



Compliance Program Essentials

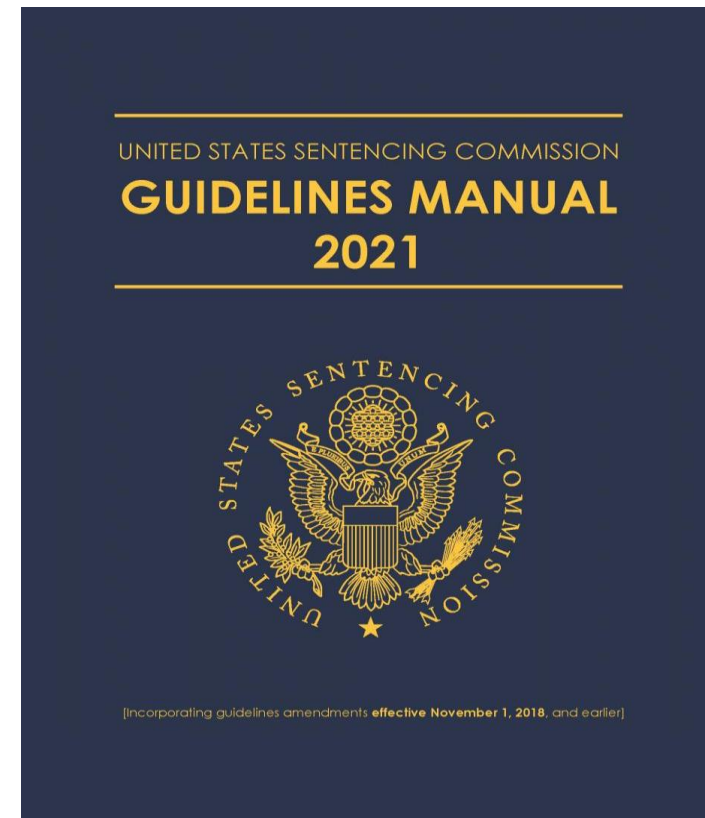
HILLARY HARLAN, BSRN, JD, CHC

A Little History...

- ▶ The 1990's and Corporate Scandals
- ▶ 2002 Sarbanes-Oxley Act
- ▶ 2004 Federal Sentencing Guidelines Amendments
- ▶ 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act
- ▶ 2010 OECD published Good Practice Guidance
- ▶ 2013 COSO adopted provisions for ethics as integral to framework

The Origin of the Sentencing Guidelines

- ▶ 1984 Sentencing Reform Act
- ▶ Creation of Sentencing Commission
- ▶ 1991 - Addition of Organizational Guidelines
- ▶ Periodic amendments to the Guidelines Manual over time



Ch. 8 U.S. Sentencing Guidelines – General Principals

1. The organization should remedy any harm caused by the offense.
2. If the organization operated primarily for a criminal purpose or primarily by criminal means, the fine should be set sufficiently high to divest the organization of all assets.
3. “Carrot and Stick Approach” – The fine range for any other organization should be based on the seriousness of the offense and the culpability of the organization. (Ch. 8 allows for substantial reductions for organizations that have established **effective compliance programs**.)
4. Probation is an appropriate sentence for an organizational defendant when needed to ensure that another sanction will be fully implemented, or to ensure that steps will be taken within the organization to reduce the likelihood of future criminal conduct.

Ch. 8 U.S. Sentencing Guidelines Elements of an Effective Compliance Program

- Implementing written standards of conduct, policies, and procedures
- Designating a compliance officer and compliance committee
- Conducting effective training and education
- Developing effective lines of communication
- Conducting internal monitoring and auditing
- Enforcing standards through well-publicized disciplinary guidelines
- Prompt response to problems and undertaking corrective action

Compliance & Ethics - A Culture of Integrity

- ▶ Tone at the Top
- ▶ Organizational Values
- ▶ Consistency of Messaging
- ▶ Middle Management
- ▶ Comfort Speaking Up
- ▶ Accountability
- ▶ The Hire-to-Retire Life Cycle
- ▶ Incentives and Rewards
- ▶ Procedural Justice

<https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Building-world-class-ethics-and-compliance-programs.pdf>

Compliance on a Budget

“You might expect that a compliance and ethics program is some exotic legal structure invented by the big accounting and law firms, or a set of detailed legal rules the government wants companies to follow. But in reality programs that work are about two things: a management commitment to do the right thing, and effective management steps to make that happen. It is about making sure that all those who work for the company know what to do, and believe that the company is serious about acting legally and ethically. The same types of management tools that make a company run successfully also need to be used to make sure it runs legally and ethically.”

- Joseph E. Murphy: A Compliance & Ethics Program on a Dollar a Day: How Small Companies Can Have Effective Programs
- https://assets.hcca-info.org/Portals/0/PDFs/Resources/library/723_0_CEProgramDollarADay-Murphy.pdf

Written Standards and Procedures

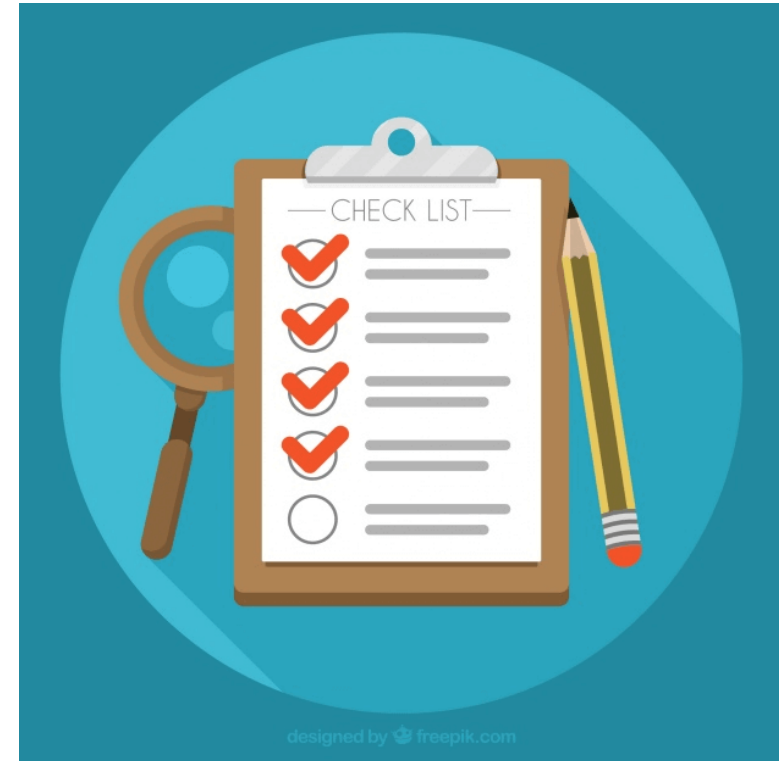
- ▶ Code of Conduct and Compliance Policies
 - ▶ Conflict of Interest, Whistleblower/Non-Retaliation, Anti-Trust, Privacy and Security, Gifts and Gratuities, Record Retention, Fraud/Waste/Abuse
- ▶ Written statement of your organization's commitment to compliance
- ▶ Compliance and Ethics Program/Plan
- ▶ Board Resolution
- ▶ Elect a Chief Compliance Officer
- ▶ Procedures / Controls (ex. Significant expenditures)
- ▶ Unannounced reviews

Designate a Compliance Officer

- ▶ A trusted Senior Manager (small-medium organizations)
- ▶ Makes regular reports to the Board and to senior management
- ▶ Provides compliance training to the Board or highest organizational authority, as well as organization-wide
- ▶ Requires that senior management report their compliance efforts/program implementation/monitoring
- ▶ Multiple locations? Consider compliance liaisons
- ▶ Personal commitment to the compliance and ethics program

Care in Hiring Practices

- ▶ Always check references prior to hire
- ▶ Check databases for excluded individuals (ex. OIG Exclusion Database, GSA Database)
 - ▶ Include vendors / 3rd parties against databases
- ▶ Management or sensitive positions – internet search and document



Dealing With Third Parties

- ▶ Do thorough research before retaining agents, consultants, and other business partners. Ask for references!
- ▶ Provide your Code of Conduct to all third parties that you do business with
- ▶ Include “compliance with all laws” language in contracts
- ▶ Ensure your business partners are aware of how to report compliance issues and require reporting of any known or suspected illegal or unethical conduct
- ▶ Require all agents and contractors to have a compliance program

Compliance Program Auditing and Monitoring

- ▶ Make the rounds and talk to your people!
- ▶ Observe, utilize a compliance checklist, document and follow-up
- ▶ Include Compliance and Ethics components in performance reviews and exit interviews
- ▶ Leverage qualitative surveys
- ▶ Establish reporting mechanisms and publicize
- ▶ Program evaluation – peer reviews

Enforcing Standards – Disciplinary Guidelines

- ▶ Discipline must be consistent and include those who should have, but did not detect violations
- ▶ Failure to complete Compliance training (ex. Bonus, promotion, etc)
- ▶ Disciplinary Guidelines
- ▶ CO should “sign off” on disciplinary cases involving compliance violations



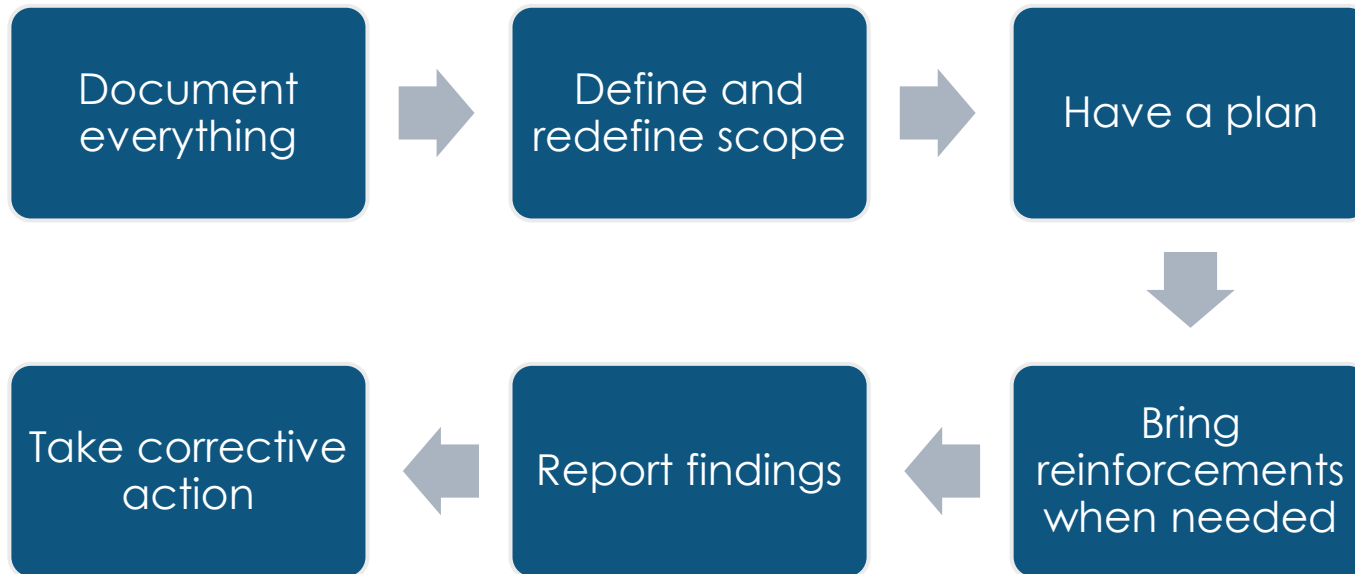
Performance Objectives, Incentives, and Appraisals

- ▶ Include Compliance Program elements into how you measure and incent performance
- ▶ Include Compliance Program elements into quarterly/annual performance appraisals/reviews
- ▶ When evaluating direct reports, ask what he/she did to advance compliance and ethics in their service line or business unit. Document and set Compliance Program goals for the next year.
- ▶ Recognition for Compliance Program leadership

Prompt Response and Corrective Action

- ▶ “See it. Say it. Fix it.”
- ▶ Launch internal investigations when applicable/assess need for privilege
- ▶ Compliance audits – follow-through with all corrective action and “spot audit”
- ▶ Discuss any compliance and ethics failures with senior management and focus on prevention
- ▶ Leverage legal counsel

Conducting Internal Investigations



The 8th Element – Risk Assessment

“The starting point for all compliance programs is knowing what areas have the highest potential for violations of law. You need to ferret out and prevent the most serious types of risk for your organization. That means you need a solid understanding of the environment you are operating in.”

Tim Cercelle, Director, Deloitte Advisory, Deloitte & Touche LLP:
Building World Class Ethics and Compliance Programs



Compliance Risk Assessment

	ERM	Internal Audit	Compliance
Objective	Identify, prioritize, and assign accountability for managing strategic, operational, financial, and reputational risks	Determine and prioritize risks to aid in developing the internal audit plan, helping to provide the board and the executive team with assurances related to risk management efforts and other compliance activities	Identify, prioritize, and assign accountability for managing existing or potential threats related to legal or policy noncompliance—or ethical misconduct—that could lead to fines or penalties, reputational damage, or the inability to operate in key markets
Scope	Any risk significantly impacting the organization's ability to achieve its strategic objectives	Financial statement and internal control risks, as well as some operational and compliance risks that are likely to materially impact the performance of the enterprise or financial statements	Laws and regulations with which the organization is required to comply in all jurisdictions where it conducts business, as well as critical organizational policies—whether or not those policies are based on legal requirements
Typical Owner	Chief Risk Officer/Chief Financial Officer	Chief Audit Executive	Chief Compliance Officer

<https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Building-world-class-ethics-and-compliance-programs.pdf>

An Effective Compliance Risk Assessment

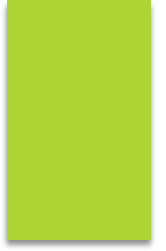
- ▶ Gather input from cross-functional stakeholders
- ▶ Leverage existing material
- ▶ Establish clear risk ownership
- ▶ Ensure the assessment is “actionable”
- ▶ Solicit external input when appropriate
- ▶ Treat the assessment as a fluid document/tool
- ▶ Use plain language
- ▶ Repeat the assessment periodically
- ▶ Leverage the data

Risk Considerations

- ▶ What are types of compliance risk impacting brand or reputation?
- ▶ Is there internal risk, supply chain risk, third party risk?
- ▶ Are there compliance issues which could cause the organization to lose the ability to sell/deliver products or services?
- ▶ Is there a need for compliance program design, technology, processes, or resource changes pursuant to strategic plan, acquisition or expansion?
- ▶ Is there sufficient communication to customers, investors, third parties and other stakeholders re: values, vision and commitment to compliance?
- ▶ Has the organization made sufficient investment in compliance (beyond salary/benefits) relative to size and risk profile?
- ▶ Is the compliance function well-positioned within the organization (has a seat at the “strategic table”)?
- ▶ What are the personal/professional exposure of executive management and Board as it relates to compliance?



QUESTIONS



References

U.S. Sentencing Guidelines:

<https://guidelines.uscourts.gov/gi/%C2%A78B2.1>

Society for Corporate Compliance and Ethics:

<https://www.corporatecompliance.org/>

Deloitte:

<https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Building-world-class-ethics-and-compliance-programs.pdf>