CCEP/CCEP-I
Study Group
February 2020
Facilitated by: Caitlyn Tobey, MBA, CCEP-I, CHC, CIPP/US/E, CIPM
With Special Guest: Bill Wong

What is on the exam?

1. Standards, Policies and Procedures
2. Compliance and Ethics Program Administration
3. Communication, Education, and Training
4. Monitoring, Auditing, and Internal Reporting Systems
5. Investigations and Response, Discipline and Incentives
6. Risk Assessment
This Session’s Focus

1. Standards, Policies and Procedures
2. Compliance and Ethics Program Administration

CCEP/CCEP-I Study Group - Caitlyn Tobey

Question 1

A compliance and ethics program should include
1. an employee benefits handbook
2. document retention guidelines
3. policies regarding confidentiality
4. a statement about the organization’s culture

A. 1, 2, and 3 only
B. 1, 2, and 4 only
C. 1, 3, and 4 only
D. 2, 3, and 4 only

CCEP/CCEP-I Study Group - Caitlyn Tobey
An employee benefits handbook usually falls under Human Resources, not Compliance. Document retention guidelines, policies regarding confidentiality, and a statement about the organization’s culture would fall under Compliance.

Question 2

A compliance and ethics professional is evaluating an organization’s employee handbook. A conflict exists between the Code of Conduct and the employee handbook. HR is responsible for the employee handbook. The documents have been approved by the board of directors. Which of the following actions should the compliance and ethics professional take FIRST?

A. Post revised documents on the organization’s website
B. Schedule time during the next board meeting to present revised documents
C. Schedule a meeting with HR, general counsel, and the board to discuss the issue
D. Contact HR to determine if the inconsistencies between the documents can be resolved
The FIRST step should always be to try and resolve an issue or investigate further before escalating it or overreacting.

CCEP/CCEP-I Study Group - Caitlyn Tobey

Question 3

A compliance and ethics professional has developed a policy intended to prohibit employees from paying, offering or promising to pay officials of other countries for the purposes of obtaining or maintaining business. This policy will help the organization comply with the

A. Sherman Act
B. USA PATRIOT Act
C. Anti-Money Laundering Act
D. Foreign Corrupt Practices Act
FCPA is the only answer that makes sense. Make sure that you know what each of these Acts relates to in case there are other questions on the exam that test your knowledge about them.

**Question 4**

Under *In re Caremark Int’l*, the basic fiduciary duty of care principle is characterized as acting in good faith with

A. reasonable care of management under similar circumstances
B. reasonable care of an organization under similar circumstances
C. the care of an ordinary prudent person under similar circumstances
D. the care of another compliance and ethics professional under similar circumstances
“The fiduciary duties of directors reflect the expectation of corporate stakeholders regarding oversight of corporate affairs. The basic fiduciary duty of care principle, which requires a director to act in good faith with the care an ordinarily prudent person would exercise under similar circumstances”

Source: https://oig.hhs.gov/fraud/docs/complianceguidance/040203corpr_esprsceguide.pdf

Question 5

A company’s Code of Conduct has not been reviewed for over 2 years. HR recommended adding content that would double its size. The compliance committee members expressed concern that adding a significant amount of content could negatively impact its effectiveness. Which of the following is the compliance and ethics professional’s NEXT step before consolidating revisions?

A. Request guidance from the board of directors
B. Contract with a consultant to rewrite the Code of Conduct
C. Compare the content outline with other organizations
D. Rewrite the content based on Federal Sentencing Guidelines
It is always best to have examples and to benchmark against other organizations before taking more drastic and expensive steps.

Question 6

According to the Sarbanes-Oxley Act, which of the following corporate employees can be employed by a corporation’s audit firm during the 1 year period preceding an audit?

A. CEO
B. Controller
C. Chief accounting officer
D. Compliance and ethics professional
SOX Section 206: Conflicts of Interest.
The CEO, Controller, CFO, Chief Accounting Officer or person in an equivalent position cannot have been employed by the company's audit firm during the 1-year period preceding the audit.

Question 7

A compliance structural policy differs from a substantive policy in that a structural policy should
A. describe the risk areas to the organization
B. describe how to operate within the regulations
C. define the regulations that apply to the organization
D. define the framework the program should operate within
A compliance and ethics professional in auditing the organization's compliance with the Sarbanes-Oxley Act. Which of the following findings indicates a violation?

A. The public accounting firm providing audit services has had the same audit partner reviewing the audits for the past 6 years.

B. The previous public accounting firm was the past employer of the company's current controller who participated in an audit 4 years ago.

C. The previous public accounting firm is providing bookkeeping related to the accounting records and financial statements they once audited.

D. The public accounting firm providing audit services has been contracted to provide tax services and the engagement was pre-approved by the board.
Standards, Policies, and Procedures

A. Assure compliance and ethics policies and procedures exist (e.g., non-retaliation, record management, conflict of interest, privacy, security, and confidentiality)
B. Maintain compliance and ethics policies and procedures
C. Consult with appropriate subject matter resources (e.g., legal, HR, finance)
D. Assure alignment among the organization's mission, vision, values, and the code(s) of conduct
E. Assure alignment of the compliance and ethics strategic plan is consistent with overall business objectives
F. Maintain a code of conduct
G. Ensure organizational value statements reflect a commitment to a culture of integrity
H. Assure policies and procedures address regulatory and legal requirements
I. Assure policies address interactions with third parties (e.g., vendors, business partners, and competitors)
J. Assure that compliance and ethics standards are included in contractual agreements with third parties (e.g., vendors, business partners, agents)
K. Document the compliance and ethics program (e.g., compliance manual/plan)
L. Assure policies and procedures around specifically identified risk areas are maintained
M. Assure governance policies for the compliance and ethics program are maintained
Key Compliance and Ethics Policies and Procedures

• Compliance Plan/Manual
  • Maintain governance policies for the compliance and ethics program
• Non-retaliation
  • Work with HR on this policy as it ties in to the HR Discipline Policy
• Record management/retention
  • Work with Legal on this (Standard is 7 years but can vary based on law)
• Conflict of Interest
• Privacy, security, and confidentiality
  • Work together with IS and Privacy Dept (if you have one)
• Code of Conduct (Keep it short, tailored to the org., and clear)

CCEP/CCEP-I Study Group - Caitlyn Tobey

Policies and Procedures

• Specifically Identified Risk Areas (e.g. conflicts of interest, privacy, anti-corruption and anti-bribery)
• Legal and Regulatory Requirements (e.g. Anti-money laundering policy for a mortgage lender)
• The only thing worse than not having a policy is having one and not following it

CCEP/CCEP-I Study Group - Caitlyn Tobey
Third Parties and Compliance

- Vendors, Business Partners, Agents
- Assure that compliance and ethics standards are included in contractual agreements (e.g. anti-slavery clause in supply chain related contracts, data protection, etc.)
- Policies about interactions with 3rd Parties
  - Conflict of Interest
  - Gifts, Gratuities and Entertainment

Mission, Vision, Values

- Assure alignment among the organization's mission, vision, values, and the code(s) of conduct
- Ensure organizational value statements reflect a commitment to a culture of integrity
- Assure alignment of the compliance and ethics strategic plan is consistent with overall business objectives
Compliance and Ethics Program Administration

A. Report compliance and ethics activity to the internal governing body (e.g., board of directors, audit committee)
B. Report compliance and ethics activity to the senior business leader (e.g., CEO, CFO)
C. Coordinate operational aspects of a compliance and ethics program with management (e.g., oversight committee, senior management)
D. Collaborate internally and externally with others to institute best practices (e.g., benchmarking)
E. Ensure that the goals and objectives of the compliance and ethics oversight committee are achieved
F. Maintain knowledge of relevant laws and regulations
G. Apply relevant laws and regulations to the needs of the organization
H. Assure the credibility and integrity of the compliance program
I. Recognize the need for outside expertise
J. Verify that the governing board understands its responsibilities related to the compliance and ethics program and culture
K. Ensure that the role of counsel in the compliance and ethics process has been defined
L. Manage resources for the compliance and ethics program (e.g., financial, personnel)
M. Integrate the compliance and ethics program into the business
N. Develop an annual compliance and ethics work plan
O. Ensure the organization has processes in place to manage identified risk areas (e.g., conflicts of interest, privacy, anti-corruption and anti-bribery)
P. Ensure background checks and screenings are conducted (e.g., new hires, substantial authority personnel, third parties, government lists)
Q. Verify the organization has defined the authority of the compliance and ethics professional

Internal Reporting Structure

- Internal governing body (e.g., board of directors, audit committee)
  - Verify that the governing board understands its responsibilities related to the compliance and ethics program and culture

- Senior business leader (e.g., CEO)

- Compliance Committee (Should include senior leaders and representation from key compliance areas)
Benchmarking

- Collaborate internally and externally with others to institute best practices
- Compare yourself to other similar companies

Annual compliance and ethics work plan

- Based on risk assessment
- Can use workforce surveys to gauge risk and awareness
- Be flexible as risks change (e.g. ransomware)
- Utilize outside resources (e.g. OIG work plan)

It is impossible to cover everything in an annual work plan so focus on your highest risk areas
Defining Roles

• Compliance Officer
  • Any limitations?
  • Do certain investigations need to be escalated to legal counsel for attorney
    client privilege?
• Legal Counsel (Outside or Inside)
• Human Resources
  • What do they investigate? (e.g. Employee Performance Issues)
  • Which policies are they responsible for? (e.g. Discipline Policy, FMLA, etc.)
  • Does Compliance have a role?

Legal Department vs. Compliance

**Legal**

“Defines and advises on the law”

• Provides Legal Advice and Analysis
• Attorney Client Privilege
• Sensitive Investigations
• Voluntary Disclosure to Regulators
• Criminal Penalties or Litigation
• Protects Against Legal Risk

**Compliance**

“Develops controls, policies, procedures, and systems”

• Advises Regarding Policies, Procedures and Processes
• Puts Controls in Place
• Routine Investigations, Auditing and Monitoring
• Fosters an Ethical Culture
Background checks

- Background checks and screenings must be conducted (e.g., new hires, substantial authority personnel, third parties, government lists)
  
  - List of Excluded Individuals/Entities (LEIE)
  - OFAC Specially Designated Nationals And Blocked Persons List (SDN)
  - Any others that your organizations use?

Credibility and Integrity

- How would you demonstrate credibility and integrity of the compliance program?
  - Discipline policy is applied regardless of rank (e.g. if a senior executive does something illegal, are they disciplined according to policy?)
Additional Resources

Compliance Podcasts
- Compliance Perspectives (SCCE)
- Privacy Advisor (IAPP)
- Great Women in Compliance with Mary Shirley and Lisa Fine
- FCPA Compliance and Ethics Report (Compliance Evangelist/Tom Fox)

Caremark Case and Board’s Fiduciary Duty
https://oig.hhs.gov/fraud/docs/complianceguidance/040203corpresprsceguide.pdf

Legal vs. Compliance Explanation

CCEP/CCEP-I Study Group - Caitlyn Tobey

Next Session’s Focus

3. Communication, Education, and Training
4. Monitoring, Auditing, and Internal Reporting Systems

CCEP/CCEP-I Study Group - Caitlyn Tobey