Entrepreneurs have too many things to do while launching their startups and too little time to do everything well. In order to be successful and sustainable, entrepreneurs need to develop a winning business model that will attract investors and meet their expectations regarding liquidity. Entrepreneurs also need to develop products and services that are innovative and competitive and demonstrate that a group of loyal followers willing to pay for the product or service can be identified and recruited. On top of all that, entrepreneurs need to fill out their management teams, recruit the necessary talent, build an infrastructure and forge relationships with multiple stakeholders.

With all this on his or her plate, it should come as no surprise that a formal compliance program is probably near the bottom of the “to do” list. There is no question that startups and emerging companies typically lack the financial and human resources to take all of the steps that would be taken by larger organizations to design and implement effective and scalable compliance program. Even so they must nonetheless be prepared to manage significant compliance risks from Day One for essentially two basic reasons. First, a compliance failure exposes the company, its directors, executives and employees to criminal, civil or administrative investigations and liability. Even if liability is avoided, the legal and investigative costs can be staggering as can the toll such a matter takes on the time and morale of a burgeoning organizations human capital.

Although ethics and compliance programs legally mandated through the U.S. Sentencing Guidelines and other statutory and regulatory schemes, for example by Sarbanes-Oxley, the Federal Acquisition Regulations; anti-money laundering laws; or strongly encouraged by the U.S. Department of Justice, these legal schemes contemplate that the smaller organization need not deploy the resources toward an ethics and compliance program to the same degree as a large, well-established company. Specifically, the comments to the U.S. Sentencing Guidelines provide that the formality and scope of the program depends on the size of the organization. U.S. Federal Sentencing Guidelines, §8B2.1, Comments While large organizations are expected to make a significant resource commitment, a smaller organization may rely on existing processes as long as it demonstrates a commitment to operating ethically and in compliance with laws. Id. The Guidelines also encourage larger organizations to collaborate with their smaller business partners in developing an effective ethics and compliance program. Id.

The U.S. Department of Justice’s recent guidance to organizations on what it expects to see in an effective ethics and compliance program mirrors the Sentencing Guidelines – in that the guidance emphasizes that all organizations should develop an ethics and compliance program that is based on a well-thought out risk assessment. Evaluation of Corporate Compliance Program, The U.S. Dep’t of Justice https://www.justice.gov/criminal-fraud/page/file/937501 (Last visited Feb. 19, 2019). The risk assessment is a vital first step as any organization, particularly an emerging company, sets out to identify and prioritize its risks. For the new organization must
efficiently and effectively deploy its resources while it strives for growth. The risk
assessment is the first step for a new company as it develops its ethics and compliance
program because it enables its leaders and executives to hone in on the most significant
legal risks – the risks that have the potential to expose the organization to significant
criminal and civil liability. Identifying these risks and then, designing both functional
and strategic plans to mitigate these risks enable the emerging company to inoculate itself
from some of its most destructive legal issues.

An emerging organization’s lawyers are uniquely situated to provide the organization the
pragmatic advice and easy-to-use tools in developing the ethics and compliance program.
Lawyers may do so by educating the directors and officers of startups on their duties and
responsibilities with respect to compliance, guide the organization through a risk
assessment, implement compliance policies and procedures that are appropriate based on
the risk assessment and on the structure of the startup organization and provide support
for organizational education and training.

However, not only should lawyers provide this governance and organizational support,
they should also advise on the legal and business risks relating to compliance; and how
mitigating those risks fits into the startup world, particularly areas of highest risk for new
companies—the issues that can truly kill the business before it ever gets started—and
provide guidance, based on decades of experience, on how to address the questions that
investors and business partners will have about a startup’s compliance and risk
management systems. Lawyers should not only work with their clients on complying
with laws but should also dive into important and sensitive conversations with
entrepreneurs regarding ethical business conduct.
Don’t Let Lack of Compliance Derail Your Startup: Practical Approaches to Compliance & Ethics

A Handout With: The Law and Some Tips
Panelists:
Robert Brown, Lynch Cox Gilman & Goodman
rbrown@globallawbusiness.com
Margaret M. Cassidy, Cassidy Law
m.cassidy@cassidylawpllc.com
Alan Gutterman, Royse Law
alangutterman@gmail.com

Moderator:
Lauren B. Ziegler, Nemphos Broue
lziegler@nemphosbraue.com
AGENDA

• Legal Requirements for Compliance Programs
• Laws & Regulations That Inform the Compliance Program
• Incentives to Disclose Corporate Wrongdoing: Whistleblowing
• Identifying and Mitigating Legal Risks
Legal Requirements for An Ethics & Compliance Program
A GOOD CORPORATE CITIZEN….

- Oversight by high-level personnel
- Due care in delegating substantial discretionary authority
- Effective communication to all levels of employees
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal
- Consistent enforcement of compliance standards including disciplinary mechanisms
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation

US Federal Sentencing Guidelines, §8B2.1
• Mandates effective means for disclosing controls and procedures over financial reporting accuracy
• Legal risks and liability may arise under different substantive areas of the law, eg: corruption, export, anti-corporation, privacy
• Disclose in organization’s financial reports
• Must disclose material weaknesses
• Ongoing disclosure requirements
• Criminal and civil penalties


cassidylawpllc.com
ADDITIONAL LEGAL REQUIREMENTS

PCAOB Auditing Standard No. 5: Audit must review for any deficiencies in controls designed to prevent and detect fraud when auditing internal controls for financial reporting and auditors must take into account these deficiencies when developing response to risk of material misstatements.

Caremark Duty of Care (In re Caremark Int’l Inc., 698 A.2d 959, Del. Ch. 1996): Boards must assure that corporate information and reporting systems are adequate; failing to do so exposes directors to liability for non-compliance.

NYSE Listed Company Manual, §303A.10: “Listed companies must adopt and disclose a code of business conduct and ethics for directors, officers and employees, and promptly disclose any waivers of the code for directors or executive officers.”
The Department has placed a high priority on combating white collar crime.

Department policy is that criminal prosecutors and civil trial counsel should timely communicate, coordinate, and cooperate with one another and agency attorneys to the fullest extent appropriate to the case and permissible by law, whenever an alleged offense or violation of federal law gives rise to the potential for criminal, civil, regulatory, and/or agency administrative parallel (simultaneous or successive) proceedings. By working together in this way, the Department can better protect the government’s interests (including deterrence of future misconduct and restoration of program integrity) and assure the full range of the government’s remedies (including incarceration, fines, penalties, damages, restitution to victims, asset seizures, civil and criminal forfeiture, and exclusion and debarment).

The potential for parallel proceedings arises in many of the Department’s white collar enforcement priorities, and it is essential that an effective and successful response involve an evaluation of criminal, civil, regulatory, and administrative remedies. Although some matters
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-17.000</td>
<td>Speedy Trial Act of 1974</td>
</tr>
<tr>
<td>9-18.000</td>
<td>Defenses</td>
</tr>
<tr>
<td>9-19.000</td>
<td>Documentary Material Held by Third Parties</td>
</tr>
<tr>
<td>9-20.000</td>
<td>Maritime, Territorial and Indian Jurisdiction</td>
</tr>
<tr>
<td>9-21.000</td>
<td>Witness Security</td>
</tr>
<tr>
<td>9-22.000</td>
<td>Pretrial Diversion Program</td>
</tr>
<tr>
<td>9-23.000</td>
<td>Witness Immunity</td>
</tr>
<tr>
<td>9-24.000</td>
<td>Requesting Special Confinement Conditions—28 C.F.R. § 501.3</td>
</tr>
<tr>
<td>9-25.000</td>
<td>26.000 [RESERVED]</td>
</tr>
<tr>
<td>9-27.000</td>
<td>Principles of Federal Prosecution</td>
</tr>
<tr>
<td>9-28.000</td>
<td>Principles of Federal Prosecution of Business Organizations</td>
</tr>
<tr>
<td>9-29.000-33.000</td>
<td>[RESERVED]</td>
</tr>
<tr>
<td>9-34.000</td>
<td>Preparation of Reports on Convicted Prisoners for the Parole Commission</td>
</tr>
<tr>
<td>9-35.000</td>
<td>International Prisoner Transfers</td>
</tr>
<tr>
<td>9-36.000</td>
<td>[RESERVED]</td>
</tr>
<tr>
<td>9-38.000</td>
<td>[RESERVED]</td>
</tr>
<tr>
<td>9-39.000</td>
<td>Contempt of Court</td>
</tr>
<tr>
<td>9-40.000</td>
<td>Bank Frauds and Related Offenses—Policy</td>
</tr>
</tbody>
</table>
FACTORS TO BE CONSIDERED USAM 9-28.300

- Nature of the offense - risk of harm to the public
- Pervasiveness of wrongdoing
- History of similar misconduct
- Disclosure of wrongdoing
- Willingness to cooperate in the investigation
- Effectiveness of compliance program
- Remedial actions the organization undertook
- Collateral consequences of prosecution
- Adequacy of prosecuting of responsible individuals
- Adequacy of other remedies - civil or regulatory enforcement
DOJ POSITION ON PROSECUTING INDIVIDUAL CORPORATE WRONGDOERS

- Yates Memo released September 9, 2015 – created guidelines for prosecuting corporations and their employees
- To get cooperation credit corporations must disclose to DOJ the individuals “responsible” for the misconduct
- DOJ criminal and civil attorneys should communicate on corporate investigations
- DOJ will pursue individuals in corporate wrongdoing cases– unless unique unique situation
DOJ Compliance Program Evaluation

• Issued in February 2017
• Latest pronouncement on expectations for effective compliance programs; prior guidance:
  • FCPA Corporate Enforcement Policy
  • A Resource Guide to the US FCPA
• Demonstrates increased sophistication of DOJ’s compliance expertise
• “Ground rules” for
  • Companies subject to federal investigation or prosecution
  • Companies designing, enhancing or implementing compliance programs
• Emphasis on 11 key topics and program assessment questions – parallel corporate compliance program requirements
Laws & Regulations That Inform An Ethics & Compliance Program
FOREIGN CORRUPT PRACTICES ACT

- Enacted in 1977 to prevent corporate bribery of foreign officials by US companies
- Anti-bribery provision is main focus
- Other provisions: books & records; internal controls
- Main U.S. government enforcement:
  - Department of Justice
  - Securities and Exchange Commission
Accurately record transactions with enough detail to identify the transactions. Create and maintain an accounting system with controls that provide reasonable assurances that:

- Transactions are executed as management has authorized.
- Transactions are recorded to assure financial statements conform with generally accepted accounting principles or any other applicable criteria for the statements.
- Assets may be accounted for.
- Access to assets is permitted consistent with management's authorization.
- Recorded transactions are compared with the existing assets at reasonable intervals and appropriate action is taken if differences are identified.
FCPA: WHAT THE GOVERNMENT WANTS

- DOJ and SEC place significance on self-disclosure
- Self-policing – ability to detect criminal activity
- Investigations must be thorough and objective
- Disclosures must be timely
- Must identify executives, employees and third parties who may be involved in wrongdoing
- Must take remedial action in response to the findings

FCPA Corporate Enforcement Policy
UK BRIBERY ACT

• “British FCPA”
• Unlike FCPA – prohibits commercial bribery
• Unlike FCPA – has offense of “failure to prevent bribery”
• Defense – adequate procedures to prevent bribery
• Broad jurisdiction
• Objective standard
  1. Was there intent to influence
  2. Was there intent to obtain, retain or get business advantage
  3. Payment or advantage not permitted
FRANCE’S NEW ANTI-CORRUPTION LAW

• New French anti-corruption law, Sapin II – compliance program requirements in effect as of June 1, 2017
• Power to investigate French nationals outside of territory of France
• Created French Anti-Corruption Agency (ACA) with broad prosecutorial power
• Robust corporate compliance program requirements for companies with at least 500 employees and revenue of at least €100M
• Strengthened internal and external reporting of whistleblower complaints for companies with 50 employees or more
• Introduced a French version of the Deferred Prosecution Agreement
Mexican anti-corruption law entered into force in July 2017

- Created National Anti-Corruption System
- Administrative liability for companies, up to US$6 million fines
- Credit for compliance programs
- Self-disclosure
FEDERAL GOVERNMENT CONTRACTORS

- **FAR 52.203-13**: Contractor Code of Business Ethics and Conduct
- **FAR 52.203-3**: Prohibition on gratuities to Federal Government officials and employees
- **FAR 52.203-7**: Anti-Kickback prohibitions
- **FAR 52.203-11**: Prohibitions and disclosures on using certain federal money to influence government award decisions
- **FAR 52.222-22, 26**: Equal employment and affirmative action requirements
The federal acquisition regulation was amended in 2008 to require that contractors with “covered” contracts must:

1. Have a compliance program and internal control system
2. Make “timely” disclosure to the government of “credible evidence” of violations of the FCA and certain federal criminal laws

A “covered” contract is any contract that has a value of $5M or greater (including options), and a performance period of greater than 120 days.
BANK SECRECY ACT
(ANTI-MONEY LAUNDERING)

- Officially the “Currency and Foreign Transactions Reporting Act of 1970”
- U.S. financial institutions must assist U.S. government in detecting and preventing money laundering
  - Requirements for record keeping and reporting by financial institutions (§1010.410)
  - Requirements for filing currency reports for transactions greater than $10,000 (§1010.311)
  - Must verify and record name and address of individuals presenting a transaction (§1010.312)
  - Multiple currency transactions treated as a single transaction if financial institution knows that transactions by or on behalf of any person result in certain transactions greater than $10,000 during any one business day. (§1010.313(b))
  - FINRA Rules (members only)

31 U.S.C. §§ 5311-5330; 31 C.F.R Chapter 10

cassidylawpllc.com
• Department of Treasury’s Office of Foreign Asset Controls (OFAC) enforces economic sanctions programs primarily against countries, entities and persons through blocking assets and trade sanctions to enable national security
• “Knowing or having reasonable cause to know”: a fine and/or up to 10 years imprisonment (18 USC § 2332d)
• Enabling statute and regulations:
  • President can take action to deal with unusual and extraordinary threat from outside the U.S. to national security, foreign or economic policy (50 USC § 1701)
  • Enabling regulations-31 CFR § 501
• OFAC Sanctions Site:
  http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx
Incentives to Disclose Corporate Wrongdoing “Whistleblowing”
INCENTIVES TO DISCLOSE - WHISTLEBLOWERS

- Enacted in 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank”) builds on the Sarbanes Oxley whistleblower requirements and allows whistleblowers who provide the SEC with original information about securities violations to obtain between 10% to 30% of any monetary sanctions in excess of $1 million recovered against a company
- Provides for anonymous reporting
- Encourages (but does not require) internal reporting prior to going to the SEC
- Includes anti-retaliation protections for whistleblowers who report possible securities laws violations
- Prohibits actions that impede whistleblower communications with the SEC including “enforcing, or threatening to enforce, a confidentiality agreement” with respect to such communications
DODD-FRANK
SECTION 21F OF SEC ACT OF 1934

• **Purpose:**
  • Monetary Incentives
  • Protect whistleblowers

• **Eligible whistleblowers:**
  • Perpetrator, auditors, third parties, clients, customers, compliance can report
  • “reasonable basis” to believe disclosing is necessary to prevent substantial financial injury
  • SEC made KBR remove language in confidentiality agreement requiring KBR legal to be notified before disclosing
  • Other recent SEC enforcement actions penalized companies impeding whistleblowers’ communications with the agency
FALSE CLAIMS ACT

• Claims for payment must be accurate, complete, and up to date
• Expectation that adequate due diligence supports statements to the Government
• Government focuses on invoices; cost & pricing information; reliance on representation in proposals and certifications
• Government has the right to audit - need to have supporting documentation
• Qui tam actions permit “private” enforcement actions

31 USC §§ 3729 et seq (civil); 18 USC § 287 (criminal)
FALSE CLAIMS ACT: QUI TAM RELATORS

• The FCA authorizes the DOJ and qui tam relators to bring civil actions against any person who knowingly makes or uses a false statement or document to either obtain money from the Government or avoid paying money owed to the Government (i.e., “reverse false claims”)

• Qui tam relators – sometimes acting as “whistleblowers” – are authorized by the FCA to act as private attorneys general by suing on behalf of the Government and receiving 15-30% of the recovery
The FCA is a federal statute – but more than 30 states have enacted “mini-FCAs”

- Texas, Florida, Illinois, Montana and the District of Columbia recently enacted FCA laws; other states are considering enhancing existing versions of the FCA (e.g., New York) or enacting new FCA statutes (Pennsylvania, South Carolina, Alabama, Wyoming)

- Even in those states that have not enacted their state FCAs yet, whistleblowers can still file a federal FCA case against individuals or businesses whom they believe have defrauded the federal government

- Foreign countries are considering enacting similar statues (UK and Australia)
IRS WHISTLEBLOWER REGULATION: INTERNAL REVENUE CODE 7623(B)

- Eligible for 15% to 30% of amount in dispute if provided information
- Disputed tax amount must exceed $2 million or individuals’ gross income must exceed $200,000
- No limit on amount of award
- Award amount reduced to up to 10% when disclosure based on:
  - Judicial or administrative hearings
  - Governmental report, hearing, audit or investigation
  - News media
- Award reduced if whistleblower “planned and initiated” the tax issue
- Whistleblower may be asked to assist IRS
- Awards can be appealed to the U.S. Tax Court
- If amount thresholds not met, IRS can pay for information under IRC 7623(a)
- Whistleblower Annual Reports

cassidylawpllc.com
**DOJ’S ANTITRUST LENIENCY POLICY**

Special Leniency Rules in the Antitrust Context
- US and over 50 jurisdictions now have corporate and individual leniency programs, which provide amnesty to the “first in the door” to cooperate
- Creates race to the government

DOJ’s Leniency Policy
- Individual and corporate leniency for those who disclose an antitrust violation first
- Disclosures received amnesty if no existing investigation and certain conditions are met
  - Amnesty can still be available if investigation has begun
- Cooperating directors, officers and employees will be considered for immunity from criminal prosecution
- Amnesty for current employees is mandatory; while DOJ considers amnesty for former employees in its discretion
STRUCTURING AN ETHICS & COMPLIANCE PROGRAM
COMPONENTS OF A PROGRAM

- Ongoing, documented ethics and compliance program
- Informed and committed leadership – a culture of ethics
- Assess risk of non-compliance
- Mitigate identified risks
- Written code of conduct
- Written policies and procedures
- Consistent and comprehensive training
- Regular communications
- Encouraging disclosing concerns and asking questions
- Prohibit retaliation for raising concerns
- Disciplinary response to transgressions
- Evaluate program effectiveness
- Monitor to detect and prevent non-compliant conduct
- Due diligence and oversight of business partners
ONE SIZE DOES NOT FIT ALL

• Formality and scope of actions.... depend on the size of the organization

• **Large Organizations**
  • More formal compliance and ethics operations than a small organization
  • Greater resource commitment
  • Shall encourage small organizations with whom they have a business relationship to implement an effective program

• **Smaller Organizations**
  • Must demonstrate the same level of commitment as a large organization
  • May rely on existing processes and resources
  • May be more informal than a large organization - train during staff meetings; monitor compliance by observing existing operations; use available personnel rather than dedicated ethics & compliance team
  • Should be similar to other similarly situated organizations

• US Federal Sentencing Guidelines, §8B2.1, Comments
STATUS OF ETHICS & COMPLIANCE PROGRAM

• No program yet
• Centralized
• International
• Mature business
• Risk averse
• Assessing risk

OR

• Robust program
• Decentralized
• Only certain countries
• Entrepreneurial/startup
• Welcomes risk
• No formal risk review
GOVERNANCE
CEO has ultimate responsibility
Senior management – directed by CEO
Board – governance, oversight, direction
Internal auditors – review effectiveness of controls
Others – controls within their duties
RISK MANAGEMENT
WHAT ROLE DOES AN ATTORNEY PLAY?

• “What is clear is that general counsel remain far more likely than any other person within the business to bear overall responsibility for corporate governance.” Baker & McKenzie, William Long Legal Risk & Compliance Survey, Law Department Quarterly, April-June 2007

• Provides framework for legal and regulatory compliance mandates

• Collaborates in defining the appetite for risk

• Assures “gaps” are covered under privilege
IDEAS ON ASSESSING RISK

• Define methodology:
  ✓ Surveys
  ✓ Targeted interviews
  ✓ Focus groups
  ✓ Leadership discussion

• Regular and systemic assessments: Identify issues in advance; respond to changing laws, regulations, political environment, business activities

• Document and review findings: A comprehensive report to share with board, leadership; helps define strategy and goals

• Leaders define mitigation: develop strategy; direction; dedicate resources

• DRIVE TO CLOSURE AND DOCUMENT
ASSESSING RISK

- Identify risks
- Prioritize risks
- Mitigate risks
- Drives the ethics & compliance program
- Drives business process improvement and/or cost savings
- Directs training, communications, process improvement
- Identifies resource needs - human capital, IT solutions, cost allocation etc.
IDENTIFYING STAKEHOLDERS

Owners
- Employees
- Business leaders
- Executive team
- Board of directors
- Shareholders
- Regulators

Working Group
- Employees
- Business leaders
- Legal/compliance
- Internal audit
- External accountants/attorneys

Business leaders should own risk management
SCOPE OF REVIEW

• Business operations and their unique risks
• Highly regulated aspects of business
• Business development methods – direct, sales agents, etc.
• New products or new markets
• Structure – subsidiaries, joint ventures, business partners
• Geographic locations of operations
• Existing processes, controls, procedures, audits, reviews, etc.
• Third party relationships and related controls
• Leadership and executive commitment to ethical decision making
• Awareness and compliance with policies and procedures
• Effectiveness of training, communications, policies, procedures
• Compliance with laws, regulations, industry standards
• Benchmark against competitors - have competitors been prosecuted, sued etc.
# RISK MATRIX

(ACQNOTES – DOD ACQUISITIONS RESOURCE)

## Risk Assessment Matrix

<table>
<thead>
<tr>
<th>Probability</th>
<th>Severity</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent (A)</td>
<td>High</td>
<td>Serious</td>
</tr>
<tr>
<td>Probable (B)</td>
<td>High</td>
<td>Serious</td>
</tr>
<tr>
<td>Occasional (C)</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Remote (D)</td>
<td>Serious</td>
<td>Medium</td>
</tr>
<tr>
<td>Improbable (E)</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Eliminated (F)</td>
<td>Eliminated</td>
<td></td>
</tr>
</tbody>
</table>
SHOULD RISK ASSESSMENT BE UNDER PRIVILEGE?

• Assessment often bubbles up “gaps”
• USAM - prosecutors should not seek the waiver of attorney-client privilege
• United States ex rel Barko v. KBR (D.C. Cir.)
• Crime-fraud exception:
  • Turns on client intent when seeking legal advice – was advice used to further crime?
  • In camera review permitted whether documentary or verbal counsel
  • In camera review when good faith showing that privilege may be overcome

In re Grand Jury Subpoena, 745 F.3d 681 (3d Cir. 2014)
INVESTIGATIONS VS RISK ASSESSMENTS

INTERNAL INVESTIGATIONS
• Reactive
• Responding to a concern
• Aware of potential non-compliance
• Need attorney-client protection
• Move swiftly
• May require disclosure to government
• Make a finding
• Define and execute remediation
• Defined period of time
• Narrow group of stakeholders

RISK ASSESSMENTS
• Proactive
• No defined issue or concern
• Process improvement
• Consider attorney-client protection
• Broad scope
• Execute as defined in scope
• Identify gaps/risk
• Prioritize risks
• Define and execute remediation
• Broad group of stakeholders
RISK ASSESSMENT DRIVES:

- Internal Controls
- Resource Needs
- Policies
- Procedures
- Training
- Communications
- Business operations
INTERNAL CONTROLS
A process put in place by leadership to provide reasonable assurance of achieving the following objectives:

- Effective and efficient business operations
- Reliable financial reports
- Compliance with laws and regulations
COMPONENTS

Control Environment: Culture, values, competence, management philosophy and operating style
Risk Assessment: Identifying and managing risks
Control Activities: Policies and procedures that execute leadership directives
Information & Communication: Reports – such as financial and compliance
Monitoring: Assess quality of the system’s performance
Audit Plan
• Internal audit plan should be documented, regularly reviewed and updated
• Define and document escalation process when there is a finding or indication of activity contrary to policy
• Document a method to close out findings and gaps to include ownership of the action
• Document a method to reconcile transactions
• Define plan to assess adequacy of procedures and controls
• Automate reviews for certain types of transactions – expense reimbursement, for example

Certifications
• Consider certifications across the organization - target toward high risk groups - should be electronic and traceable
• Reach 100% completion
• Establishes whether employees understand policies and procedures
• For leaders, requires some due diligence to make the certification for area under their responsibility
POLICIES AND PROCEDURES

**Policy:** Fundamental principles or standards that require or restrict certain activities or establish terms and conditions for achieving certain business objectives

**Procedures:** The processes by which business objectives are to be accomplished

**Work Instruction:** Step-by-step instructions on how to complete a task

**Owner/Developer:** A competent individual with subject matter expertise or the individual who owns the activities or processes

**Reviewer:** Should be an attorney and the appropriate business leader
Develop an annual curriculum for leaders, employees and relevant third parties

- Document an annual training and communications plan
- Identify owners - business leaders should be included
- Identify topics based on risk exposure
- Include commitment to integrity and ethics
- Develops shared values

After an Acquisition/Merger/Joint Venture

- Senior leaders of the new organizations should be trained in person
- As many of the new employees as possible should be trained in person
- Allow for opportunity for questions
- Training needs to cover values and policies
- Furthers the integration process
HELPLINES

- Capabilities for anonymous reporting
- Case management system - track and close concerns
- Method to notify and close out with person who raised concern
- Clear message of no retaliation
- Broadly communicated across many mediums
- Method to run reports, queries
- Regular review for patterns and analysis of data
- Should help identify trends, needs for improvement
- Method to develop reports to leadership and to the board
- Outside parties should be able to report concerns and ask questions
MONITORING

• Effectiveness and accuracy of accounting procedures
• Revenues and losses - When recorded
• Expenses – Travel, gifts, meals, entertainment
• Political contributions/Lobbying activity
• Charitable contributions
• Accuracy and completeness of invoices
• Compliance with policies and procedures
• Helpline data
• Training completion
• Effectiveness of IT systems
• Investigation outcomes
• Third party relationships - commissions paid, expenses submitted
• Supply chain - purchasing processes, vendor approval
TAKE-AWAYS

• Foster strong compliance culture
• Develop clear compliance policies and processes; make them easily accessible
• Conduct risk assessments and investigations; follow through on remediation
• Conduct tailored training for employees on compliance issues of relevance to their specific duties, provide concrete examples and allow for feedback and discussions
• Develop a speak up culture
Panelists are speaking in their individual capacities, not on behalf of their respective employers. The views expressed in this deck do not necessarily reflect the views of all panelists or their respective employers.
Example Due Diligence Questionnaire

OPERATIONS

Where is the entity incorporated, where does it do business, what is its business structure?
How long has the entity been in business?
Does it have the required permits, licenses, etc. to conduct its business?
Who are its leaders, executives, major owners?
How are leaders, executives, employees compensated?
Does leadership have a reputation for being responsible, ethical and experienced?
Are leaders, owners related to or in a business arrangement with any government official?
Does the entity have a compliance program and infrastructure, including policies, training; is it effective?
Does the entity have a system to report concerns, ask questions, or raise issues?
How many employees does the entity have? Where are they located?
Does the entity have human resource policies that foster fair treatment?
What is the entity’s financial condition?
Does the entity have adequate financial, accounting, IT, HR, legal and operational systems and support?
Does the entity have appropriate insurance coverage?
What is the entity’s debt structure? lines of credits, mortgages, leases, etc.
Where does the entity bank and invest?

REPUTATION

Obtain references from the entity’s professional advisors. For example:
- Bankers
- Accountants
- Clients
- Lawyers
Has the entity ever been debarred or suspended by any government or quasi-government agency?
Is there negative news on the entity, its owners, or its executive management?
Does the entity have a satisfactory record of integrity and ethics?
Is the entity current on its tax obligations?
Is the entity involved in any litigation, administrative actions, audits, or investigations?
Has the entity been involved in any litigation, administrative actions, or investigations in the past five years?
If the entity is publicly traded, are its public filings timely and accurate?
Are there any auditor letters to management on internal controls?
EXPERTISE, SKILLS, AND CAPABILITIES

Does the entity and its employees have the necessary education, training, skills, experience and capabilities to provide the goods/services?
Does the executive management team have the necessary education, experience, and capabilities to manage the organization?
Considering the entity’s existing work, does it have the ability and time to comply with the proposed delivery schedule?
What is the entity’s history of past performance?
What do its manufacturing and office sites look like? Are they clean, safe?
Do employees live at the entity’s sites? What are the living conditions?

BUSINESS DEVELOPMENT, MARKETING, PRICING

What are the entity’s products and services?
Who are its major competitors?
Is the entity’s pricing, costs, commissions, agreements, discounts, financing, payment system standard in the industry and/or competitive?
Do agreements include a clear, defined statement of work?
What does the entity’s website, press releases, marketing materials say?
How does the company go to market? Identify customers?

BUSINESS RELATIONSHIPS

Does the entity have: subsidiaries, joint ventures, partnerships, if so, with whom?
Who are the entity’s material suppliers? Does the entity sole source or rely on only a few suppliers?
Who are the entity’s material customers? Does it only have a few customers?
Does the entity rely on sales agents, sales consultants, distributors? If so, who are they and how do they select them?
## Example Matrix of Authority

<table>
<thead>
<tr>
<th>Action/Event</th>
<th>Required Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amending Corporate By-Laws</td>
<td><strong>Executive Team</strong>, Board Governance Committee, <strong>Legal</strong></td>
</tr>
<tr>
<td>Capital Spending Over $1,500,000</td>
<td><strong>Division CEO</strong>, <strong>Division CFO</strong>, Consult <strong>Legal</strong> if needed</td>
</tr>
<tr>
<td>Real Estate Transactions Over $1,000,000</td>
<td><strong>CEO, CFO</strong>, Consult <strong>Legal</strong> if needed</td>
</tr>
<tr>
<td>Supplier Agreements Over $1,500,000</td>
<td><strong>Division CEO</strong>, <strong>Division CFO</strong>, <strong>Legal</strong></td>
</tr>
<tr>
<td>Agreements When Non-Standard Agreement Used</td>
<td><strong>Division CEO</strong>, <strong>Division CFO</strong>, <strong>Legal</strong></td>
</tr>
<tr>
<td>Agreements to sell/transfer/share Intellectual Property</td>
<td><strong>Division CEO</strong>, Division Chief Engineer, <strong>IP Counsel</strong></td>
</tr>
<tr>
<td>Consulting Agreements Over $50,000</td>
<td><strong>CEO, CFO, Legal, Board</strong> if CEO, CFO or Legal determine necessary</td>
</tr>
<tr>
<td>Mergers, Acquisitions, Joint Ventures of Any Size</td>
<td><strong>Executive Team</strong>, <strong>Board</strong></td>
</tr>
<tr>
<td>Financial Fraud, Financial Statement Manipulation</td>
<td><strong>Legal</strong>, Audit Committee; <strong>Legal</strong> determines others who need to know</td>
</tr>
<tr>
<td>Press Releases</td>
<td><strong>Chief Communications Officer</strong> or their designee. Communications determines whether others should be informed</td>
</tr>
<tr>
<td>Any indication of a government investigations or litigation such as:</td>
<td><strong>Legal</strong>. Legal must determine the scope of the matter, who is implicated, and then determine others who need to know.</td>
</tr>
<tr>
<td>• receipt of a subpoena</td>
<td></td>
</tr>
<tr>
<td>• execution of a search warrant</td>
<td></td>
</tr>
<tr>
<td>• civil investigative demands</td>
<td></td>
</tr>
<tr>
<td>• requests to interview employees</td>
<td></td>
</tr>
<tr>
<td>• request for an audit or review</td>
<td></td>
</tr>
<tr>
<td>• request to produce documents</td>
<td></td>
</tr>
<tr>
<td>Disclosures to any government or to any business partner including but not limited to:</td>
<td><strong>Legal</strong>. Legal must determine the scope of the matter, who is implicated, and then determine others who need to know.</td>
</tr>
<tr>
<td>• export/import violations</td>
<td></td>
</tr>
<tr>
<td>• cyber security or privacy breaches</td>
<td></td>
</tr>
<tr>
<td>• concerns in handling classified information</td>
<td></td>
</tr>
<tr>
<td>• instances of a government overpayment; potential non-compliant conduct</td>
<td></td>
</tr>
</tbody>
</table>