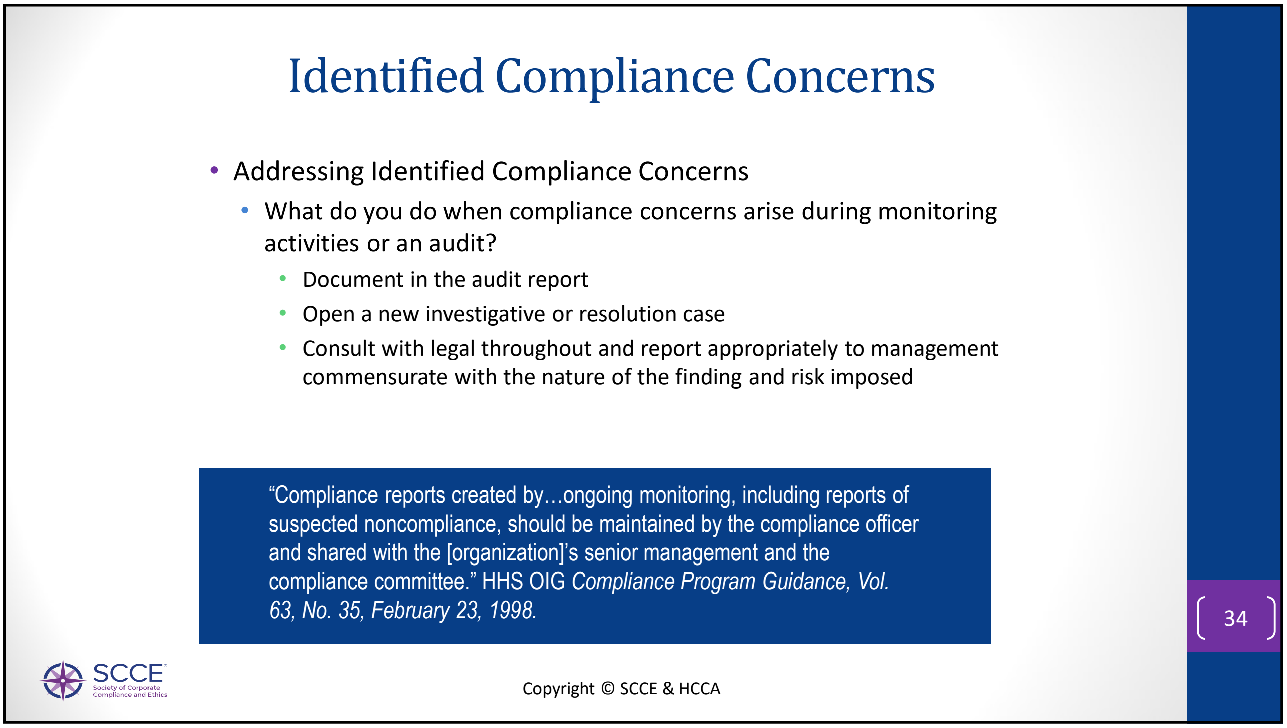


Reporting Audit Results

- Reporting to appropriate leaders/stakeholders
  - MAPs should be routinely reported in your key touch base meetings (Compliance Committee, Board Audit & Compliance Committee) until they are completed
  - Management Action Plans will need to be tracked and followed-up on over time, so the MAP format provides a convenient tracking mechanism.
    - Consider having a MAP tracking tool that can be added to your standing agenda in these meetings for follow-up and to ensure corrective action was taken.

SCCE Society of Corporate Compliance and Ethics

33



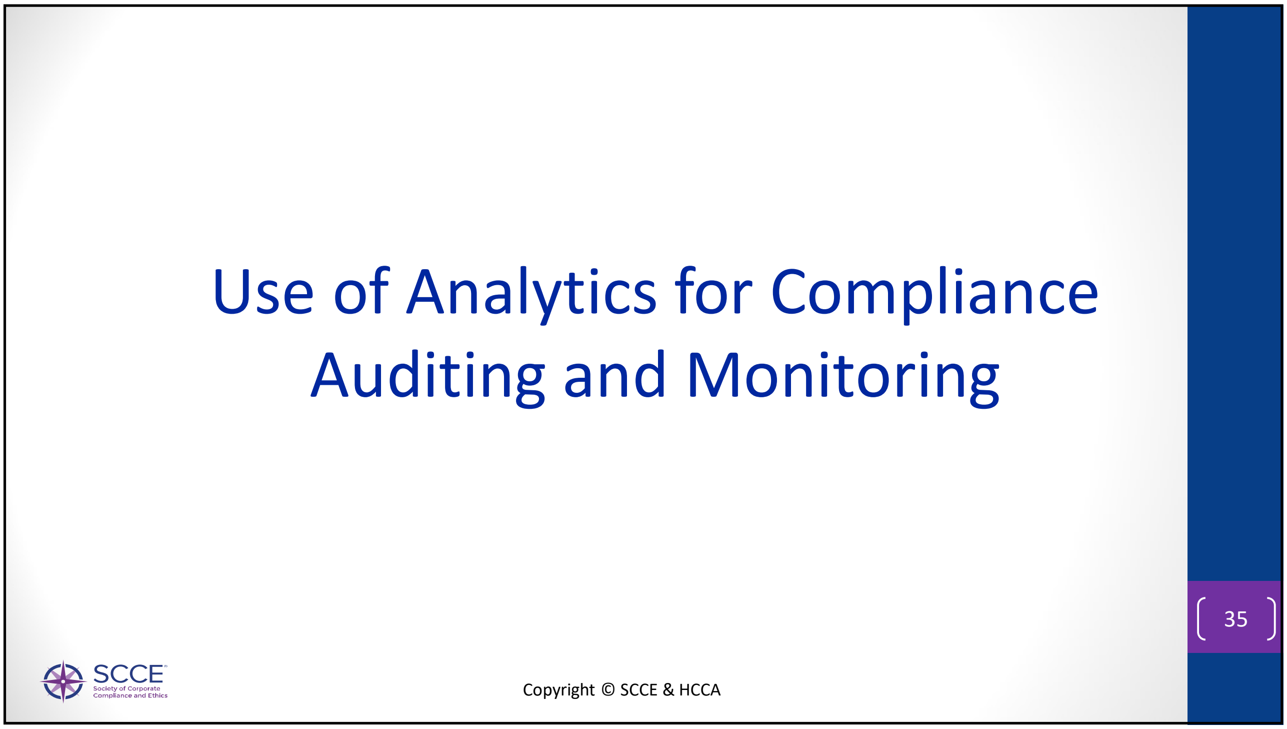
Identified Compliance Concerns

- Addressing Identified Compliance Concerns
  - What do you do when compliance concerns arise during monitoring activities or an audit?
    - Document in the audit report
    - Open a new investigative or resolution case
    - Consult with legal throughout and report appropriately to management commensurate with the nature of the finding and risk imposed

> "Compliance reports created by…ongoing monitoring, including reports of suspected noncompliance, should be maintained by the compliance officer and shared with the [organization]'s senior management and the compliance committee." HHS OIG *Compliance Program Guidance, Vol. 63, No. 35, February 23, 1998.*

SCCE Society of Corporate Compliance and Ethics

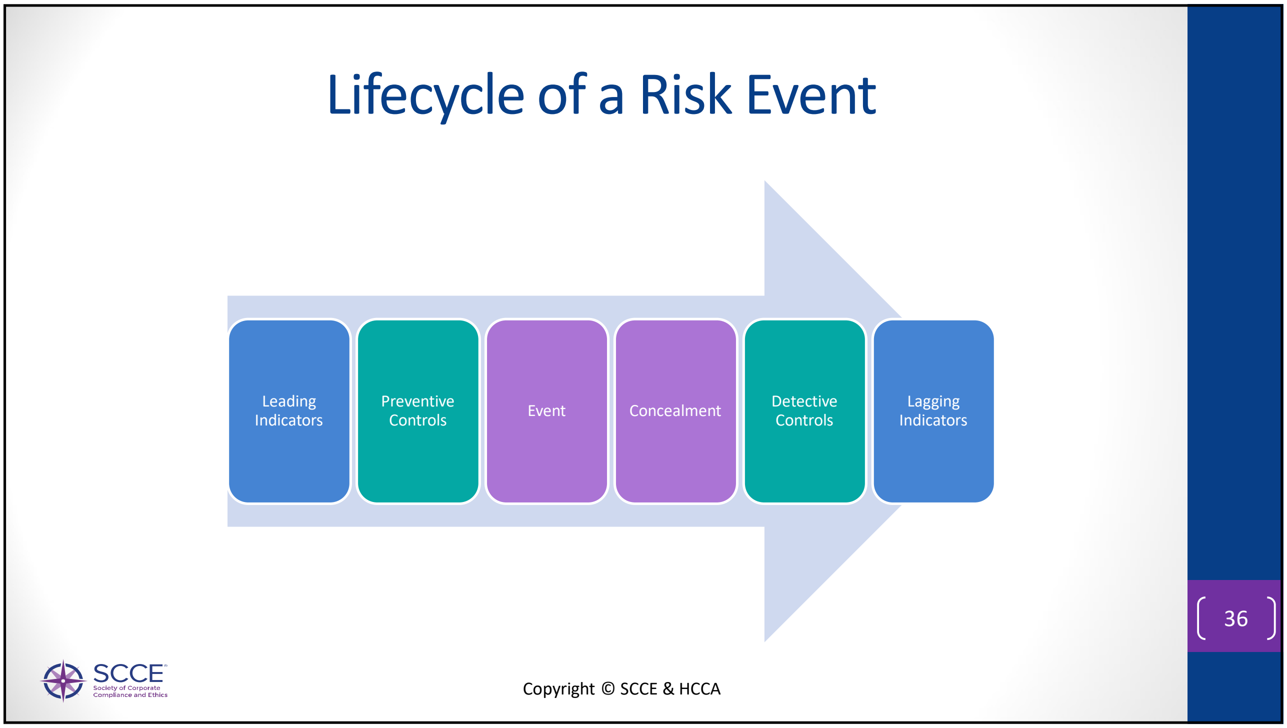
34



Use of Analytics for Compliance Auditing and Monitoring

35

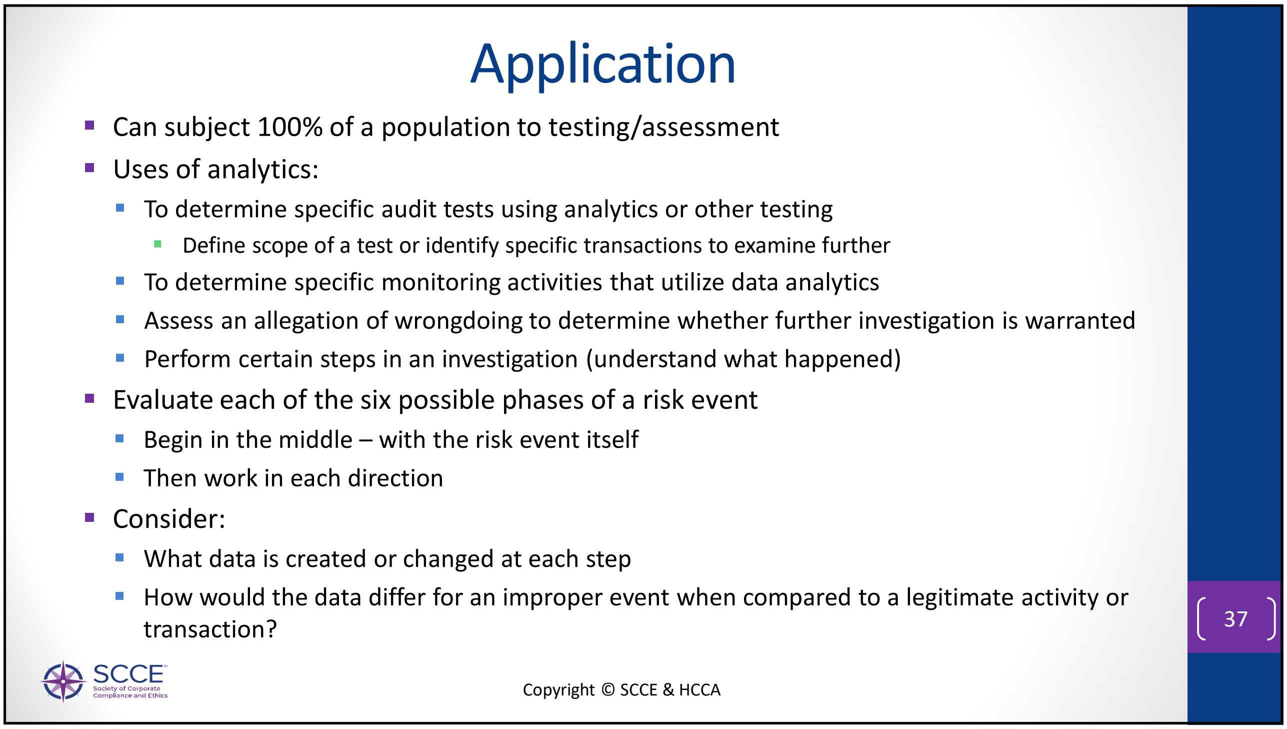
35



Lifecycle of a Risk Event

36

36



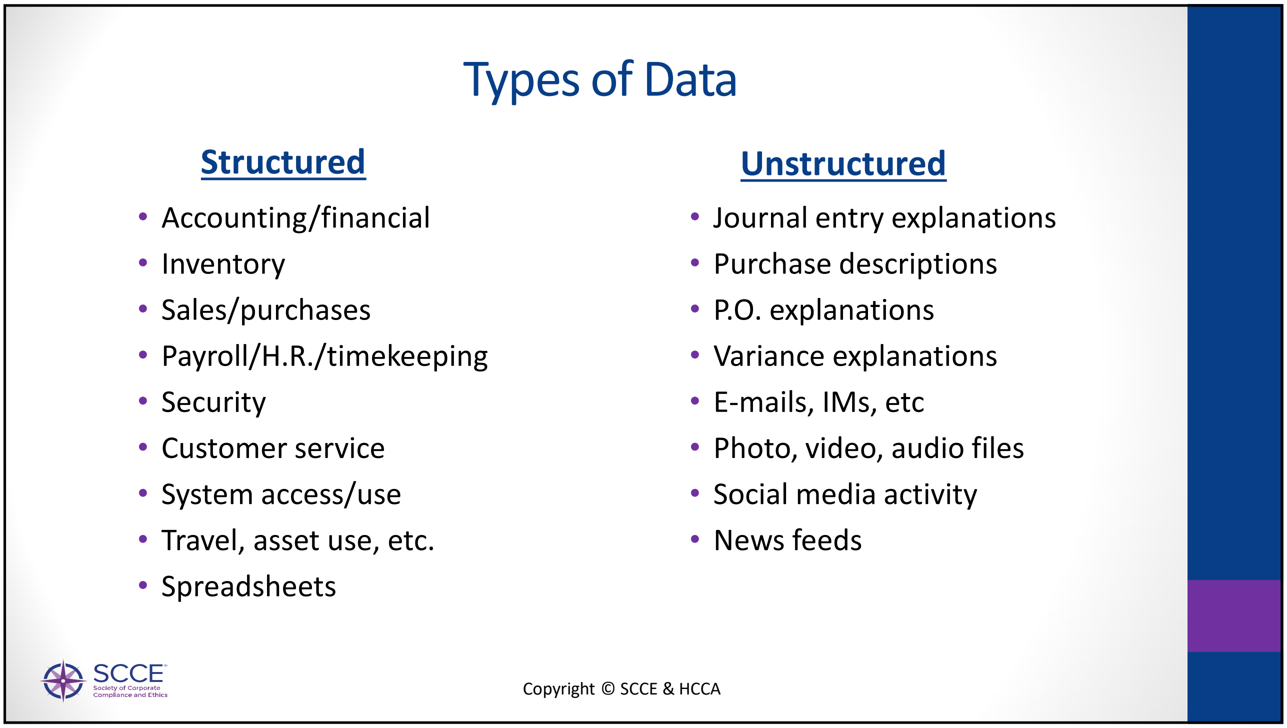
Application

- Can subject 100% of a population to testing/assessment
- Uses of analytics:
  - To determine specific audit tests using analytics or other testing
    - Define scope of a test or identify specific transactions to examine further
  - To determine specific monitoring activities that utilize data analytics
  - Assess an allegation of wrongdoing to determine whether further investigation is warranted
  - Perform certain steps in an investigation (understand what happened)
- 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
- Consider:
  - What data is created or changed at each step
  - How would the data differ for an improper event when compared to a legitimate activity or transaction?

37

SCCE Society of Corporate Compliance and Ethics

37



Types of Data

Structured

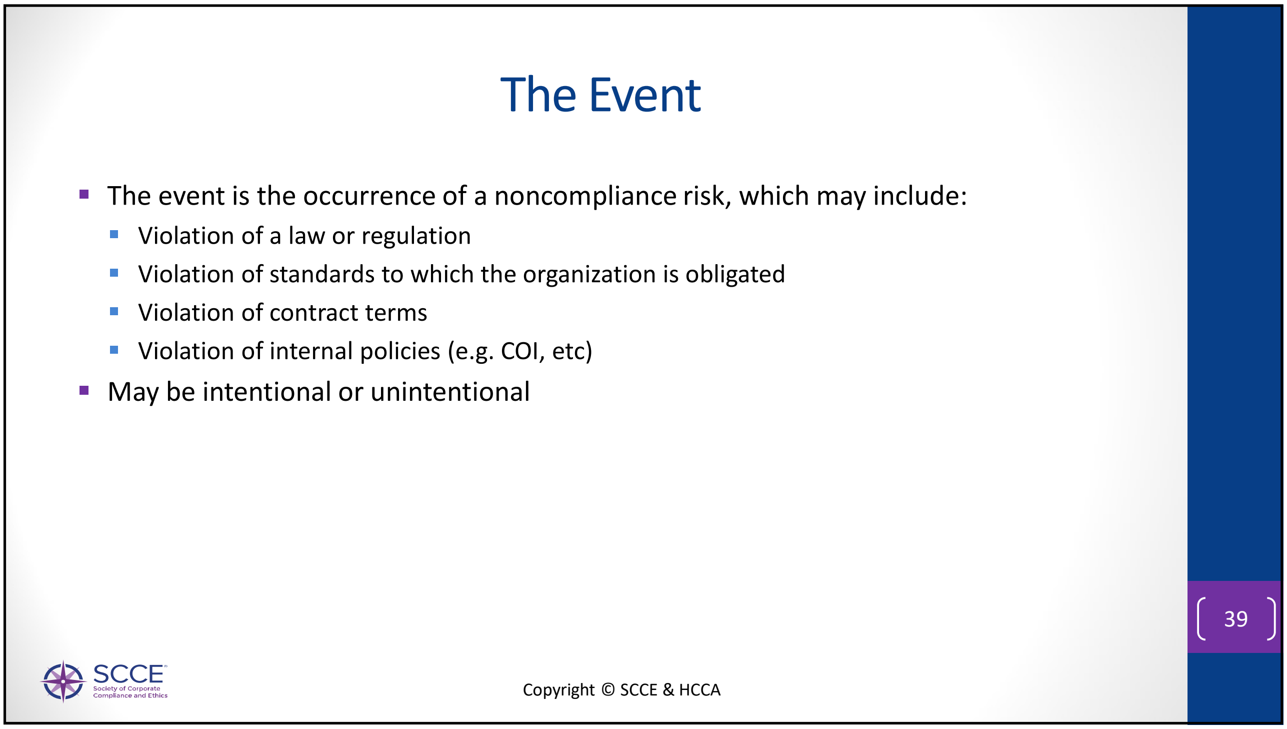
- Accounting/financial
- Inventory
- Sales/purchases
- Payroll/H.R./timekeeping
- Security
- Customer service
- System access/use
- Travel, asset use, etc.
- Spreadsheets

Unstructured

- Journal entry explanations
- Purchase descriptions
- P.O. explanations
- Variance explanations
- E-mails, IMs, etc
- Photo, video, audio files
- Social media activity
- News feeds

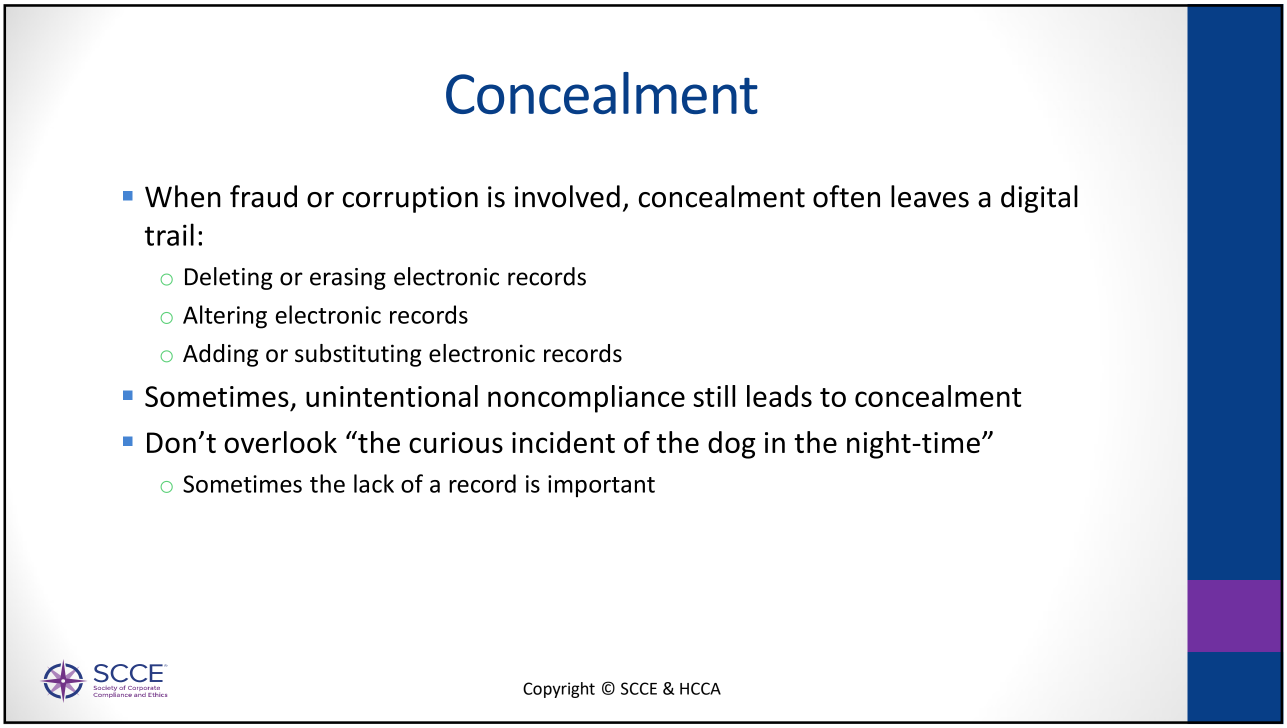
SCCE Society of Corporate Compliance and Ethics

38



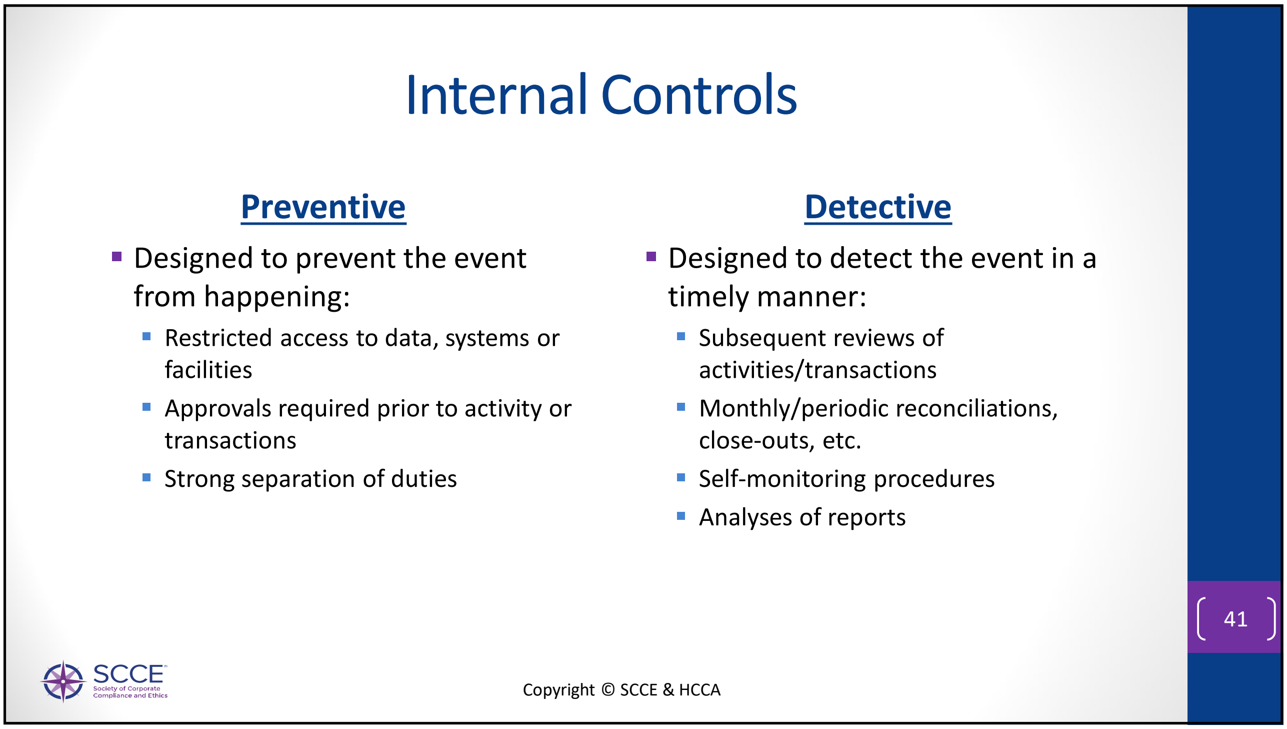
The Event

- The event is the occurrence of a noncompliance risk, which may include:
  - Violation of a law or regulation
  - Violation of standards to which the organization is obligated
  - Violation of contract terms
  - Violation of internal policies (e.g. COI, etc)
- May be intentional or unintentional



Concealment

- When fraud or corruption is involved, concealment often leaves a digital trail:
  - ○ Deleting or erasing electronic records
  - ○ Altering electronic records
  - ○ Adding or substituting electronic records
- Sometimes, unintentional noncompliance still leads to concealment
- Don’t overlook “the curious incident of the dog in the night-time”
  - ○ Sometimes the lack of a record is important



Internal Controls

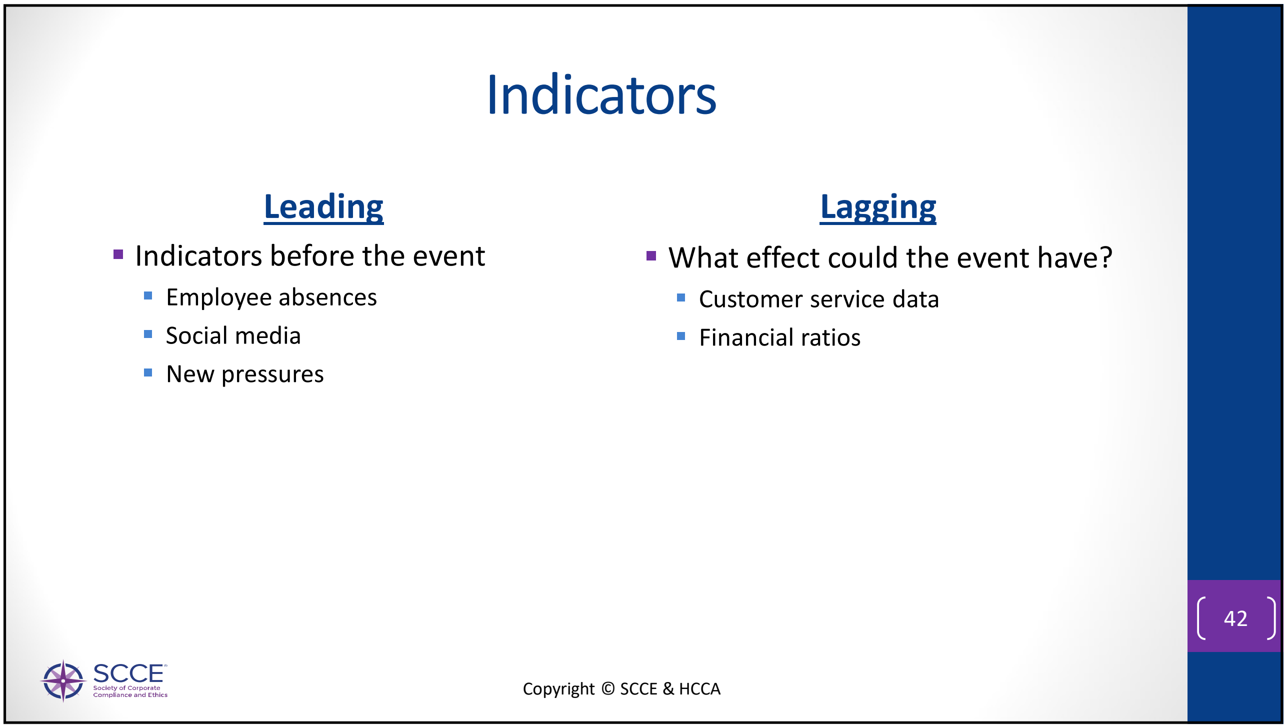
Preventive

- Designed to prevent the event from happening:
  - Restricted access to data, systems or facilities
  - Approvals required prior to activity or transactions
  - Strong separation of duties

Detective

- Designed to detect the event in a timely manner:
  - Subsequent reviews of activities/transactions
  - Monthly/periodic reconciliations, close-outs, etc.
  - Self-monitoring procedures
  - Analyses of reports

41



Indicators

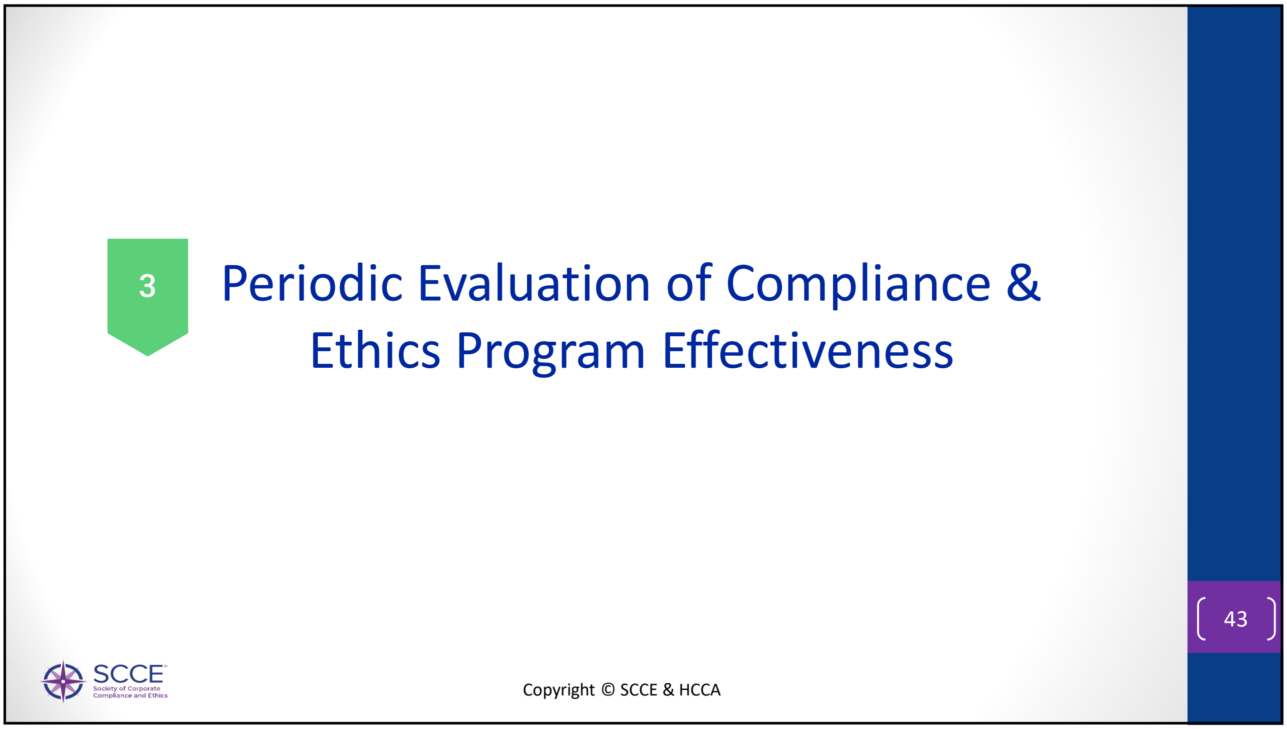
Leading

- Indicators before the event
  - Employee absences
  - Social media
  - New pressures

Lagging

- What effect could the event have?
  - Customer service data
  - Financial ratios

42

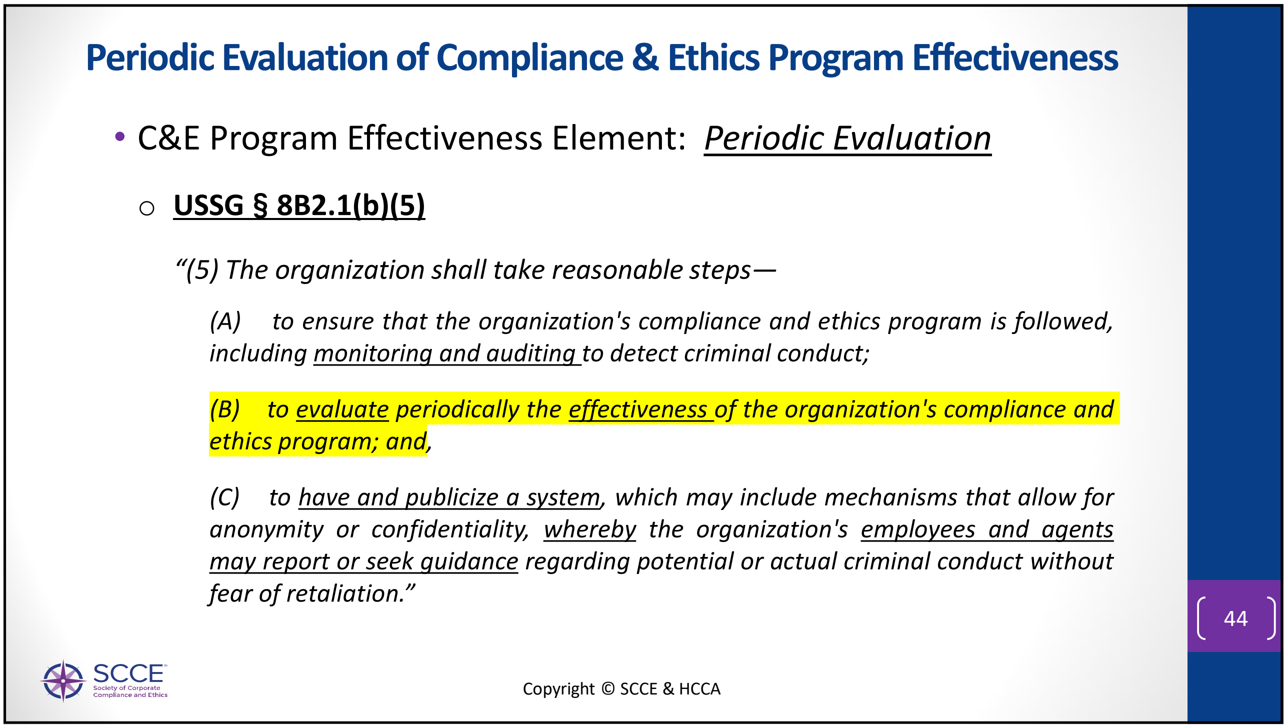


3

Periodic Evaluation of Compliance & Ethics Program Effectiveness

43

43



Periodic Evaluation of Compliance & Ethics Program Effectiveness

- C&E Program Effectiveness Element: *Periodic Evaluation*
  - **USSG § 8B2.1(b)(5)**

    "(5) The organization shall take reasonable steps—

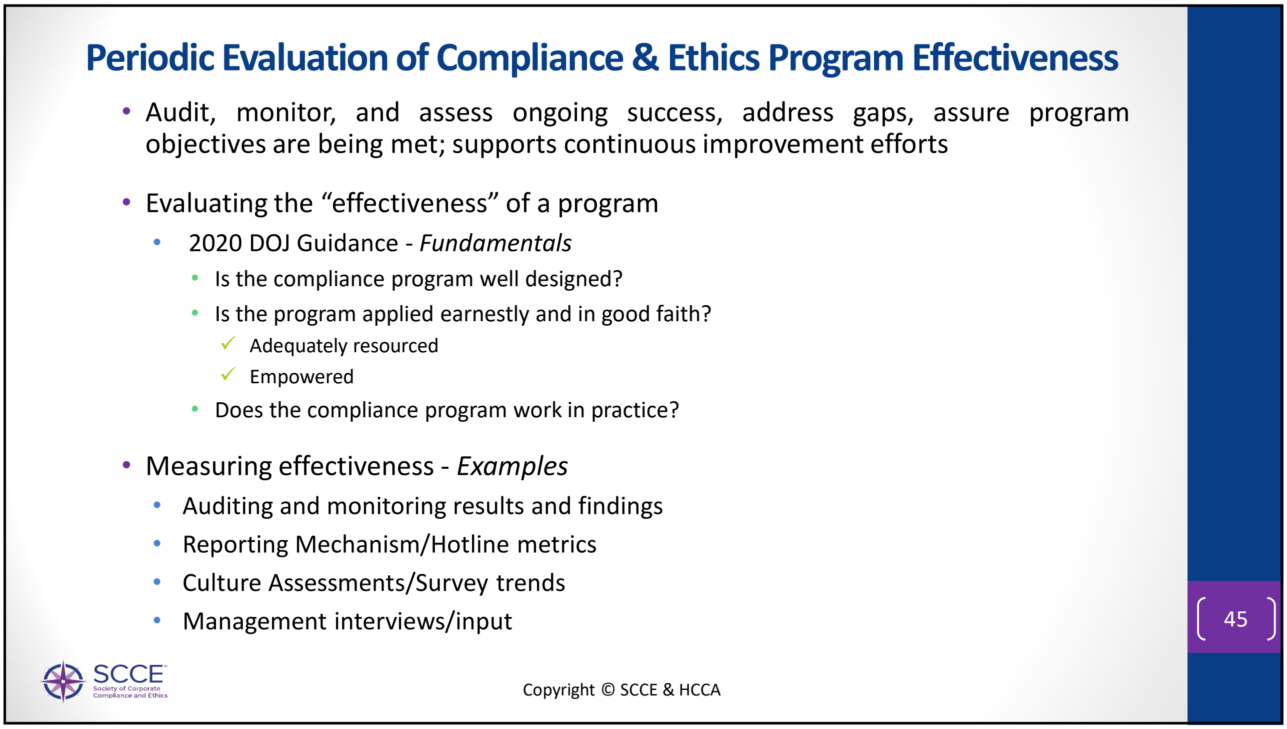
    (A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

    (B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and,

    (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."

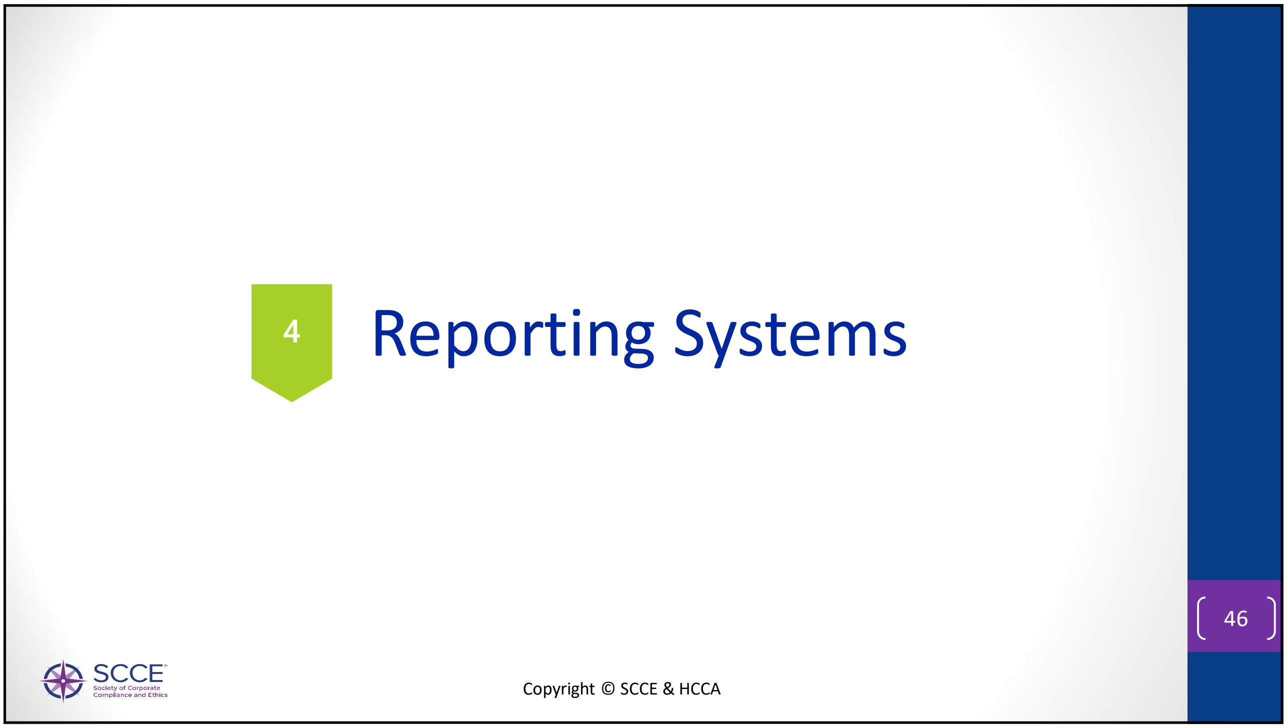
44

44



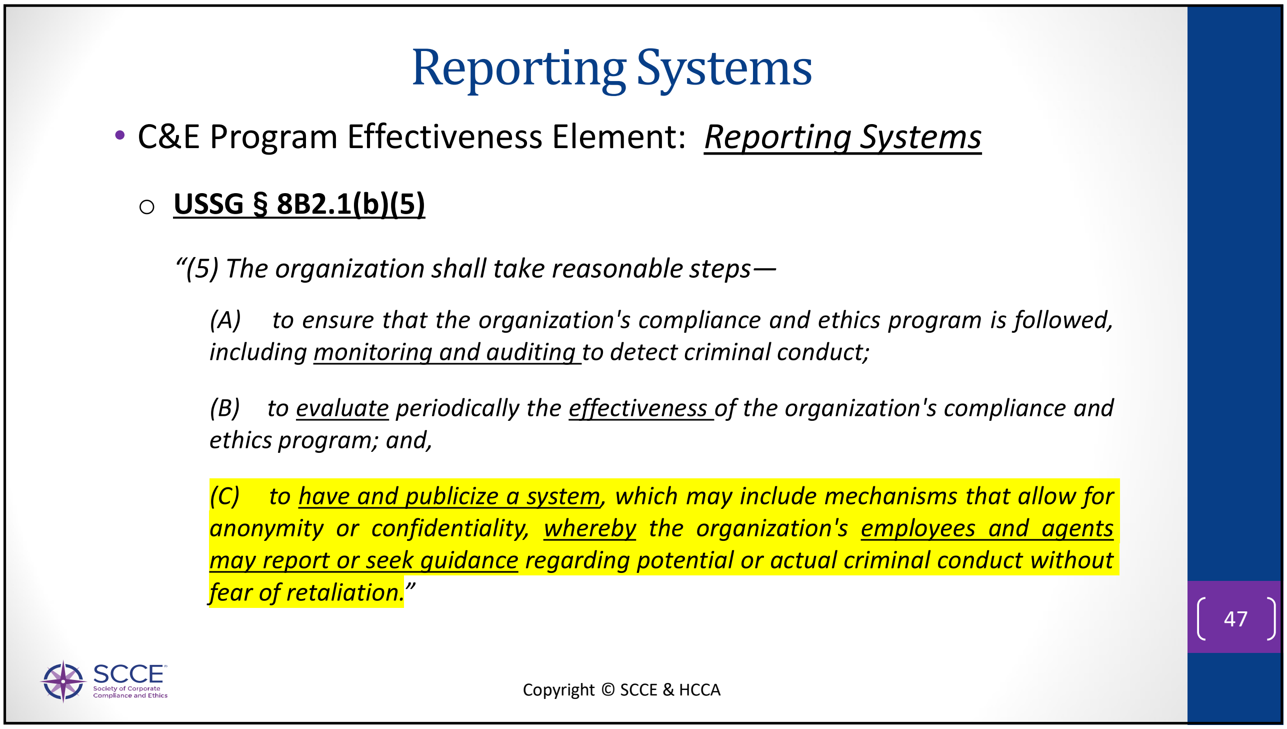
Periodic Evaluation of Compliance & Ethics Program Effectiveness

- Audit, monitor, and assess ongoing success, address gaps, assure program objectives are being met; supports continuous improvement efforts
- Evaluating the “effectiveness” of a program
  - 2020 DOJ Guidance - *Fundamentals*
    - Is the compliance program well designed?
    - Is the program applied earnestly and in good faith?
      - ✓ Adequately resourced
      - ✓ Empowered
    - Does the compliance program work in practice?
- Measuring effectiveness - *Examples*
  - Auditing and monitoring results and findings
  - Reporting Mechanism/Hotline metrics
  - Culture Assessments/Survey trends
  - Management interviews/input



4

Reporting Systems



Reporting Systems

- C&E Program Effectiveness Element: *Reporting Systems*
  - ○ **USSG § 8B2.1(b)(5)**

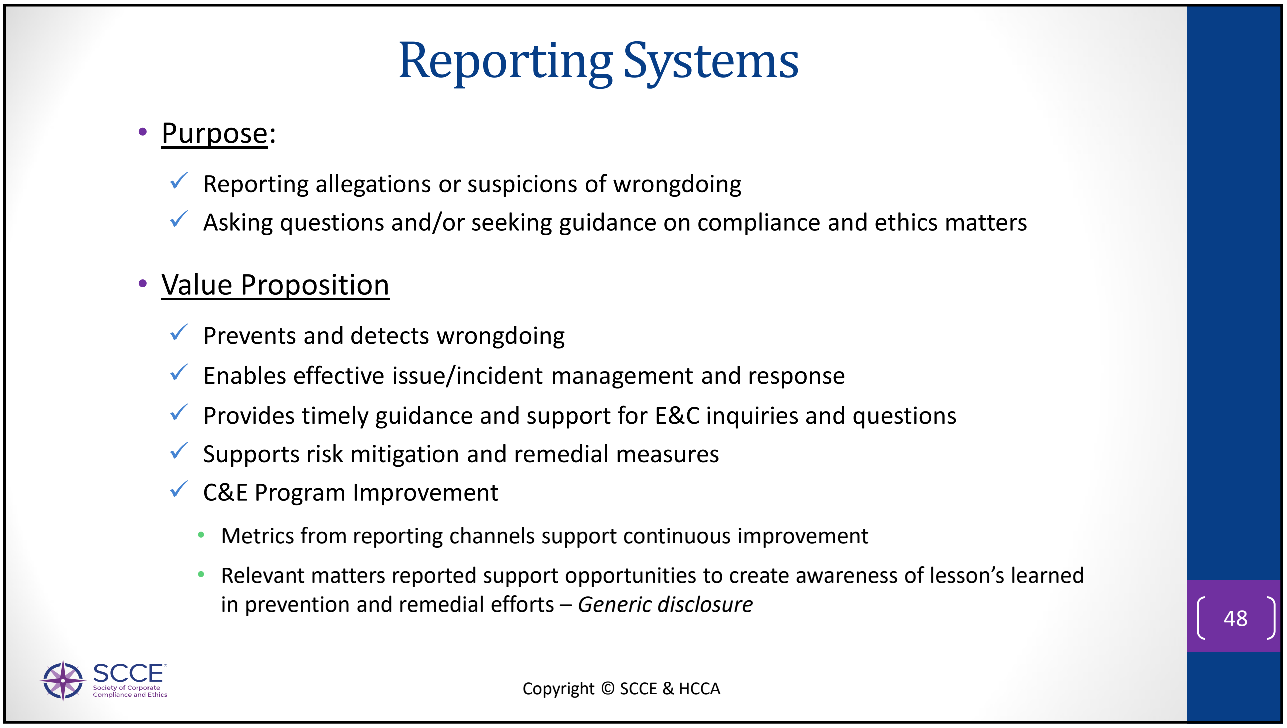
    "(5) The organization shall take reasonable steps—

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

    (B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and,

    (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."

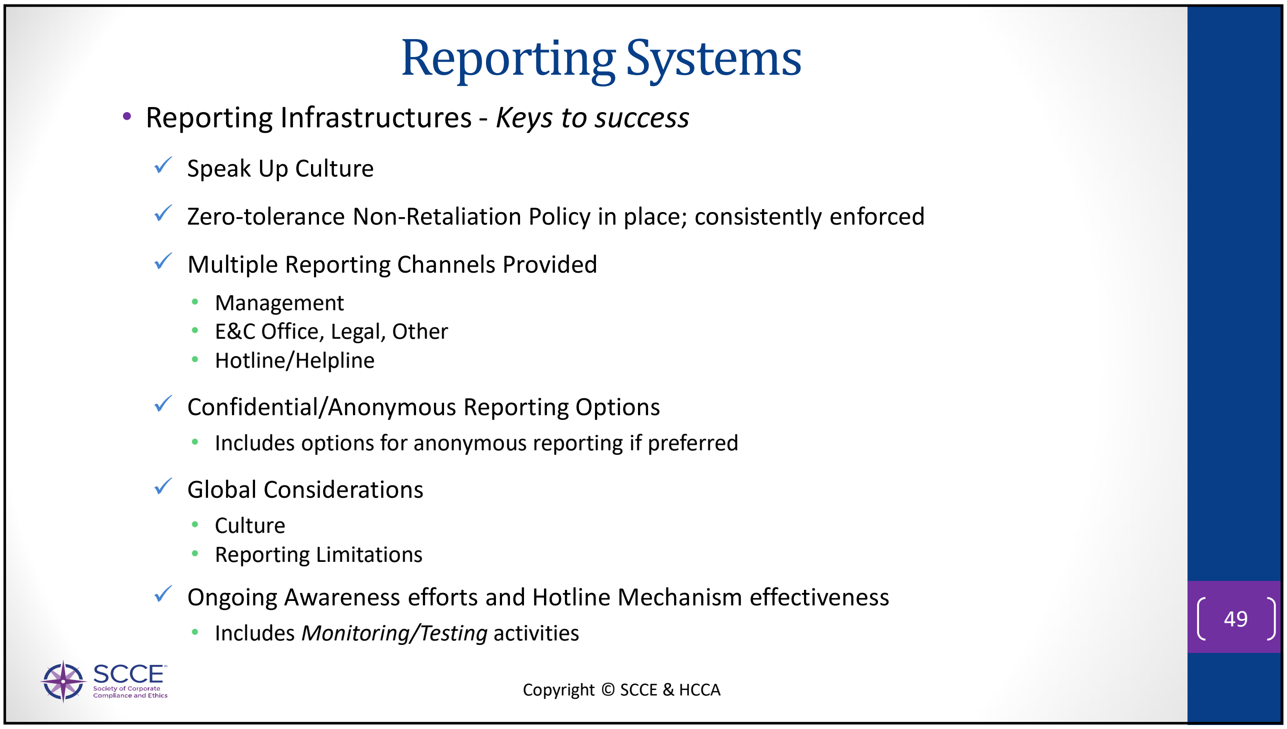
47



Reporting Systems

- Purpose:
  - ✓ Reporting allegations or suspicions of wrongdoing
  - ✓ Asking questions and/or seeking guidance on compliance and ethics matters
- Value Proposition
  - ✓ Prevents and detects wrongdoing
  - ✓ Enables effective issue/incident management and response
  - ✓ Provides timely guidance and support for E&C inquiries and questions
  - ✓ Supports risk mitigation and remedial measures
  - ✓ C&E Program Improvement
    - Metrics from reporting channels support continuous improvement
    - Relevant matters reported support opportunities to create awareness of lesson's learned in prevention and remedial efforts – *Generic disclosure*

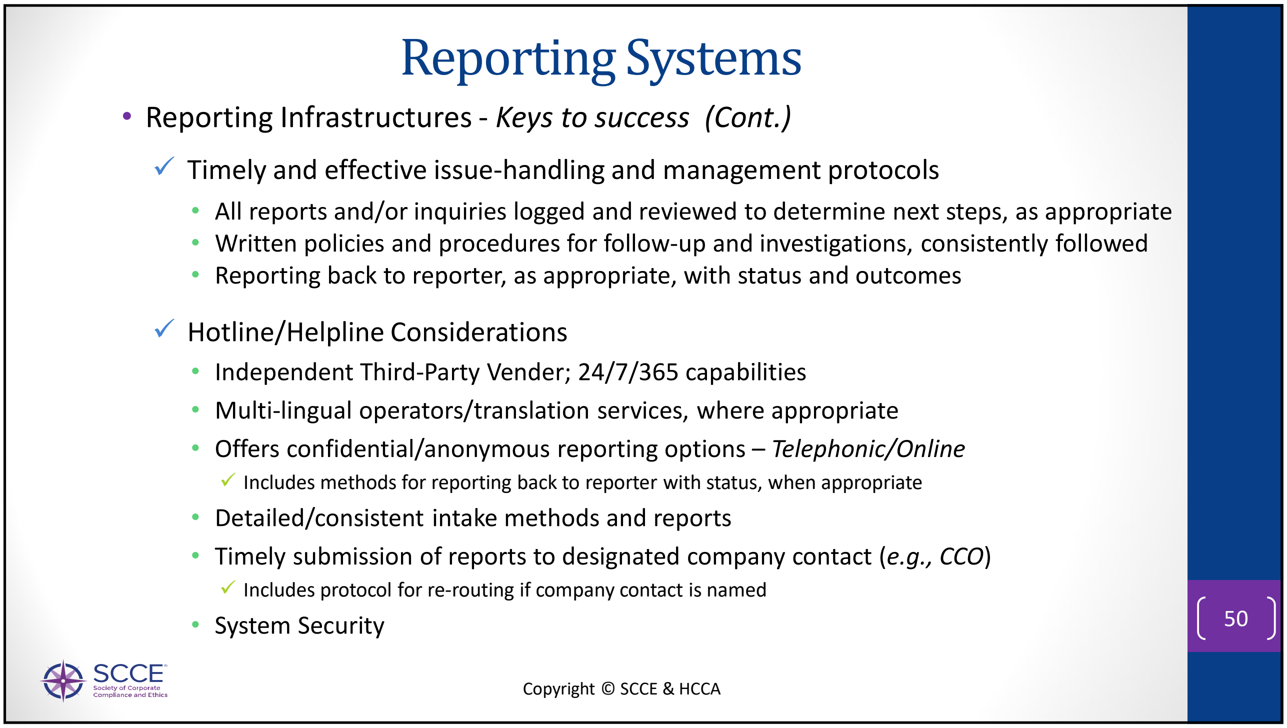
48



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
  - ✓ 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

49



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
  - ✓ Hotline/Helpline Considerations
    - Independent Third-Party Vender; 24/7/365 capabilities
    - Multi-lingual operators/translation services, where appropriate
    - Offers confidential/anonymous reporting options – *Telephonic/Online*
      - ✓ Includes methods for reporting back to reporter with status, when appropriate
    - Detailed/consistent intake methods and reports
    - Timely submission of reports to designated company contact (*e.g., CCO*)
      - ✓ Includes protocol for re-routing if company contact is named
    - System Security

50

Questions??

51

51

Compliance Essentials Workshop

Compliance Investigations

SCCE & HCCA

Wendy Evans
SCCE Virtual Academy Faculty
and
Senior Investigator & Senior Manager, Ethics Core Programs
Lockheed Martin

1

1

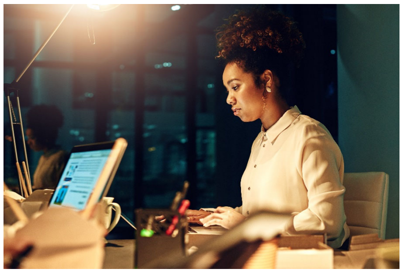
Key Topics for Today

- 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

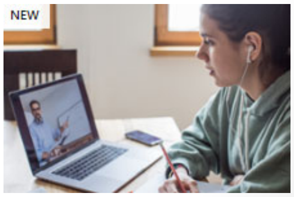
2

Initiating an investigation



Contact Methods

- Instant Message, Skype
- Virtual platforms (Zoom, Microsoft Teams, etc.)
- Direct email/phone of compliance officer
- Corporate or local Helpline
- Corporate or local email resource account
- “Ask a Question” website, or FAQs
- Ethics and Compliance Website
- Digital or hard copy posters, contact cards
- Newsletters
- Directory information



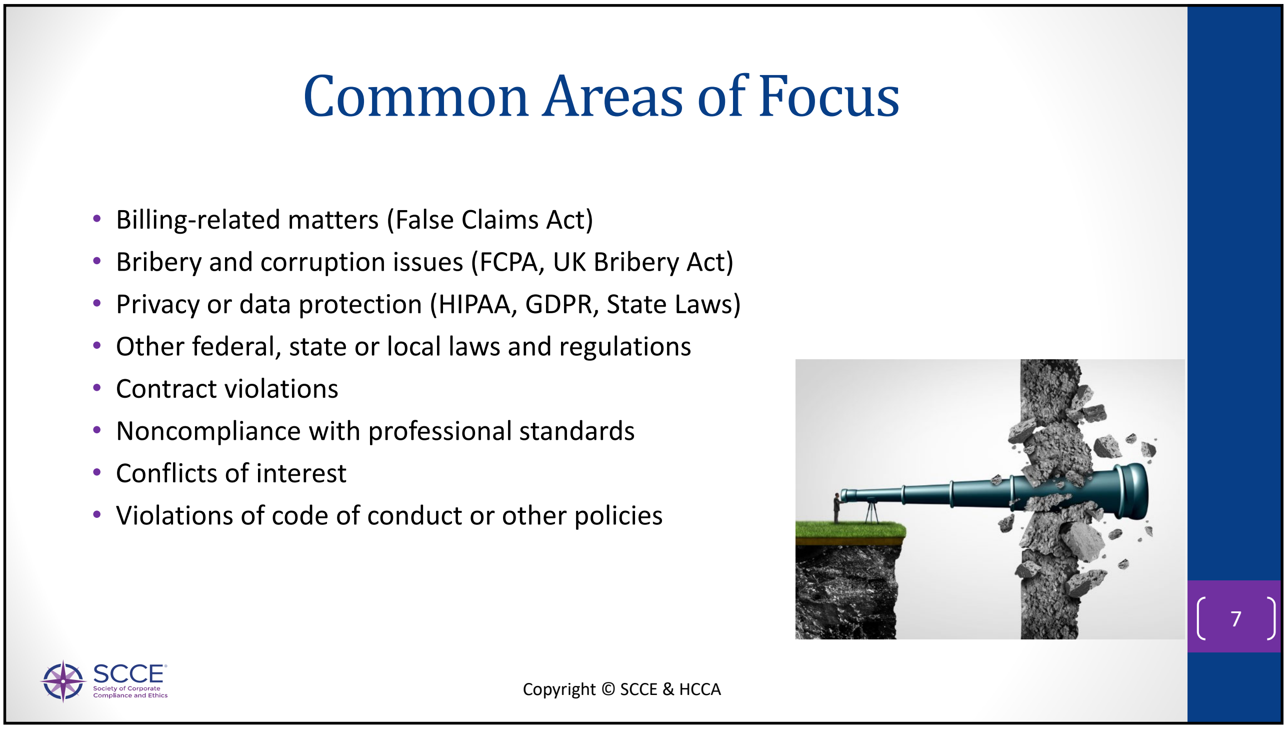
What initiates an investigation?

- 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 which warrants follow-up
  - Clear violation (policy/regulation/law/process) identified
  - Gaps in process identified
  - Potential misconduct identified

Purposes of an Investigation

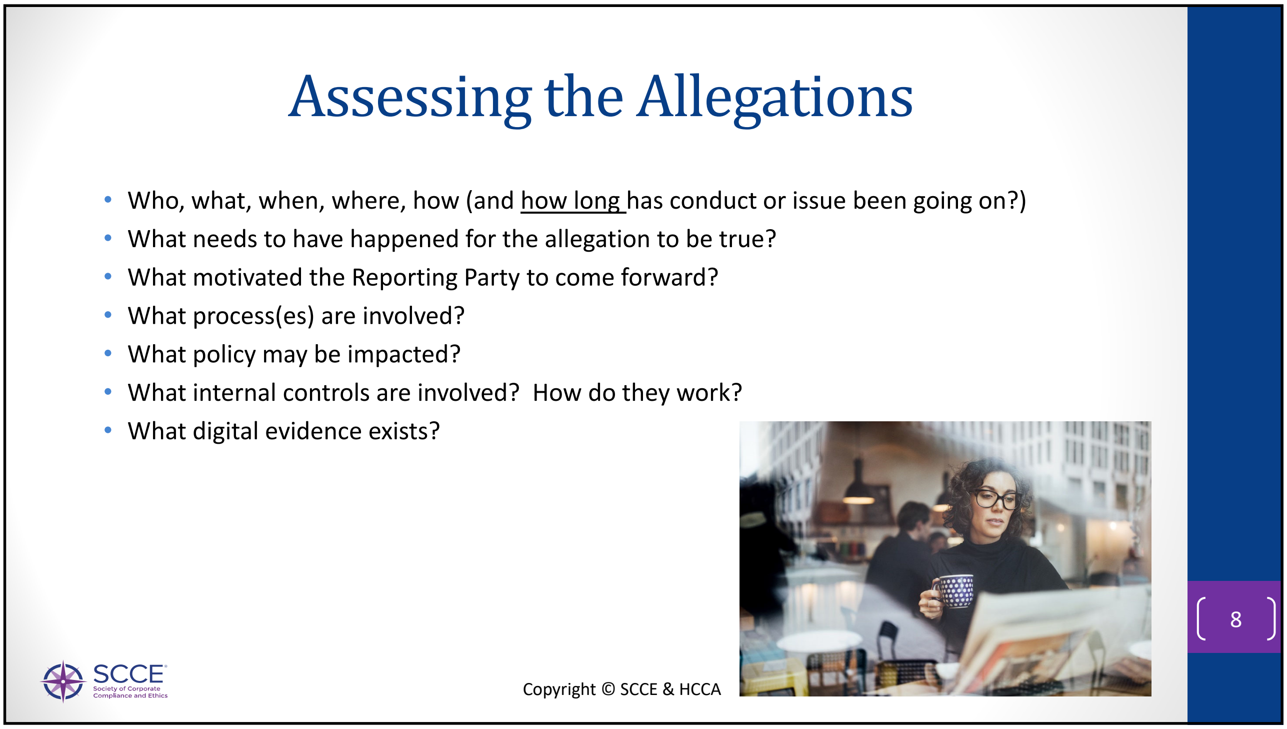
- Determining whether an act of non-compliance occurred
- Determining who was involved
- Determining how the act(s) occurred
  - **Incidental or Systemic Issue**?
  - Remediation to prevent future risks
- Determining extent of damages
  - Are disclosures necessary to government? Notifications to stakeholders?



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

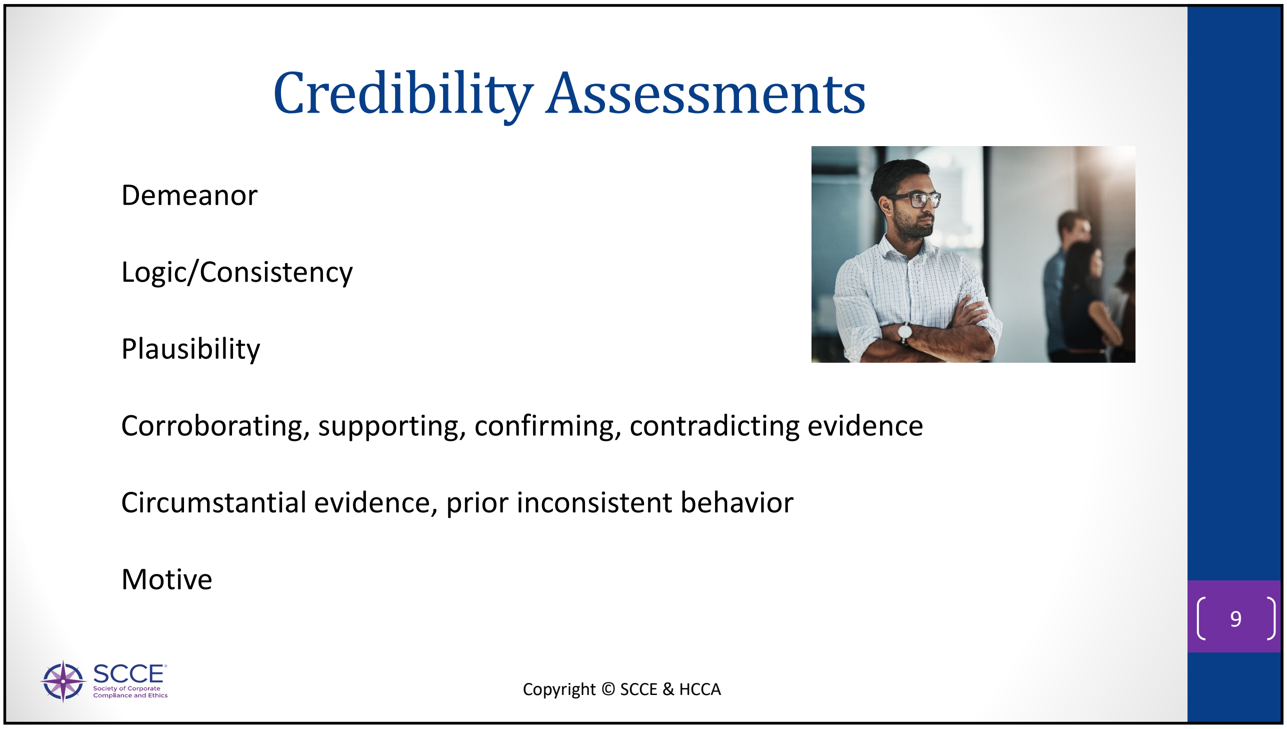
SCCE Society of Corporate Compliance and Ethics



Assessing the Allegations

- Who, what, when, where, how (and how long has conduct or issue been going on?)
- What needs to have happened for the allegation to be true?
- What motivated the Reporting Party to come forward?
- What process(es) are involved?
- What policy may be impacted?
- What internal controls are involved? How do they work?
- What digital evidence exists?

SCCE Society of Corporate Compliance and Ethics



Credibility Assessments

Demeanor

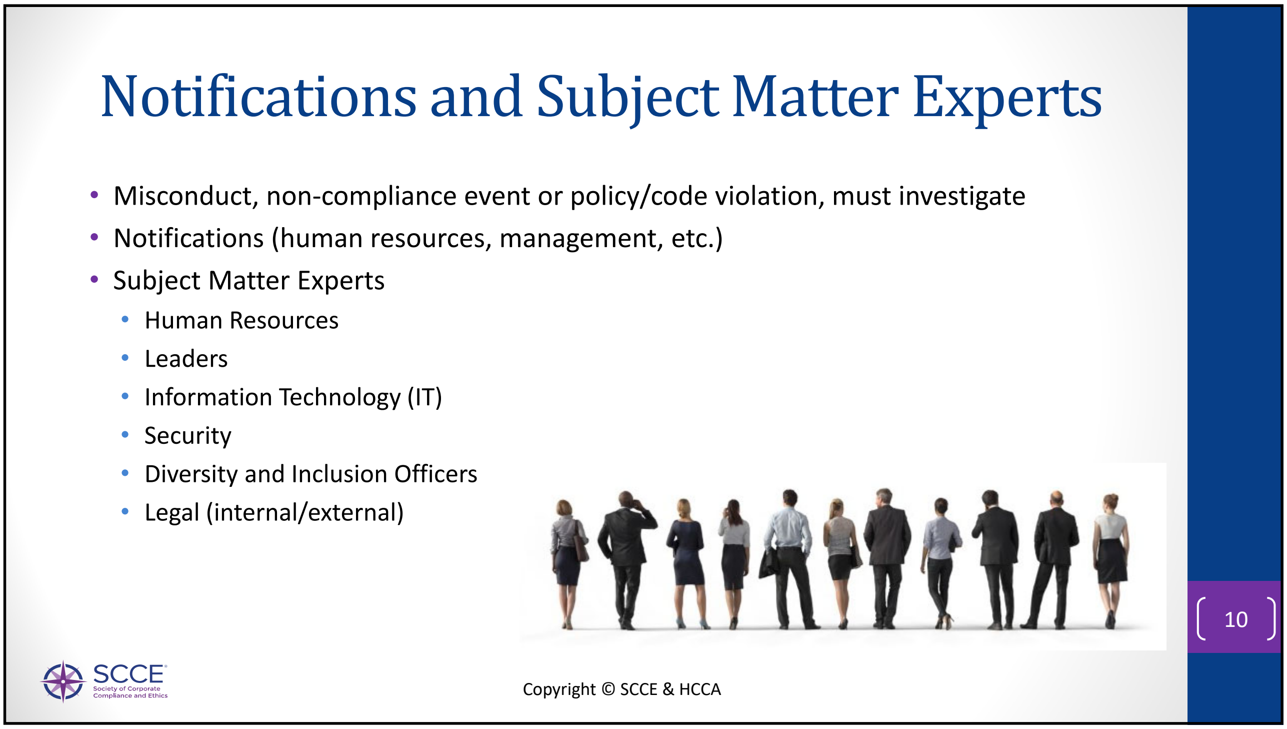
Logic/Consistency

Plausibility

Corroborating, supporting, confirming, contradicting evidence

Circumstantial evidence, prior inconsistent behavior

Motive



Notifications and Subject Matter Experts

- Misconduct, non-compliance event or policy/code violation, must investigate
- Notifications (human resources, management, etc.)
- Subject Matter Experts
  - Human Resources
  - Leaders
  - Information Technology (IT)
  - Security
  - Diversity and Inclusion Officers
  - Legal (internal/external)

Gathering Data and Documents

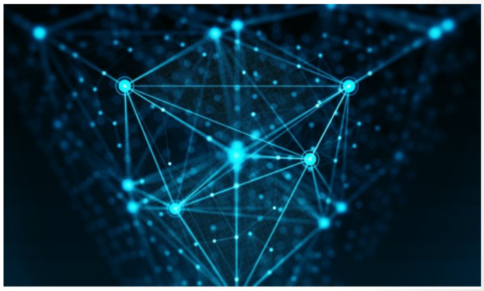
11

SCCE Society of Corporate Compliance and Ethics

11

Identifying Records & Data Needed

- Process Maps
  - MUST understand how the transaction cycle operates to identify relevant records needed
  - Process gaps? People or a process issue—or both? Systemic or incidental?
- Identify:
  - Leaders/stakeholders
  - Witnesses
  - SMEs
  - Internal controls
  - Documents and records
    - Expense report records
    - Timekeeping records
    - Forensic reviews (computer systems, etc.)
    - Emails, Instant Messages, other documents



12

SCCE Society of Corporate Compliance and Ethics

12

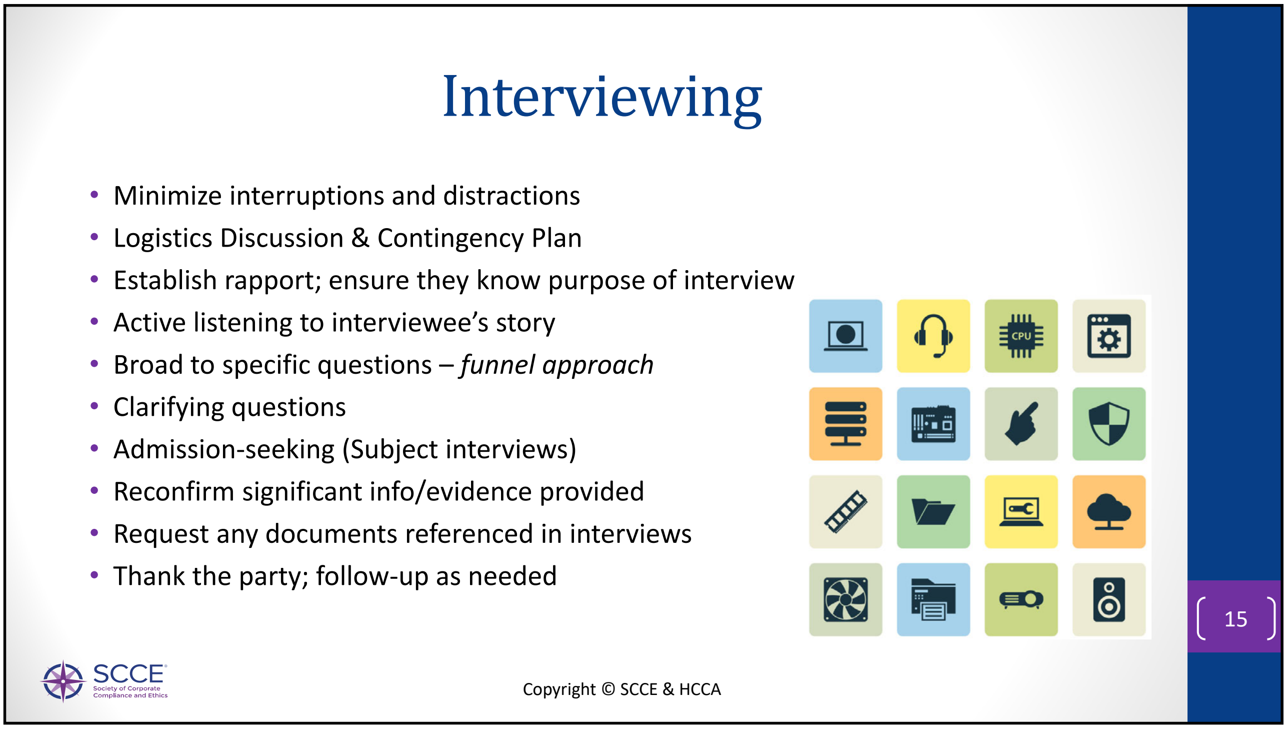
Conducting Interviews

SCCE Society of Corporate Compliance and Ethics

Interview Planning

- Goal – what is the problem or issue being addressed?
- Interview Plan
- Witness list
- Order of interviews
- Scheduling
- Virtual vs. In-Person (and logistics for each)
- Rules for Recording of interviews by either party (or not)
- Outline for topics to cover
- Active listening is critical
- Avoid ‘scope creep’ (keep investigation focused)

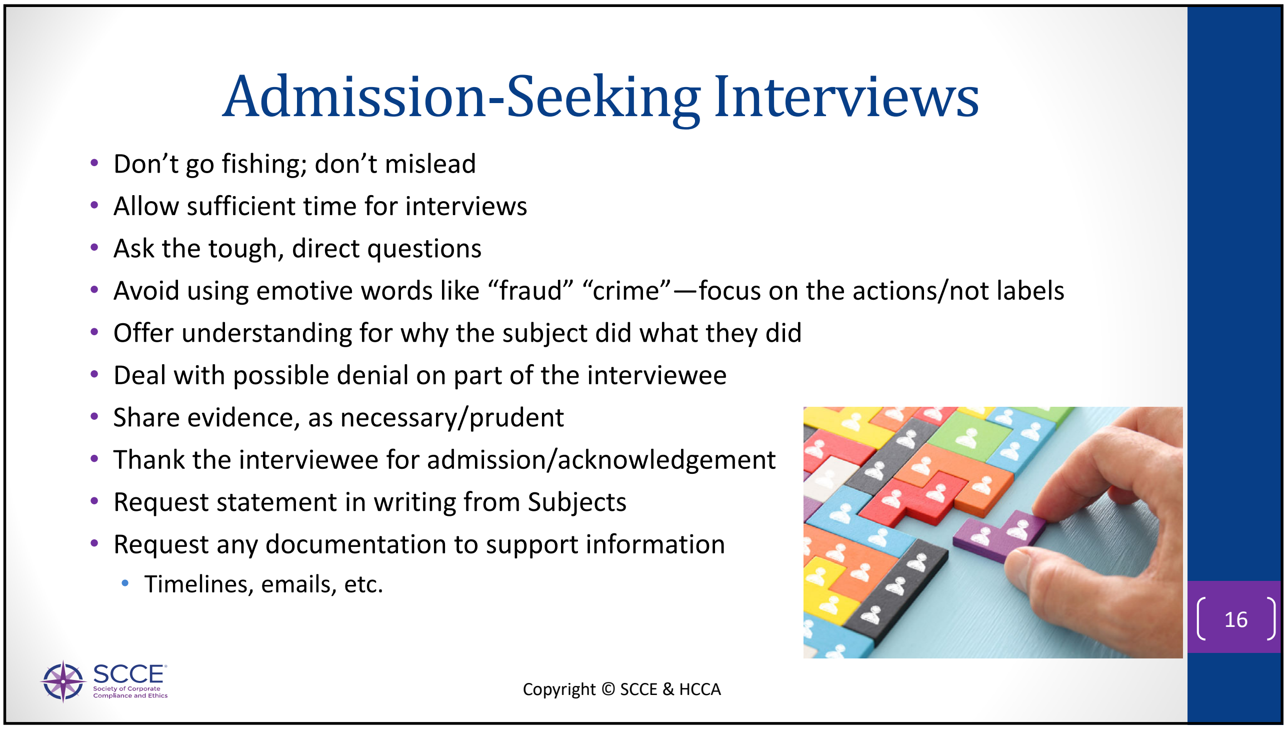
SCCE Society of Corporate Compliance and Ethics



Interviewing

- Minimize interruptions and distractions
- Logistics Discussion & Contingency Plan
- Establish rapport; ensure they know purpose of interview
- Active listening to interviewee’s story
- Broad to specific questions – *funnel approach*
- Clarifying questions
- Admission-seeking (Subject interviews)
- Reconfirm significant info/evidence provided
- Request any documents referenced in interviews
- Thank the party; follow-up as needed

SCCE Society of Corporate Compliance and Ethics



Admission-Seeking Interviews

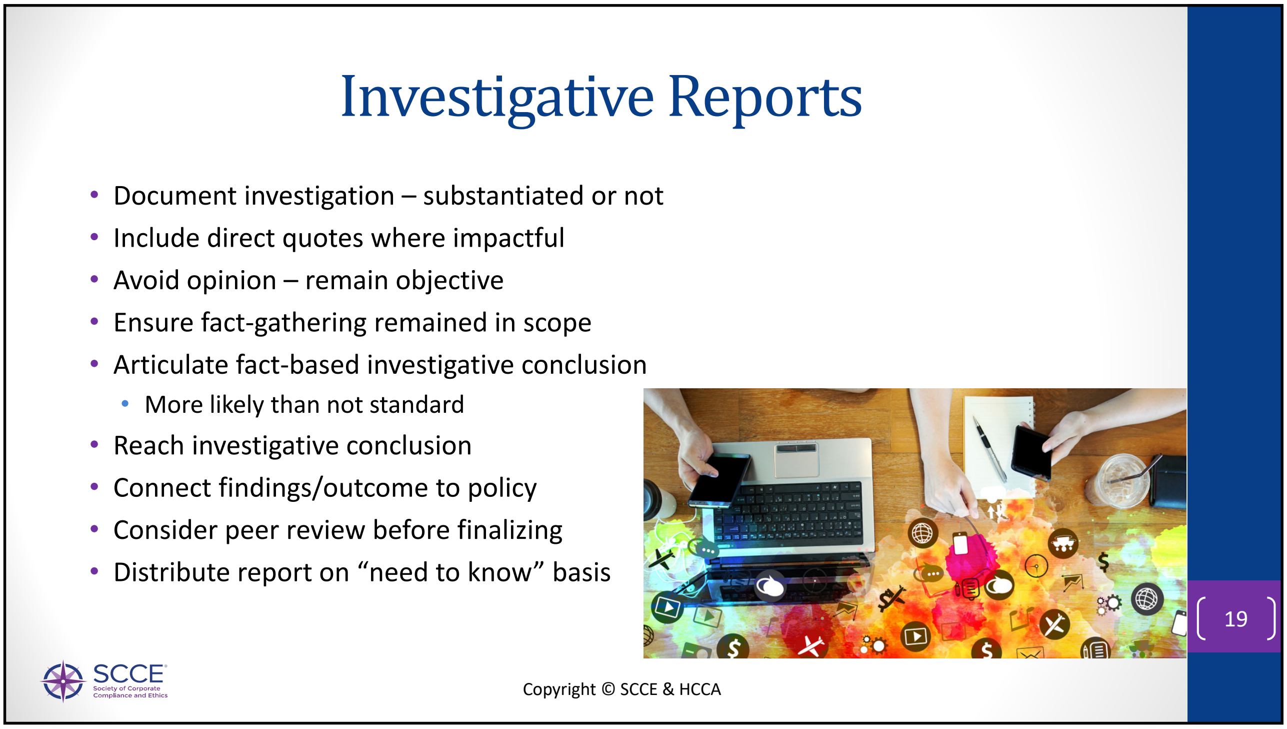
- Don’t go fishing; don’t mislead
- Allow sufficient time for interviews
- Ask the tough, direct questions
- Avoid using emotive words like “fraud” “crime”—focus on the actions/not labels
- Offer understanding for why the subject did what they did
- Deal with possible denial on part of the interviewee
- Share evidence, as necessary/prudent
- Thank the interviewee for admission/acknowledgement
- Request statement in writing from Subjects
- Request any documentation to support information
  - Timelines, emails, etc.

SCCE Society of Corporate Compliance and Ethics

Dealing with Difficulties

- Resistance to being interviewed
  - Explain value of their perspective
  - Explain process – fair and objective investigation
  - Discuss confidentiality
  - Discuss policy regarding cooperation with internal investigations
- Volatile interviewees
  - Two interviewers
  - Surprise/simultaneous interviews
  - De-escalate
  - Duty to cooperate policy
- Technical Issues
  - Remote/hybrid work environments
  - Various technology capabilities

Investigative Reports



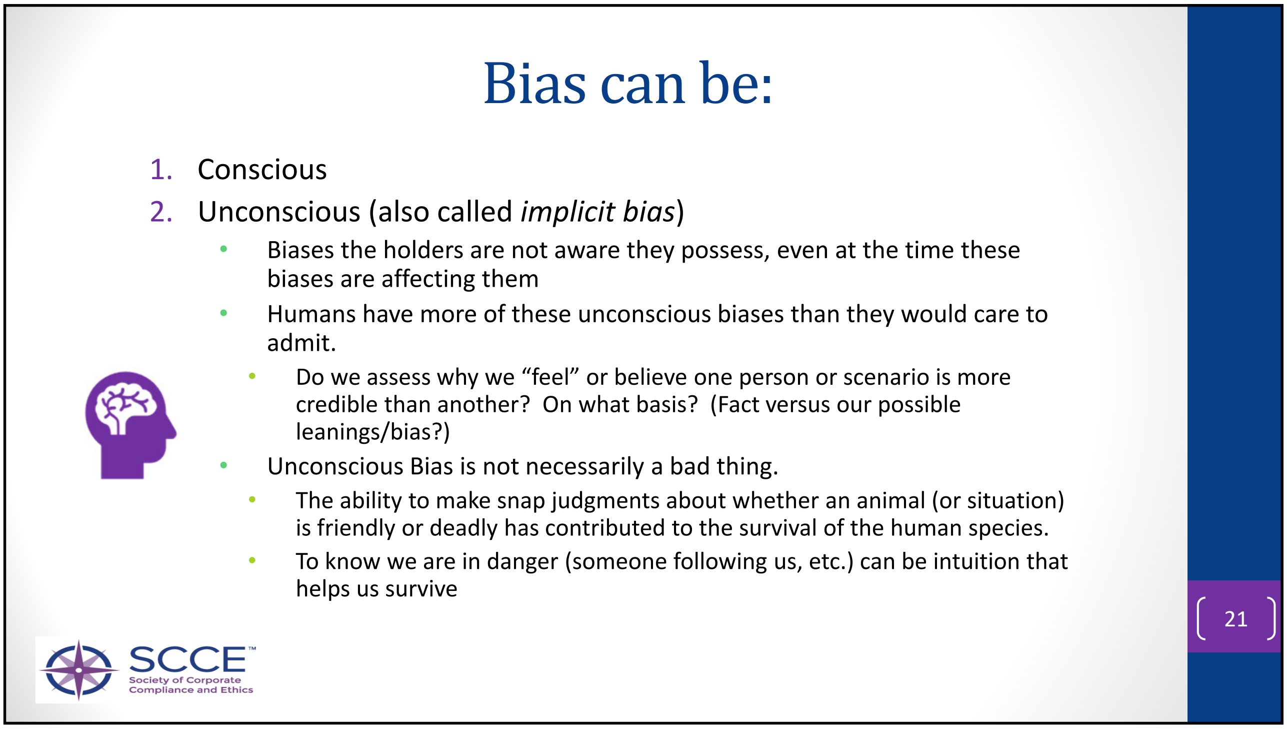
Investigative Reports

- 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
- Reach investigative conclusion
- Connect findings/outcome to policy
- Consider peer review before finalizing
- Distribute report on "need to know" basis

SCCE Society of Corporate Compliance and Ethics

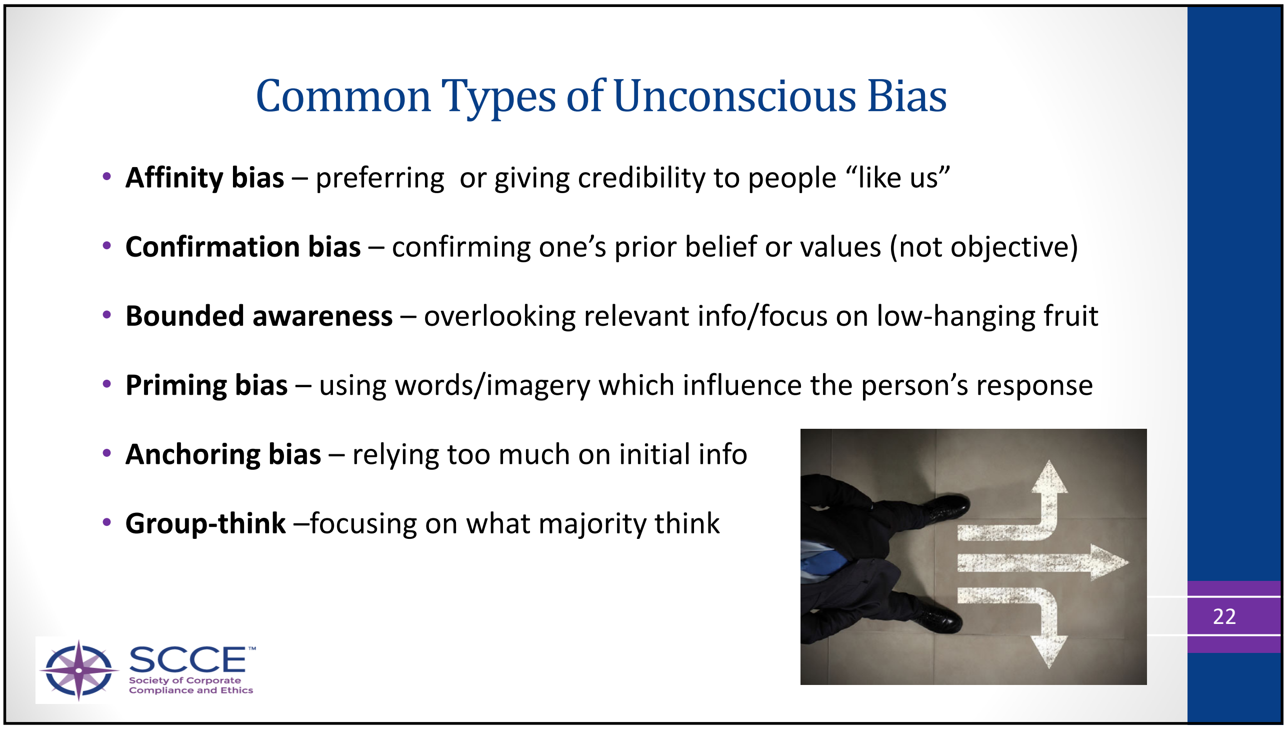
How Bias Impacts Investigations

SCCE Society of Corporate Compliance and Ethics



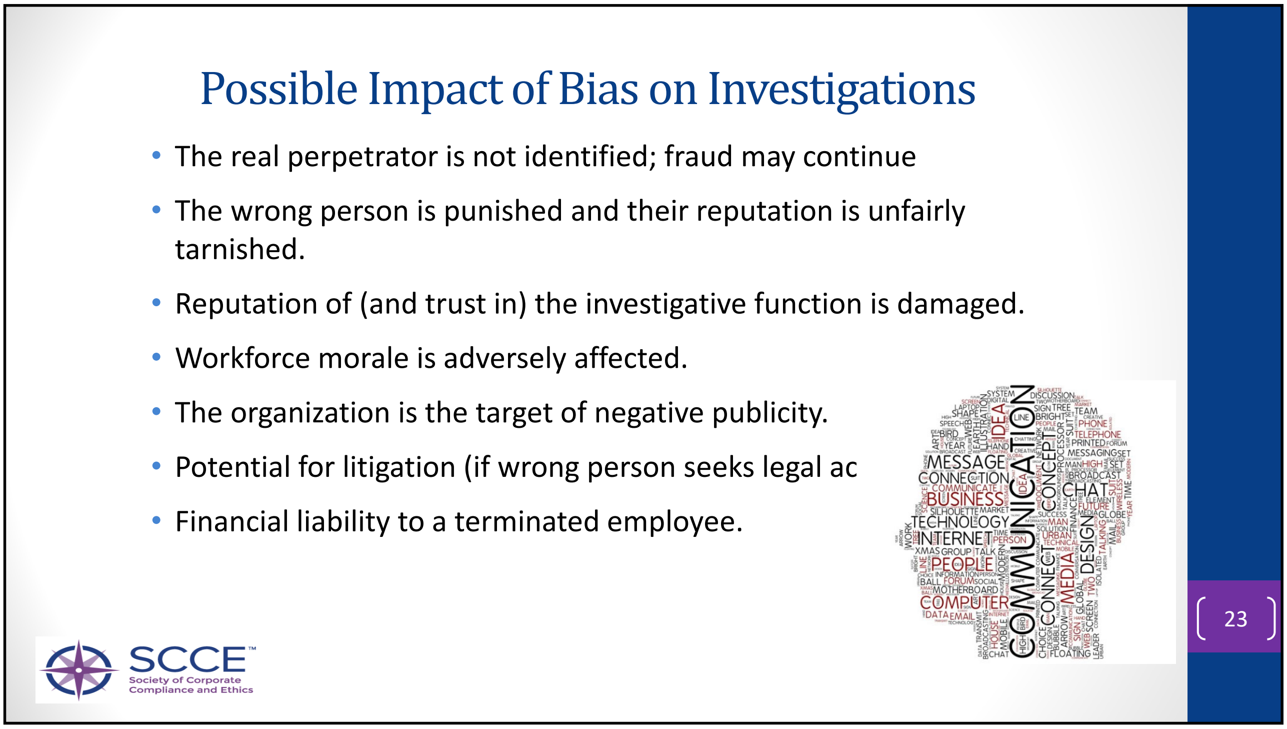
Bias can be:

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



Common Types of Unconscious Bias

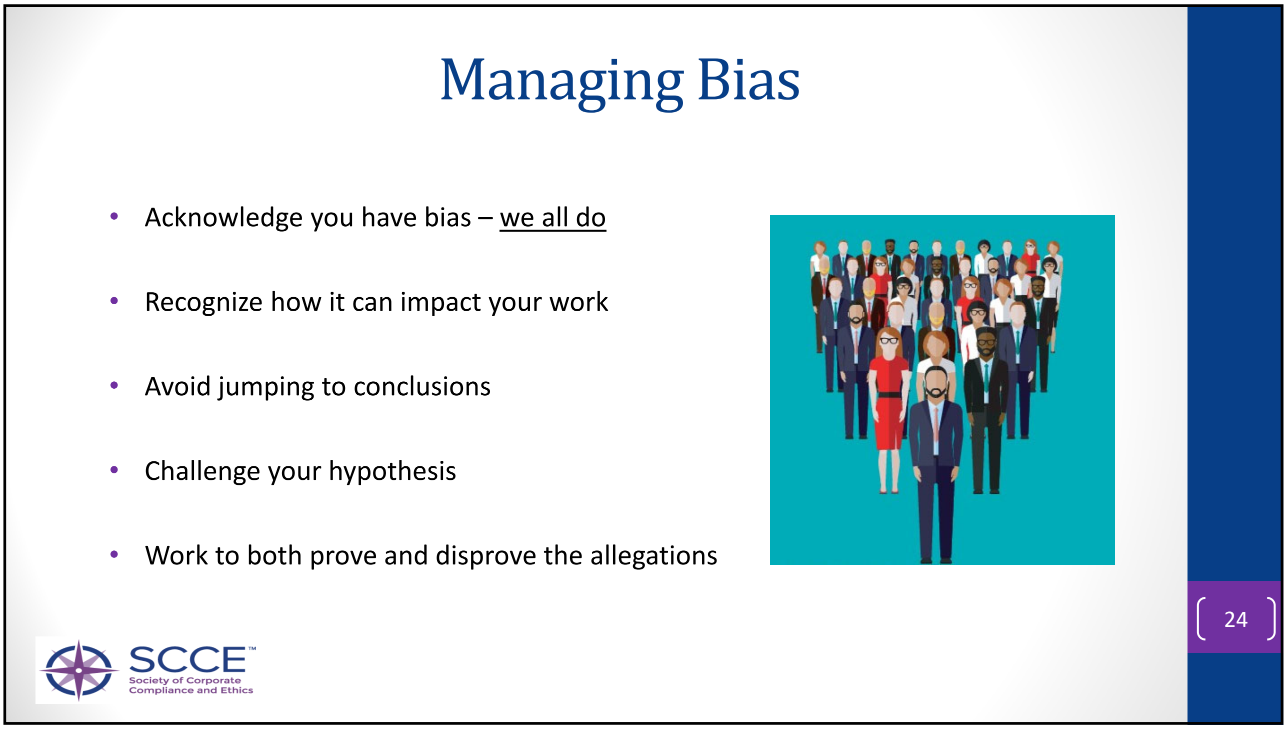
- **Affinity bias** – preferring or giving credibility to people "like us"
- **Confirmation bias** – confirming one's prior belief or values (not objective)
- **Bounded awareness** – overlooking relevant info/focus on low-hanging fruit
- **Priming bias** – using words/imagery which influence the person's response
- **Anchoring bias** – relying too much on initial info
- **Group-think** –focusing on what majority think



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.

23



Managing Bias

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

24

Using Third Parties to Assist in Performing Investigations

25

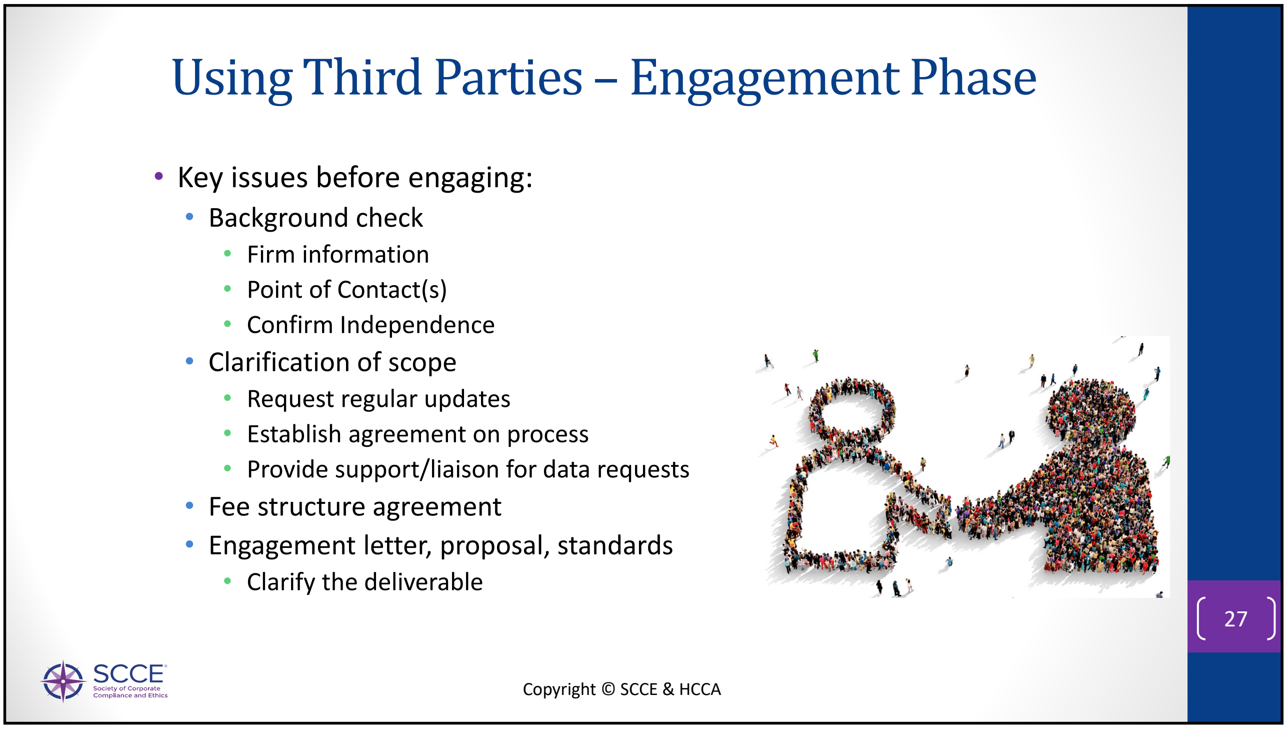
SCCE Society of Corporate Compliance and Ethics

When/Why Use Third Parties?

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

26

SCCE Society of Corporate Compliance and Ethics



Using Third Parties – Engagement Phase

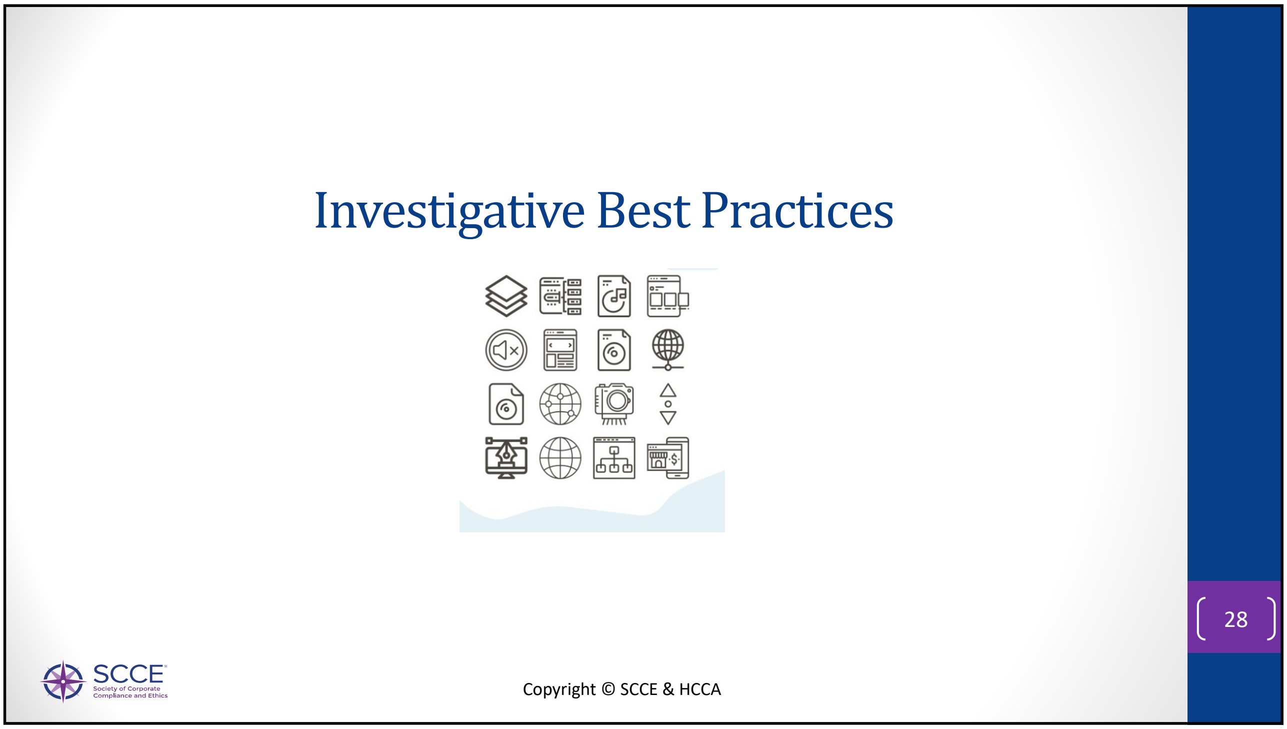
- Key issues before engaging:
  - Background check
    - Firm information
    - Point of Contact(s)
    - Confirm Independence
  - Clarification of scope
    - Request regular updates
    - Establish agreement on process
    - Provide support/liaison for data requests
  - Fee structure agreement
  -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

27

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

27



Investigative Best Practices

28

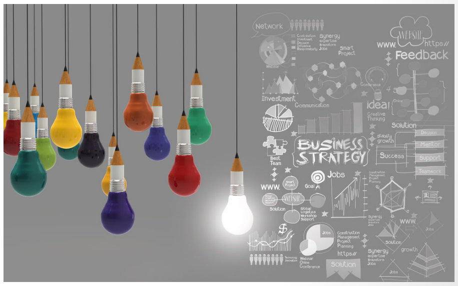
SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

28

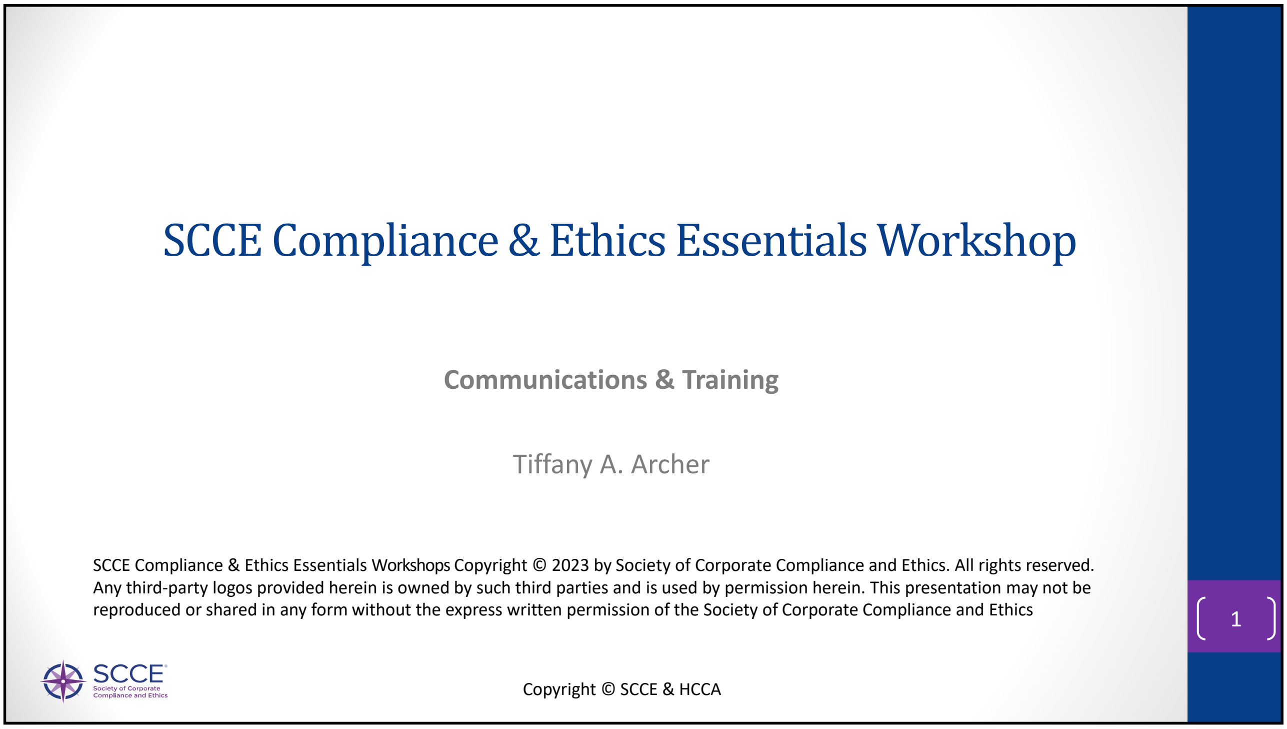
Best Practices

- In-house policy on investigations
- Clear expectations of employee participation
- Established process for intake of concerns
- Investigative Plans
- Case management system
- Escalation and notification guidelines
- Documentation requirements
- Toolkit – templates and forms
- Review (quality control) processes
- Training for investigators
- Post-investigative surveys re: process



Questions ?

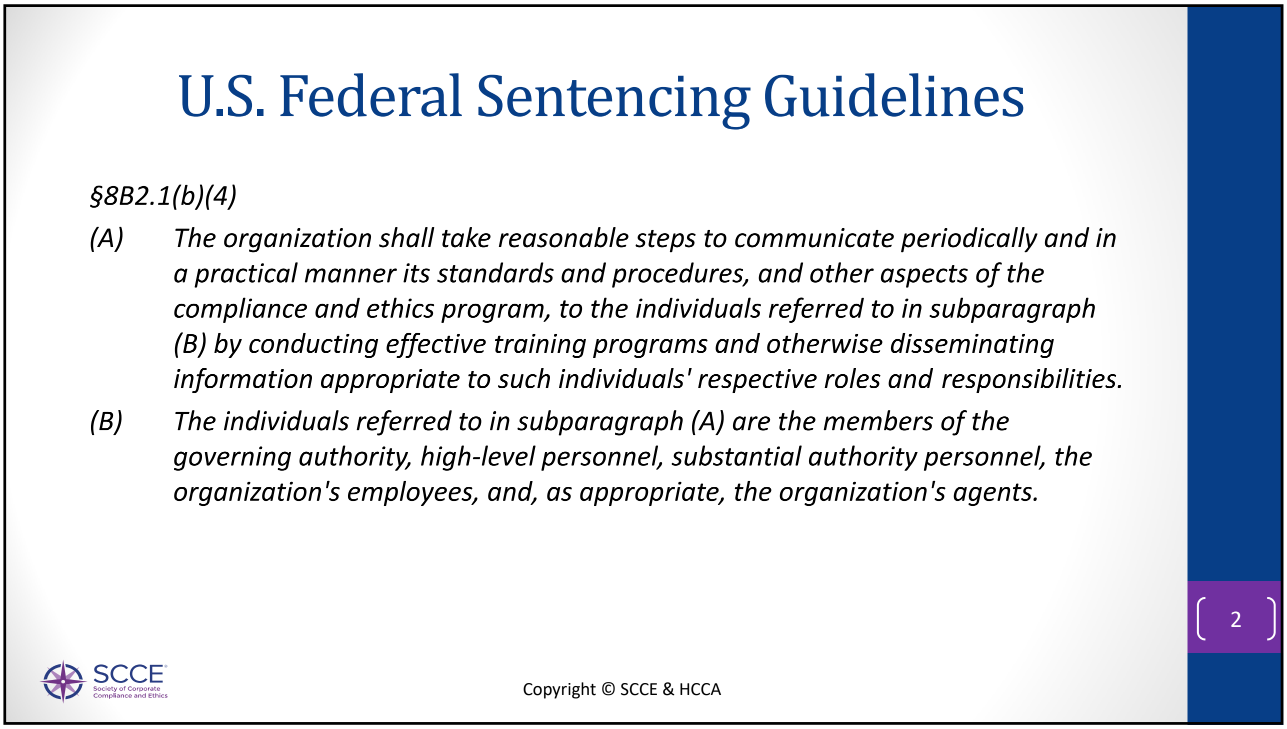
wendy.w.evans@lmco.com



SCCE Compliance & Ethics Essentials Workshop

Communications & Training

Tiffany A. Archer



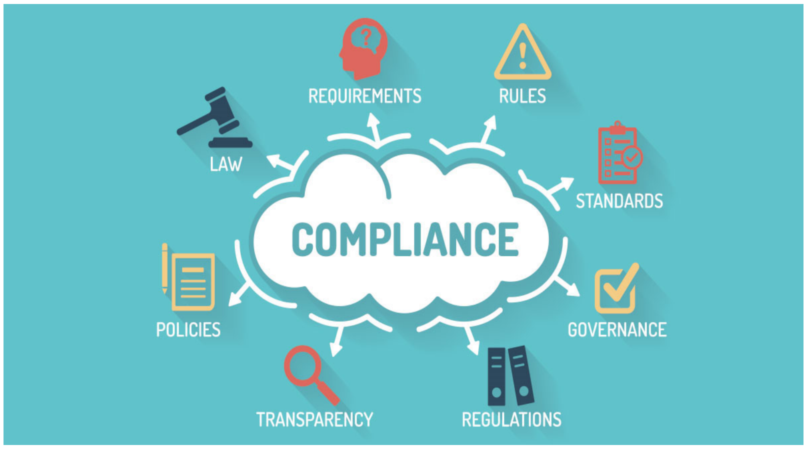
U.S. Federal Sentencing Guidelines

§8B2.1(b)(4)

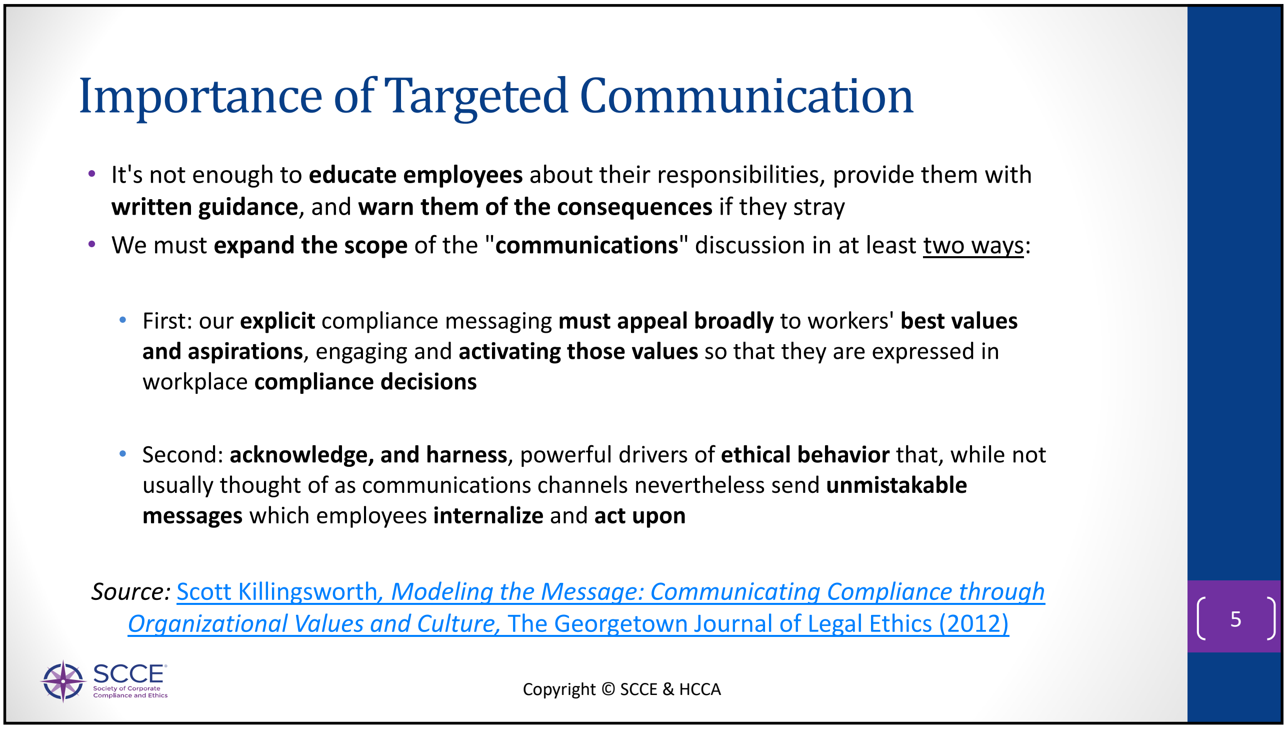
(A) *The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating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

What does a "Compliance Officer" really do?



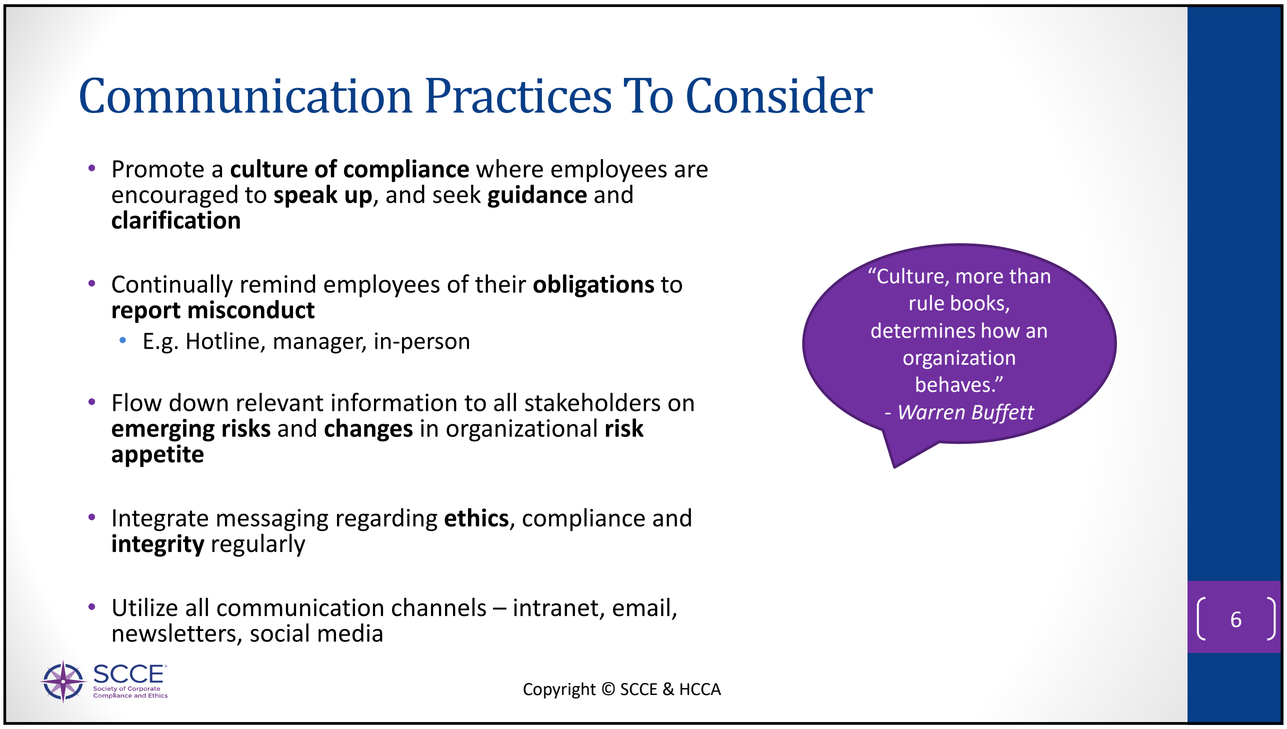
The Problem: A Not So Unfamiliar Training Scenario



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 two ways:
  - 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)



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 communication channels – intranet, email, newsletters, social media

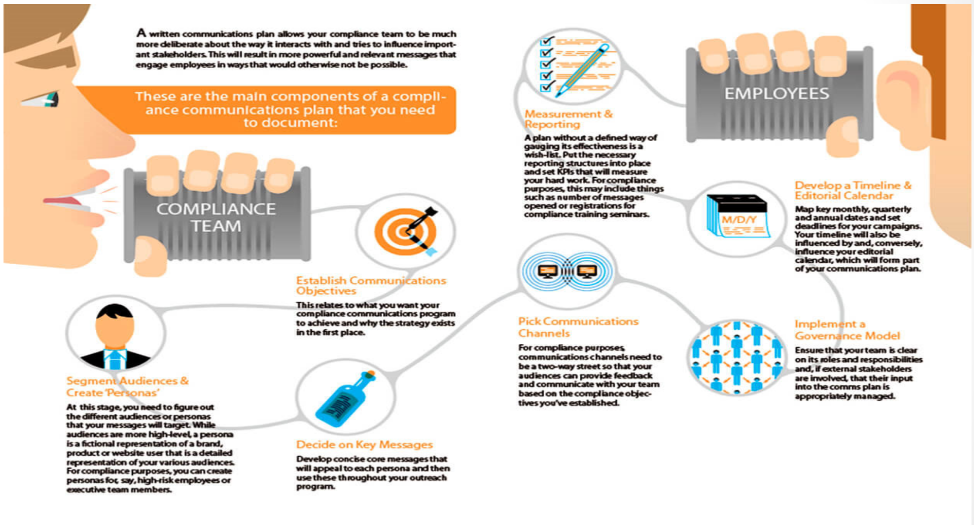
"Culture, more than rule books, determines how an organization behaves."
- *Warren Buffett*

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***

SCCE Society of Corporate Compliance and Ethics

2020 Guidance: "Effective" Compliance Programs

- Significantly, the DOJ calls out the **criticality of training and communications** in an effective program

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

- Includes specific "Training & Communications" guidelines

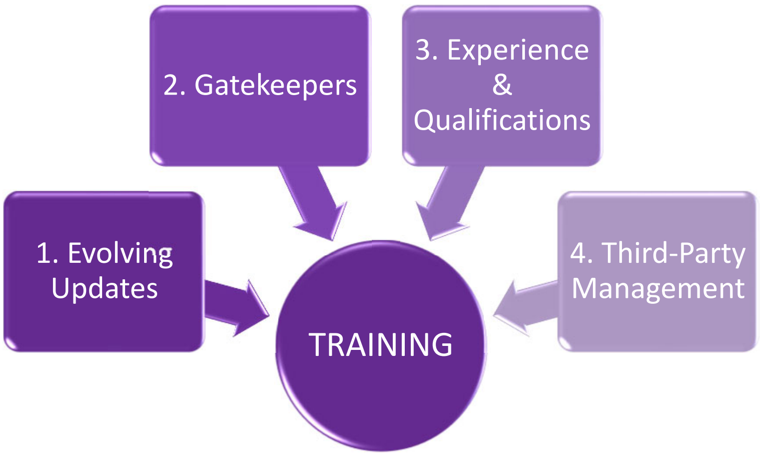
- Highlights the importance of **critical <u>touchpoints</u>** between training, communications and other compliance program areas to ensure program *effectiveness*

SCCE Society of Corporate Compliance and Ethics

Polling Slide

- Has your Compliance Function actively integrated the guidelines related to Training & Communication in the DOJ's June 2020 *Evaluation of Corporate Compliance Programs?*
  - Yes
  - No, but we are working on it

2020 Guidance: 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**

“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** will help preserve the **integrity** of the internal control framework

“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**

15

SCCE Society of Corporate Compliance and Ethics

15

“Training Touchpoint”: Third-Party Management

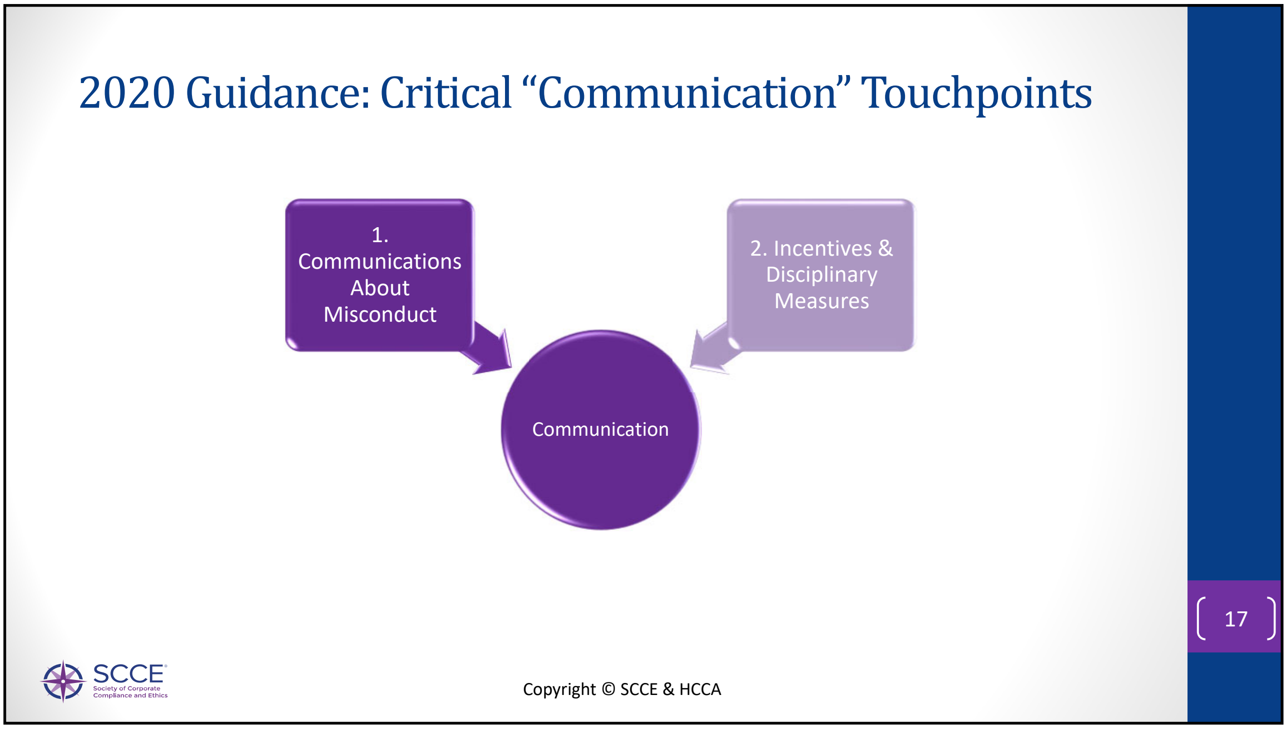
- To mitigate risk, maintain familiarity with your **third parties’ qualifications** and perform **ongoing monitoring** of the relationship
- **Avoid check the box training**: engage, interact and discuss to ensure understanding
- Provide **periodic, targeted training**, e.g. anti-corruption & bribery,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

WILL YOUR THIRD-PARTY MANAGEMENT PROGRAM HOLD UP UNDER SCRUTINY?

16

SCCE Society of Corporate Compliance and Ethics

16

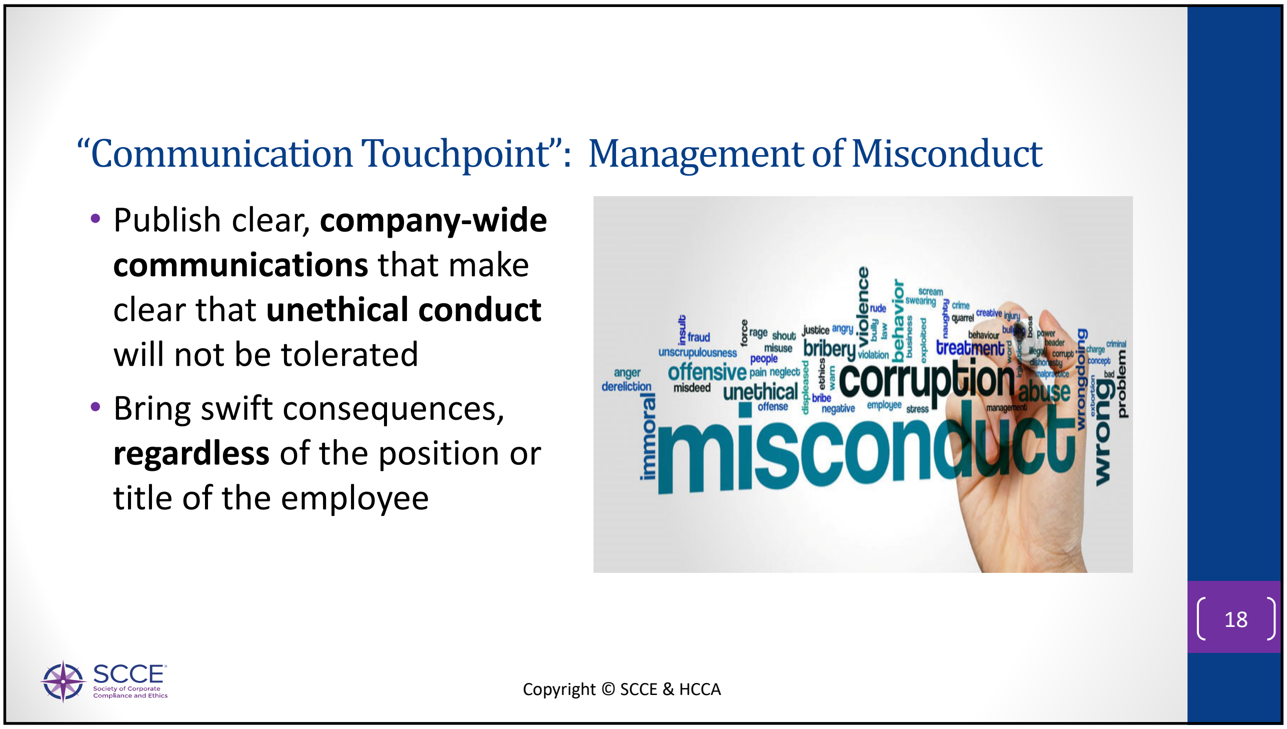


2020 Guidance: Critical “Communication” Touchpoints

1. Communications About Misconduct

2. Incentives & Disciplinary Measures

Communication



“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
immoral
wrong
wrongdoing
problem
abuse
unethical
offensive
bribery
treatment
violence
behavior
fraud
unscrupulousness
anger
dereliction
misdeed
insult
force
rage
shout
misuse
people
justice
angry
pain
neglect
offense
bribe
negative
employee
stress
management
crime
quarrel
scream
swearing
rude
bully
law
violation
ethics
displeased
warn
exploited
business
naughty
behaviour
power
criminal
charge
concept
bad
extortion

"Communication Touchpoint": Incentives & Disciplinary Measures

- Consider how to **encourage deterrence** (e.g. publicize disciplinary actions versus provide positive incentives for good behavior)

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**

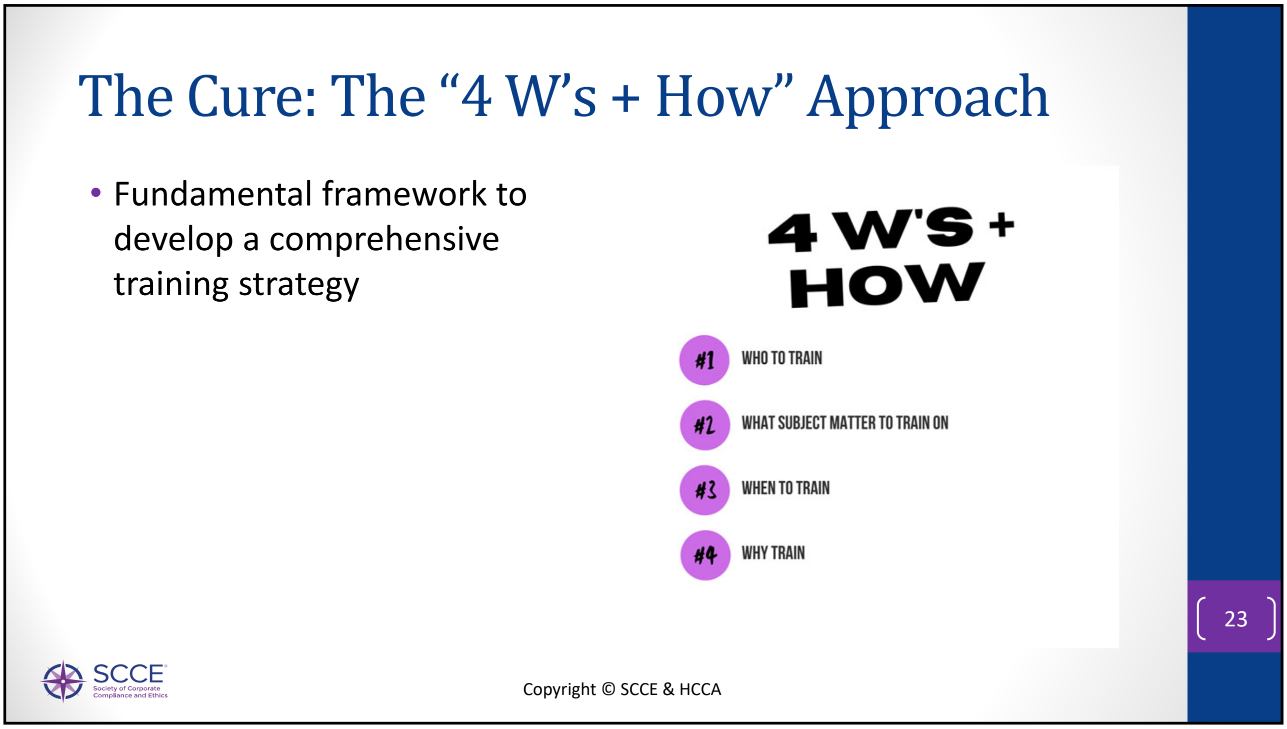
Polling Slide

- 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

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



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

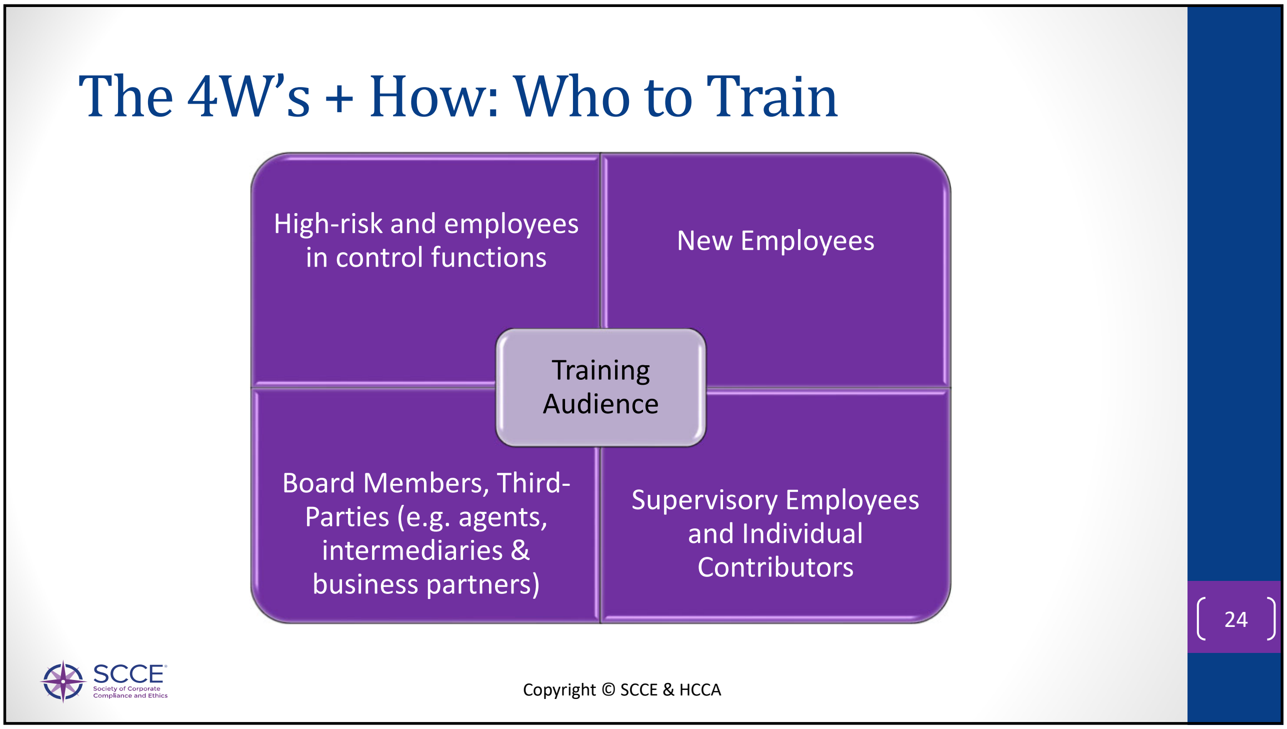
#4 WHY TRAIN

23

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

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)

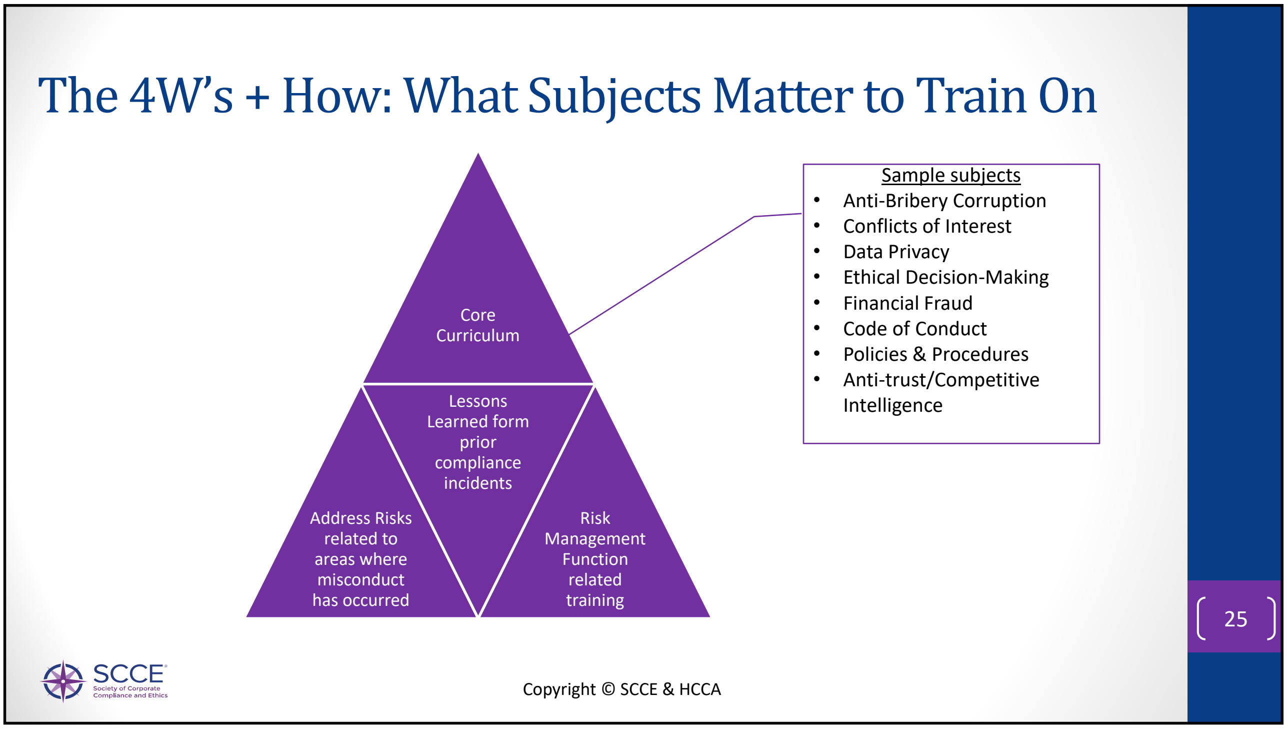
Supervisory Employees and Individual Contributors

24

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

24



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

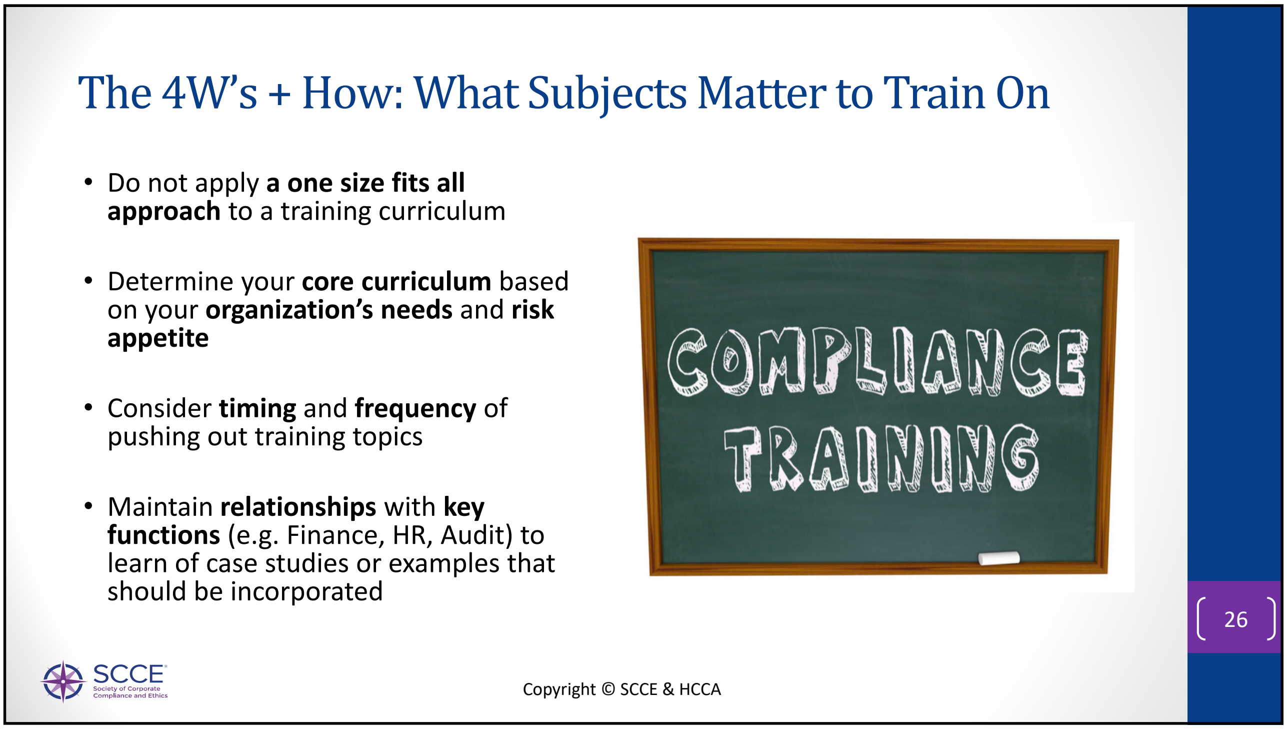
Core Curriculum

Lessons Learned form prior compliance incidents

Address Risks related to areas where misconduct has occurred

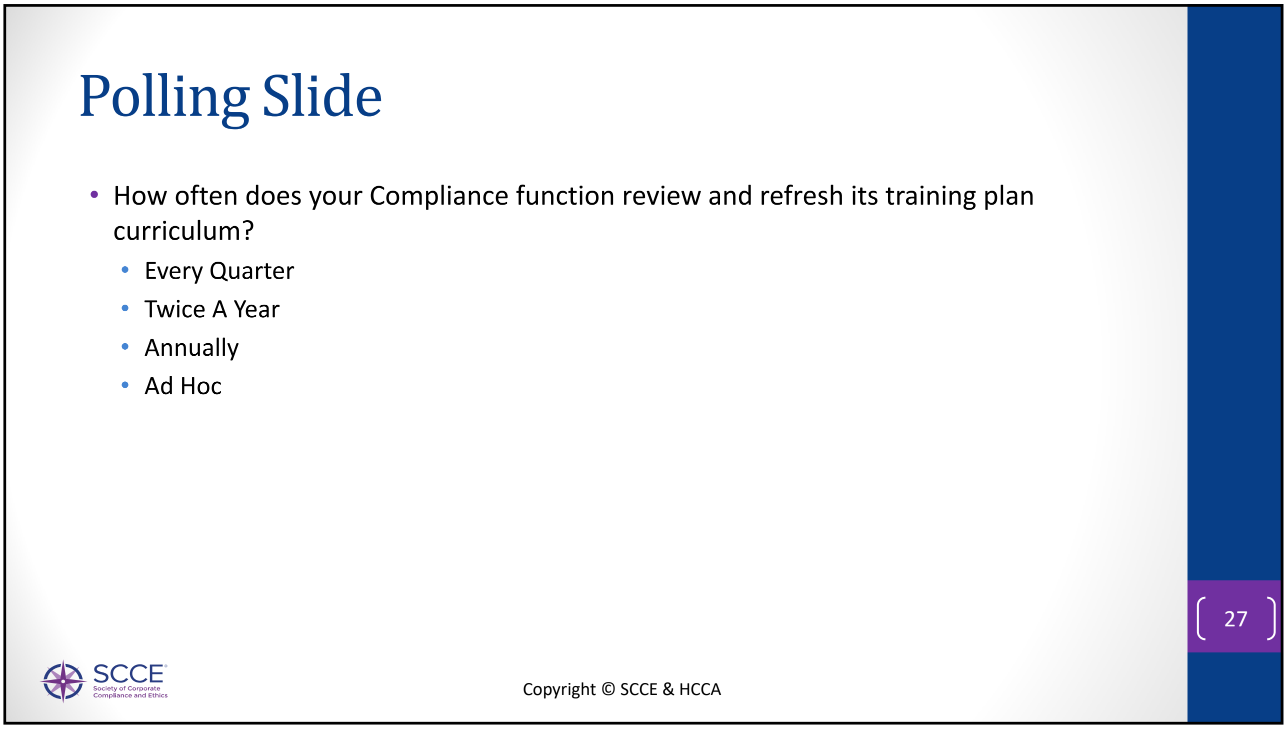
Risk Management Function related training

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



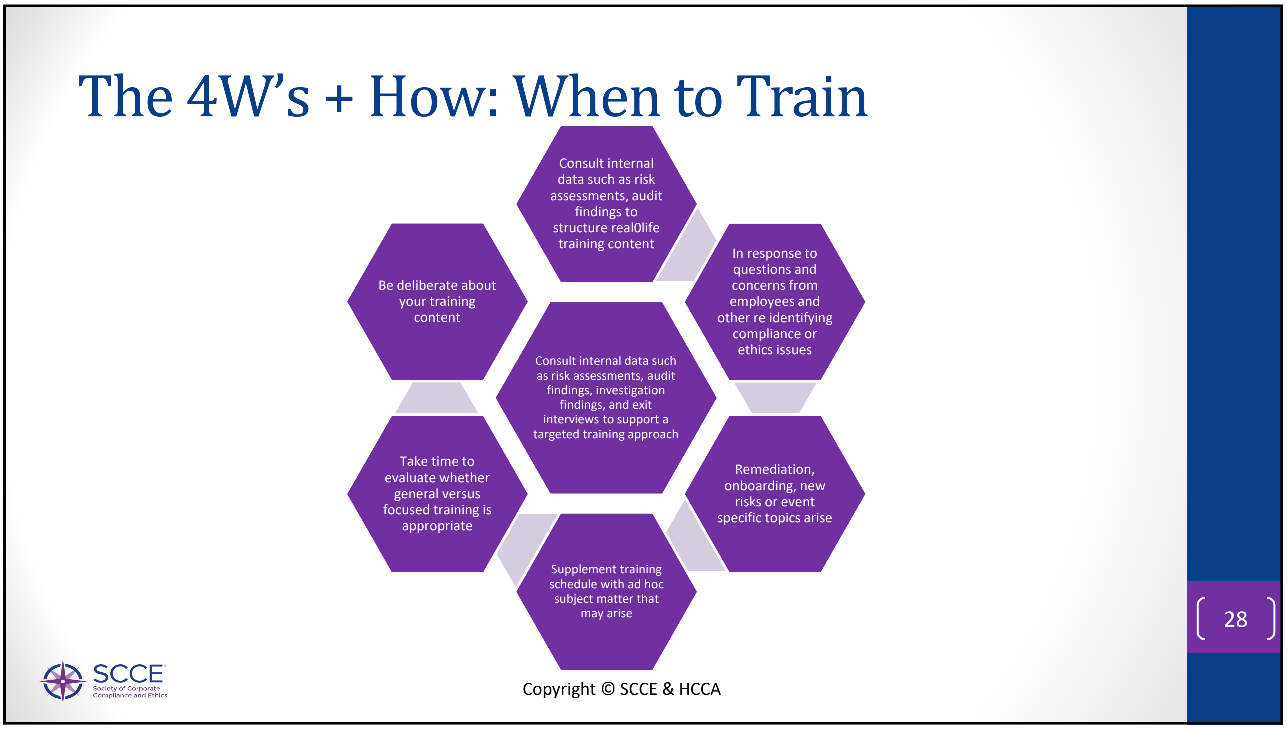
The 4W's + How: What Subjects Matter to Train On

- 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



Polling Slide

- How often does your Compliance function review and refresh its training plan curriculum?
  - Every Quarter
  - Twice A Year
  - Annually
  - Ad Hoc



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

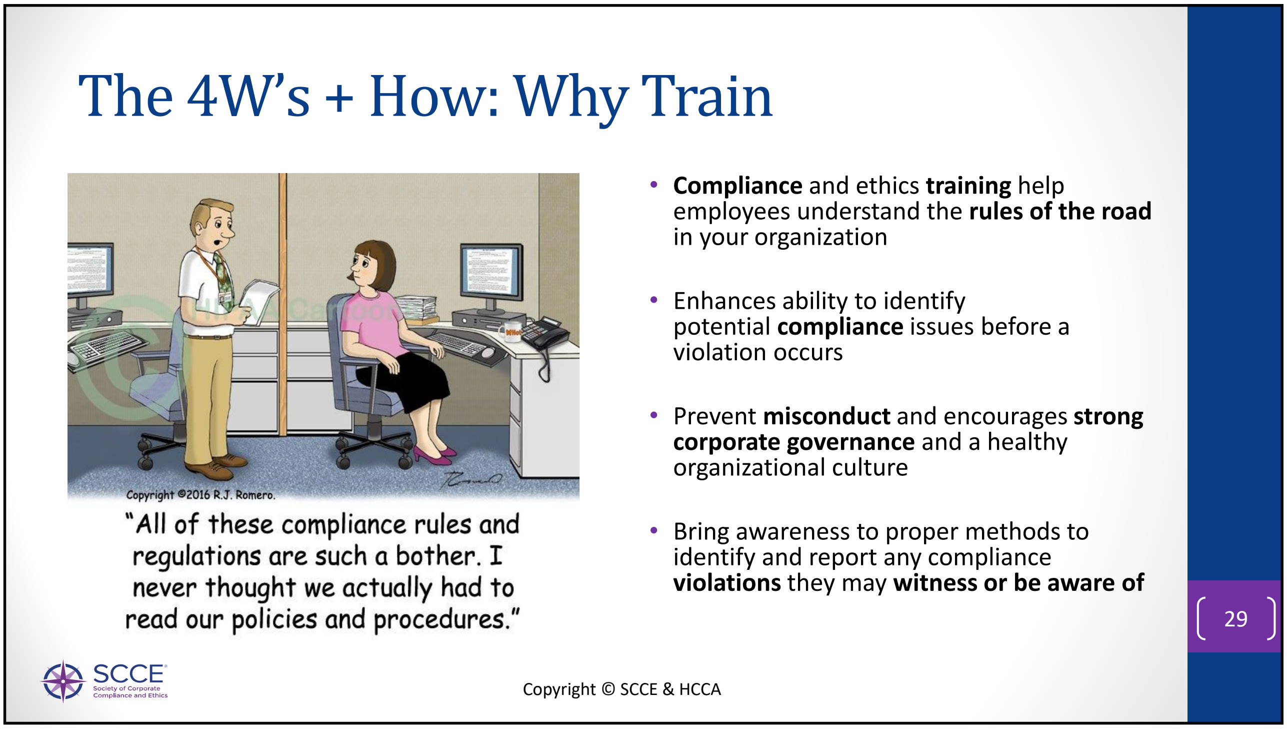
Be deliberate about your training content

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

Take time to evaluate whether general versus focused training is appropriate

Remediation, onboarding, new risks or event specific topics arise

Supplement training schedule with ad hoc subject matter that may arise



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."

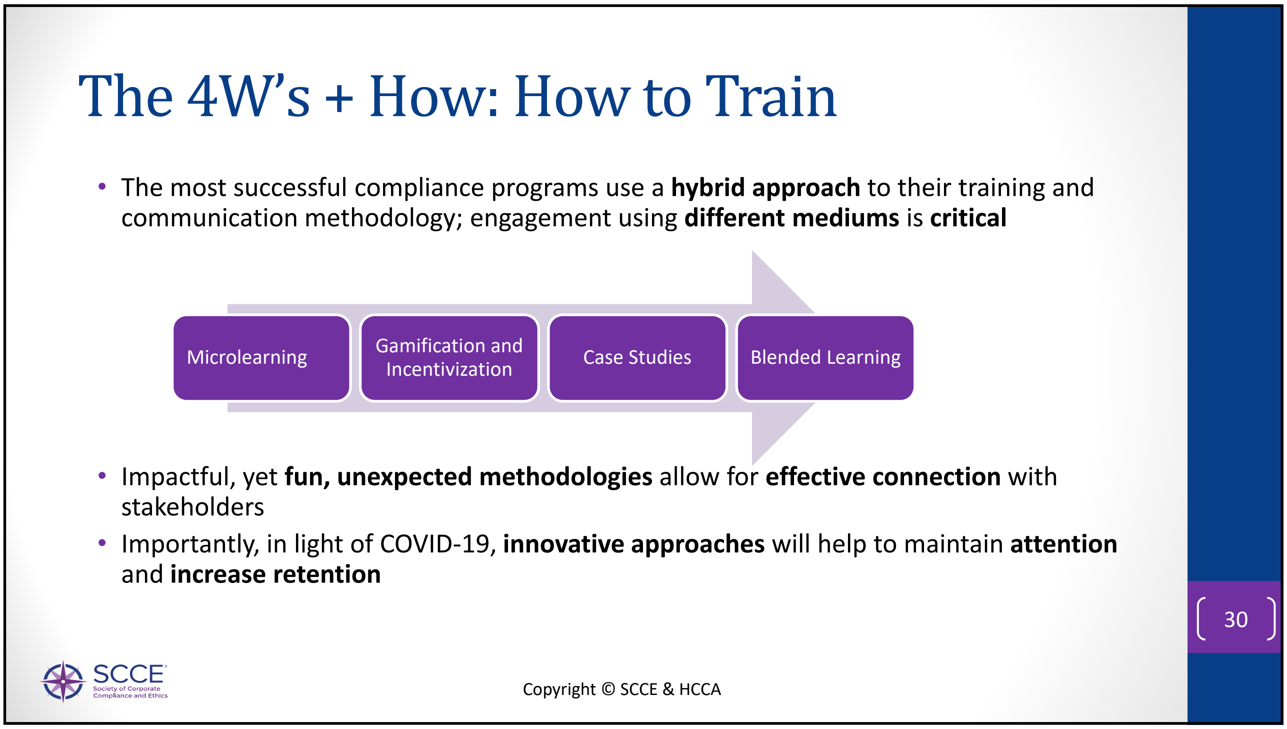
- **Compliance** and ethics **training** help employees understand the **rules of the road** in your organization
- Enhances ability to identify potential **compliance** issues before a violation occurs
- Prevent **misconduct** and encourages **strong corporate governance** and a healthy organizational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

29

SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

29



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**

30

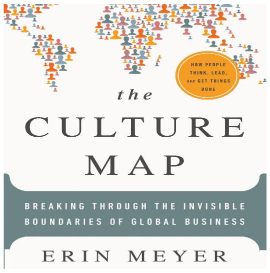
SCCE Society of Corporate Compliance and Ethics

Copyright © SCCE & HCCA

30

The 4W's + How: How to Train

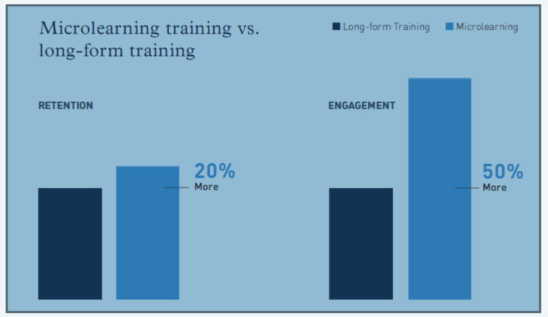
- Be mindful of **audience size**, level of sophistication and **subject matter expertise**
- Multinational organizations should consider **cultural nuances** and **native language** in message preparation


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**

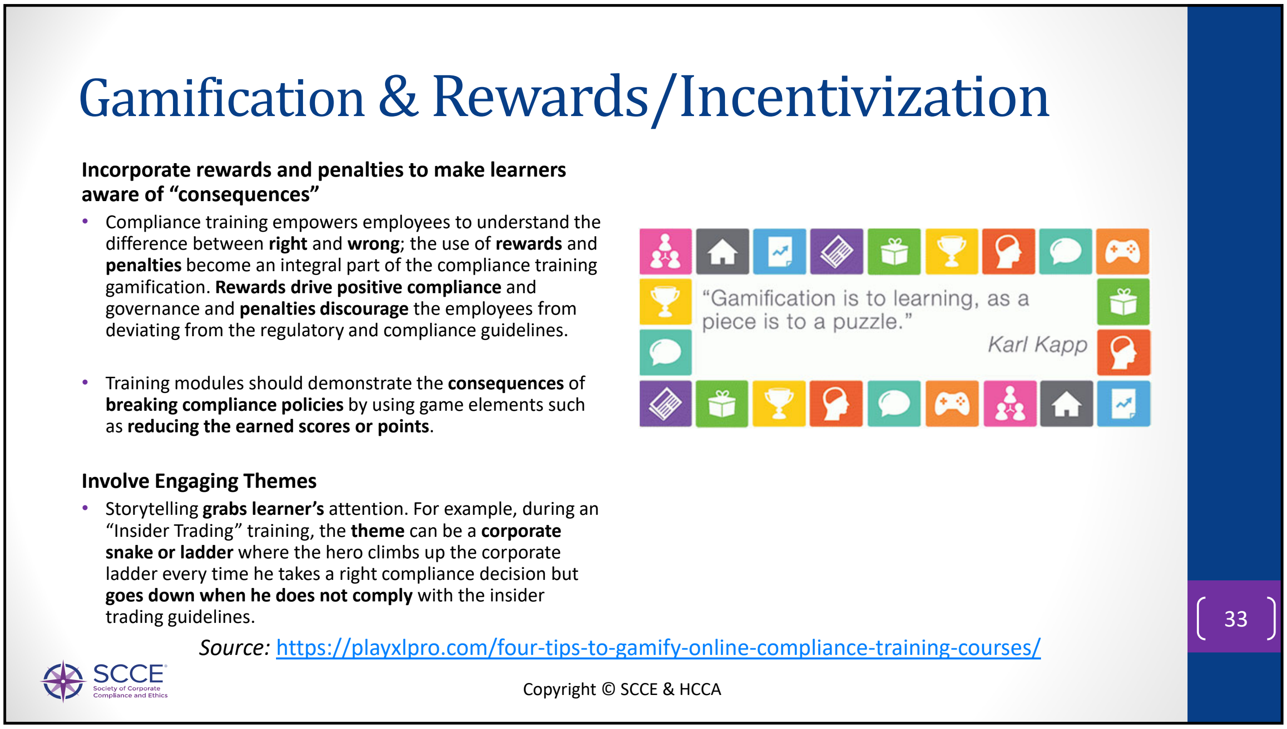
Microlearning

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



- 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** <u>**microlearning creates an enormous opportunity**</u> **for compliance trainers**

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



Gamification & Rewards/Incentivization

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

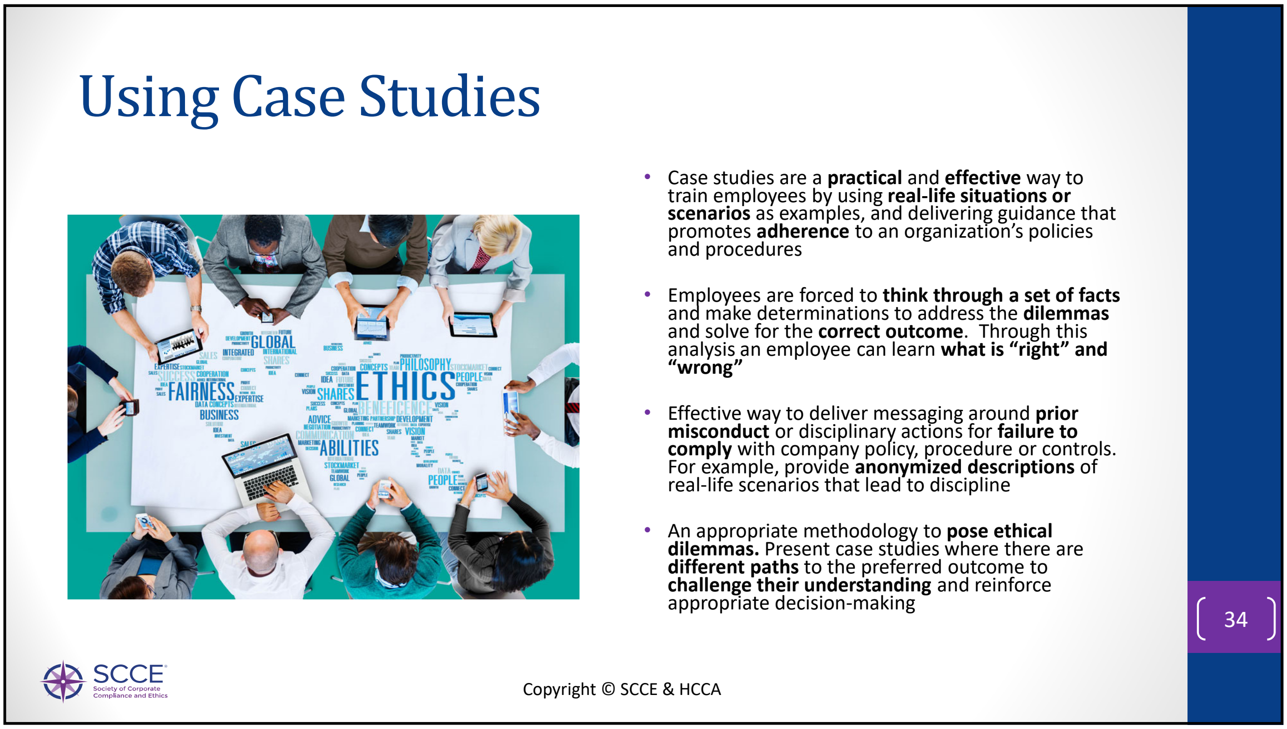
- Compliance training empowers employees to understand the difference between **right** and **wrong**; the use of **rewards** and **penalties** become an integral part of the compliance training gamification. **Rewards drive positive compliance** and governance and **penalties discourage** the employees 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 learner's** attention. For example, during an "Insider Trading" training, the **theme** can be a **corporate snake or ladder** where the hero climbs up the corporate ladder every time he takes a right compliance decision but **goes down when he does not comply** with the insider trading guidelines.

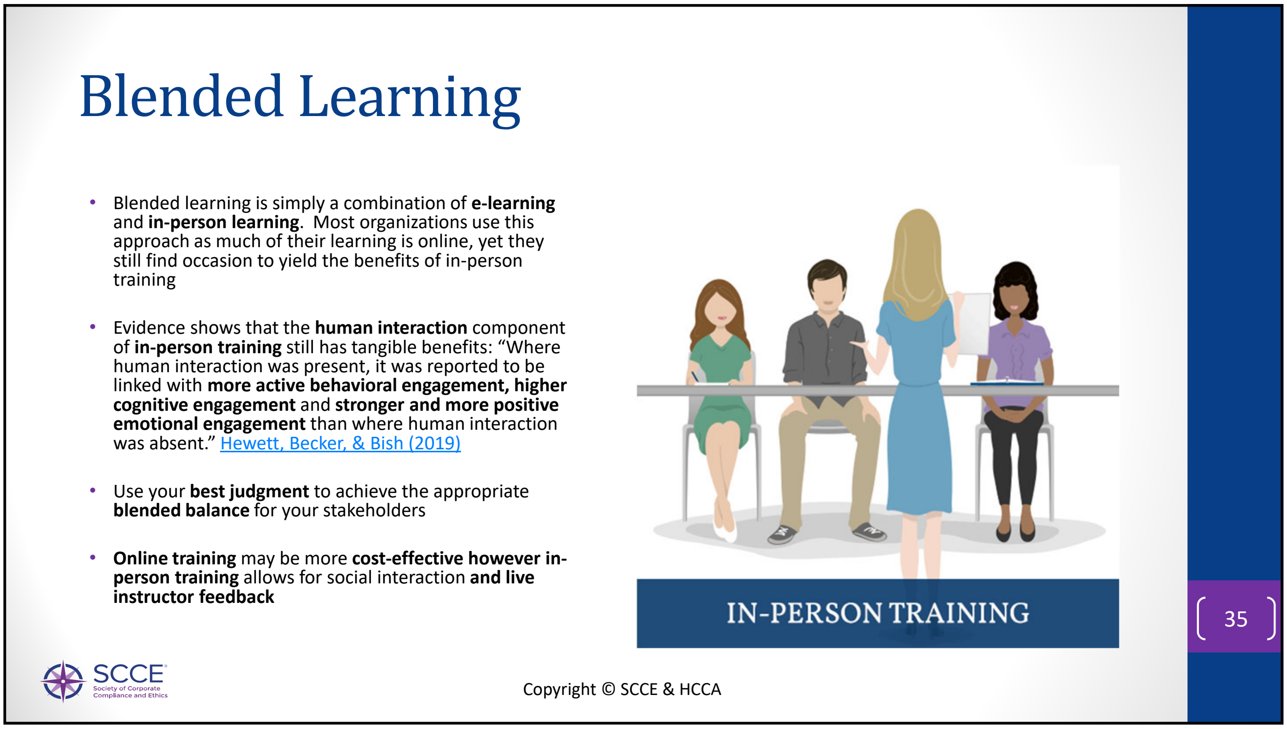
> "Gamification is to learning, as a piece is to a puzzle."
>
> *Karl Kapp*

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



Using Case Studies

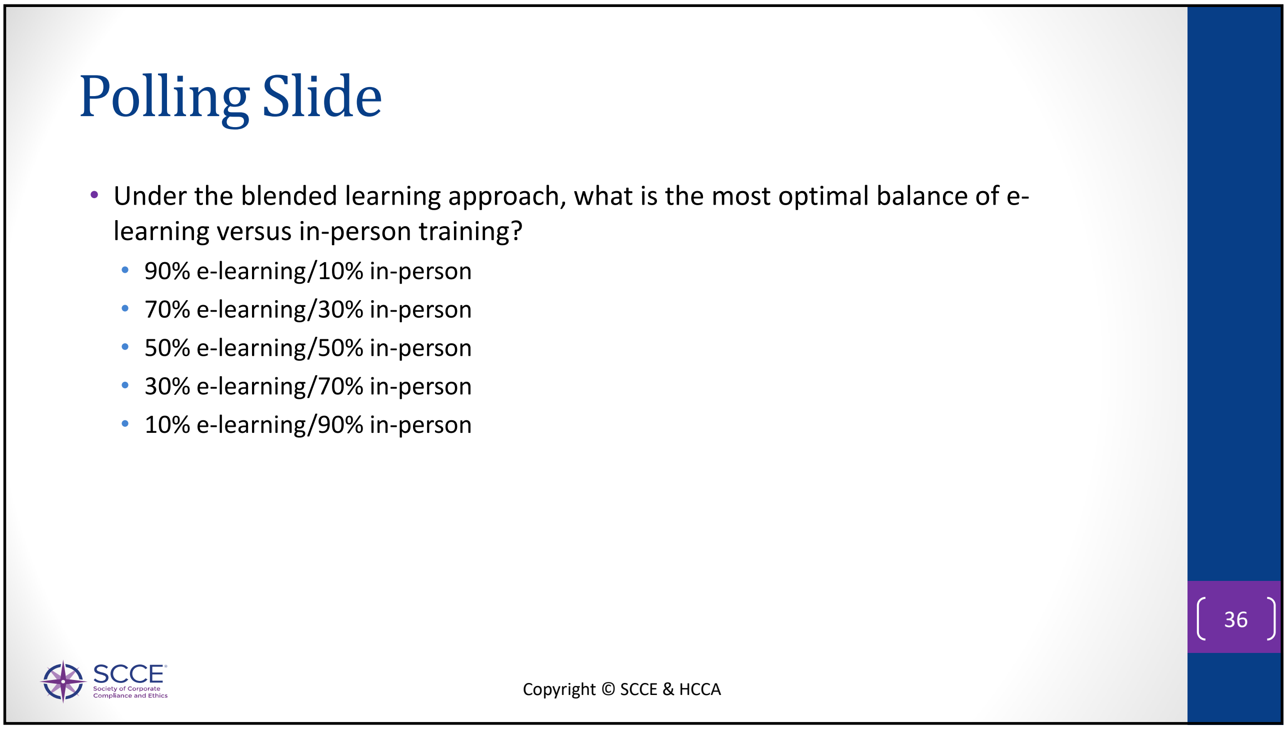
- Case studies are a **practical** and **effective** way to train employees by using **real-life situations or scenarios** as examples, and delivering guidance that promotes **adherence** to an organization's policies and procedures
- Employees are forced to **think through a set of facts** and make 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



Blended Learning

- Blended learning is simply a combination of **e-learning** and **in-person learning**. Most organizations use this approach as much of their learning is online, yet they still find occasion to yield the benefits of in-person training
- 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**

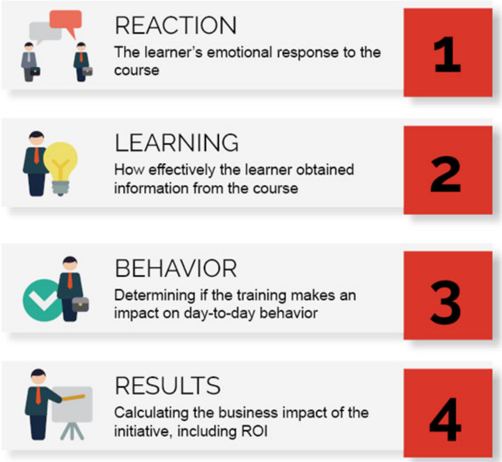
IN-PERSON TRAINING



Polling Slide

- Under the blended learning approach, what is the most optimal balance of e-learning versus in-person training?
  - 90% e-learning/10% in-person
  - 70% e-learning/30% in-person
  - 50% e-learning/50% in-person
  - 30% e-learning/70% in-person
  - 10% e-learning/90% in-person

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

37

37

38

38

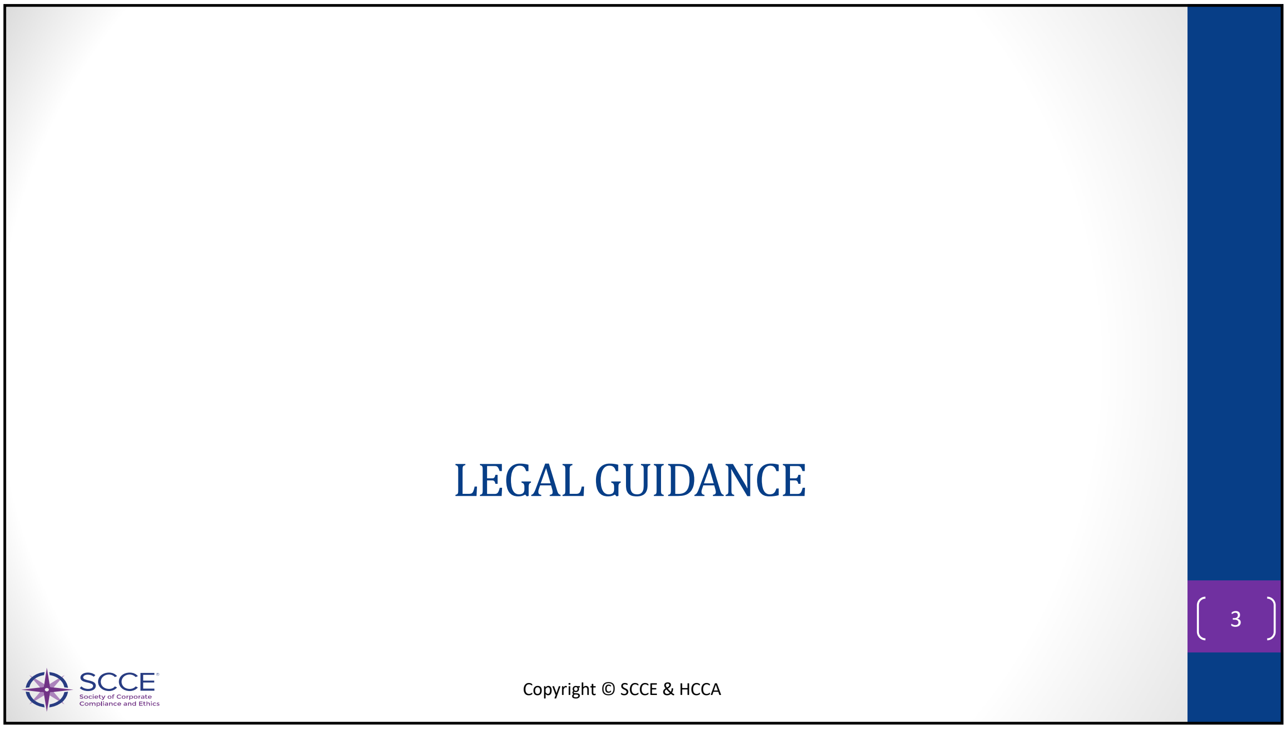
SCCE Compliance & Ethics Essentials Workshop

Program Improvement

Rebecca Walker
Kaplan & Walker LLP

Content

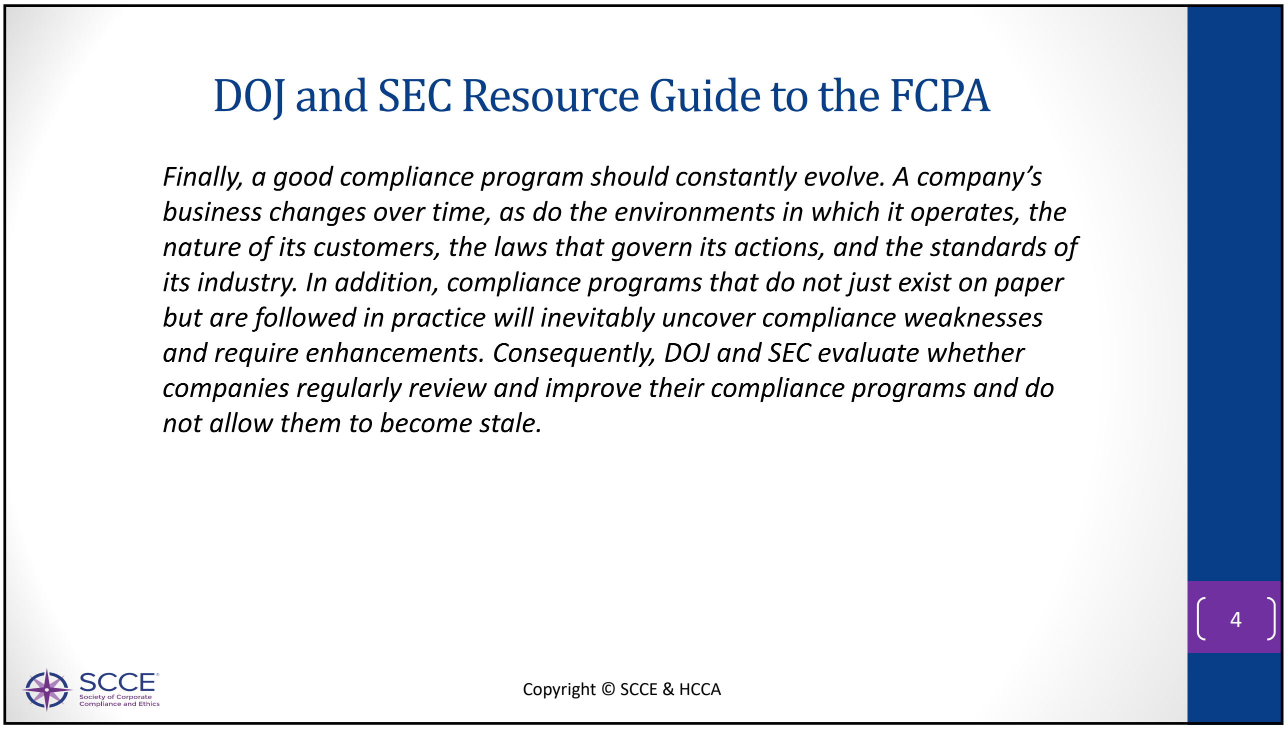
- Legal guidance
- Program self-assessments
- Involvement of internal audit
- Third party assessments



LEGAL GUIDANCE

3

Copyright © SCCE & HCCA

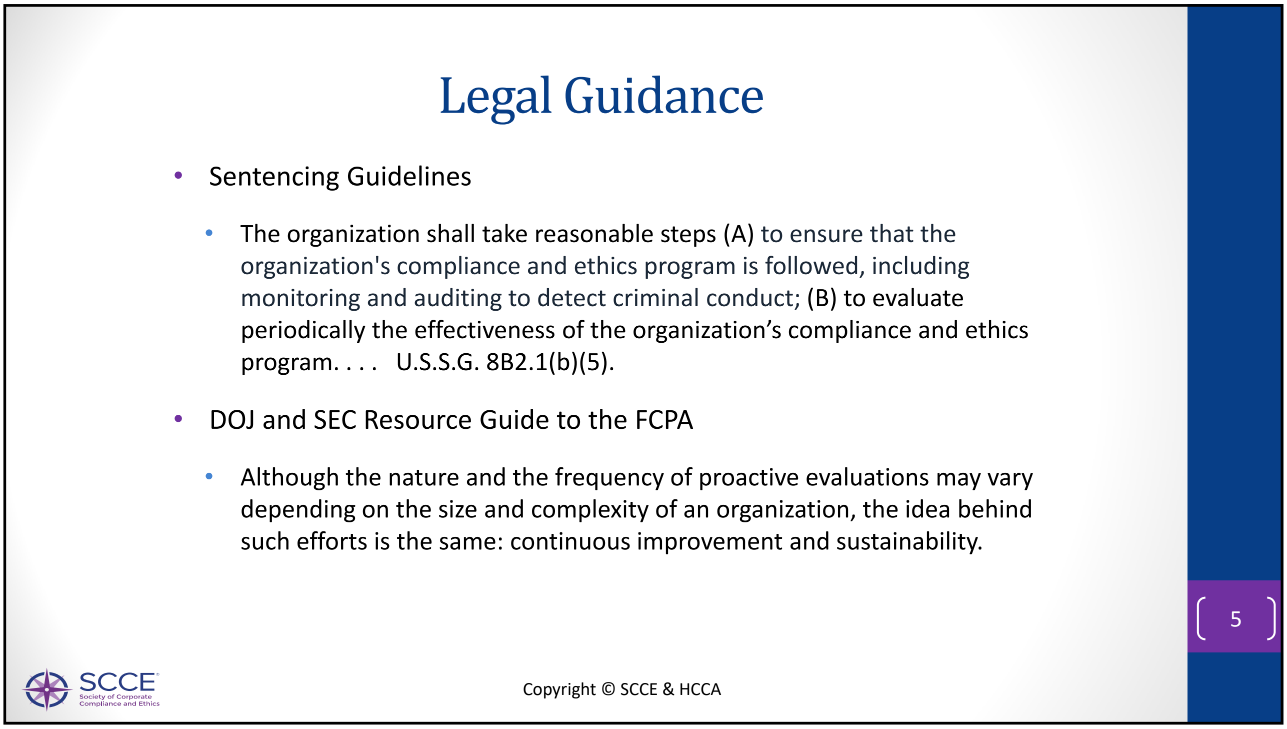


DOJ and SEC Resource Guide to the FCPA

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.

4

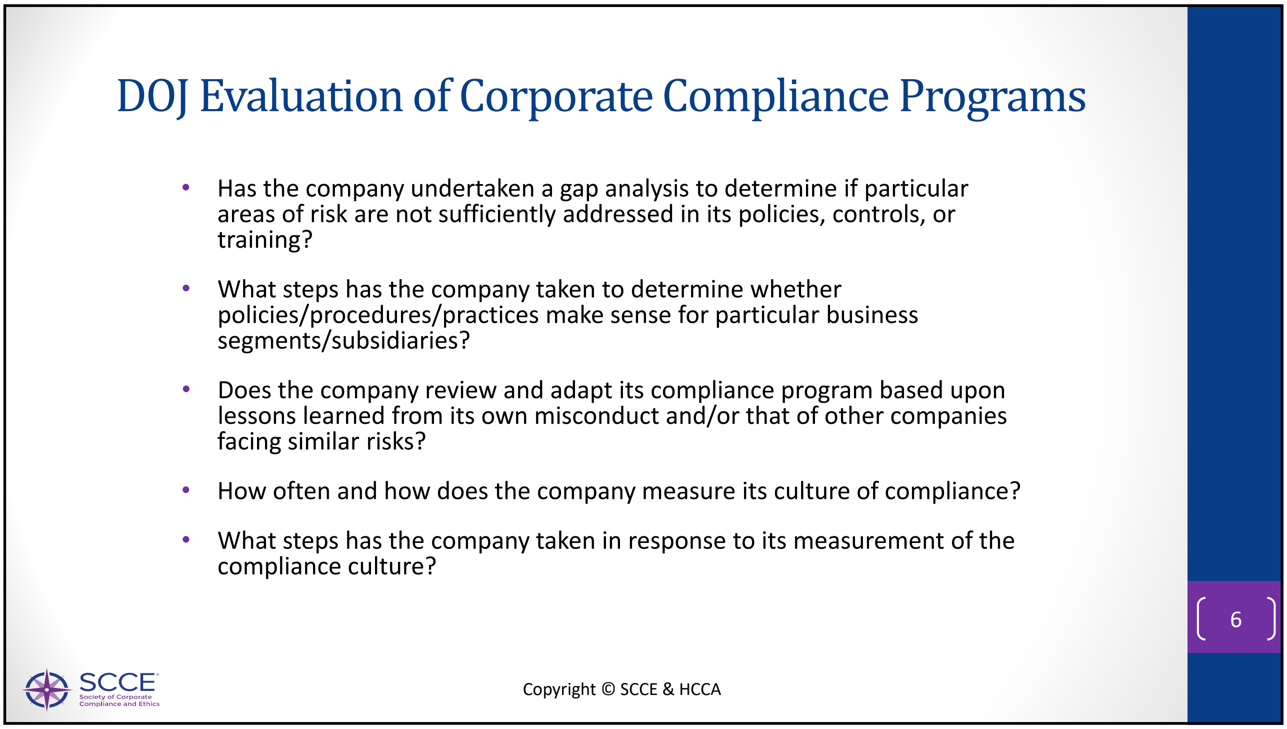
Copyright © SCCE & HCCA



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.

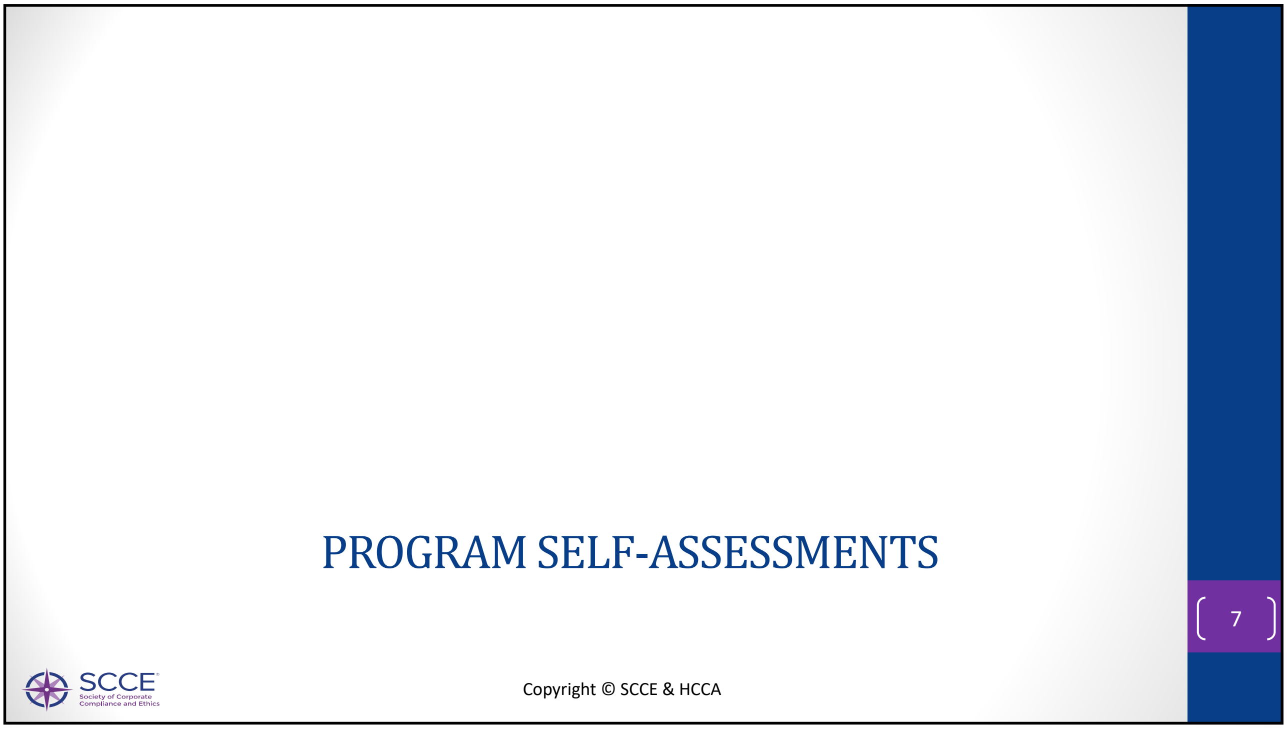
5



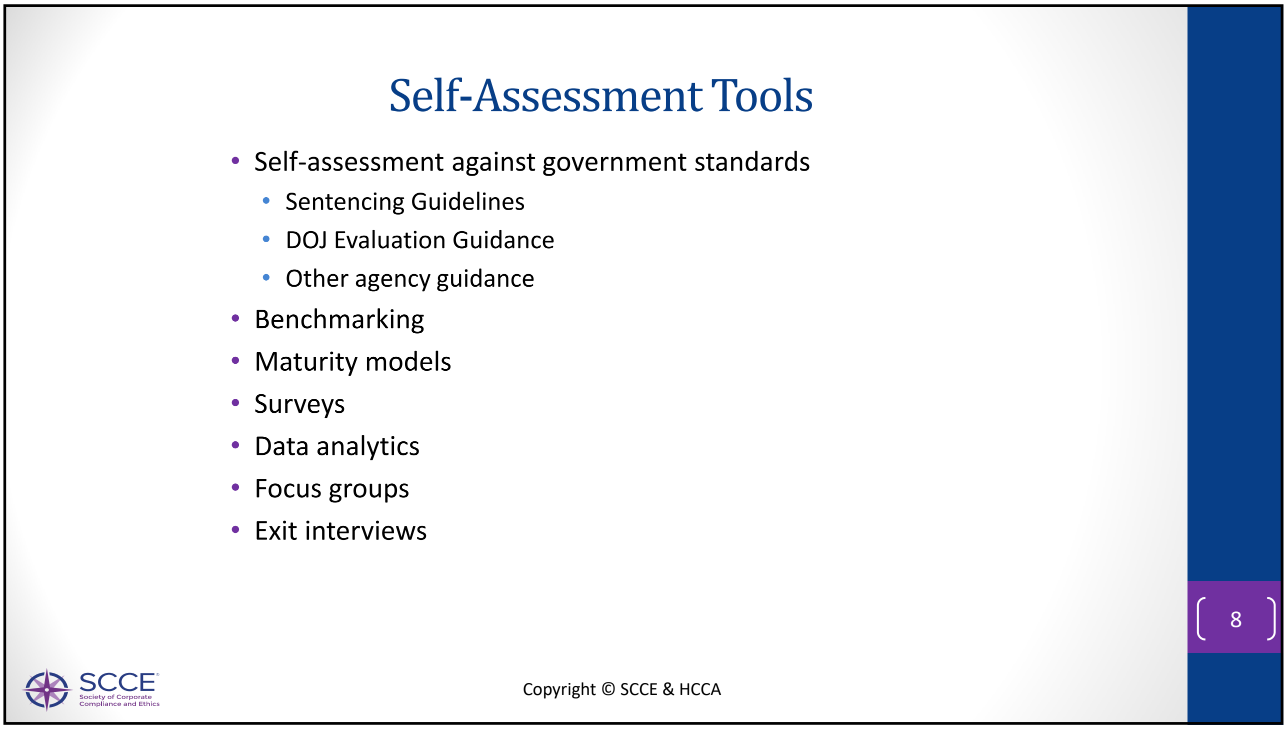
DOJ Evaluation of Corporate Compliance Programs

- 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?

6

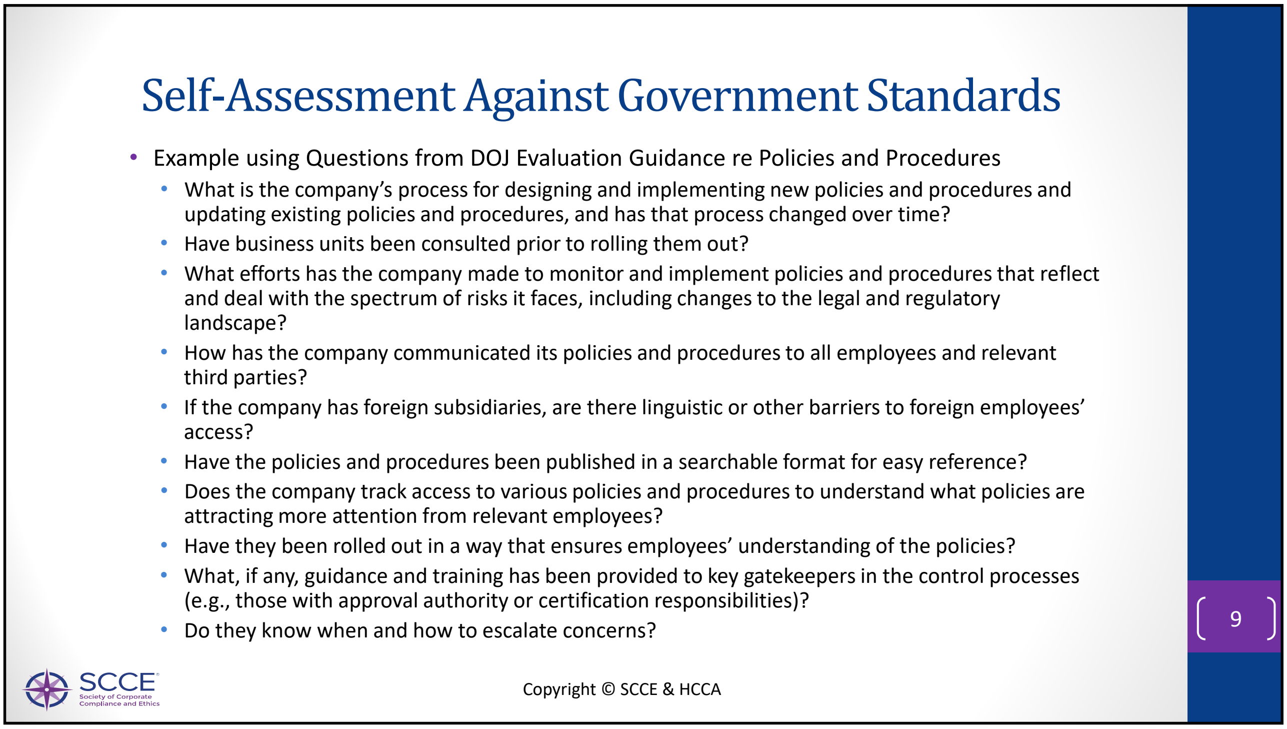


PROGRAM SELF-ASSESSMENTS



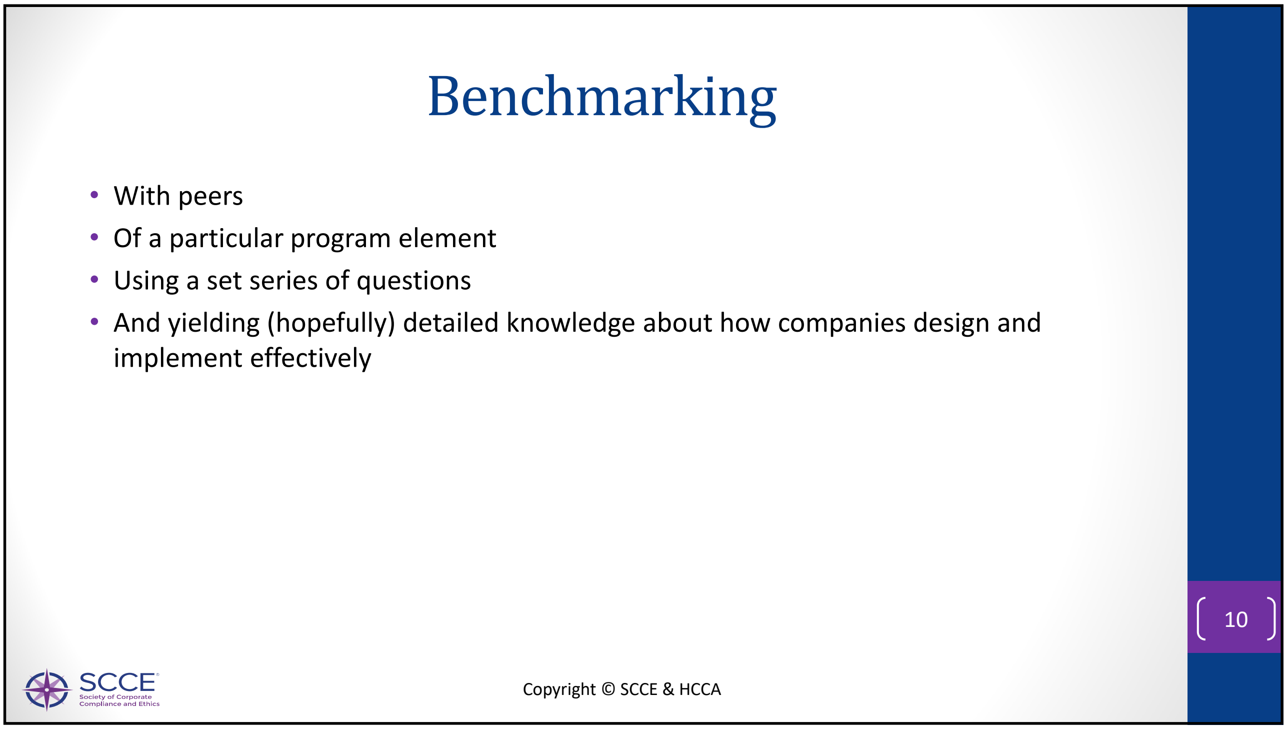
Self-Assessment Tools

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



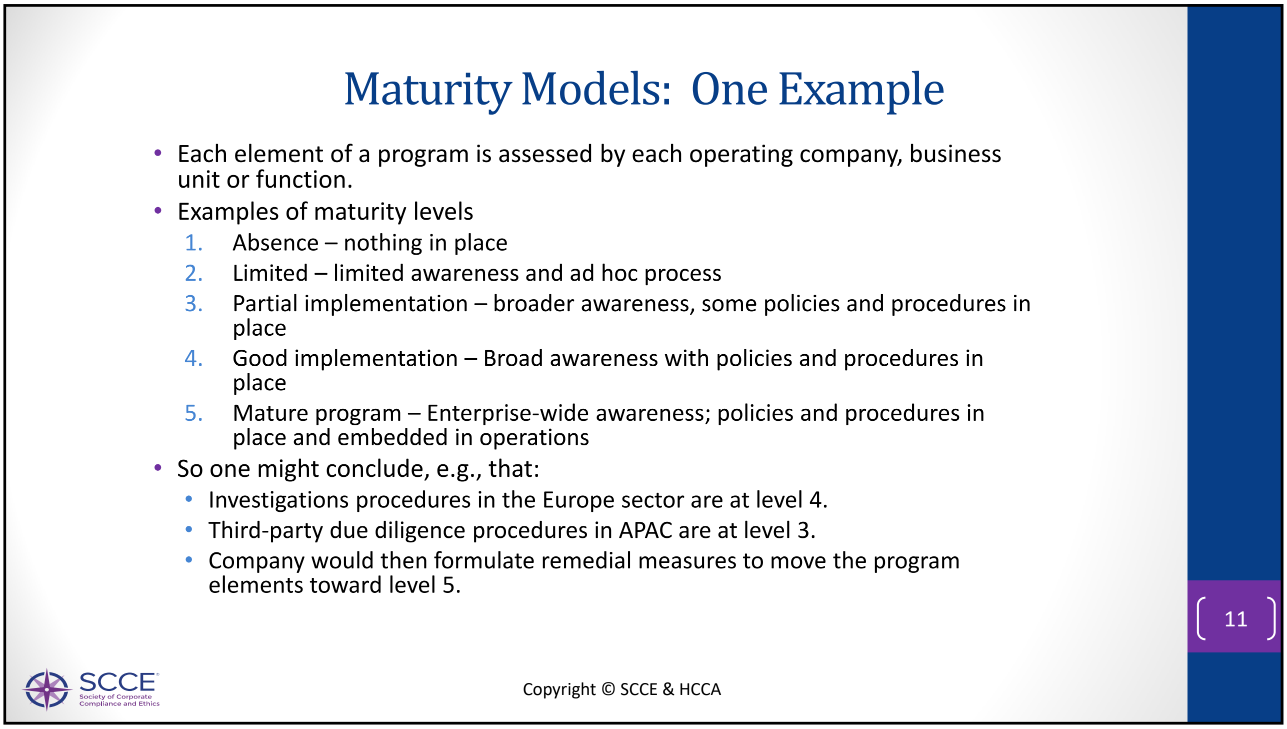
Self-Assessment Against Government Standards

- 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?



Benchmarking

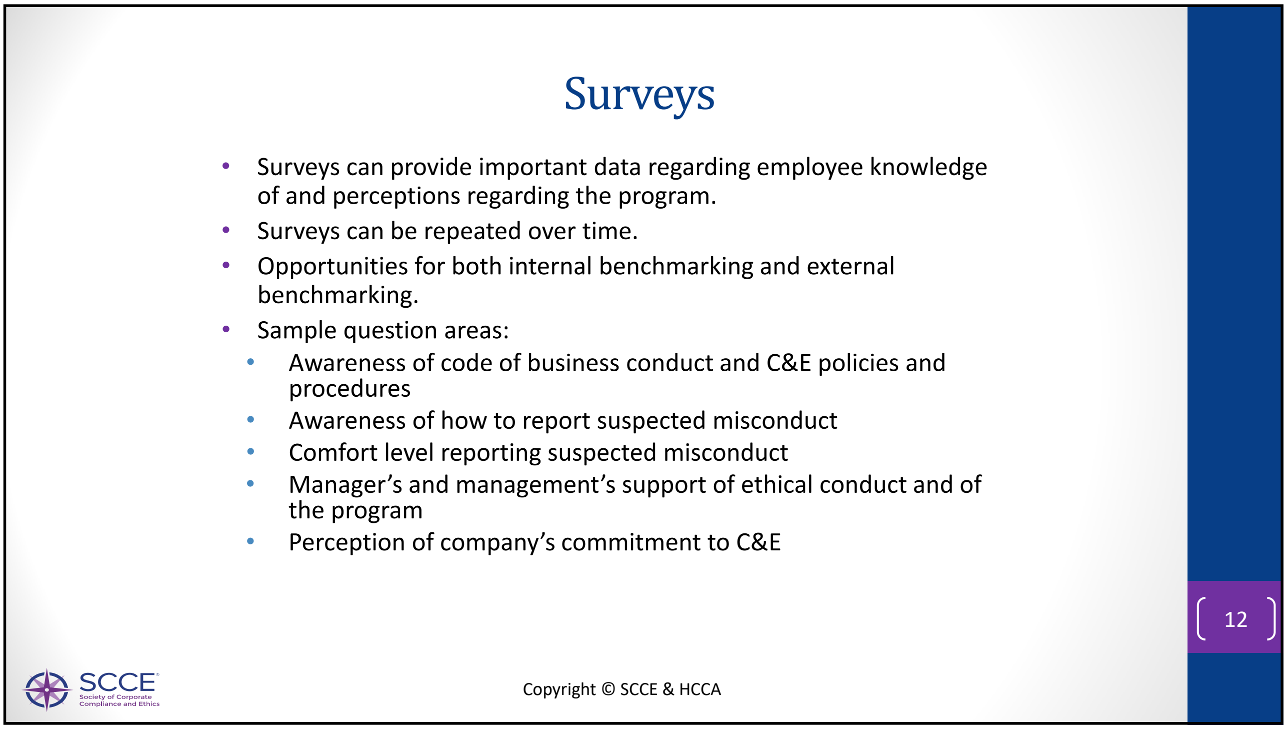
- With peers
- Of a particular program element
- Using a set series of questions
- And yielding (hopefully) detailed knowledge about how companies design and implement effectively



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 program – 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.

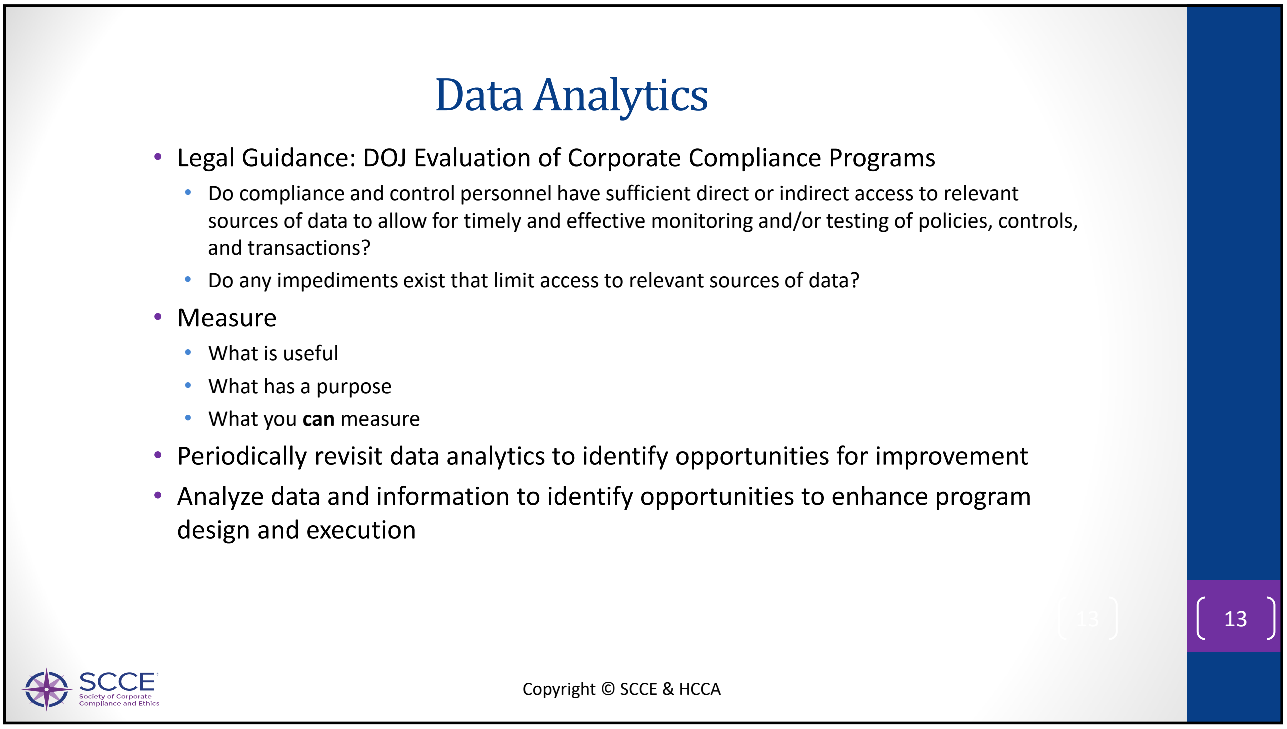
11



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

12

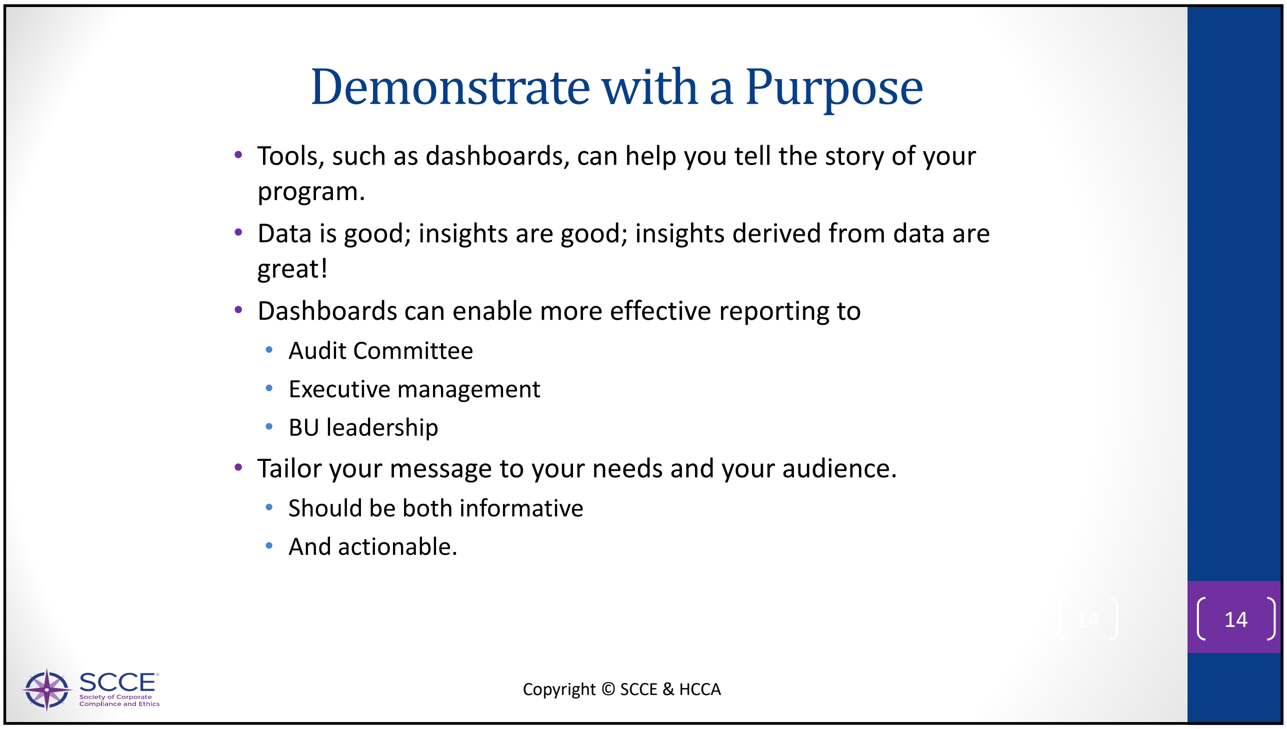


Data Analytics

- 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

13

13

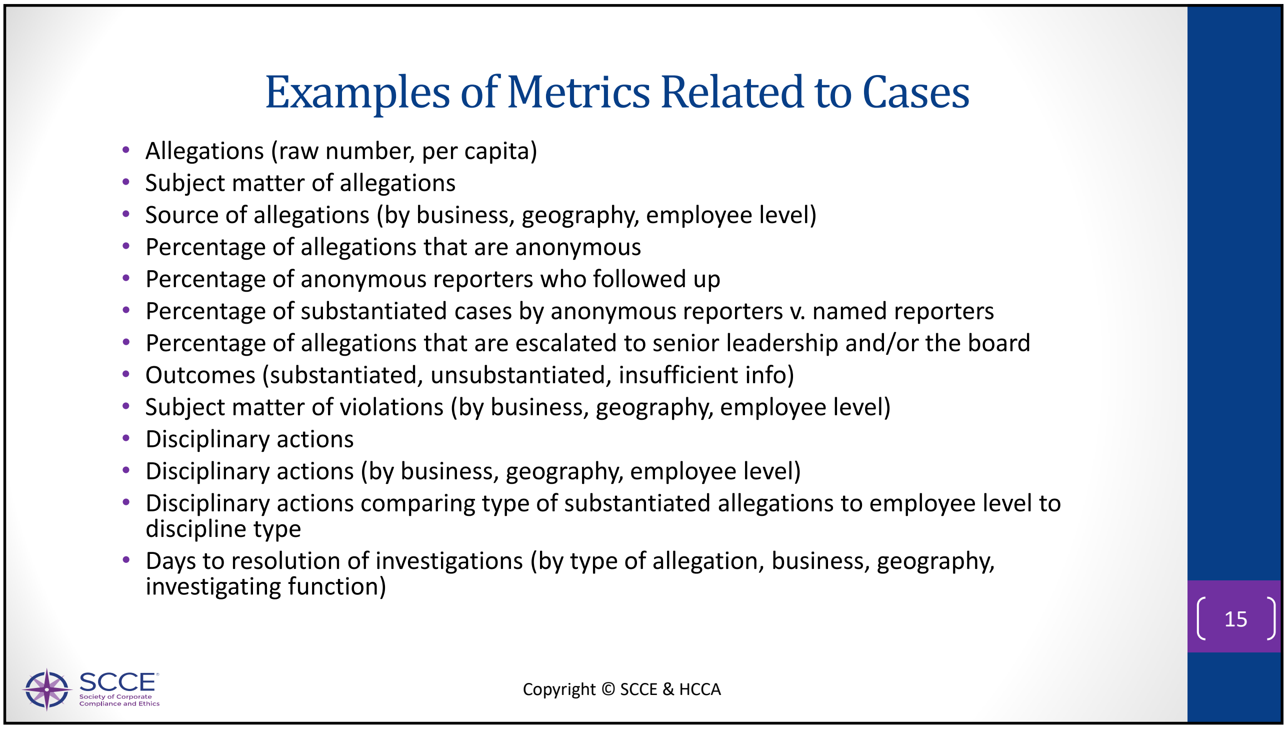


Demonstrate with a Purpose

- Tools, such as dashboards, can help you tell the story of your program.
- Data is good; insights are good; insights derived from data are great!
- Dashboards can enable more effective reporting to
  - Audit Committee
  - Executive management
  - BU leadership
- Tailor your message to your needs and your audience.
  - Should be both informative
  - And actionable.

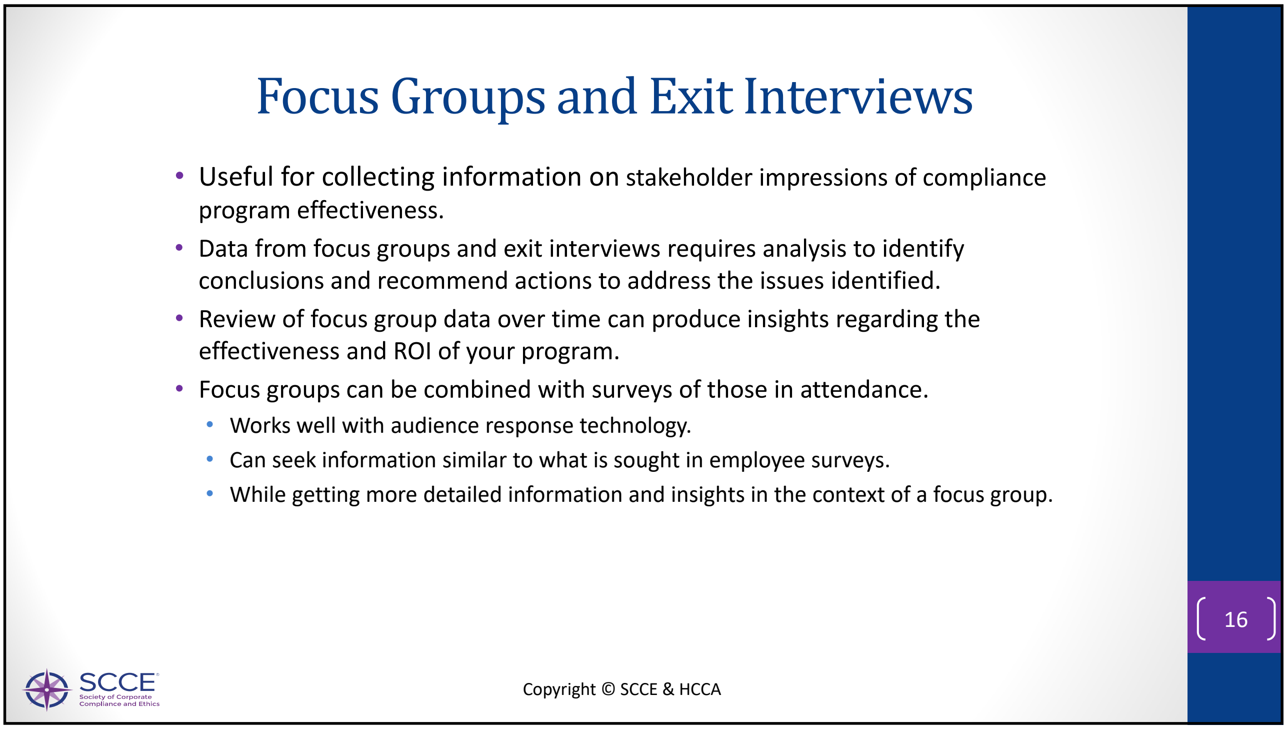
14

14



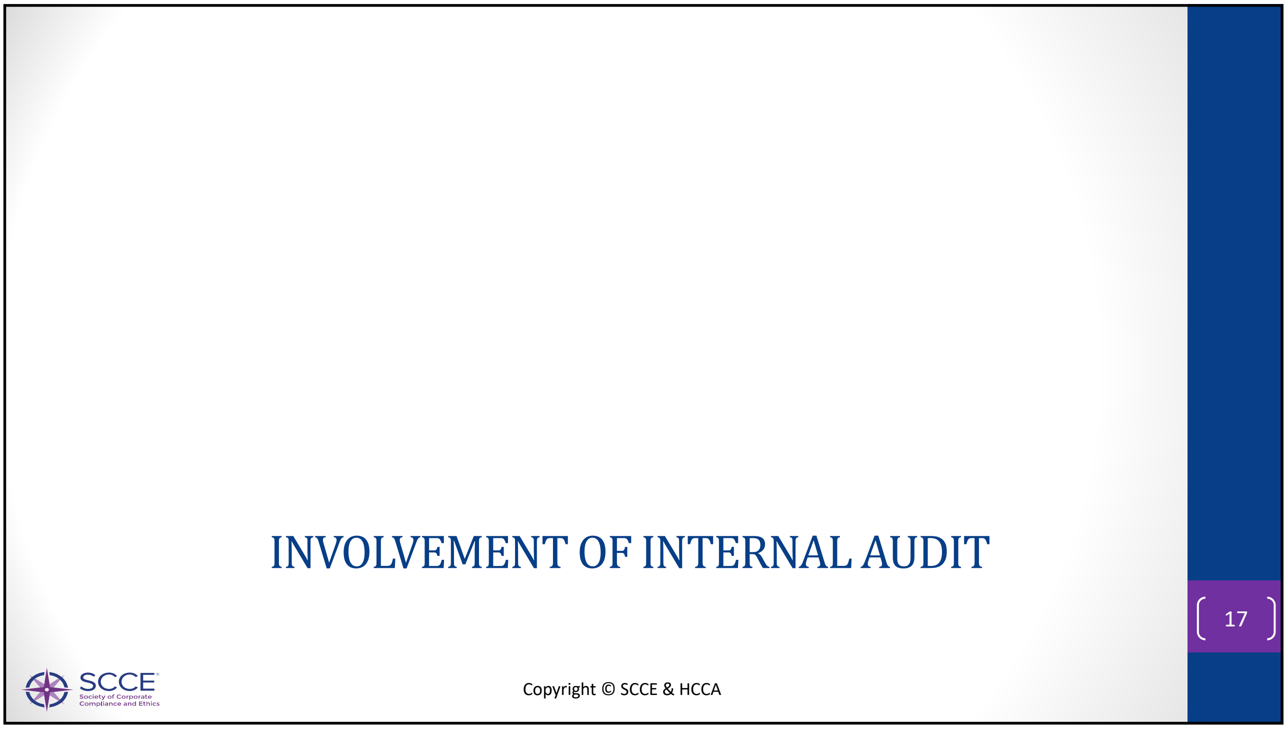
Examples of Metrics Related to Cases

- 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)

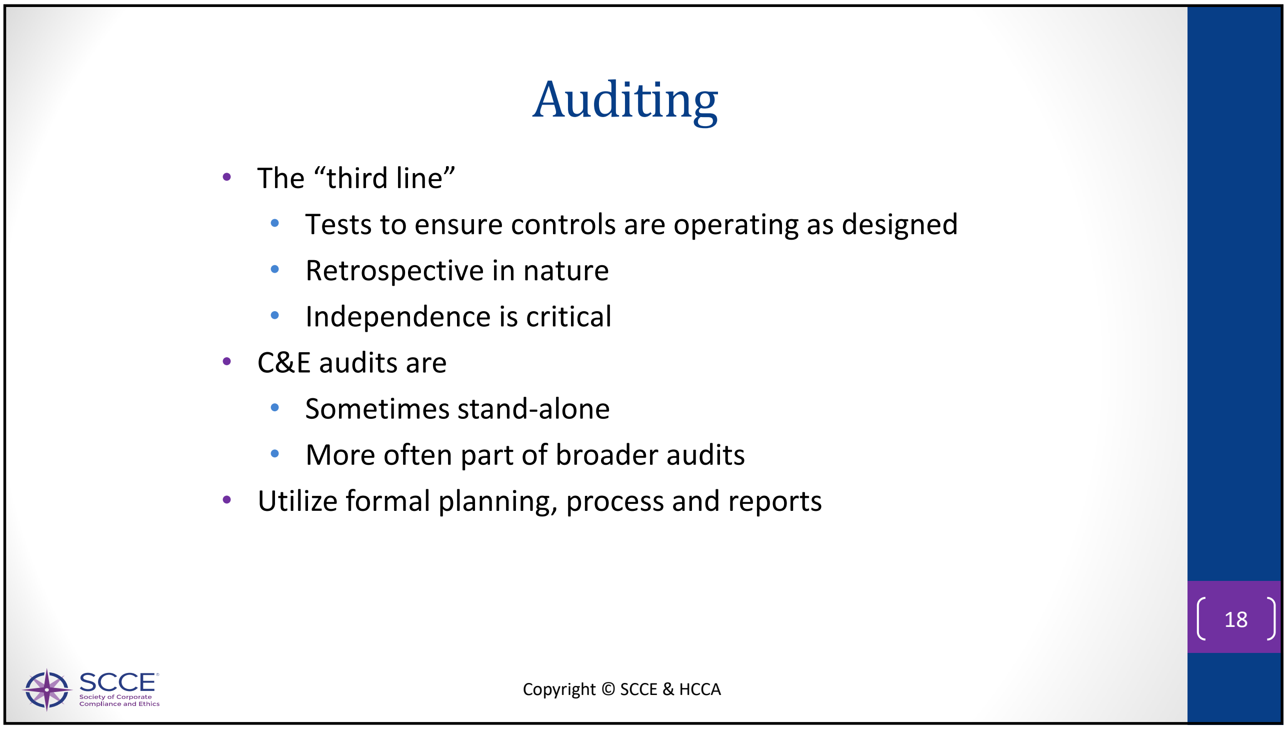


Focus Groups and Exit Interviews

- 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.

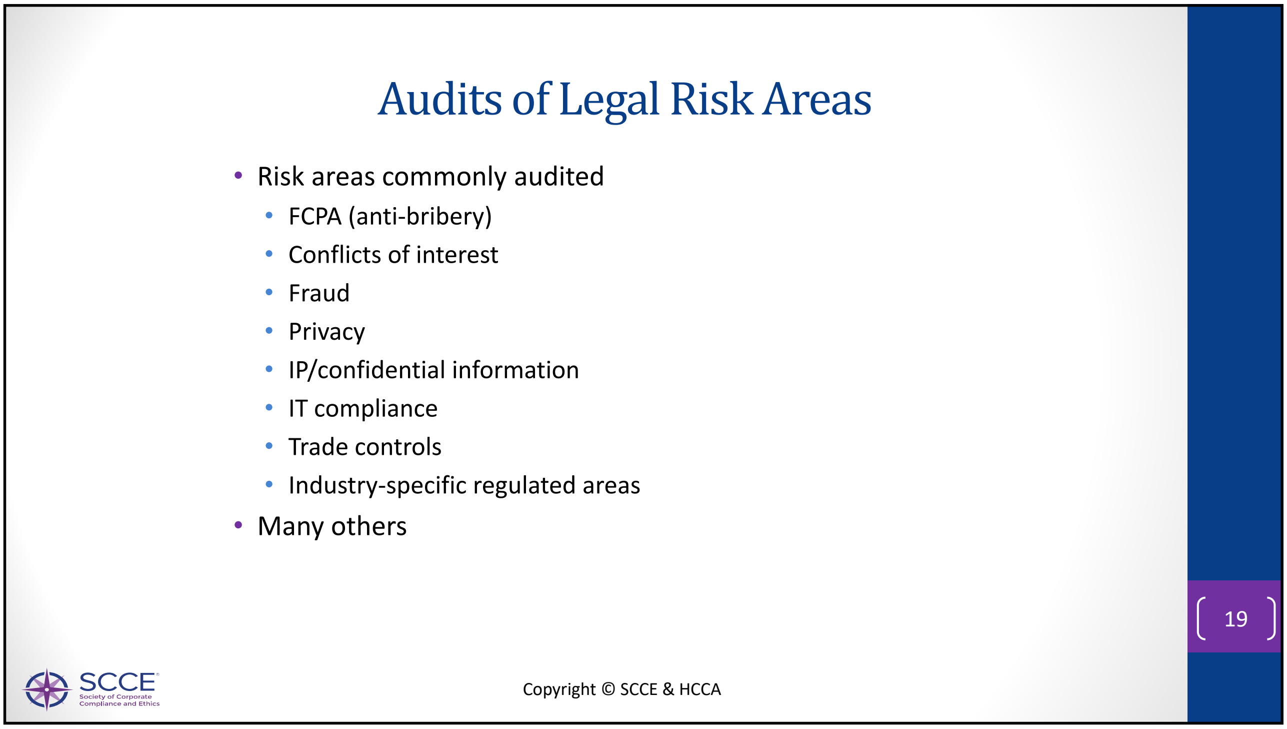


INVOLVEMENT OF INTERNAL AUDIT



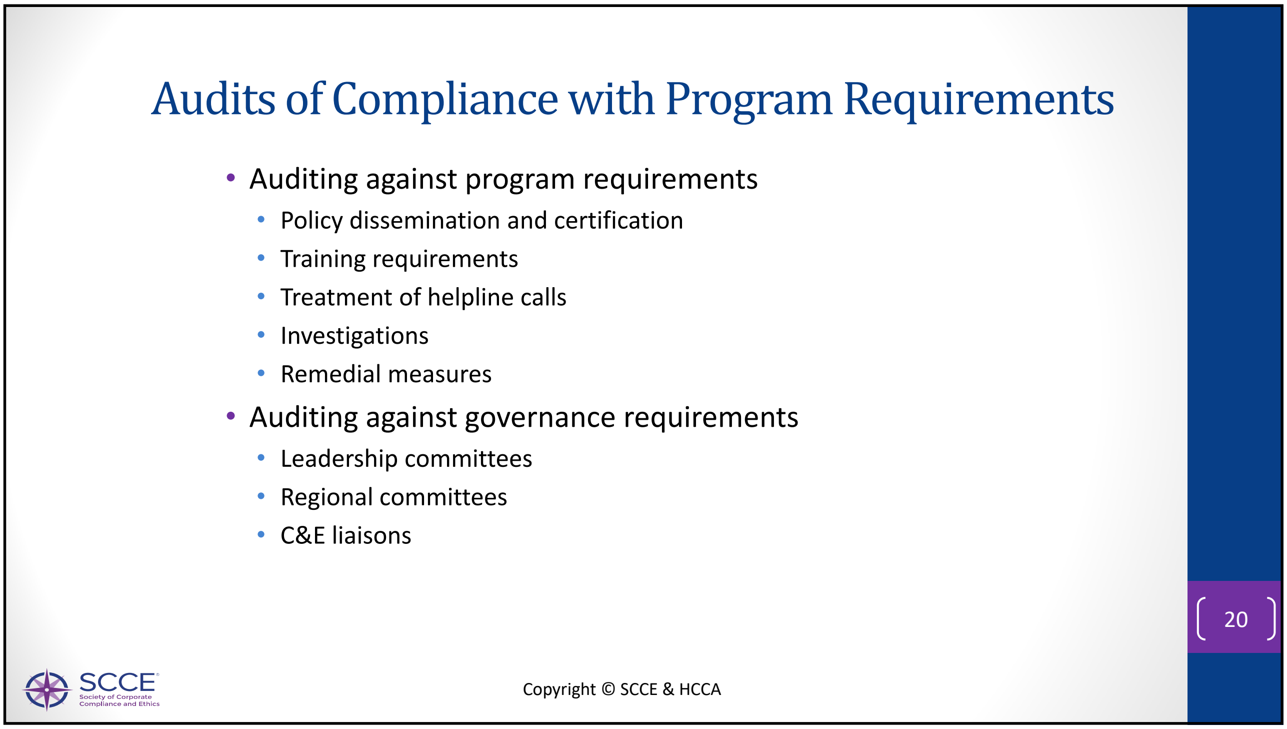
Auditing

- 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



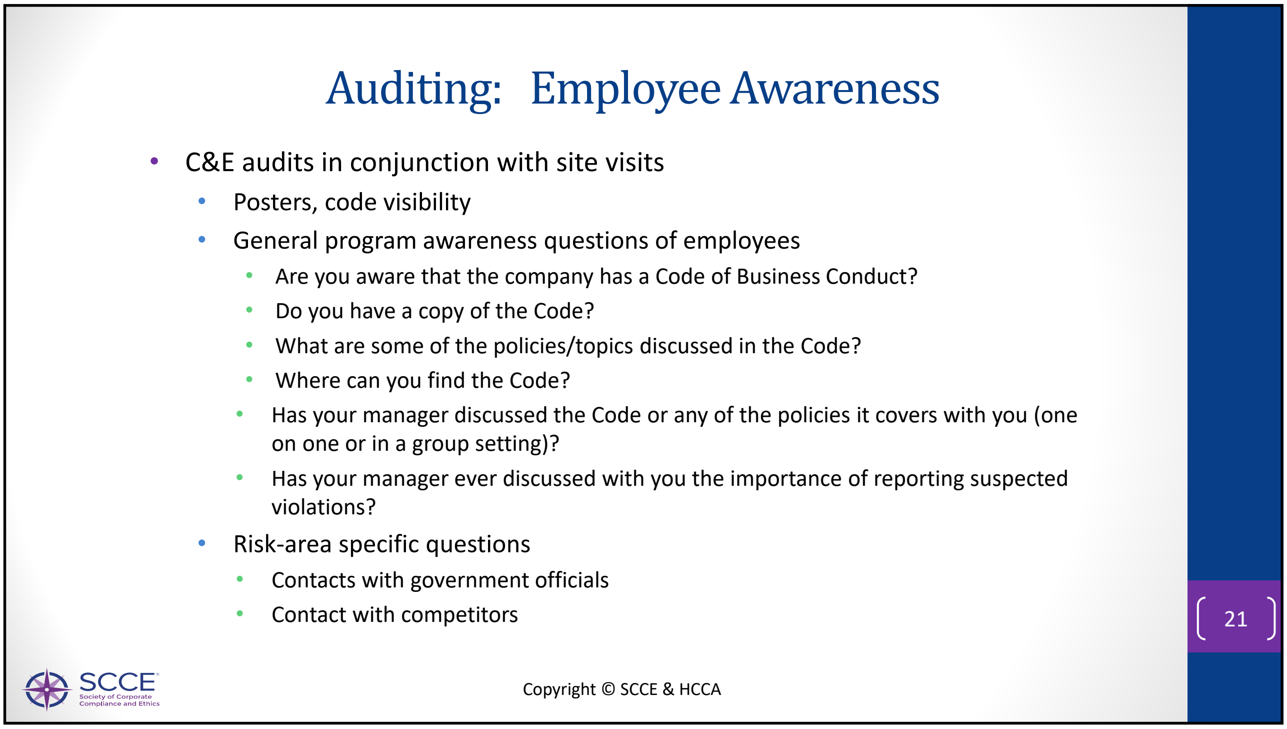
Audits of Legal Risk Areas

- 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



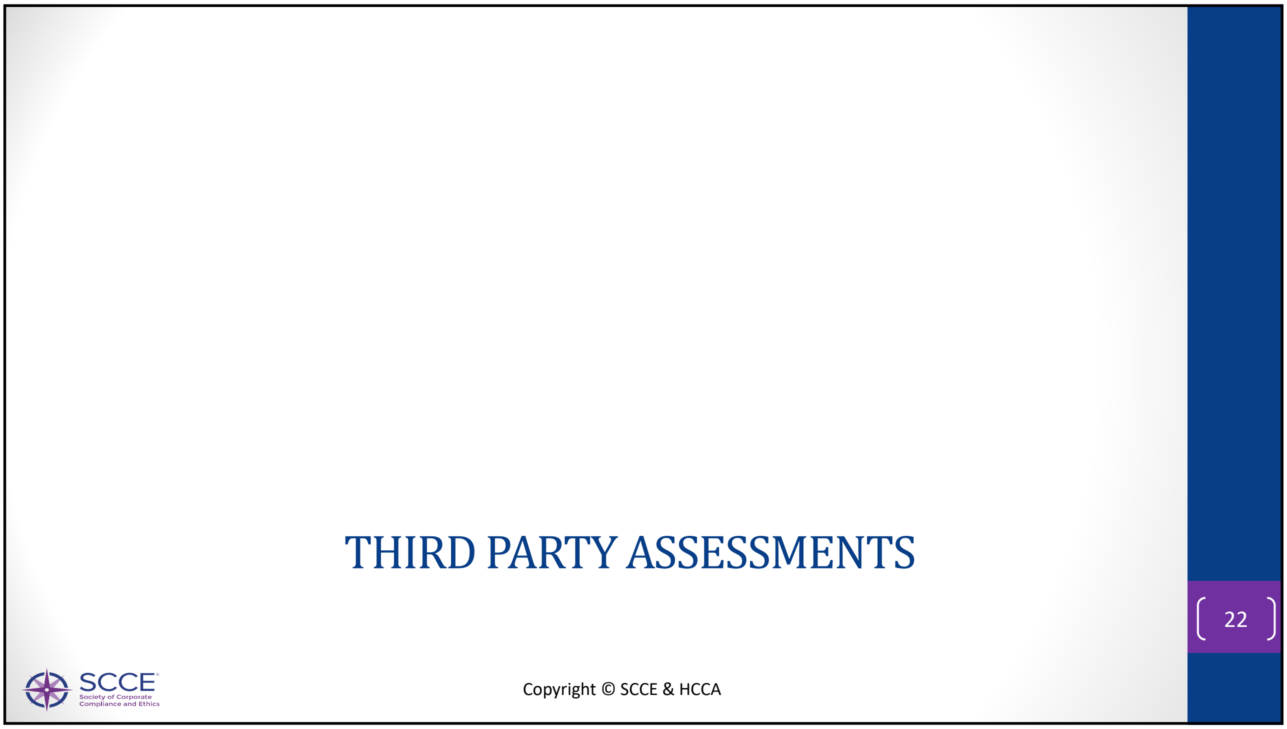
Audits of Compliance with Program Requirements

- 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

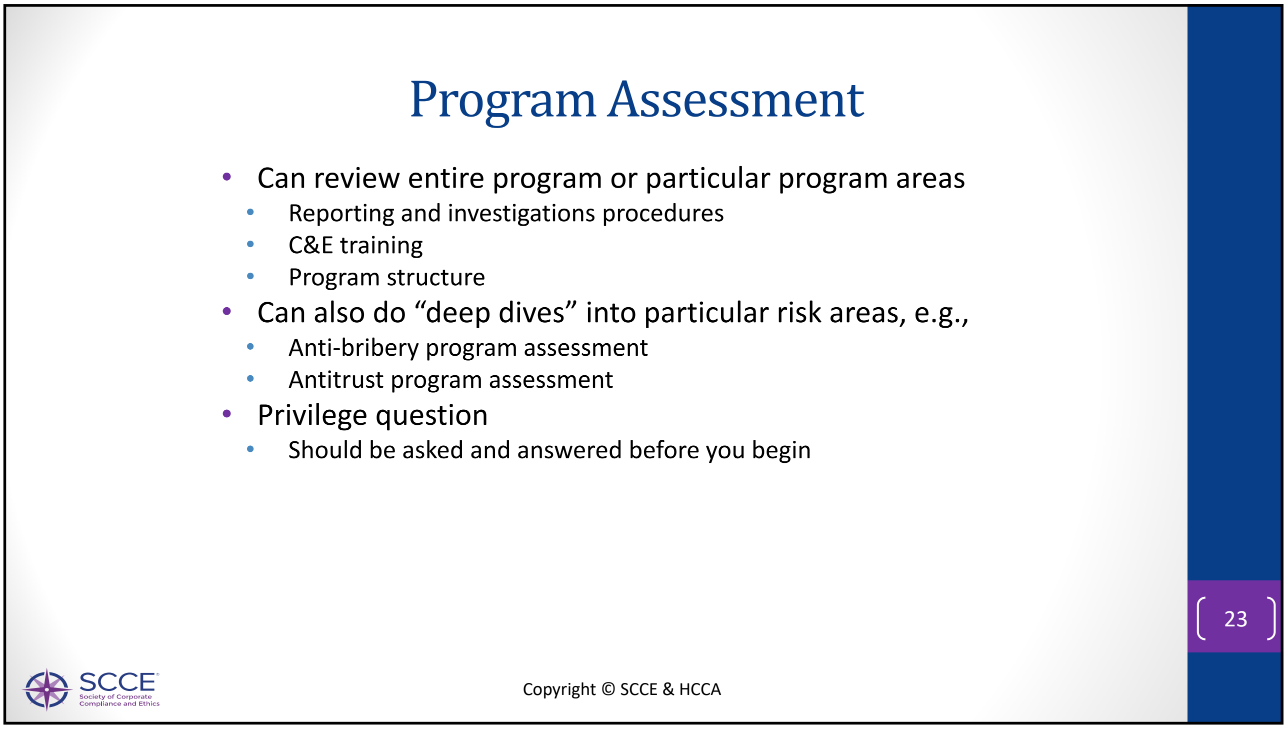


Auditing: Employee Awareness

- 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



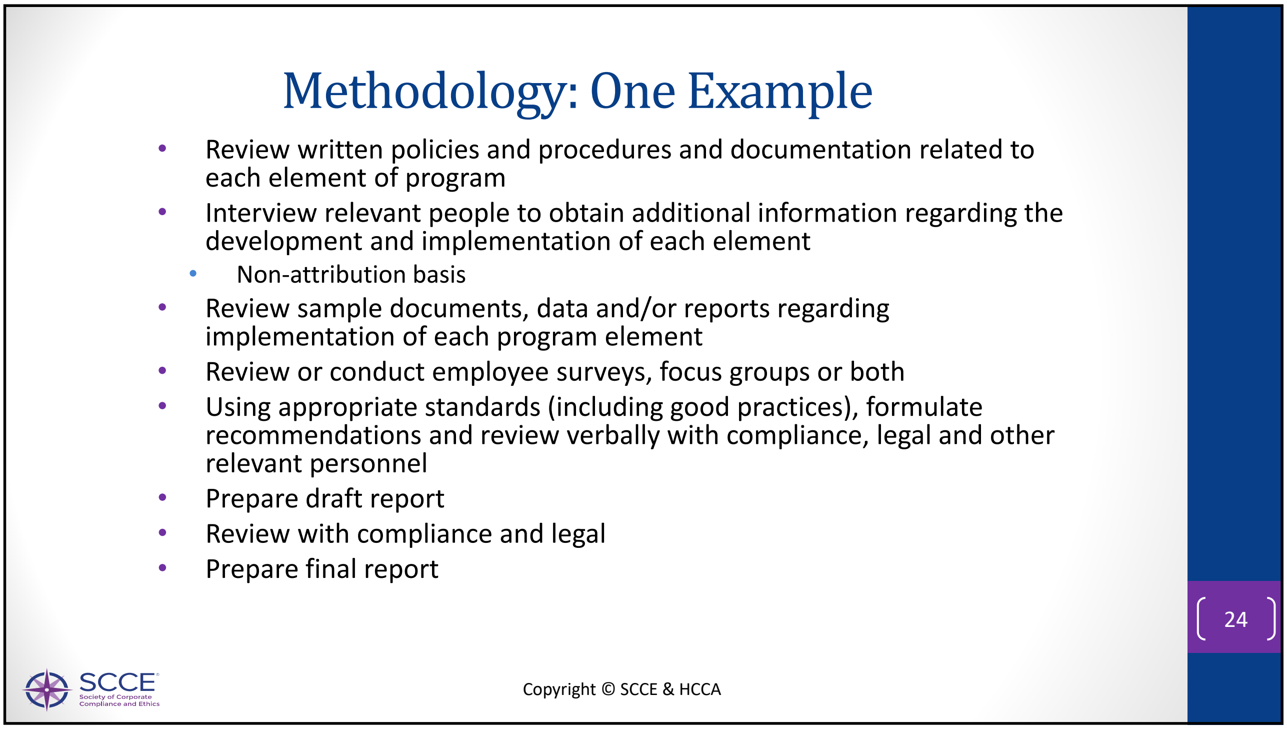
THIRD PARTY ASSESSMENTS



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

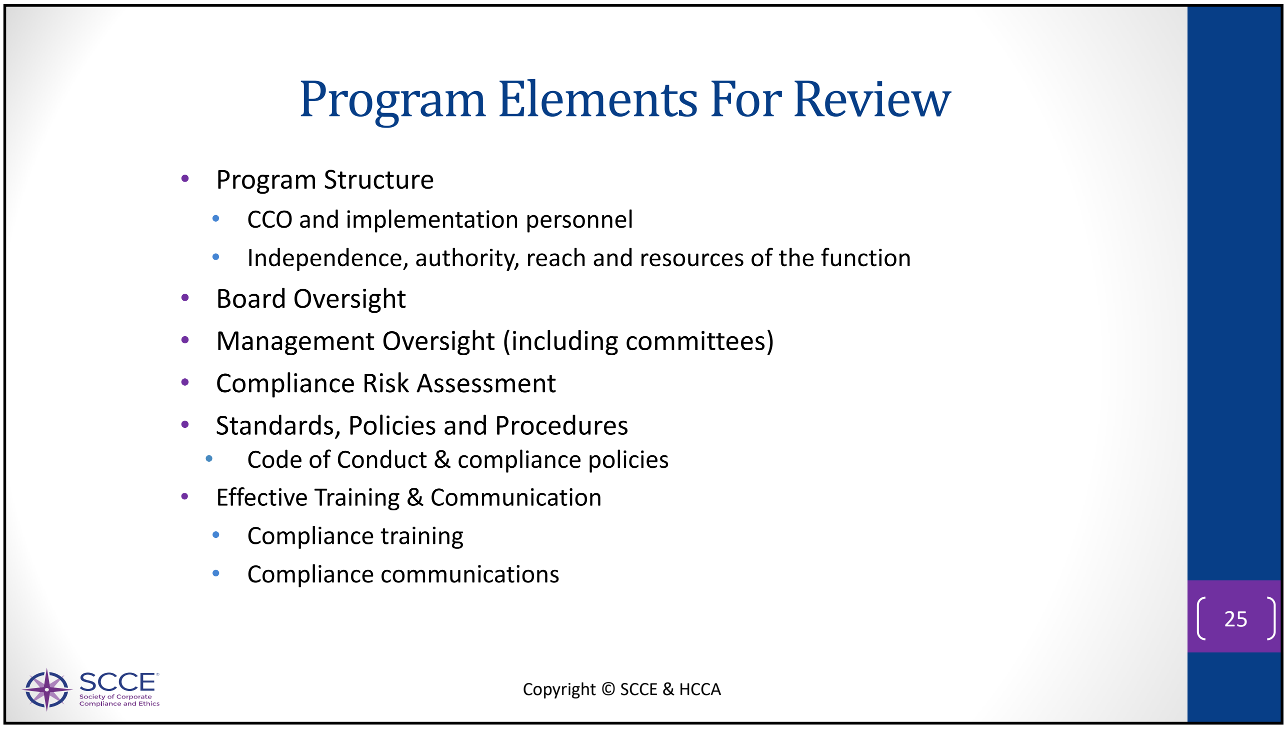
23



Methodology: One Example

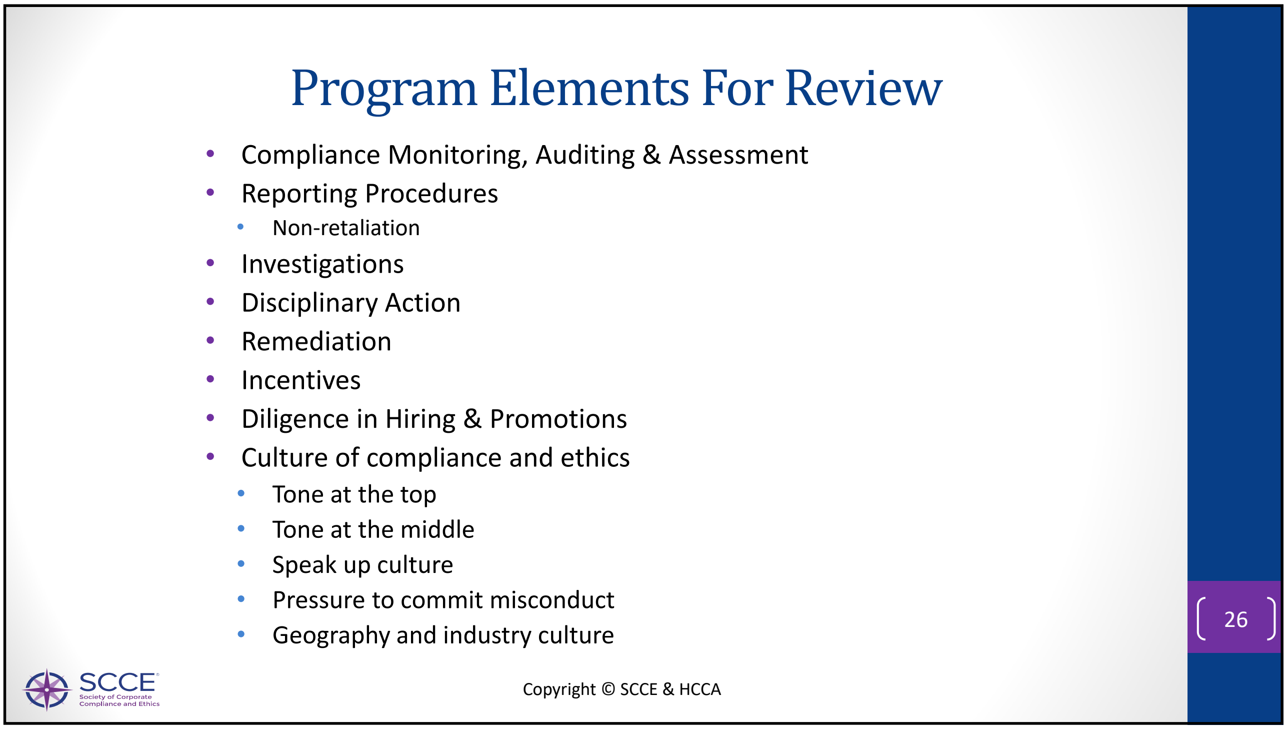
- Review written policies and procedures and documentation related to each element of program
- Interview relevant people to obtain additional information regarding the development and implementation of each element
  - Non-attribution basis
- Review sample documents, data and/or reports regarding implementation 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



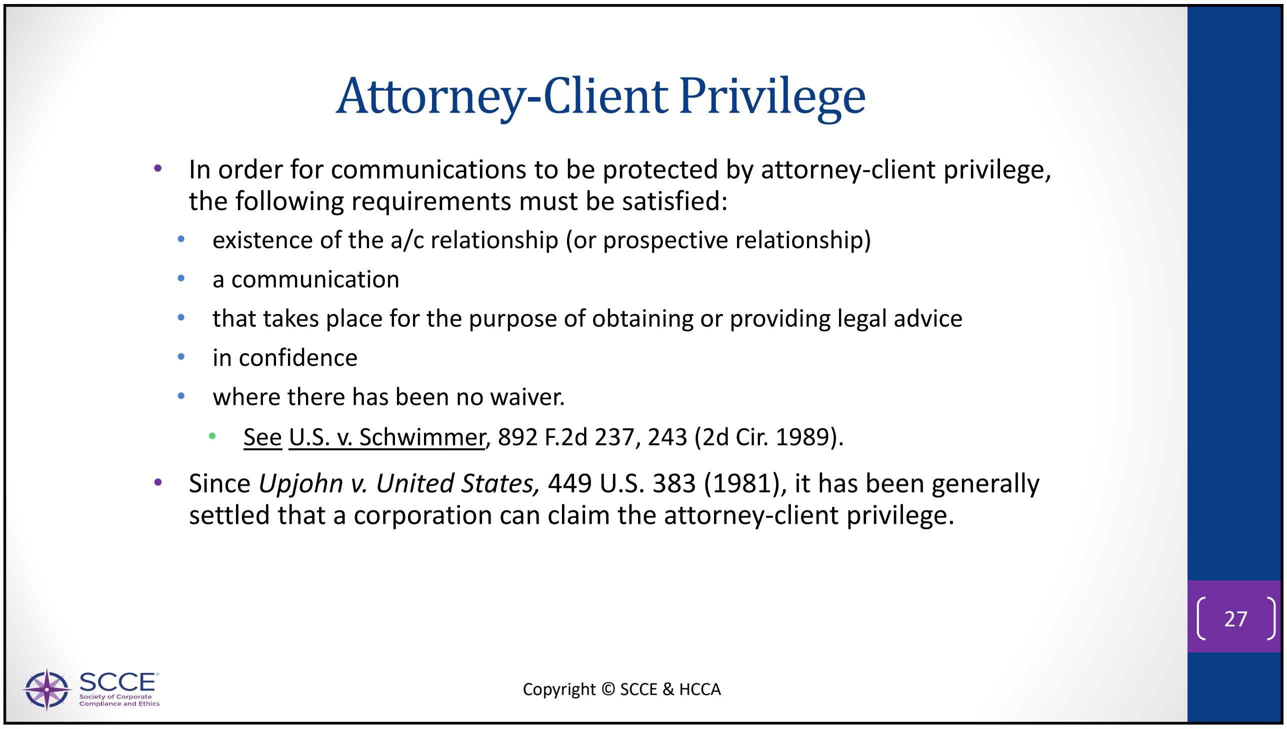
Program Elements For Review

- 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



Program Elements For Review

- Compliance 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
  - Geography and industry culture

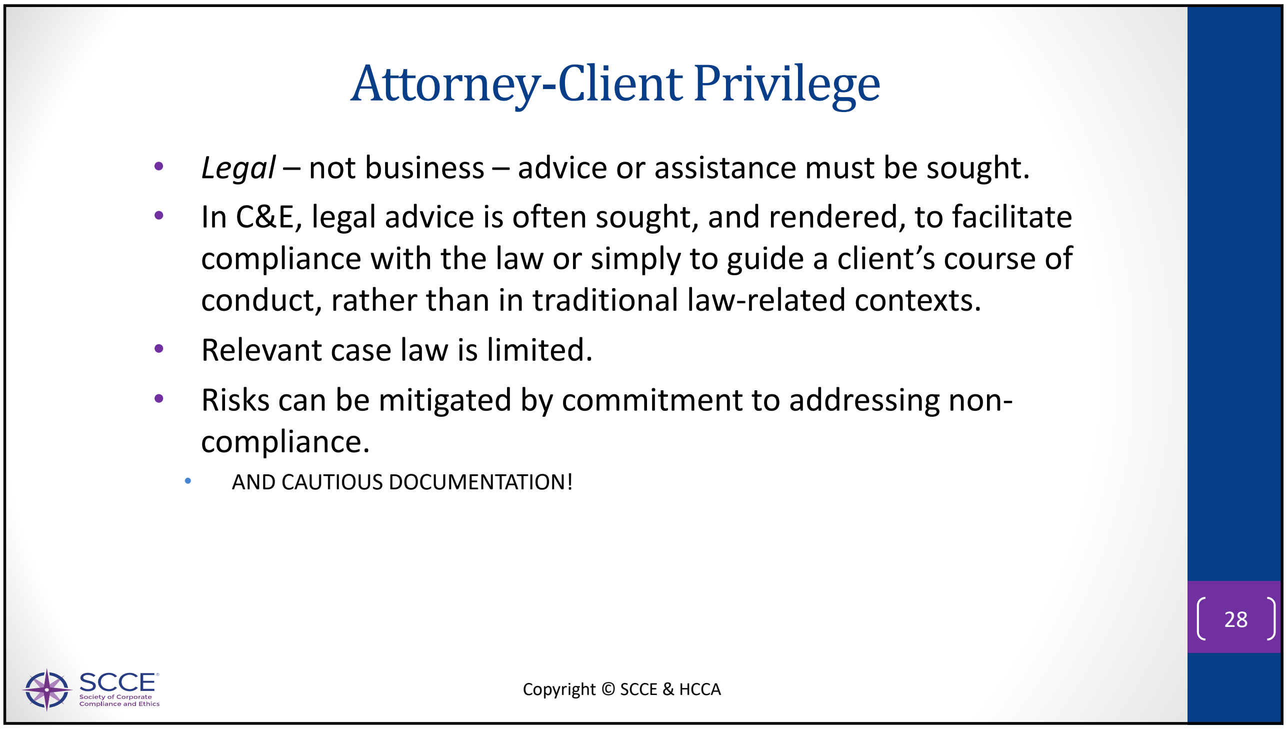


Attorney-Client Privilege

- 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.

27

27

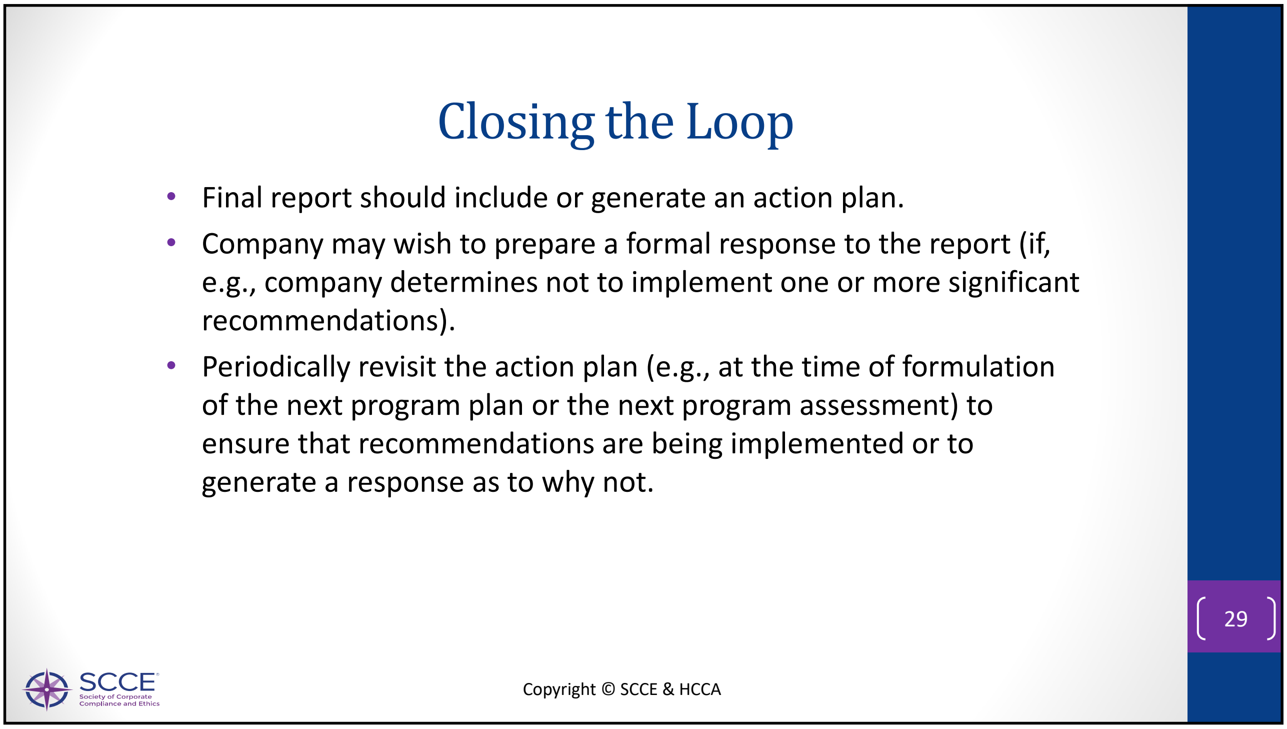


Attorney-Client Privilege

- *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!

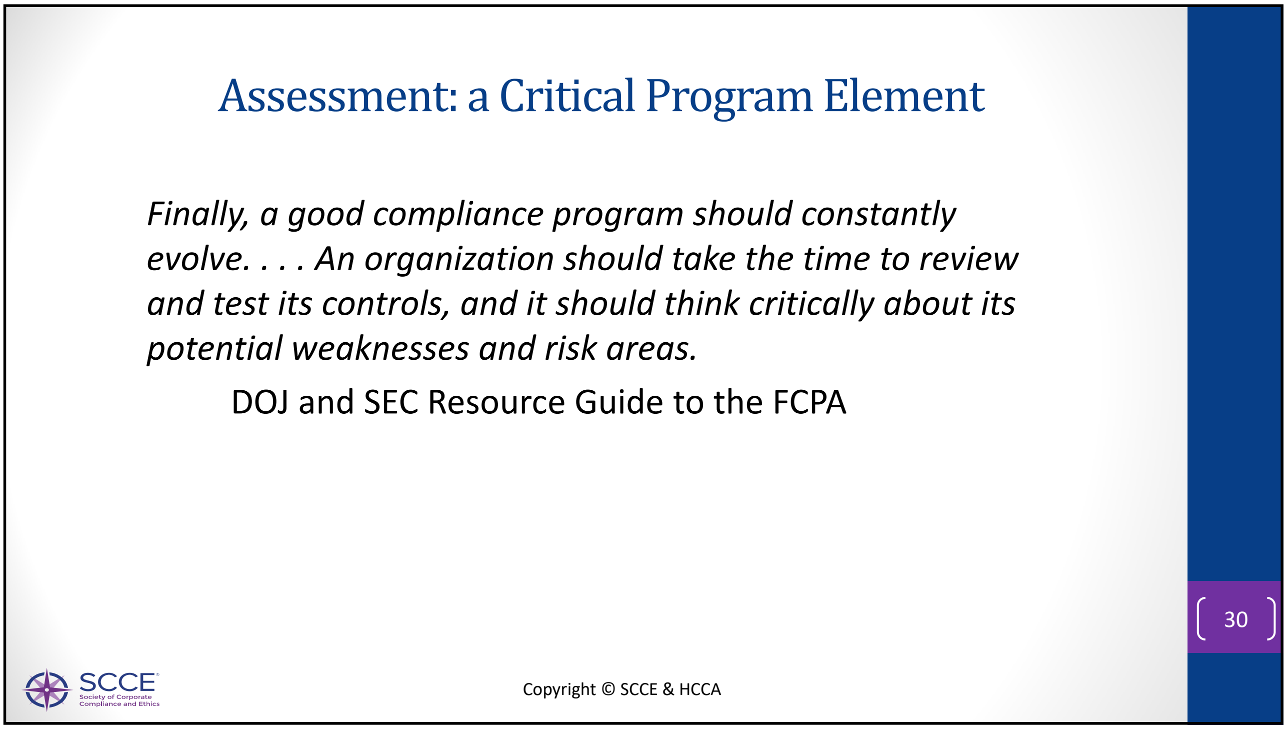
28

28



Closing the Loop

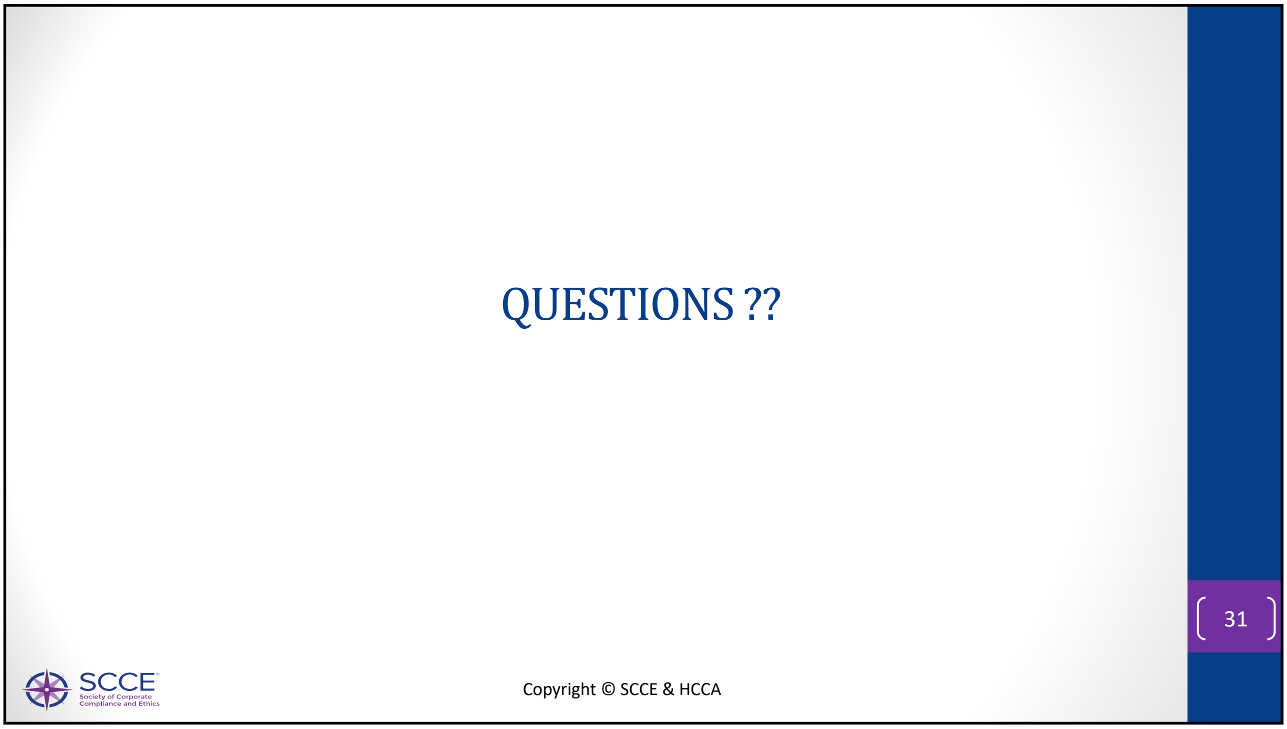
- Final report should include or generate an action plan.
- Company may wish to prepare a formal response to the report (if, e.g., company determines not to implement one or more significant recommendations).
- Periodically revisit the action plan (e.g., at the time of formulation of the next program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

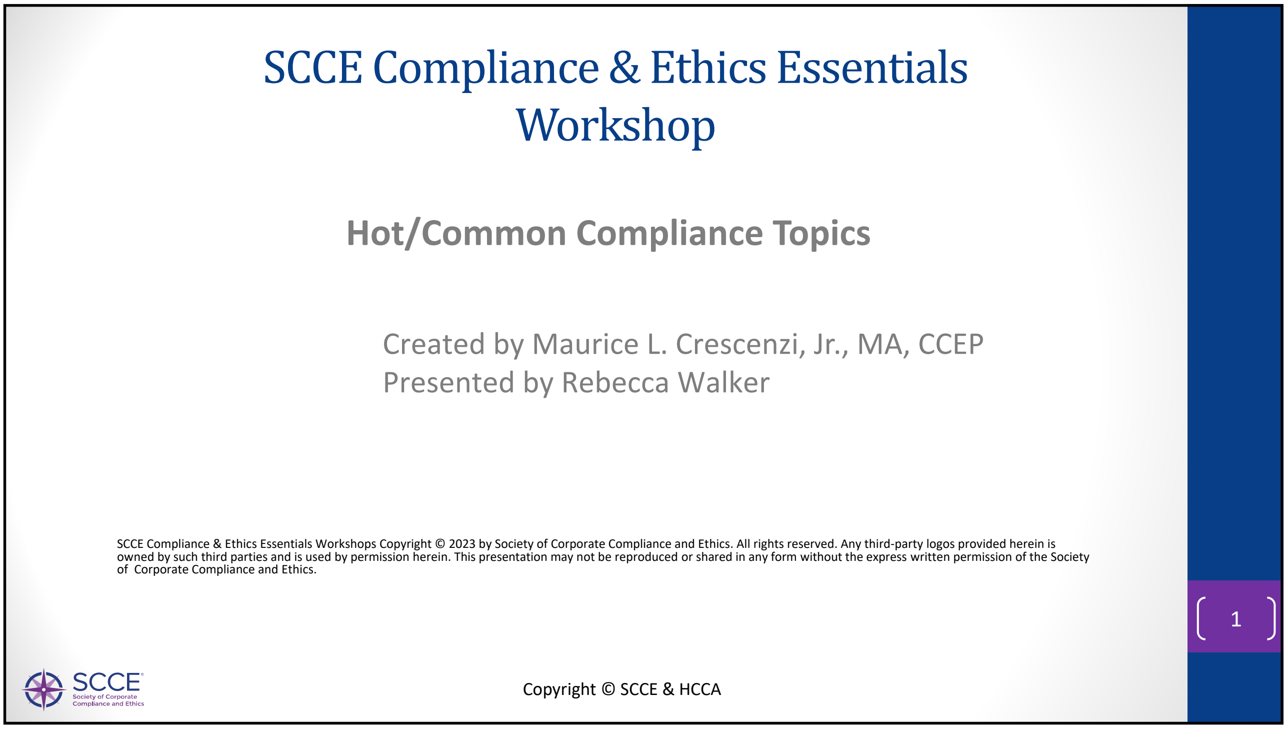


QUESTIONS ??

31

Copyright © SCCE & HCCA

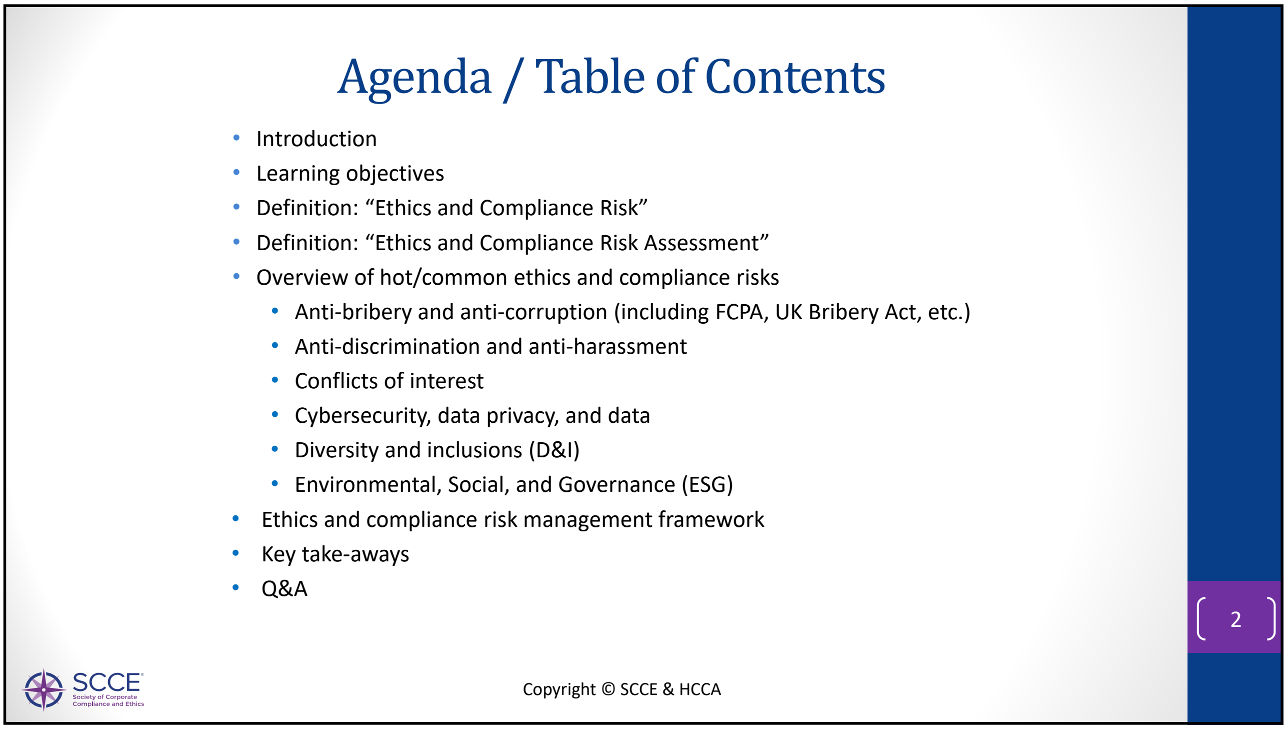
31



SCCE Compliance & Ethics Essentials Workshop

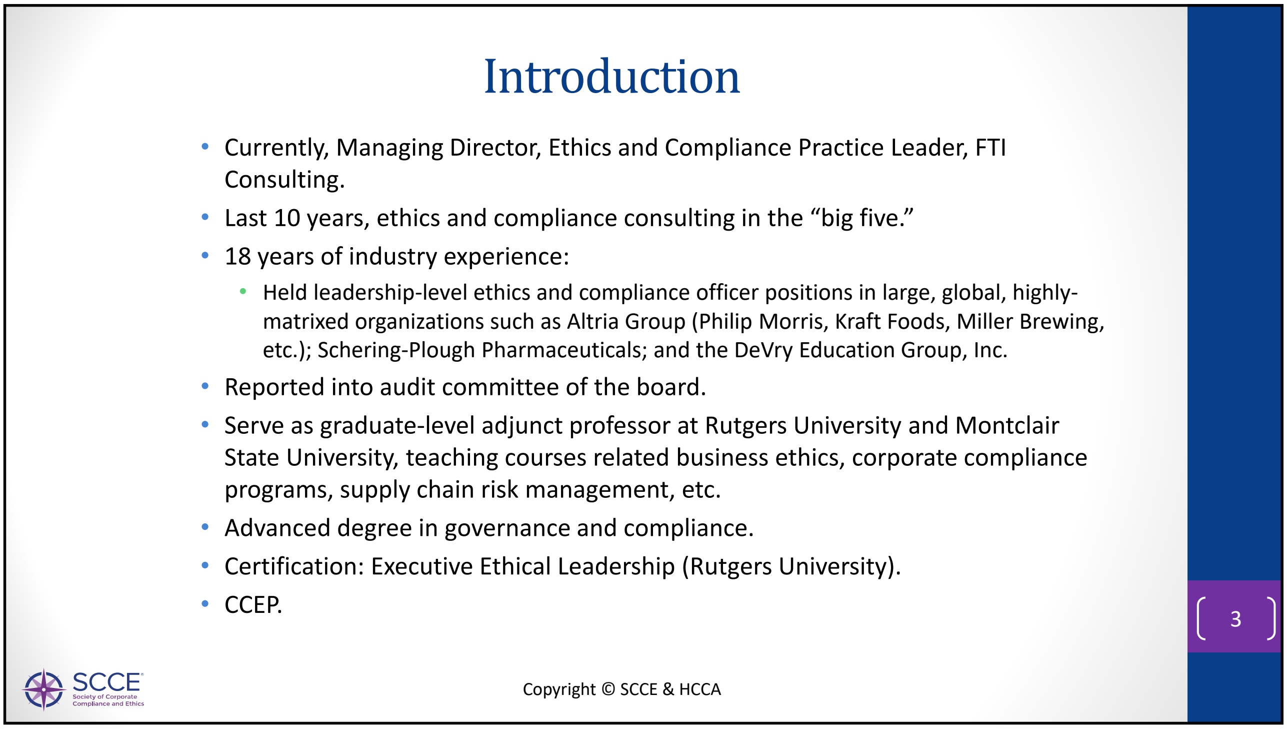
Hot/Common Compliance Topics

Created by Maurice L. Crescenzi, Jr., MA, CCEP
Presented by Rebecca Walker



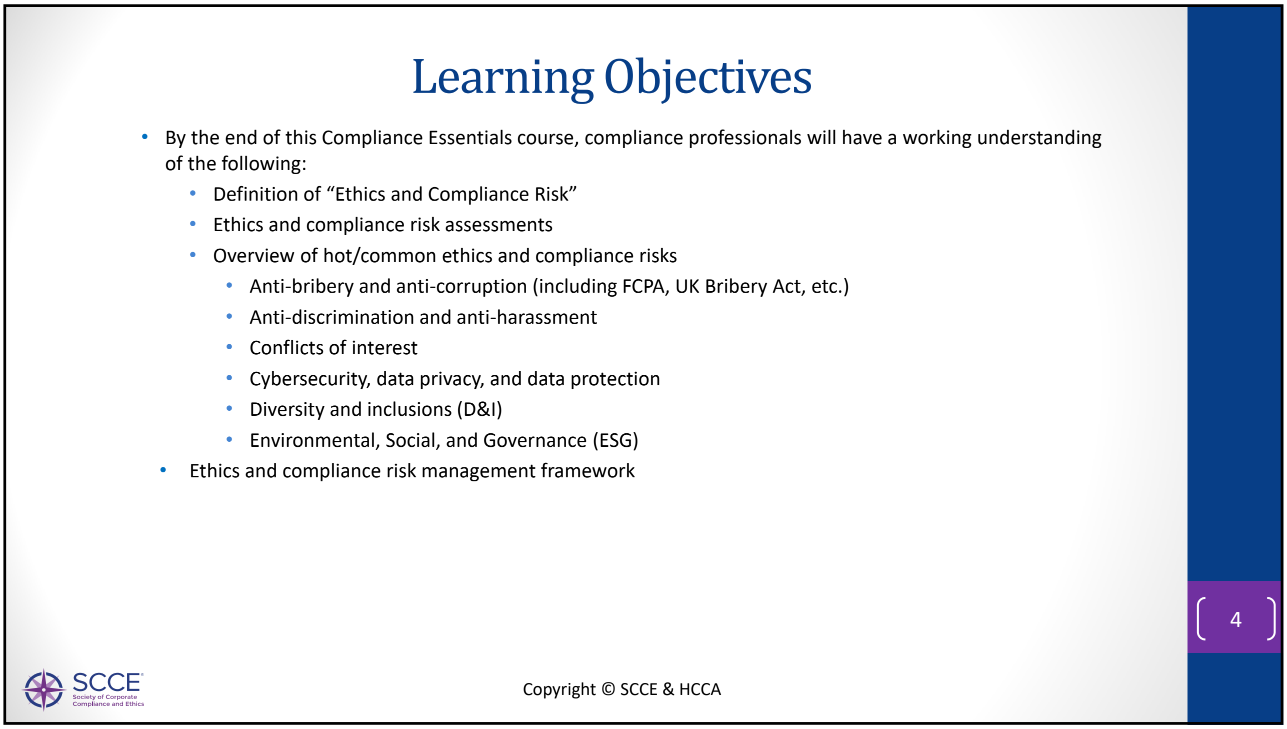
Agenda / Table of Contents

- Introduction
- Learning objectives
- Definition: “Ethics and Compliance Risk”
- Definition: “Ethics and Compliance Risk Assessment”
- Overview of hot/common ethics and compliance risks
  - Anti-bribery and anti-corruption (including FCPA, UK Bribery Act, etc.)
  - Anti-discrimination and anti-harassment
  - Conflicts of interest
  - Cybersecurity, data privacy, and data
  - Diversity and inclusions (D&I)
  - Environmental, Social, and Governance (ESG)
- Ethics and compliance risk management framework
- Key take-aways
- Q&A



Introduction

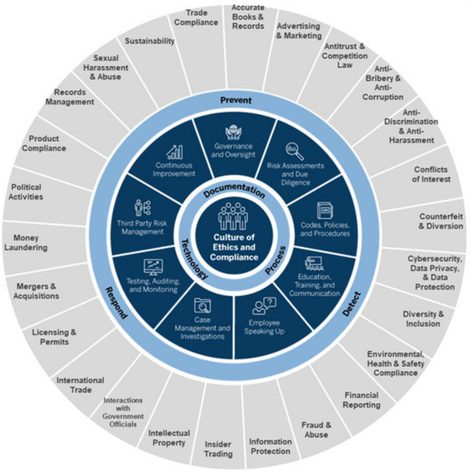
- Currently, Managing Director, Ethics and Compliance Practice Leader, FTI Consulting.
- Last 10 years, ethics and compliance consulting in the "big five."
- 18 years of industry experience:
  - Held leadership-level ethics and compliance officer positions in large, global, highly-matrixed organizations such as Altria Group (Philip Morris, Kraft Foods, Miller Brewing, etc.); Schering-Plough Pharmaceuticals; and the DeVry Education Group, Inc.
- Reported into audit committee of the board.
- Serve as graduate-level adjunct professor at Rutgers University and Montclair State University, teaching courses related business ethics, corporate compliance programs, supply chain risk management, etc.
- Advanced degree in governance and compliance.
- Certification: Executive Ethical Leadership (Rutgers University).
- CCEP.



Learning Objectives

- By the end of this Compliance Essentials course, compliance professionals will have a working understanding of the following:
  - Definition of "Ethics and Compliance Risk"
  - Ethics and compliance risk assessments
  - Overview of hot/common ethics and compliance risks
    - Anti-bribery and anti-corruption (including FCPA, UK Bribery Act, etc.)
    - Anti-discrimination and anti-harassment
    - Conflicts of interest
    - Cybersecurity, data privacy, and data protection
    - Diversity and inclusions (D&I)
    - Environmental, Social, and Governance (ESG)
- Ethics and compliance risk management framework

Definition:
Ethics and Compliance Risk

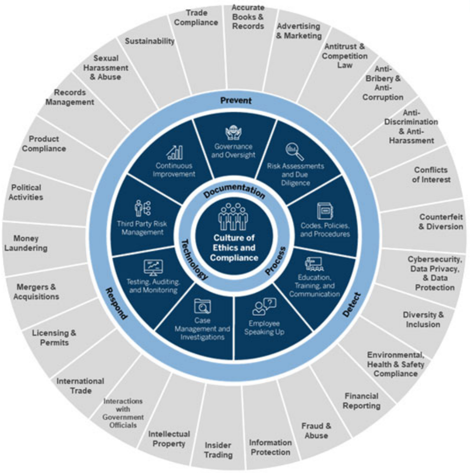


- Organizations are exposed to a wide variety of internal and external risks that can be organized into the following four categories:
  - Financial
  - Strategic
  - Operational
  - Ethics and Compliance
- An ethics and compliance risk can be defined as an "existing or emerging threat to the organization related to (1) potential violations of law or policy or (2) unethical conduct that could result in:
  - Civil or criminal fines or penalties
  - Reputational brand damage
  - Negative financial or operational impact

5

5

Definition:
Ethics and Compliance Risk

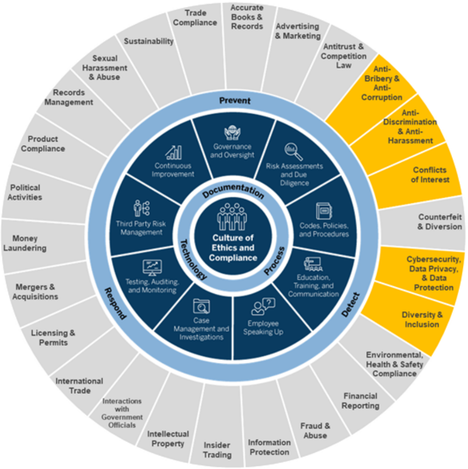


- Organizations are exposed to a wide variety of ethics and compliance risks, which include the following:
  - Accurate books and records
  - Advertising and marketing
  - Antitrust and competition law
  - Anti-bribery and anti-corruption
  - Anti-discrimination and anti-harassment
  - Conflicts of interest
  - Cybersecurity
  - Data privacy
  - Environmental compliance
  - Insider trading
  - International trade
  - Mergers and acquisitions
  - Money laundering
  - Political activities
  - Records and information management

6

6

Definition: Ethics and Compliance Risk Assessment



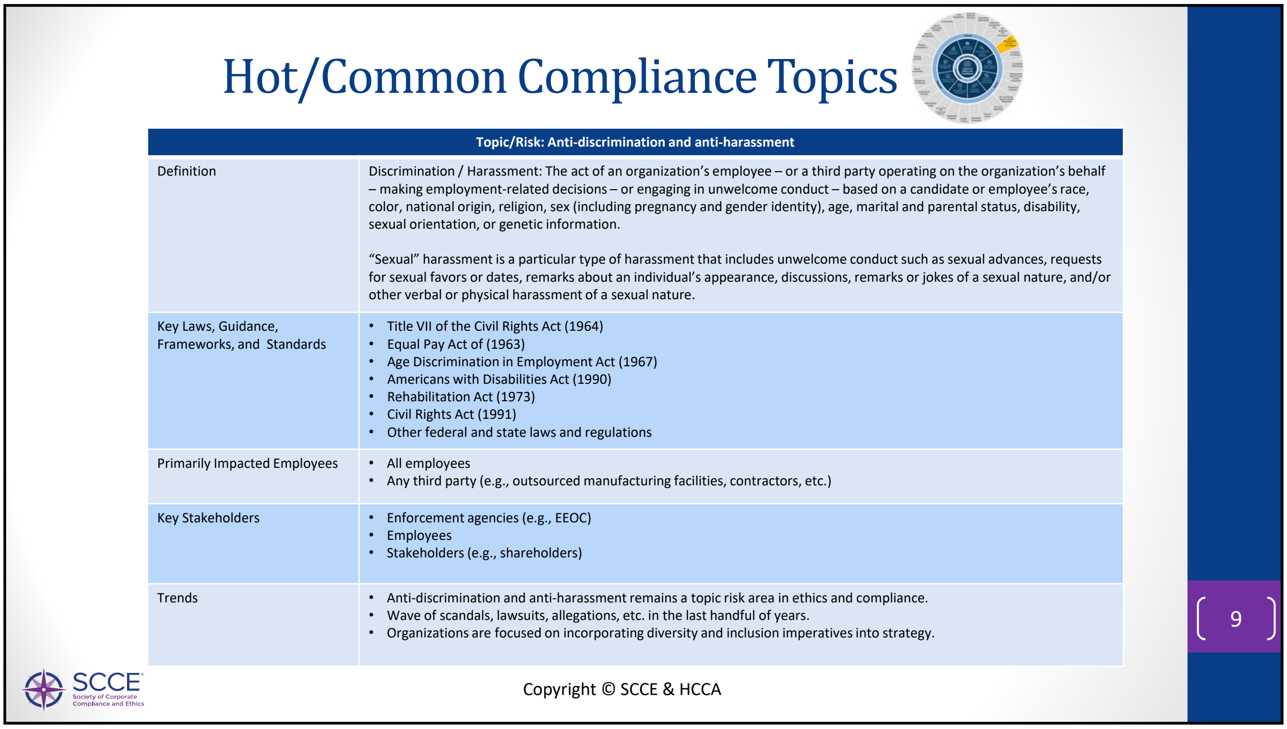
- The process of defining an organization's ethics and compliance risk profile (the outer ring) can be referred to as an "ethics and compliance risk assessment."
- An ethics and compliance risk assessment can be defined as "a process designed to (1) identify, (2) prioritize, and (3) assign internal responsibility for leading the management of ethics and compliance risks."
- Organizations should ensure that traditional areas of compliance risk – as well as "hot" areas of risk – are included in their ethics and compliance risk profiles.
- Note: this session does not explore the methodologies and processes for designing and implementing ethics and compliance risk assessments, which is covered in a different session.

SCCE Society of Corporate Compliance and Ethics

Hot/Common Compliance Topics

Topic/Risk: Anti-bribery and anti-corruption	
Definition	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	• US Foreign Corrupt Practices Act • UK Bribery Act • DOJ/SEC Guidance • OECD Framework • ISO 37001
Primarily Impacted Employees	• Sales representatives • Business development professionals • Any third party (e.g., customs brokers, freight forwarders, consultants, distributors, etc.)
Key Stakeholders	• Enforcement agencies (e.g., DOJ / SEC) • Employees • Stakeholders (e.g., shareholders)
Trends	• FCPA continues to be a top priority for DOJ/SEC (e.g., DOJ has brought more than 25 actions since January 2020). • Corporate compliance program design and implementation guidance has become more detailed. • Organizations are predicating the design of their ABAC programs in numerous key laws (e.g., UK Bribery Act), not just the FCPA.

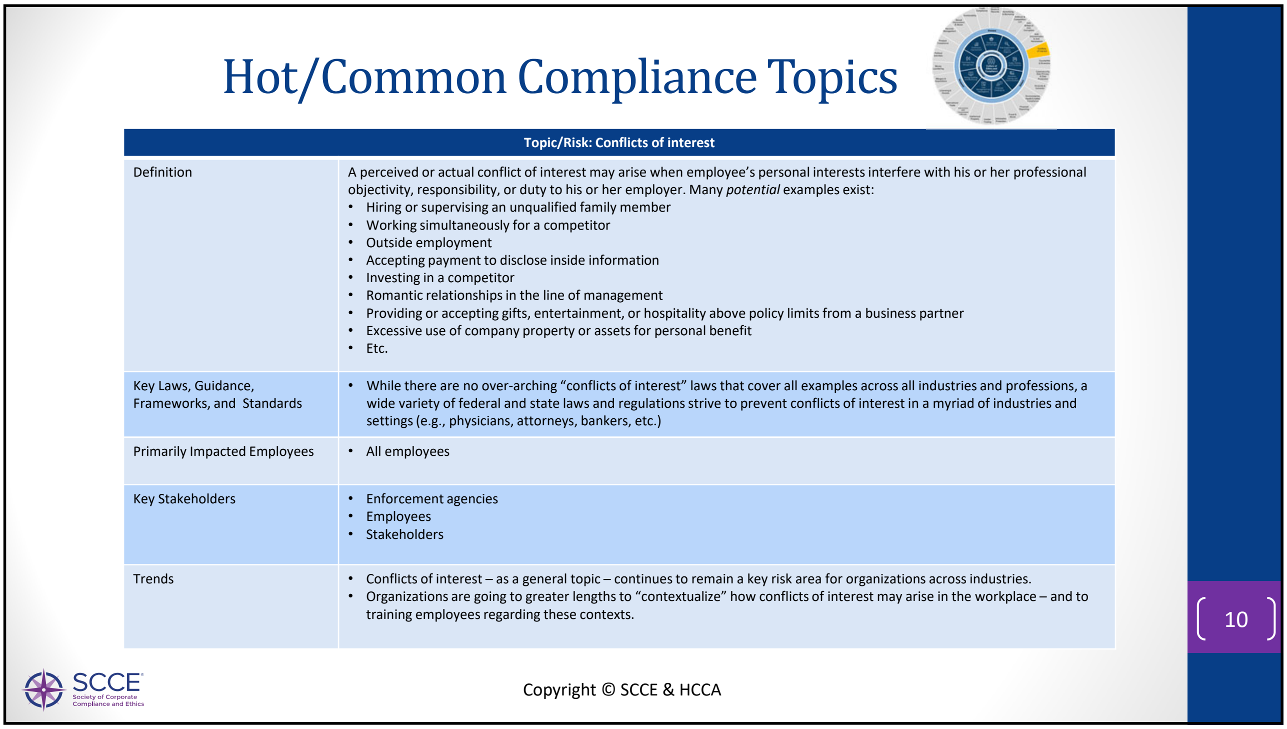
SCCE Society of Corporate Compliance and Ethics



Hot/Common Compliance Topics

Topic/Risk: Anti-discrimination and anti-harassment	
Definition	Discrimination / Harassment: The act of an organization's employee – or a third party operating on the organization's behalf – making employment-related decisions – or engaging in unwelcome conduct – based on a candidate or employee's race, color, national origin, religion, sex (including pregnancy and gender identity), age, marital and parental status, disability, sexual orientation, or genetic information. "Sexual" harassment is a particular type of harassment that includes unwelcome conduct such as sexual advances, requests for sexual favors or dates, remarks about an individual's appearance, discussions, remarks or jokes of a sexual nature, and/or other verbal or physical harassment of a sexual nature.
Key Laws, Guidance, Frameworks, and Standards	• Title VII of the Civil Rights Act (1964) • Equal Pay Act of (1963) • Age Discrimination in Employment Act (1967) • Americans with Disabilities Act (1990) • Rehabilitation Act (1973) • Civil Rights Act (1991) • Other federal and state laws and regulations
Primarily Impacted Employees	• All employees • Any third party (e.g., outsourced manufacturing facilities, contractors, etc.)
Key Stakeholders	• Enforcement agencies (e.g., EEOC) • Employees • Stakeholders (e.g., shareholders)
Trends	• Anti-discrimination and anti-harassment remains a topic risk area in ethics and compliance. • Wave of scandals, lawsuits, allegations, etc. in the last handful of years. • Organizations are focused on incorporating diversity and inclusion imperatives into strategy.

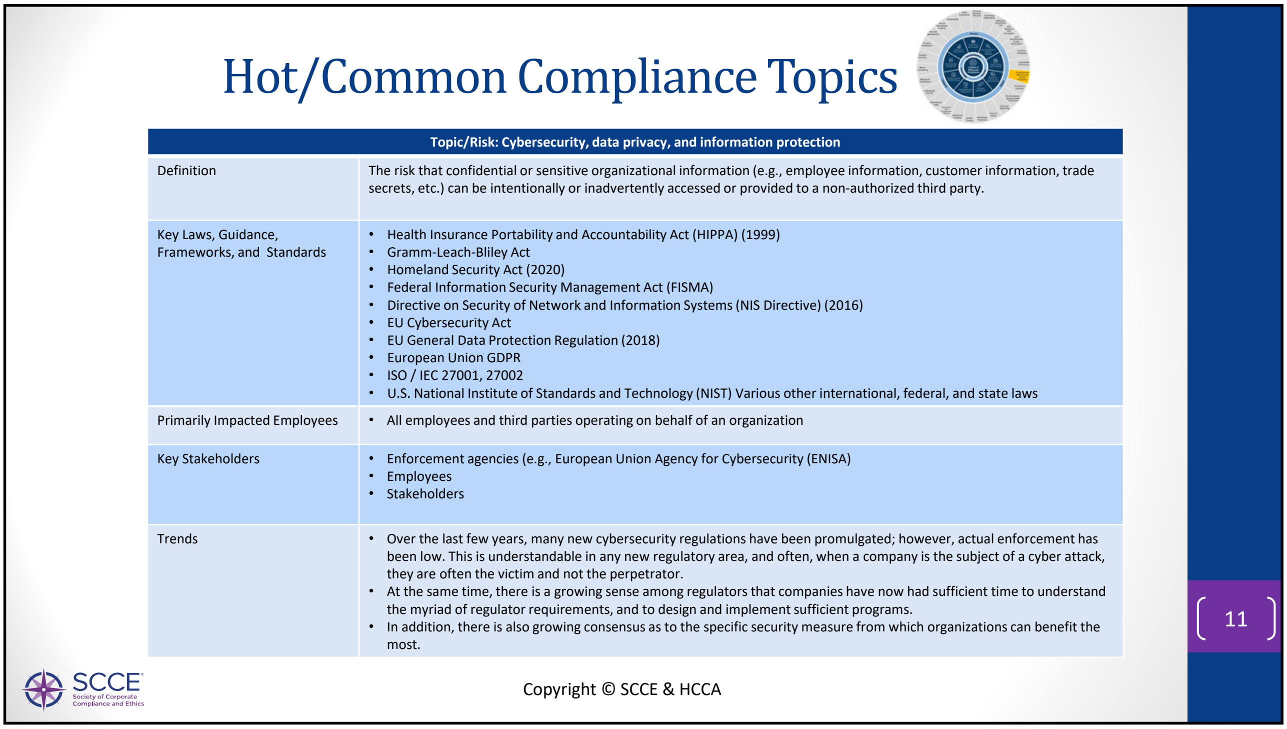
9



Hot/Common Compliance Topics

Topic/Risk: Conflicts of interest	
Definition	A perceived or actual conflict of interest may arise when employee's personal interests interfere with his or her professional objectivity, responsibility, or duty to his or her employer. Many *potential* examples exist: • Hiring or supervising an unqualified family member • Working simultaneously for a competitor • Outside employment • Accepting payment to disclose inside information • Investing in a competitor • Romantic relationships in the line of management • Providing or accepting gifts, entertainment, or hospitality above policy limits from a business partner • Excessive use of company property or assets for personal benefit • Etc.
Key Laws, Guidance, Frameworks, and Standards	• While there are no over-arching "conflicts of interest" laws that cover all examples across all industries and professions, a wide variety of federal and state laws and regulations strive to prevent conflicts of interest in a myriad of industries and settings (e.g., physicians, attorneys, bankers, etc.)
Primarily Impacted Employees	• All employees
Key Stakeholders	• Enforcement agencies • Employees • Stakeholders
Trends	• Conflicts of interest – as a general topic – continues to remain a key risk area for organizations across industries. • Organizations are going to greater lengths to "contextualize" how conflicts of interest may arise in the workplace – and to training employees regarding these contexts.

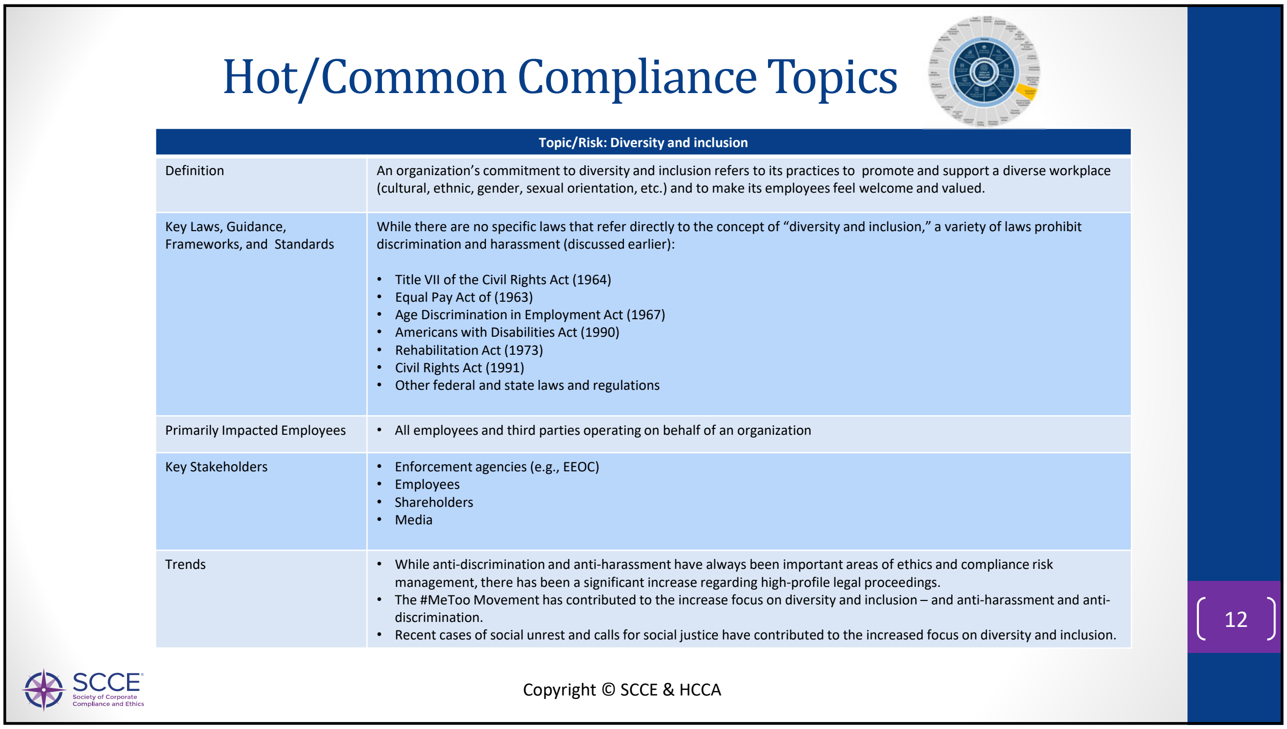
10



Hot/Common Compliance Topics

Topic/Risk: Cybersecurity, data privacy, and information protection	
Definition	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.
Key Laws, Guidance, Frameworks, and Standards	• Health Insurance Portability and Accountability Act (HIPPA) (1999) • Gramm-Leach-Bliley Act • Homeland Security Act (2020) • Federal Information Security Management Act (FISMA) • Directive on Security of Network and Information Systems (NIS Directive) (2016) • EU Cybersecurity Act • EU General Data Protection Regulation (2018) • European Union GDPR • ISO / IEC 27001, 27002 • U.S. National Institute of Standards and Technology (NIST) Various other international, federal, and state laws
Primarily Impacted Employees	• All employees and third parties operating on behalf of an organization
Key Stakeholders	• Enforcement agencies (e.g., European Union Agency for Cybersecurity (ENISA) • Employees • Stakeholders
Trends	• Over the last few years, many new cybersecurity regulations have been promulgated; however, actual enforcement has been low. This is understandable in any new regulatory area, and often, when a company is the subject of a cyber attack, they are often the victim and not the perpetrator. • At the same time, there is a growing sense among regulators that companies have now had sufficient time to understand the myriad of regulator requirements, and to design and implement sufficient programs. • In addition, there is also growing consensus as to the specific security measure from which organizations can benefit the most.

SCCE Society of Corporate Compliance and Ethics

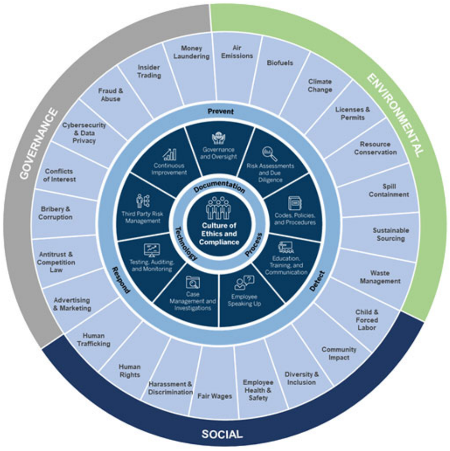


Hot/Common Compliance Topics

Topic/Risk: Diversity and inclusion	
Definition	An organization's commitment to diversity and inclusion refers to its practices to promote and support a diverse workplace (cultural, ethnic, gender, sexual orientation, etc.) and to make its employees feel welcome and valued.
Key Laws, Guidance, Frameworks, and Standards	While there are no specific laws that refer directly to the concept of "diversity and inclusion," a variety of laws prohibit discrimination and harassment (discussed earlier): • Title VII of the Civil Rights Act (1964) • Equal Pay Act of (1963) • Age Discrimination in Employment Act (1967) • Americans with Disabilities Act (1990) • Rehabilitation Act (1973) • Civil Rights Act (1991) • Other federal and state laws and regulations
Primarily Impacted Employees	• All employees and third parties operating on behalf of an organization
Key Stakeholders	• Enforcement agencies (e.g., EEOC) • Employees • Shareholders • Media
Trends	• While anti-discrimination and anti-harassment have always been important areas of ethics and compliance risk management, there has been a significant increase regarding high-profile legal proceedings. • The #MeToo Movement has contributed to the increase focus on diversity and inclusion – and anti-harassment and anti-discrimination. • Recent cases of social unrest and calls for social justice have contributed to the increased focus on diversity and inclusion.

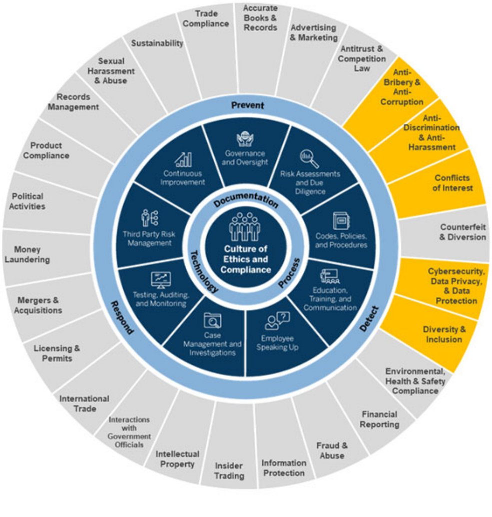
SCCE Society of Corporate Compliance and Ethics

Hot/Common Compliance Topics: Environmental, Social, and Governance (ESG)

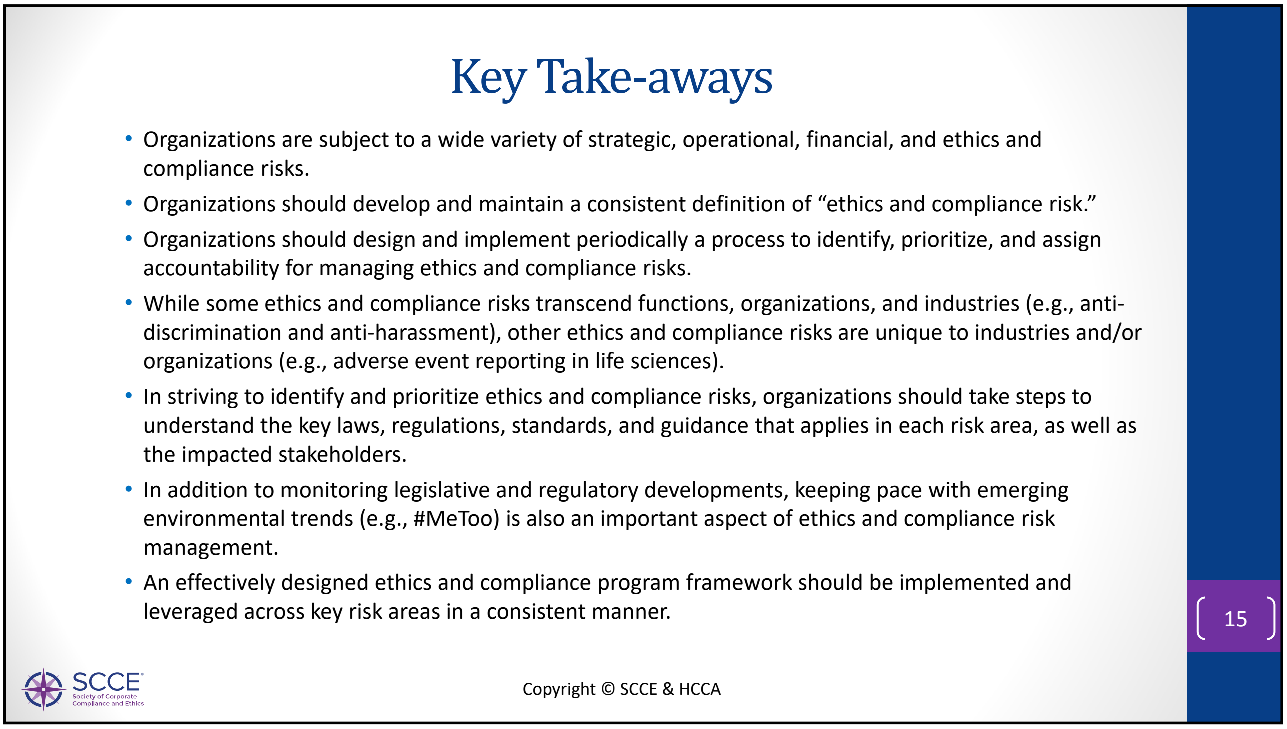


- Environmental, Social, and Governance (ESG) refers to the three general areas of evaluating the societal and environmental impact of an investment in a company.
- As assessment of an organization's ESG risk profile and ESG performance helps investors to determine potential future performance.
- In some ways, ESG is the most recent way or referring to related concepts used over the last few decades (e.g., Corporate Social Responsibility, Triple Bottom Line Reporting, etc.)
- In many ways, an organizations ESG "risk profile" is another way of referring to the organization's ethics and compliance risk profile.

Ethics and Compliance Risk Management Framework



- An effectively designed ethics and compliance program is composed of approximately ten specific programmatic elements.
- Effective program design is covered in another course.
- Organizations should strive to design and implement a program framework that manages all key ethics and compliance risk in a consistent manner.
- While certain program elements will be unique to each risk area (e.g., the unique nature of policy content), other program elements can be leveraged across multiple risk areas (e.g., Employee Speaking Up).

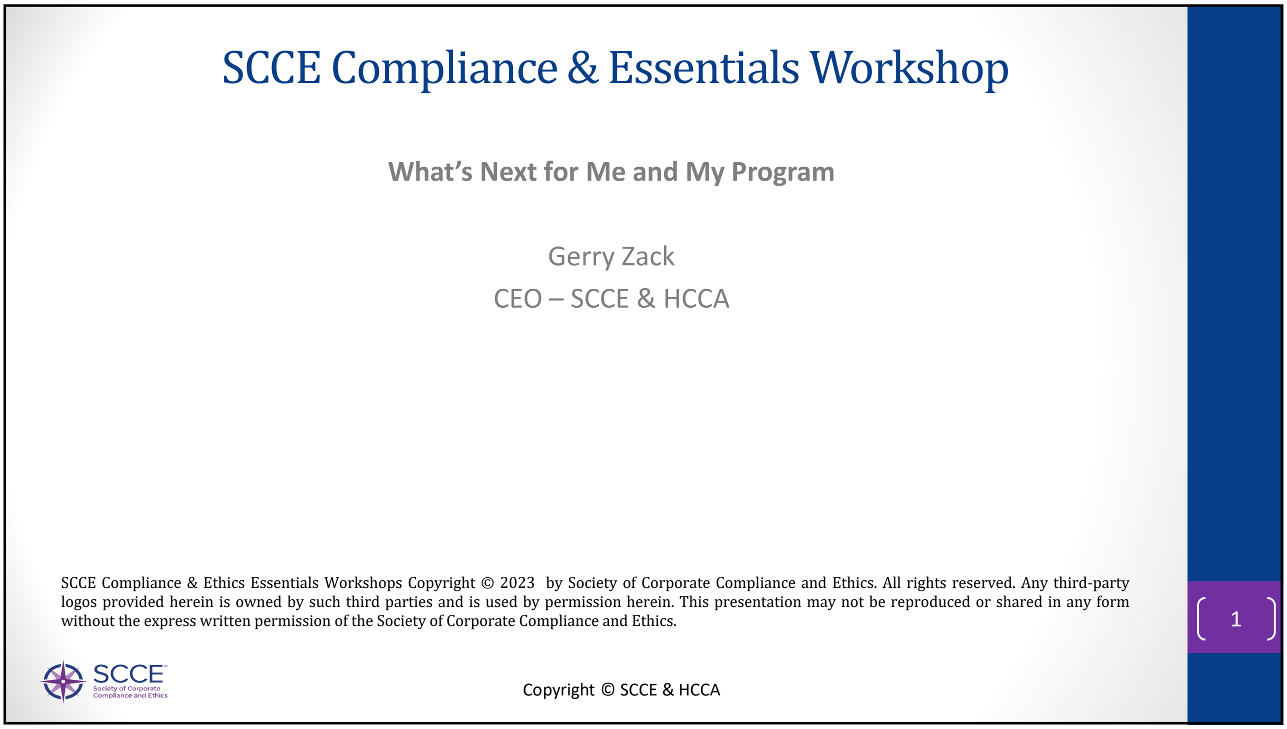


Key Take-aways

- Organizations are subject to a wide variety of strategic, operational, financial, and ethics and compliance risks.
- Organizations should develop and maintain a consistent definition of “ethics and compliance risk.”
- Organizations should design and implement periodically a process to identify, prioritize, and assign accountability for managing ethics and compliance risks.
- While some ethics and compliance risks transcend functions, organizations, and industries (e.g., anti-discrimination and anti-harassment), other ethics and compliance risks are unique to industries and/or organizations (e.g., adverse event reporting in life sciences).
- In striving to identify and prioritize ethics and compliance risks, organizations should take steps to understand the key laws, regulations, standards, and guidance that applies in each risk area, as well as the impacted stakeholders.
- In addition to monitoring legislative and regulatory developments, keeping pace with emerging environmental trends (e.g., #MeToo) is also an important aspect of ethics and compliance risk management.
- An effectively designed ethics and compliance program framework should be implemented and leveraged across key risk areas in a consistent manner.

Q&A

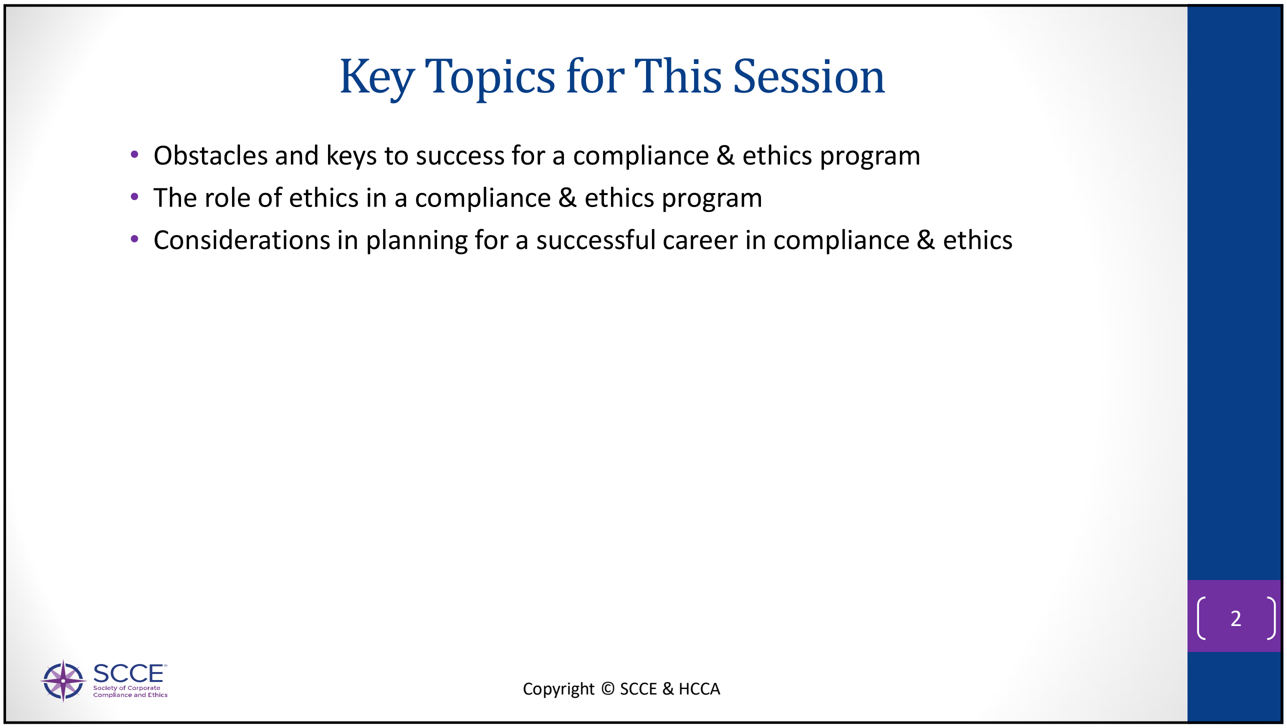
Thank you.



SCCE Compliance & Essentials Workshop

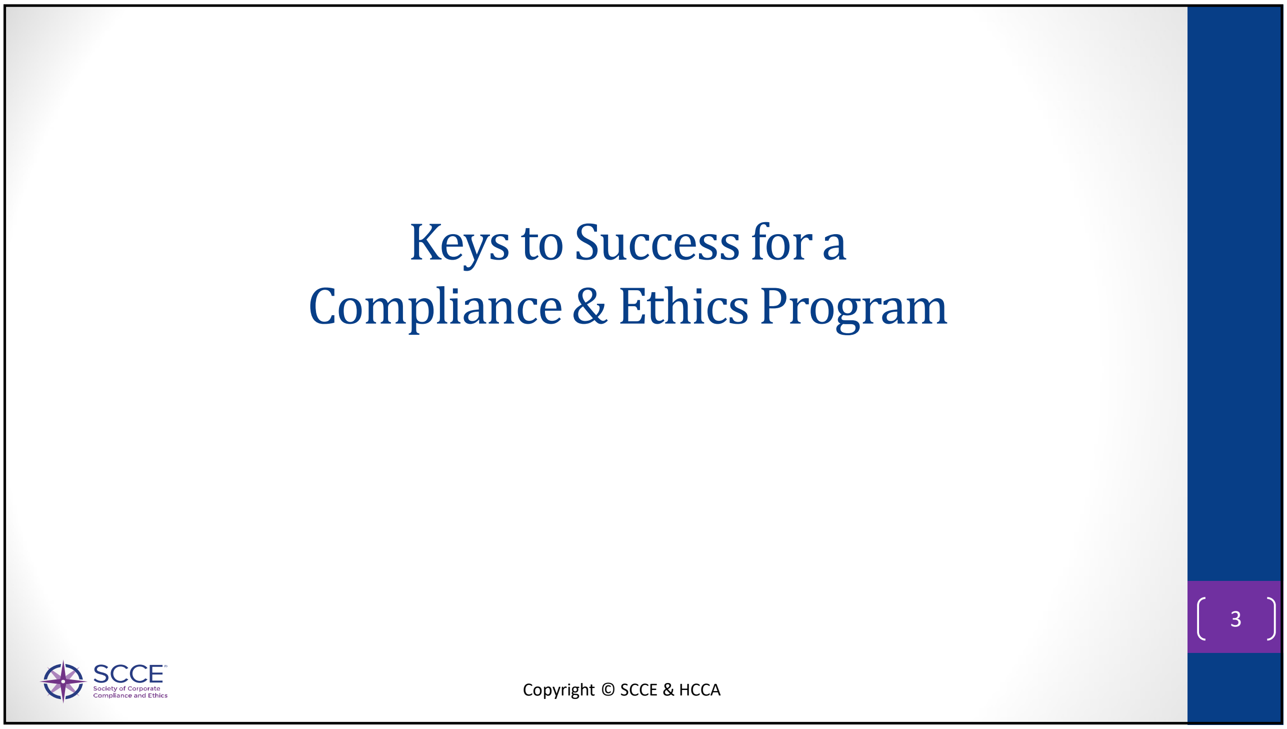
What's Next for Me and My Program

Gerry Zack
CEO – SCCE & HCCA

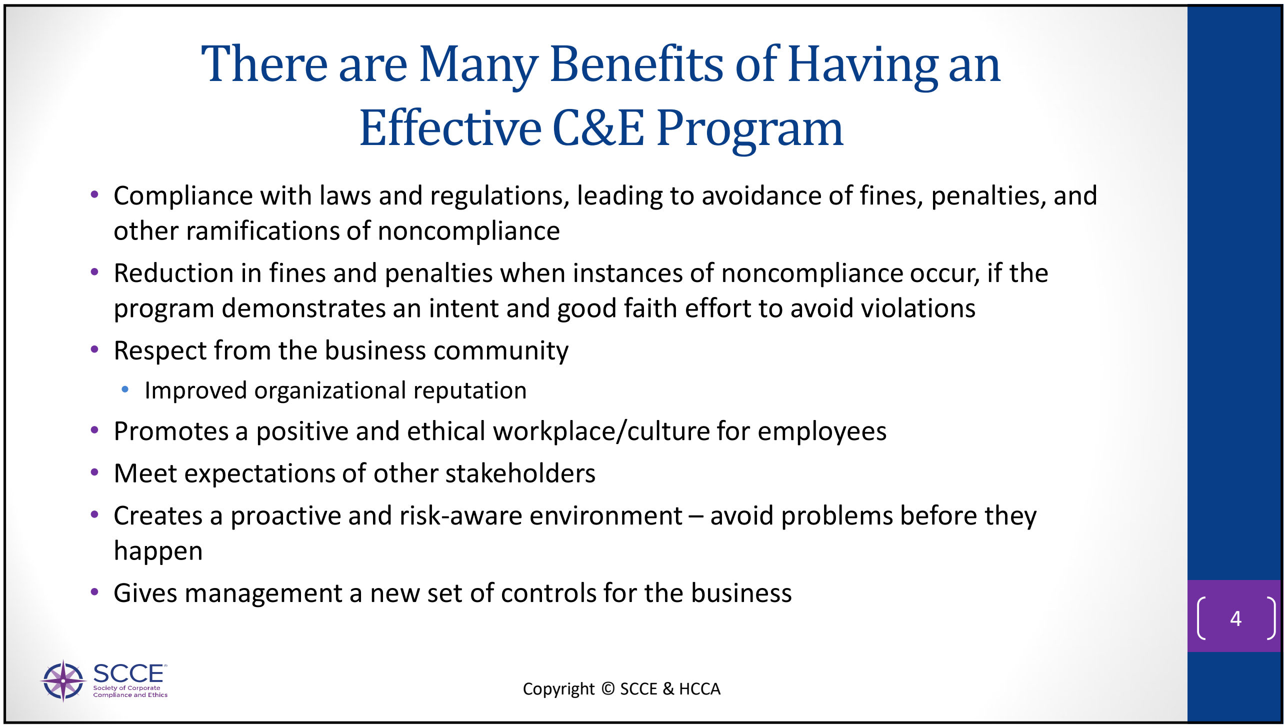


Key Topics for This Session

- 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

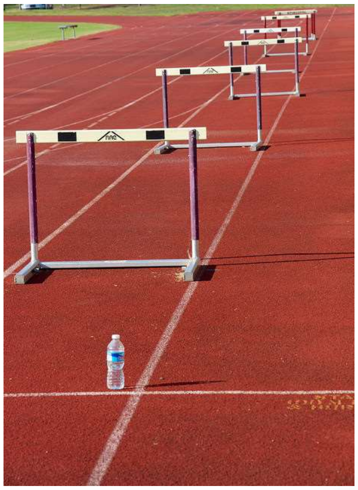


There are Many Benefits of Having an Effective C&E Program

- 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

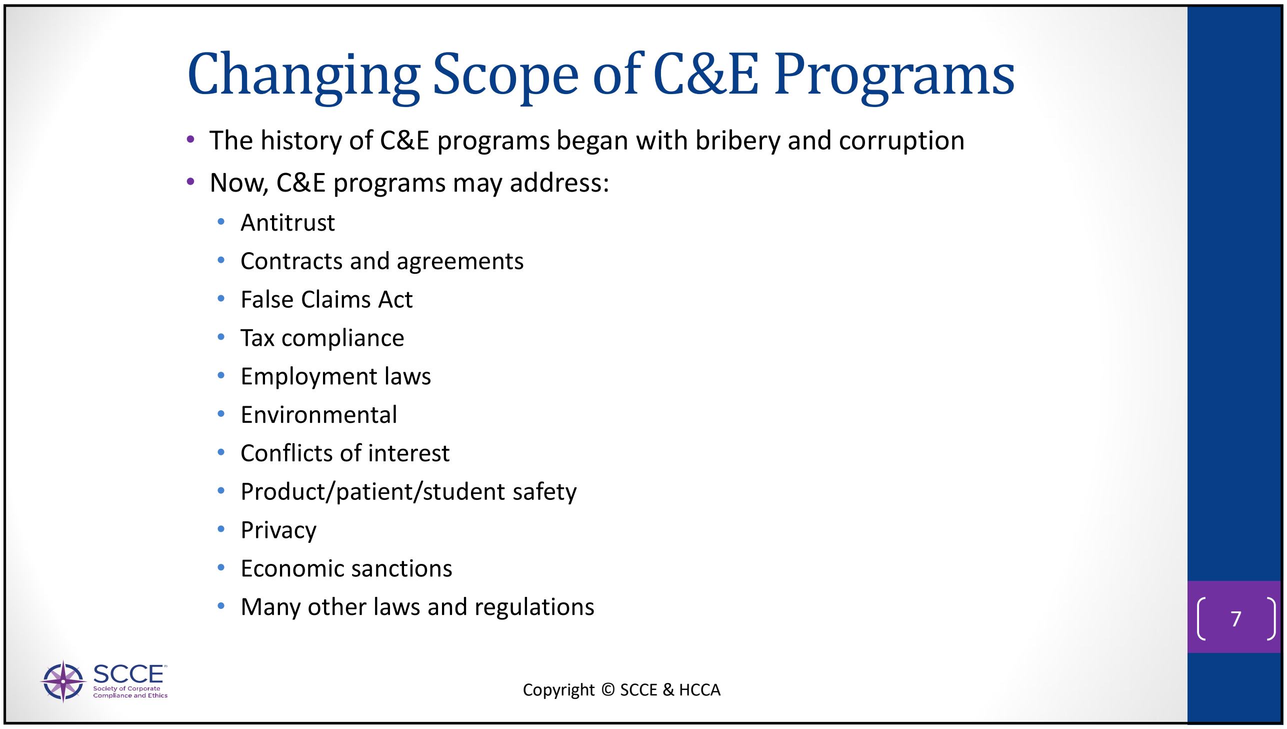
But, There are Ongoing Challenges

- 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



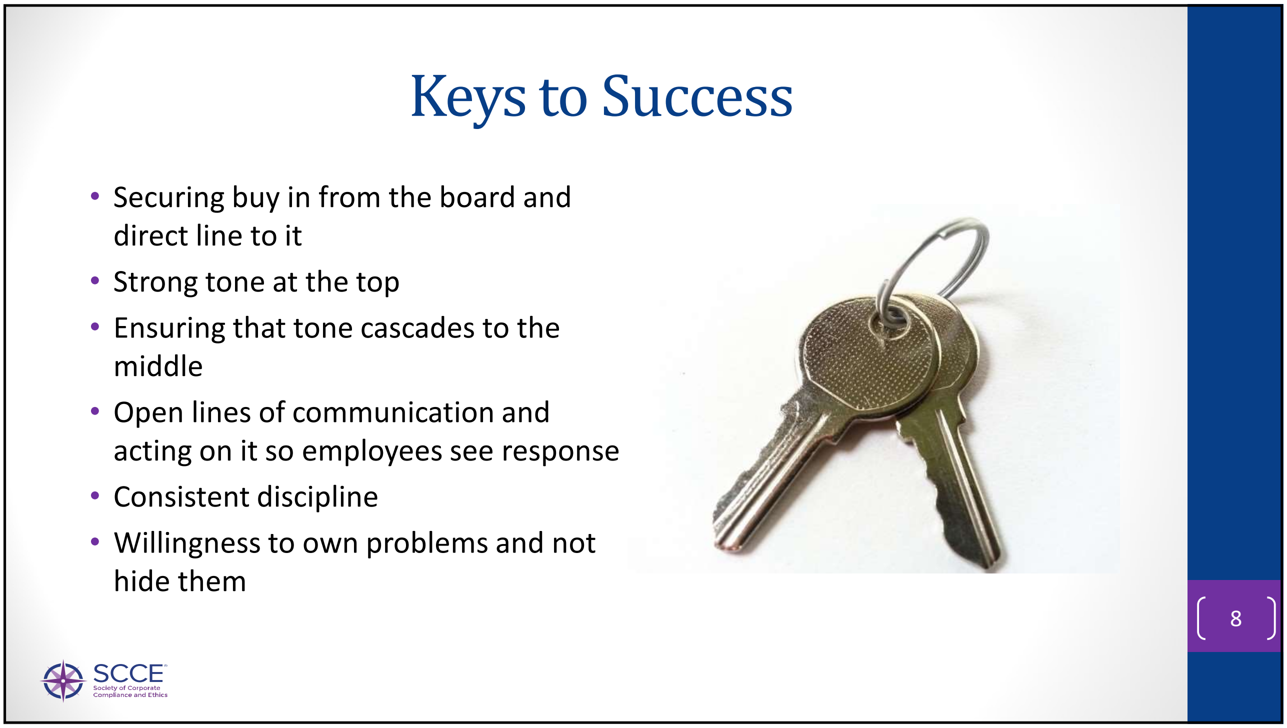
Ongoing Challenges

- 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



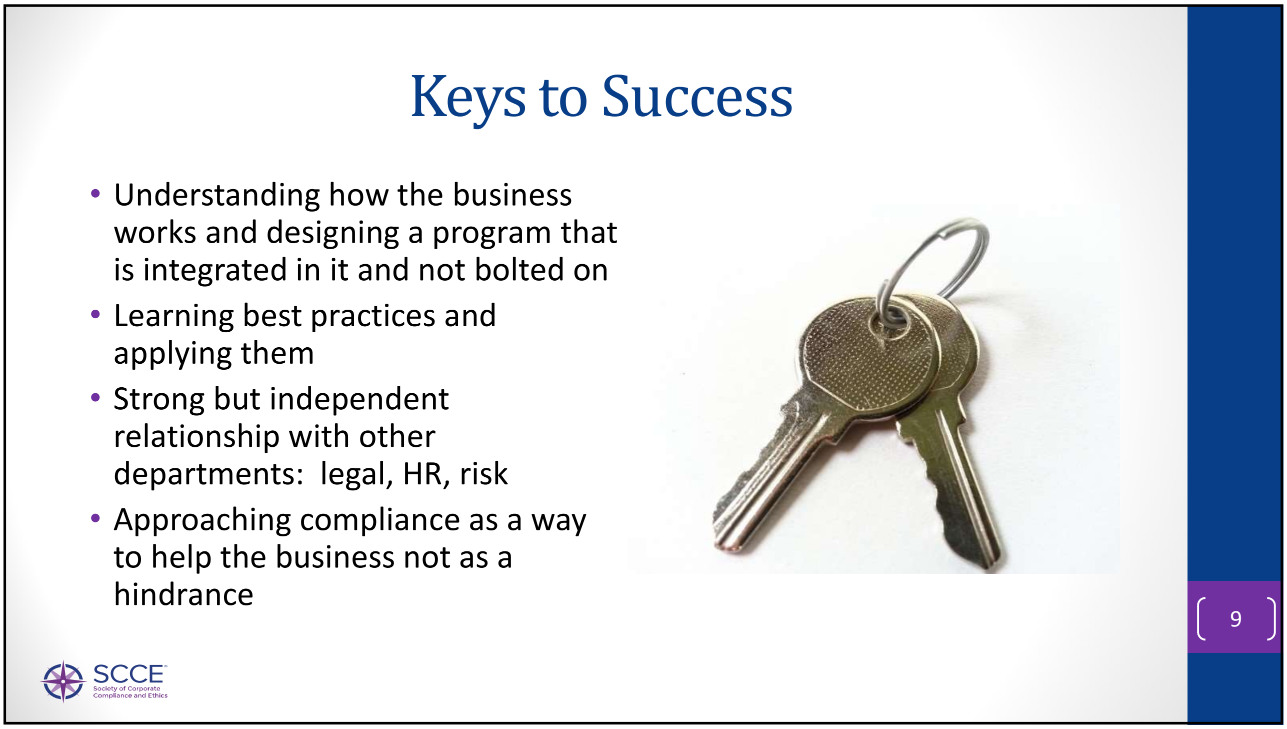
Changing Scope of C&E Programs

- 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



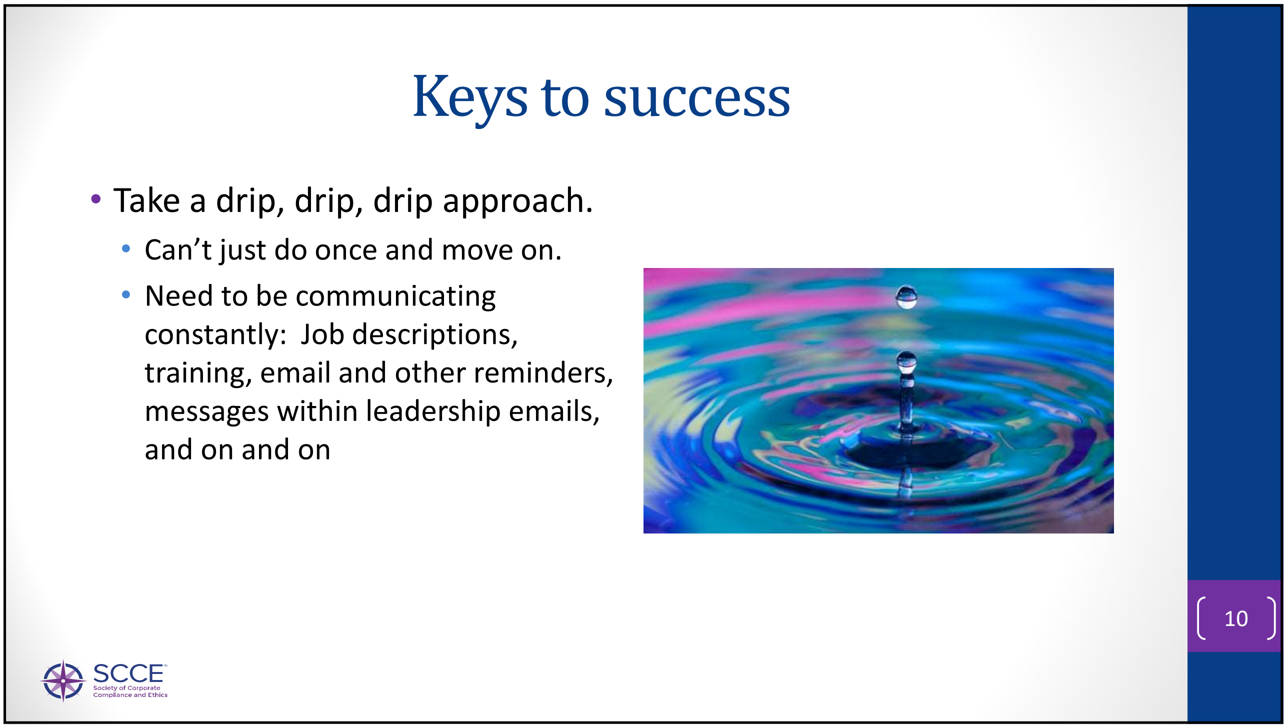
Keys to Success

- 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



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



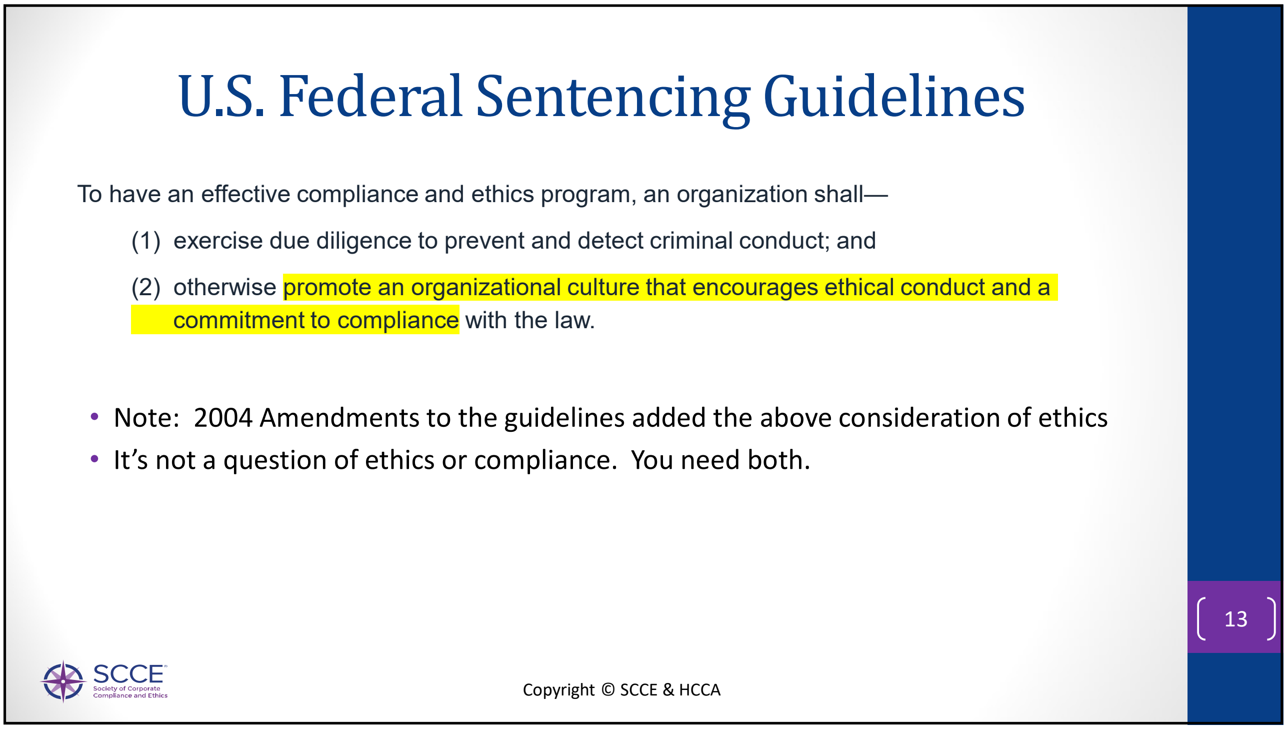
Keys to success

- 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

The Role of Ethics



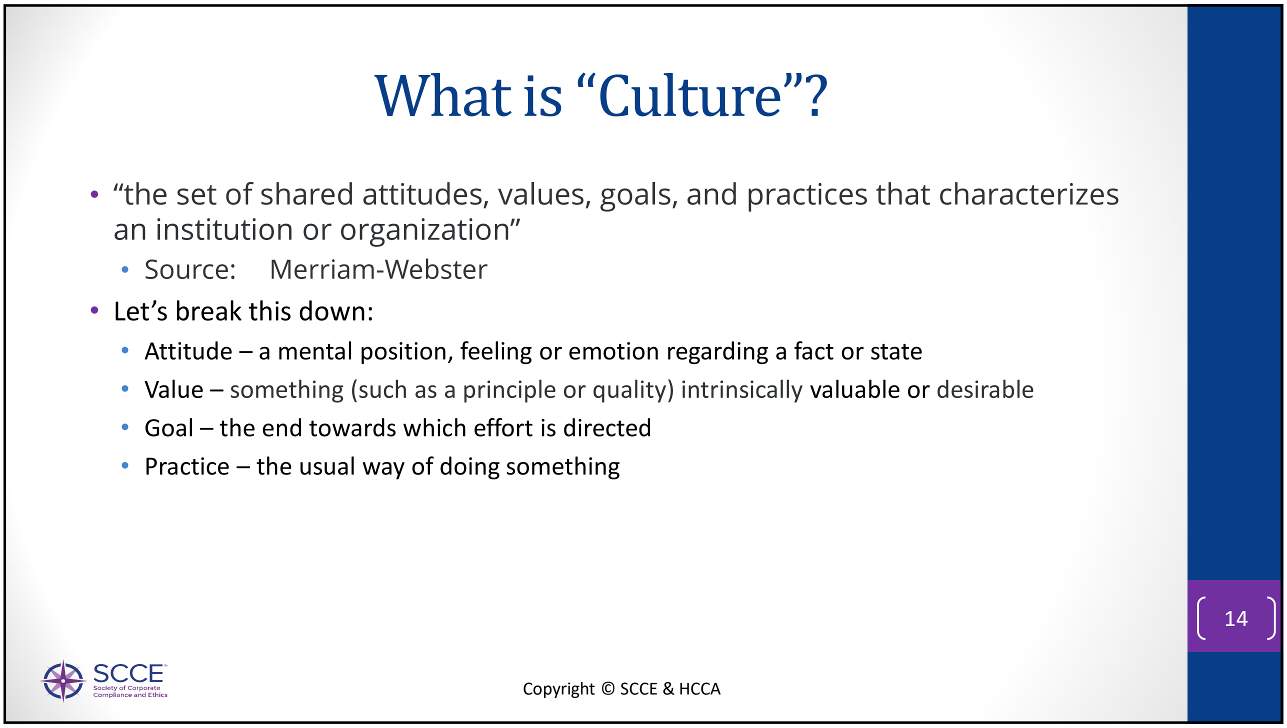
U.S. Federal Sentencing Guidelines

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

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

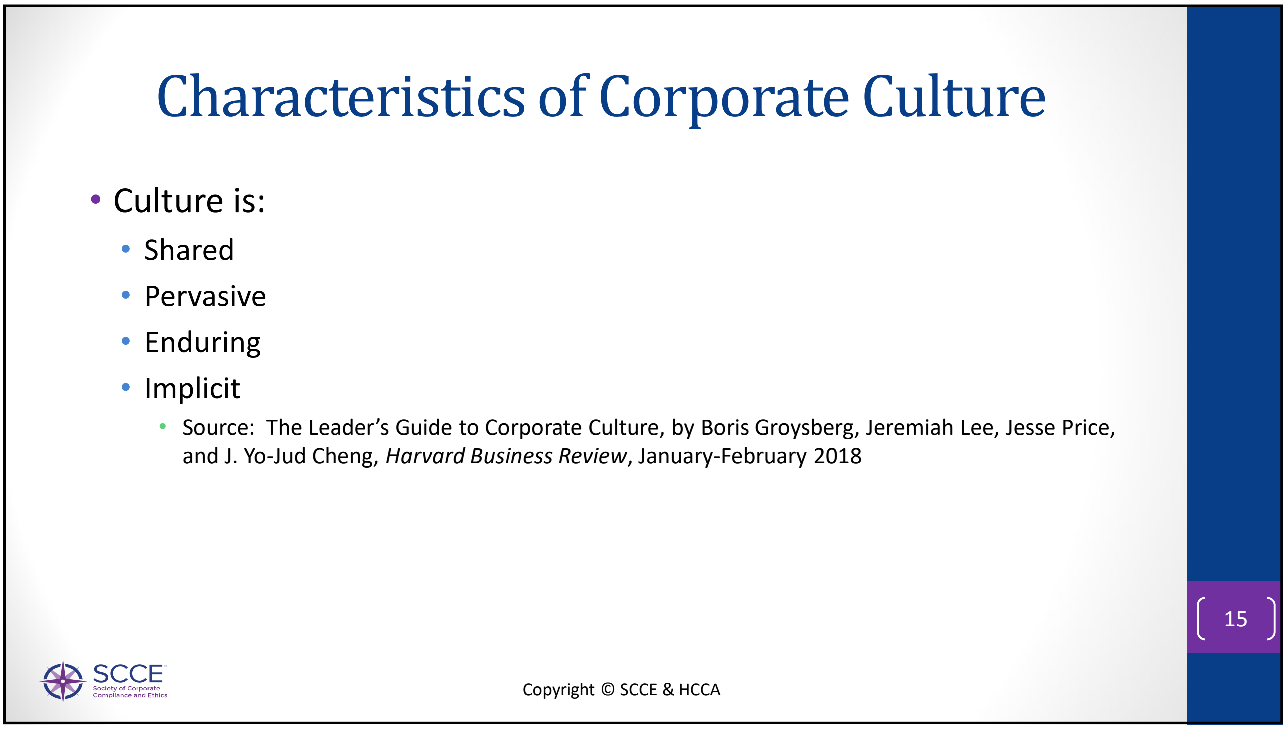
(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

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



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

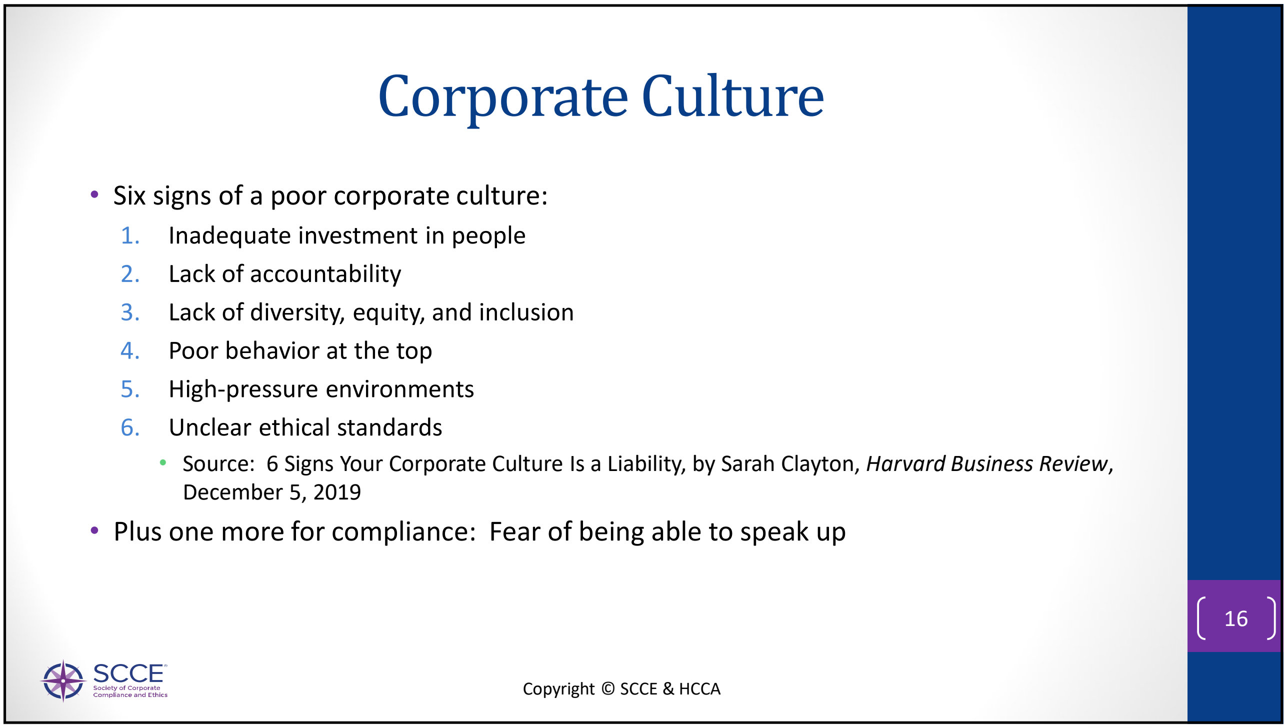


Characteristics of Corporate Culture

- 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

15

15

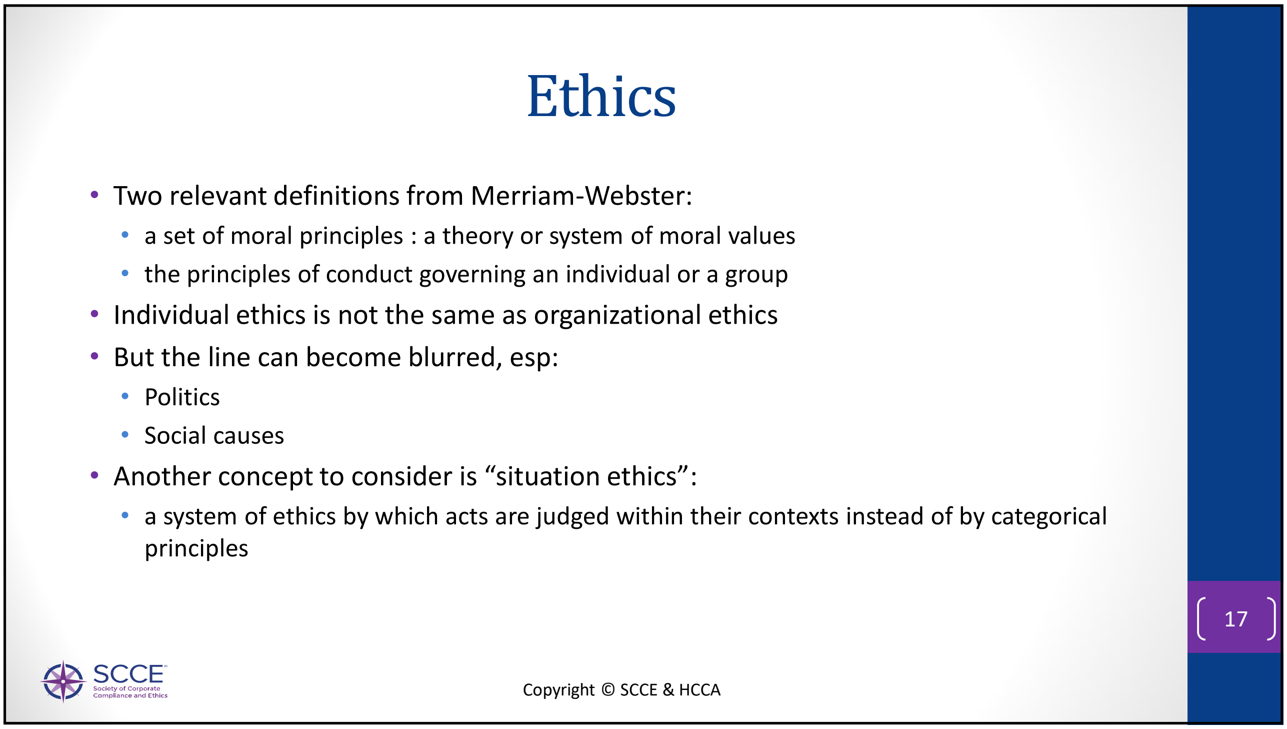


Corporate Culture

- 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

16

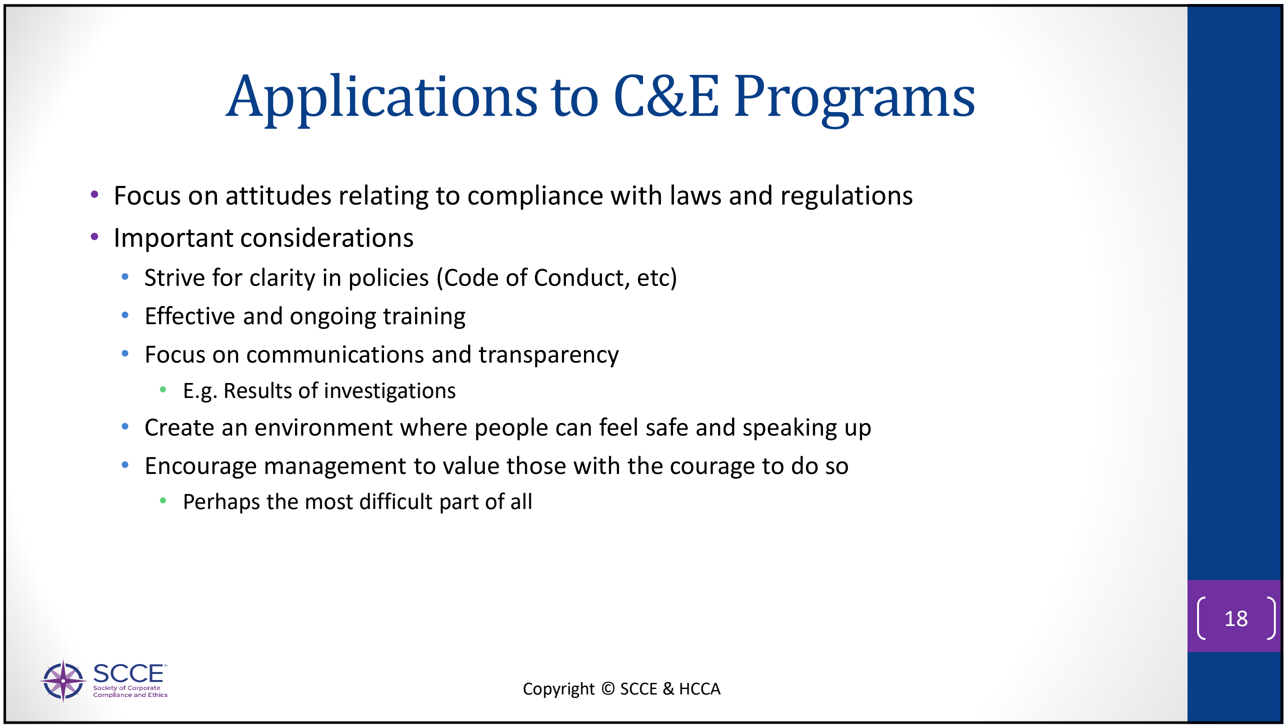
16



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

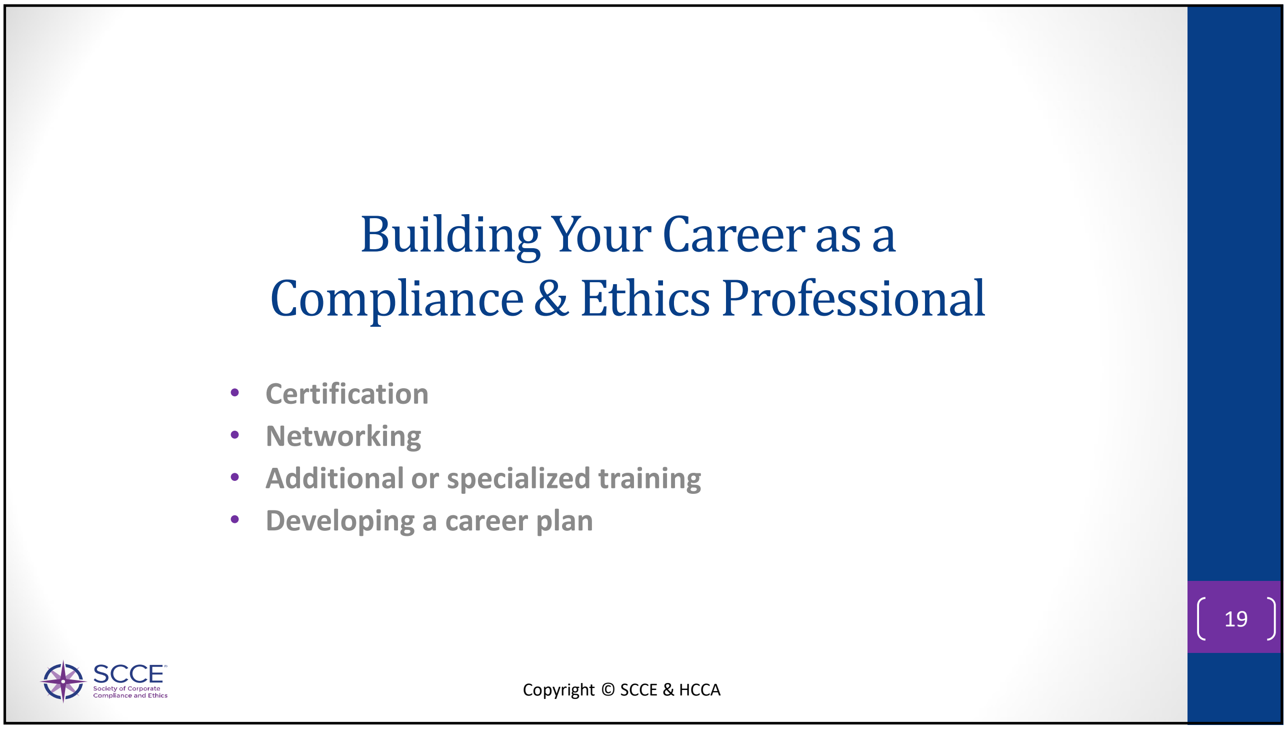
17



Applications to C&E Programs

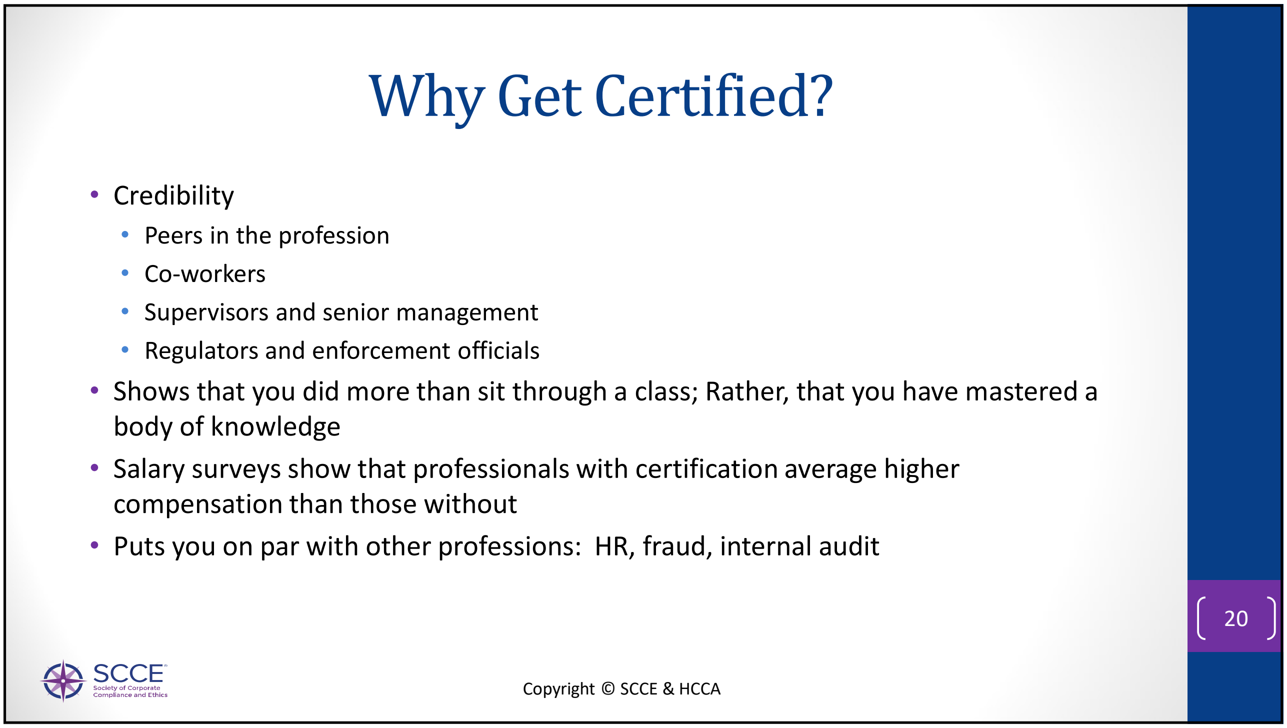
- Focus on attitudes relating to compliance with laws and regulations
- Important considerations
  - Strive for clarity in policies (Code of Conduct, etc)
  - Effective and ongoing training
  - Focus on communications and transparency
    - E.g. Results of investigations
  - Create an environment where 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



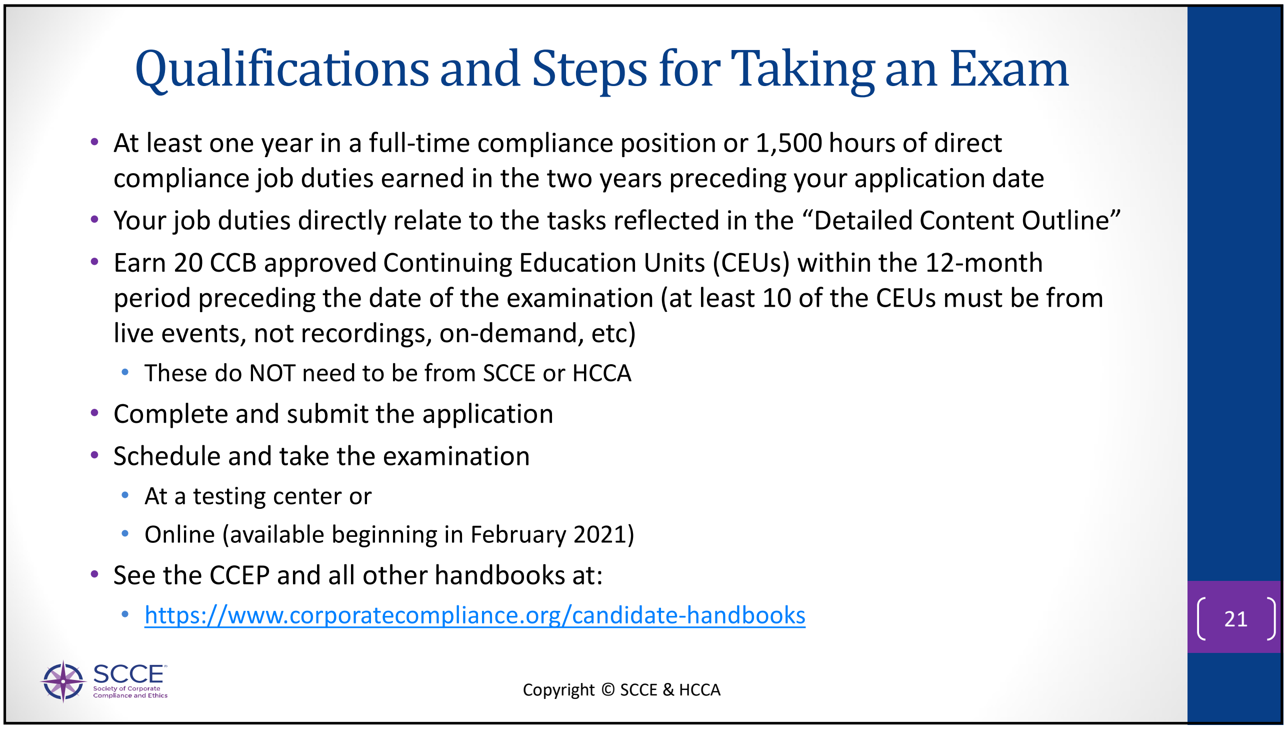
Building Your Career as a Compliance & Ethics Professional

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



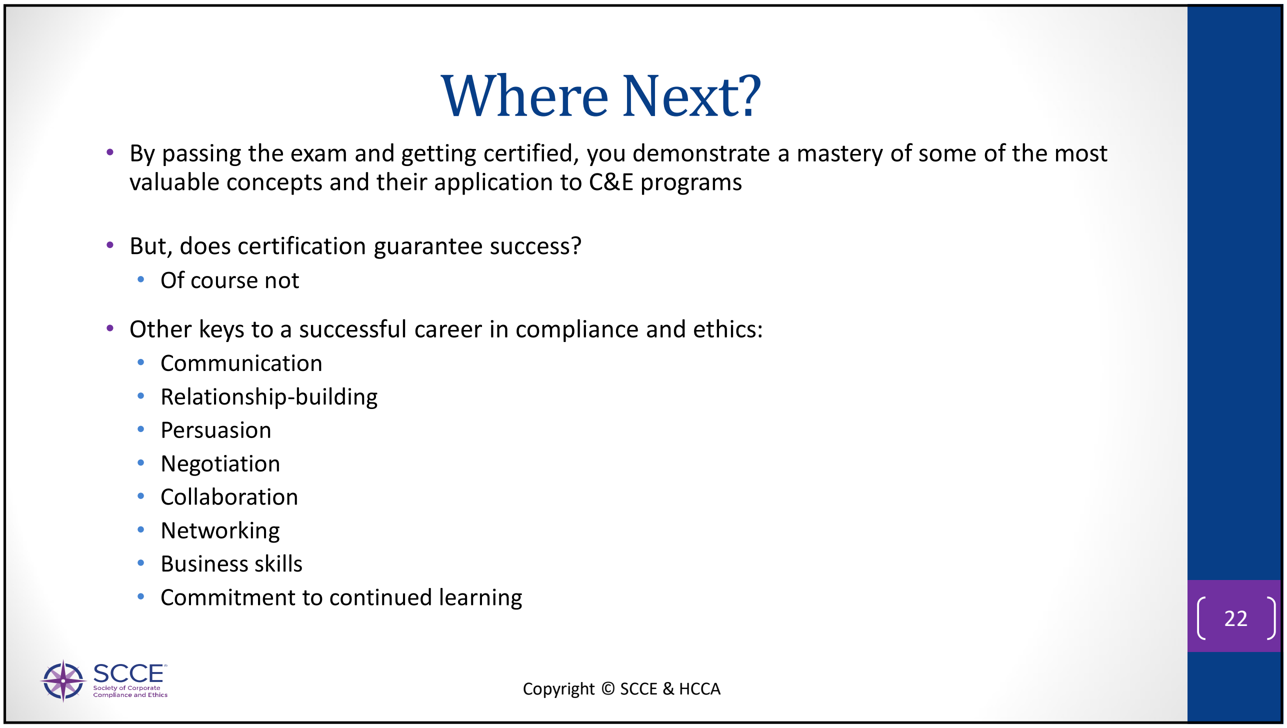
Why Get Certified?

- 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



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

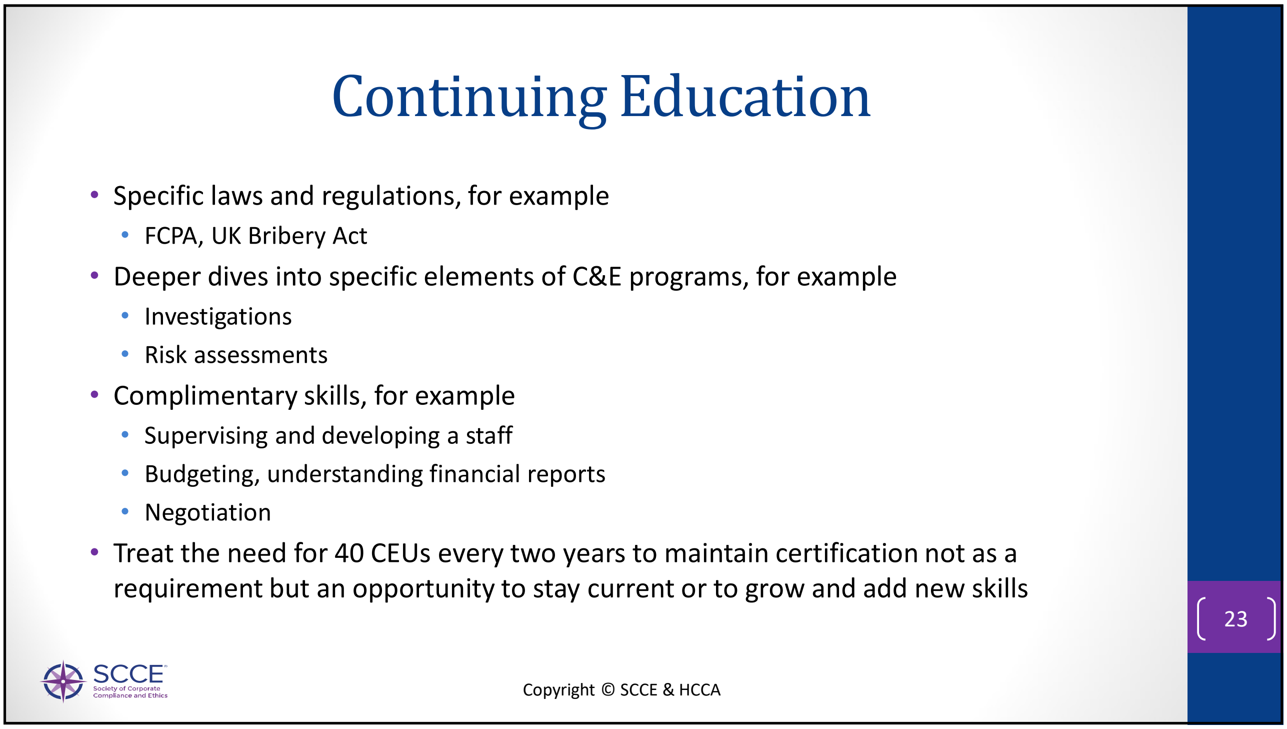


Where Next?

- 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

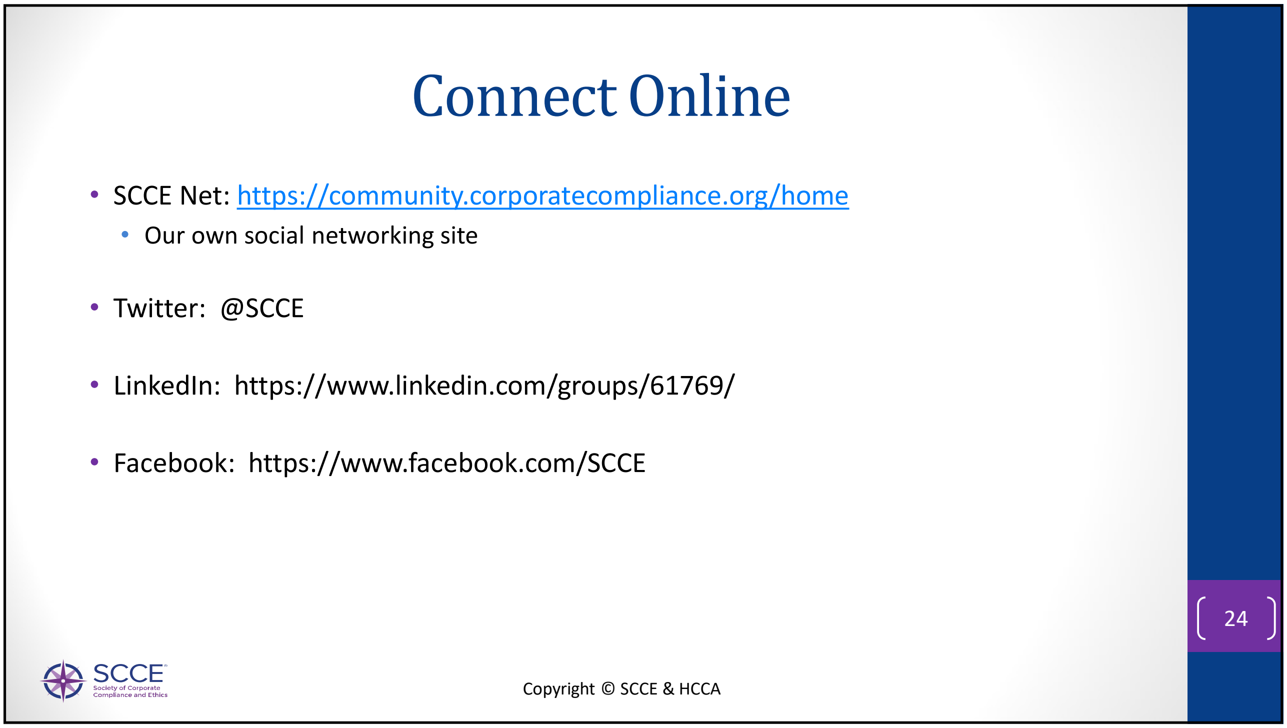
- But, does certification guarantee success?
  - Of course not

- Other keys to a successful career in compliance and ethics:
  - Communication
  - Relationship-building
  - Persuasion
  - Negotiation
  - Collaboration
  - Networking
  - Business skills
  - Commitment to continued learning



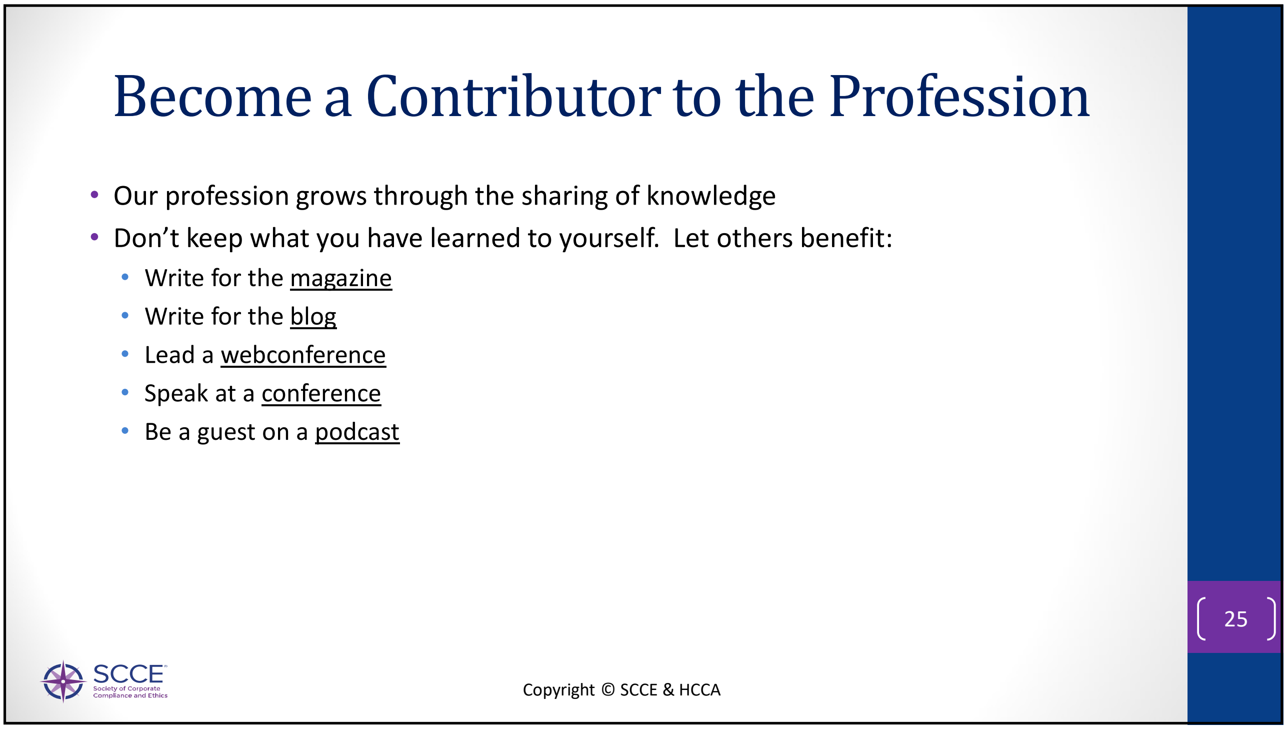
Continuing Education

- 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

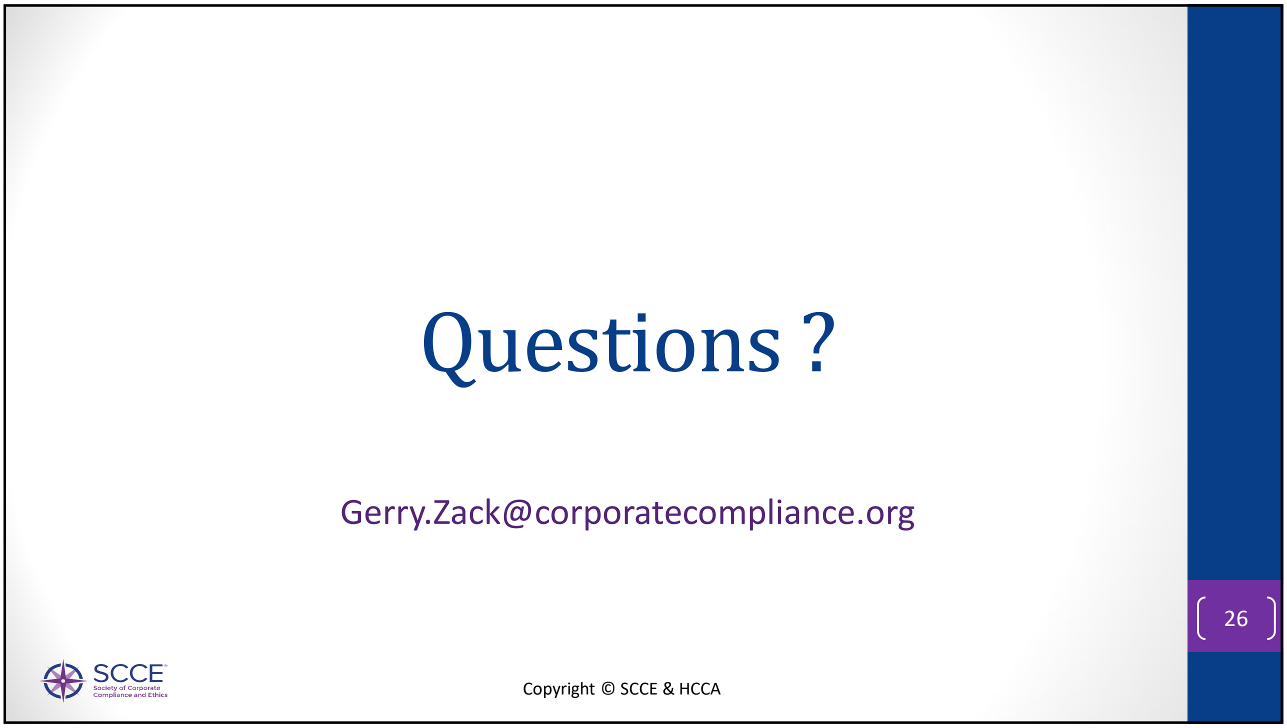
- SCCE Net: https://community.corporatecompliance.org/home
  - Our own social networking site
- Twitter: @SCCE
- LinkedIn: https://www.linkedin.com/groups/61769/
- Facebook: https://www.facebook.com/SCCE



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

SCCE Society of Corporate Compliance and Ethics



Questions ?

Gerry.Zack@corporatecompliance.org

SCCE Society of Corporate Compliance and Ethics