KAPLAN & WALKER LLP

Compliance and Ethics Risk Assessment: The Foundation of an Effective C&E Program

SCCE Alaska Regional Conference

February 23, 2023

Amii Barnard-Bahn, JD, CCEP
Kaplan & Walker LLP

Rebecca Walker, JD, CCEP
Kaplan & Walker LLP

1

Agenda

- Why conduct a C&E risk assessment
- Legal guidance
- Methodologies
- Attorney-client privilege
- Program improvements
- Reporting the results
- Pitfalls to avoid

2

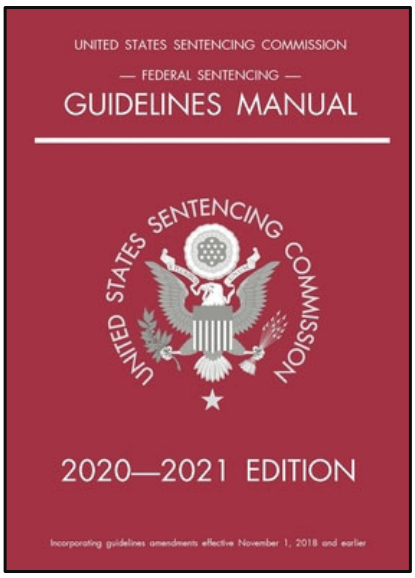
Why do it?

- Efficient use of program resources
- Broad-based contributions to the program
  - Greater buy-in
  - Program improvements
- Rationalizes program components
  - For You
  - For Senior Leadership
  - For the Board
- Legal guidance places great importance on risk assessments

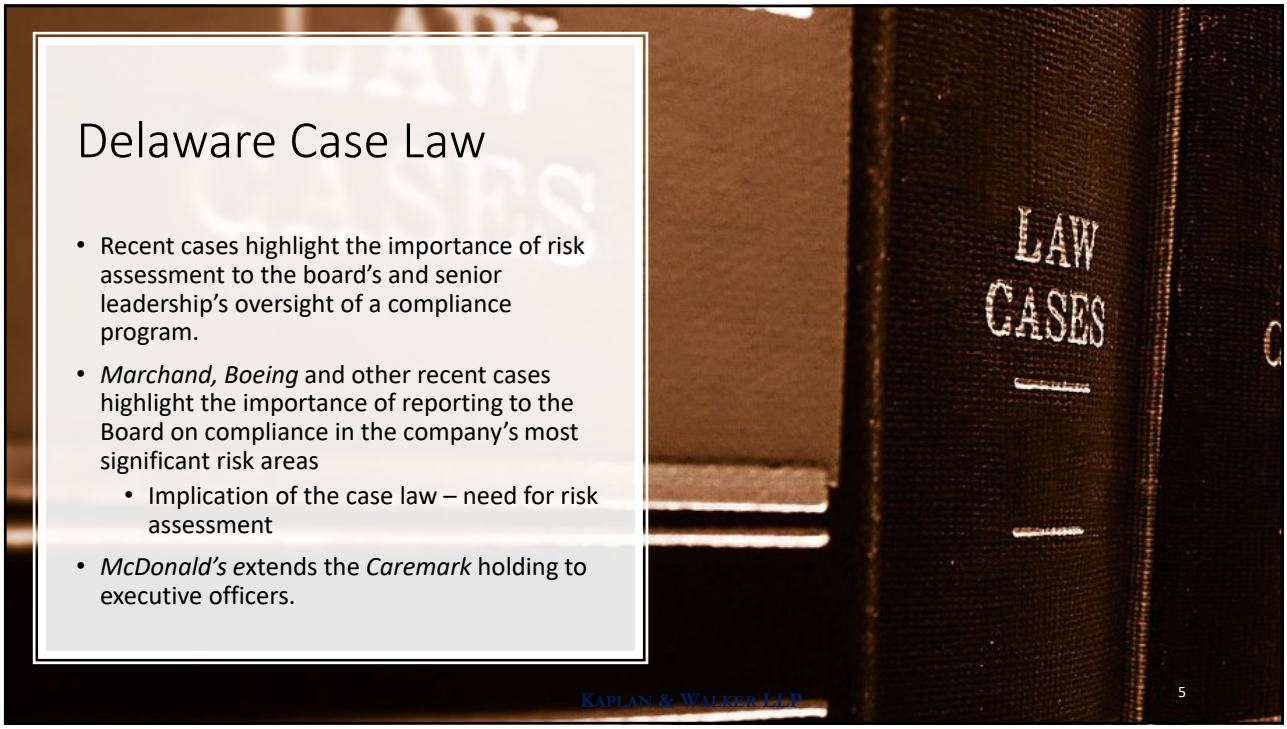
3

Legal Guidance

- Sentencing Guidelines
  - "The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each (of the components of an effective compliance and ethics program) to reduce the risk of criminal conduct identified through this process." - U.S.S.G. 8B2.1(c)
- DOJ Guidance Memo
  - Prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the ***location*** of its operations, the ***industry*** sector, the competitiveness of the ***market***, the ***regulatory landscape***, potential ***clients*** and ***business partners***, ***transactions with foreign governments***, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.
  - Prosecutors should also consider the effectiveness of the company's risk assessment and the manner in which the company's compliance ***program*** has been ***tailored based on that risk assessment*** and whether its criteria are periodically updated.
- Some of the questions the DOJ will ask:
  - 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?
  - Does the risk assessment consider lessons learned?



4



5

Methodology

- Determine scope
- Document and information review
- Interviews
- Surveys or questionnaires
- Focus groups?
- Report out

6

Relationship to ERM

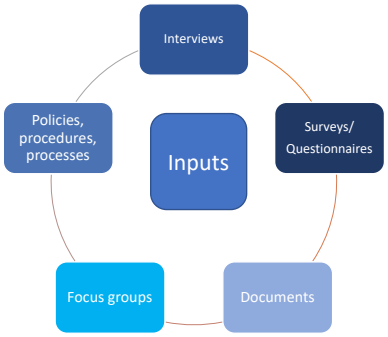
- Plenty of overlap in concept and practice
  - And synergies can exist, in particular with respect to employee interviews
- But embedding C&E into ERM entirely may be suboptimal
  - C&E risks may not be significant enough to warrant a lot of attention in relation to other enterprise risks.
  - ERM process typically does not include the level of granularity that may be necessary for a robust C&E risk assessment process.
  - The ERM process may not be focused on mitigation in the same way that C&E risk assessment is.

Scope of the Assessment

- May choose to omit risk areas from scope because:
  - Risks are too remote (either likelihood or impact) for inclusion
    - e.g., FCPA risks for an entirely U.S./domestic organization
  - There already exists a defined and sufficiently robust risk assessment process. Possible areas include, e.g.,
    - Environmental
    - Product safety
    - Workplace safety
  - The risk is owned by another function.
  - **Other reasons?**
- Cyber?
- ESG?

Inputs

- Employee (and director) interviews
- Interviews of third parties (lawyers, consultants)
- Surveys
- Questionnaires
- Existing documents and data
- Focus groups?
- Policies, procedures, documentation of existing controls and mitigation strategies
- What else?



Documents and Data

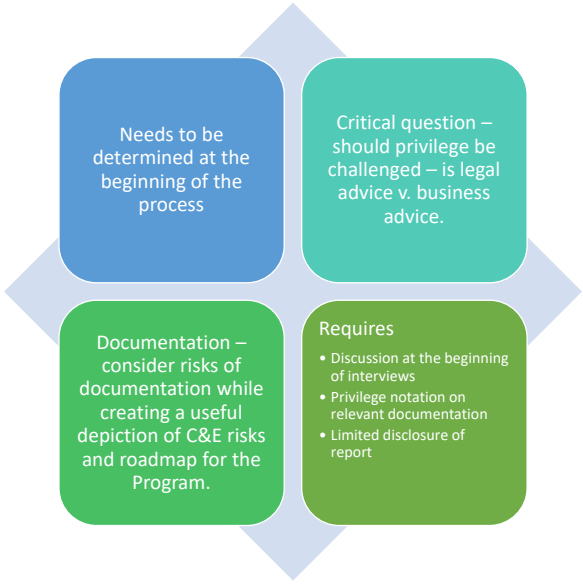
- Helpline and other reports of suspected misconduct
- Investigations and substantiated allegations
- Internal audit reports
- Employee culture survey data
- Litigation records
- Enforcement activity
- Compliance program information
  - Remember that you also need information on controls!
- Other?

Interviews

- Who should be interviewed?
- How valuable is the information?
- Interviews provide opportunity to
  - Gather information AND
  - Impart information regarding the program
- Be prepared to be challenged
  - "I just did this with ERM."
  - "What do you mean by 'legal and compliance risks' anyway?"
  - "How am I supposed to measure the impact of a violation?"
- Focus on the positive is sometimes more effective (e.g., "in what areas would the company benefit from additional controls?")
- Interviews can be useful in understanding the causes of risks, which is essential for recommending appropriate controls.

11

Privilege?



12

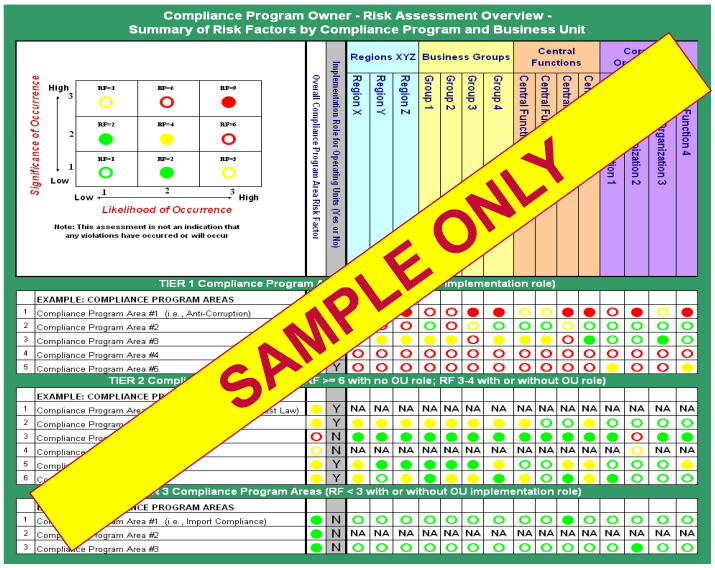
Rating Risks

- Are numbers/ratings useful?
- Balancing likelihood against impact
- Consistency of ratings across risk areas
- Look out for ratings being skewed by
  - Undue focus by enforcement officials in pronouncements
  - Our own cognitive biases
- Inherent v. residual
  - Scoring can ignore critical risks where likelihood is low
  - Measurements can contain a high degree of guess work where certainty is low
- Ratings may lead to undervaluation of soft risks like culture and behavior
- Where do general compliance controls fit in?

Looking "Inward": The Importance of Granularity

- C&E risk is are often more local than global, and
- C&E risk mitigation is often more effective at local level
- Consider risk in three dimensions
  - Geography, business unit and/or product/service
  - Risk area (e.g., harassment, antitrust, corruption)
  - Mitigation tool, e.g.:
    - Training
    - Due diligence
    - Auditing

Sample: A Consolidated View



Using the Results: Some Examples

- Determine whether additional C&E policies are needed for any part of the company (e.g., business or geographical unit) on any given topic, or whether any policies need to be revised
- Develop company-specific examples or Q&A that can help make a code of conduct less abstract
- Determine whether any additional C&E training or communications should be disseminated to any part of the company on any given topic
- Develop/enhance C&E audit protocols and/or monitoring tools
- Identify risk areas for which pre-approvals by management or staff for specified (high-risk) activities are warranted
- Modify performance objectives to mitigate C&E risk
- Add C&E components to job descriptions, performance-evaluation criteria or business unit plans in a risk-based way
- Establish additional C&E oversight/reporting responsibilities for high-risk areas

Reporting the Results

To the Board

- *Boeing* and *Marchand v. Barnhill* have highlighted the importance of the Board's oversight of compliance in high-risk areas.

To senior management

- *McDonald's*

To employees

17

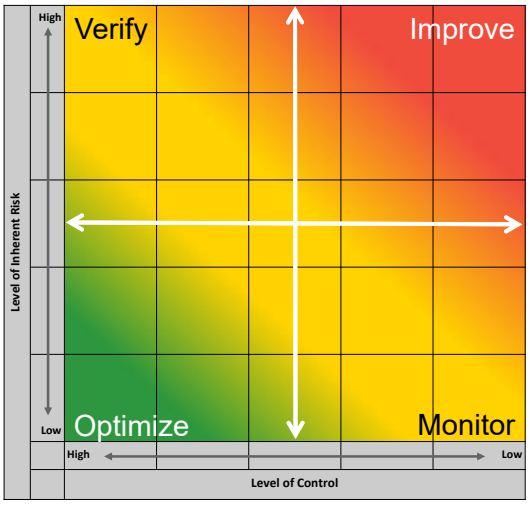
Risk Assessment Prioritization

Improve
- *High risk exposures with low levels of control form the priorities for improvement opportunities.*

Verify
- *High risk exposures with strong controls form the focus for audit to provide assurance that controls are adequate and efficient.*

Monitor
- *Low risk exposures accompanied by a lower level of control are often considered emerging and must remain a focus of ongoing monitoring efforts*

Optimize
- *Low risk exposures with a moderate level of control may be consciously accepted or may be a focus to optimize the processes and controls for greater efficiency.*



18

Pitfalls to Avoid

Biting off more than you can chew (i.e., ignoring the importance of prioritizing)

Risk assessment fatigue (often the result of parallel risk assessments)

Duplicating risks with other groups

Impractical recommendations and failure to act on risk assessment results

- Discuss recommendations with the BU and with Legal before finalizing

Not involving leadership or key positions (e.g., folks from each BU, geography, function)

Focusing on isolated comments that may not be representative

Overstating or using inflammatory language about risks

- Be careful not to confuse opinion or conjecture with fact