RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING

JOSH WALLENSTEIN
MANAGING MEMBER, THE WALLENSTEIN LAW GROUP

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING

THE SAME OLD DISCLAIMER.

These materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem.

Feel free to contact:

Josh Wallenstein

jwallenstein@wallensteinlawgroup.com

+1.713.598.4581

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING

CAVEAT #1: AN ABC COMPLIANCE FOCUS

- Though the concepts, approach, and process map may be similar, we are not addressing:
  - QHSE
  - Antitrust / competition law
  - AML
  - SOX and similar
  - Sector-specific regulations (e.g., HIPAA, Truth in Lending, etc.)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

DISTINGUISHING BETWEEN RISK ASSESSMENTS, EVALUATIONS, AUDITS, AND CONTINUOUS MONITORING*

➢**Risk Assessments**	Determine and assess risks and mitigation strategies	Required
➢**Audits**	Review discreet scopes for compliance (with policies, laws)	Required
➢**Monitoring**	Routinely effect plans and review metrics	Expected
➢**Evaluations**	Formally assess adequacy and effectiveness	A Good Idea

*definitions per author, and somewhat arbitrary (but based on good sense!)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING

CAVEAT #2: OUR MAIN FOCUS IN ON ABC RISK ASSESSMENTS

- Risk Assessment: a regular and systematic identification and assessment of risks followed by an action plan to control or mitigate against these risks.
- Since our focus is on ABC Risk Assessments, we'll hit on some of the answers to "why do this" (and, "who wants us to do this" in later slides.
  - Sample categories at Appendix A

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

AUDITS - DEFINITION

- **Required***.
  - The audit process, as it relates to books and records, assesses whether books and records are reasonably:
    - accurate,
    - transparent,
    - complete, and
    - supported with documentation.
  - It is one of the foundations of our system of corporate disclosure.

* Whether by law, universal expectation, and/or contractual provision.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

AUDITS – EXAMPLE SCOPES

- Audits look at records, which by their nature record past acts and decisions.
- Types of Compliance Audits:
  - Routine Compliance (e.g., Policy Adherence) Audits
  - External (Agent/JV/Other Third Party) Audits
  - Procurement Audits
  - Directed Audits / Internal Investigations

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

AUDITS – SCOPES CAN EXTEND BEYOND "BOOKS AND RECORDS"

- Some see "audits" as merely reviewing the books and records of issuers under applicable US law.
- My view of "audits" is broader than merely reviewing "books and records" of "issuers". Why?
  1. Because Wikipedia says so.*
  2. Because COSO requires "audits" to more broadly assess "internal controls", defined by COSO to cover:
     - ✓ Effectiveness and efficiency of operations
     - ✓ Reliability of financial reporting
     - ✓ Compliance with applicable laws and objectives
  3. Because the purpose of an audit is not a reconciliation (i.e., to "tie out the math"); it's to detect irregularities, systemic failures and illegal activity, in part *through* the math.

And…

*Audit: "a systematic and independent examination of books, accounts, statutory records, documents and vouchers of an organization *to ascertain how far the financial statements as well as non-financial disclosures present a true and fair view of the concern*." (Wikipedia, 16 Dec 18, *emphasis* mine) Also, note that the word's Latin progenitor *audire* means "a hearing". We use the term, "hearing" in all manner of non-financial contexts.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

AUDITS – SCOPES CAN EXTEND BEYOND "BOOKS AND RECORDS" (II)

Because enforcement agencies believe that audits are meant to more broadly assess internal controls.

- The SEC and DOJ consider "periodic internal audits" as a distinct "compliance procedure" that support its "compliance program". A "compliance program" is in turn part of a company's "internal controls". (*See* Resource Guide at 62, 68) As an example:
  - Jennings (2011) – former CEO consented to an SEC injunction and disgorgement for, *inter alia*, signing false SOX certifications **and annual compliance certifications** re the Code of Conduct. (He later pled guilty in the UK to bribing Iraqi and Indonesian government officials.)
  - This tells us that the SEC viewed both financial and non-financial material misstatements to be violations of the internal controls provisions of the FCPA.
- The SEC's Public Company Accounting Oversight Board rules and standards govern the (external) auditor's responsibility. They require that the auditor, *inter alia,* ascertain illegal acts that may lead to material misstatements in financial reporting. (*See,* for example, PCAOB AS 2405.08, that recommends, among other things, reviewing minutes and management interviews when effecting an audit.)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

AUDITS – EXAMPLE PROCESS MAPS FOR INTERNAL AUDITS

EXAMPLE: G&E AUDIT

- Review of Policy requirements.
- Review of records to determine adherence to policy.
- Issuance of a report.

EXAMPLE: THIRD PARTY AUDIT

- Creation of a checklist (of internal controls).
- Review of known concerns / allegations.
  - If external, a review of applicable contractual obligations and scopes of work.
- Document and data requests (both internally and from the third party).
- In-country visits and interviews (of both internal and external personnel).
- Review of books and records (inclusive of invoices and receipts).
- Further investigation of any red flags.
- Issuance of a report.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

CONTINUOUS MONITORING - DEFINITION

- **Expected.**
  - Financials.
    - "Monitoring" is explicitly included as a crucial component of effective internal controls. (Resource Guide at 40.)
  - Risky third parties.
    - "…[C]ompanies should undertake some form of ***ongoing monitoring*** of third-party relationships…Where appropriate, this may include updating due diligence periodically, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party." (Resource Guide at 60 [quoting ICC Rules on Combating Corruption at 8.])
  - The compliance program, generally.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

CONTINUOUS MONITORING - DEFINITION

- Enforcement agencies expect companies to regularly review and improve their compliance programs. (FCPA; UKBA; Sapin II; etc.)
- Don't just *do* it; *document* that you do it.
  - Plans: create preliminary (e.g., annual) plans that demonstrate a routine for review. (e.g., Code revisions; new training decks; employee ethics surveys; country or office spot checks)
  - Metrics: by collecting data into helpful metrics, you can (i) measure effectiveness, (ii) see trends, and (iii) report on both.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

AND…ON THE SUBJECT OF "METRICS"

- There are helpful metrics and unhelpful metrics. Some can actually be misleading. Just a few examples:

Common	Better
# of hotline calls	# of substantiated hotline calls
global training completion rates	training completion rates by location/function/legal entity/etc.
attestation rates	% of attestations resulting in disclosures

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

MONITORING – SAMPLE TOPICS

RISKY AREAS REVIEW

- Business with State-Owned Entities
- Licensing and Permitting
- Regulatory Audits / Examinations
- Dealings with Local Regulators (Police, Military)
- Customs
- Immigration
- The Use of Intermediary Agents
- Petty Cash
- Travel and Hospitality Expenses
- Charitable Contributions
- Joint Ventures

SYSTEMS REVIEW

- Code of Conduct
- Policies and Procedures
- Department Size and Setup
- Training
- Delegations of Authority
- Forms and Workflows
- Compliance Contract Clauses

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

EVALUATIONS - DEFINITION

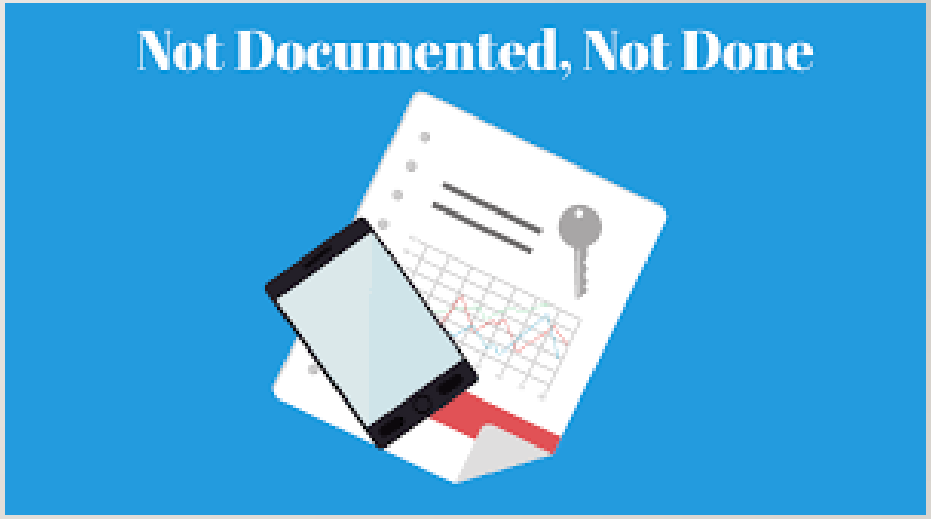
- **Expected**.
  - The only 1 of these 4 concepts not mentioned in the Resource Guide.
  - For me: deals with the "soft" side of compliance. This is one area where our subject matter expertise adds significant value.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

EVALUATIONS – WHY FORMALIZE MY EXPERT MANAGEMENT OF MY FUNCTION?

Documentation

- facilitates the auditing and review process, as well as the monitoring process.
- tangibly and permanently demonstrates your acumen…and the Company's dedication to the continual evolution and improvement of its compliance program.



RISK ASSESSMENTS

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – REQUIRED BY ENFORCEMENT AGENCIES

- **Required.**
  - US and other enforcement authorities
    - SEC/DOJ - FCPA Resource Guide (2012); US Federal Sentencing Guidelines
      - DOJ/SEC, SFO and others expressly note that effective risk assessments are one element of an effective compliance program
    - SFO – Code of Practice Dealing with Overseas Corruption
    - Other national ABAC legislation (e.g., Sapin II)
  - International expectations
    - UN, OECD, World Bank,…

SAPIN II

DEPARTMENT OF JUSTICE

SFO serious fraud office

U.S. SECURITIES AND EXCHANGE COMMISSION

WORLD BANK

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – A DEFENSE TO PROSECUTIONS

- Supports the "adequate procedures" defense (UK SFO, others)
- Undermines the "mens rea" element (US DOJ, others)
- Bolsters the assertion of "adequate internal controls" (US SEC)
- Can provide credit (or reduced fines/penalties) (US Federal Sentencing Guidelines, multilateral development banks, etc.)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

OBJECTIVE OF A RISK ASSESSMENT

1. understand the spectrum of compliance risks in each part of the organization, and
2. apply mitigation strategies to address the most serious risks.

To do this right…can generate significant human and financial costs.
It can also ultimately save the company a bundle.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – A WISE USE OF LIMITED RESOURCES

- Focuses corporate attention on material risks
  - Guides the proper allocation of limited resources
  - Highlights "bet the company" risks*, i.e., those that could impact the organization's ability to achieve its strategic objectives
- Reveals material gaps in processes and controls that could be exploited
- Demonstrates inefficiencies that, once corrected, could save company resources
  - Guides the proper allocation of limited resources
  - Helps avoid negative reputational impact

*Example "bet the company" risks:

- Bribery- and money laundering-related risks
- Antitrust / competition law risks
- Fraud on the company / conflicts of interest risks (?)
- IP and trade secret risks
- Data protection / data privacy / cybersecurity risks
- Business continuity risks
- Supply chain / procurement risks
- HR-related risks (?)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – TYPES

- Timing Considerations
  - Annual? Bi-annual? Other?
- Scope Considerations
  - Enterprise-wide?
  - Specific to country? Function? Risk area?

✓ Key: make the Risk Assessment reasonably routine and (in the aggregate) comprehensive (i.e., not merely a "check the box" exercise)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

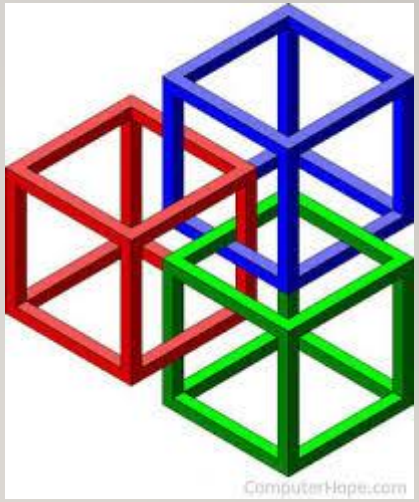
RISK ASSESSMENTS – EXTERNAL VERSUS INTERNAL RESOURCES

- Cost considerations
- Subject matter expertise considerations
- Benchmarking ability
  - Internal trends v.
  - External metrics
- Attorney-client privilege with external counsel

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – APPROPRIATE SCOPE AND DESIGN

- Use a seasoned and accepted overarching framework (e.g., the Ten Hallmarks)
- Develop a Scope. Ideas:
  - business lines
  - products and services
  - the sales process
  - distribution channels
  - customer bases
  - geographies
  - compliance headcount and resources
  - commercial activities
  - culture
  - training
  - corporate communications
  - financial and accounting controls
  - software systems
  - human resources
  - policies and procedures



RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – DEVELOP A RISK INVENTORY (OBJECTIVE)

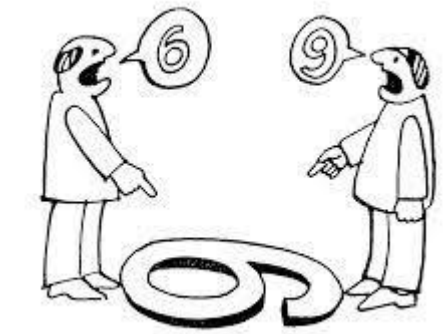
- Prior risk assessments (if available)
- Publicly disclosed "Risk Factors" (if applicable)
- Competitor missteps (if applicable)
- Hotline allegations and internal investigations
- Contracts

- Books and records
  - Focus on high-risk transactions
  - "Follow the money"
- Policies and procedures (and controls and mechanisms implemented thereunder)
- Publicly available metrics (e.g., hotline information, training information, country-specific corruption indices)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – DEVELOP A RISK INVENTORY (SUBJECTIVE)

- Interviews: use a cross-functional approach (i.e., include functions beyond legal and compliance); e.g.:
  - Finance / accounting
  - Sales / marketing
  - Regional and country management
  - Internal audit
  - Procurement / supply chain
  - Government relations
  - Risk management and security personnel
  - Specific personnel in high-risk functions
  - The outside auditor (if applicable)
- Cultural Surveys
- Exit Interviews
- Training Discussions
- Your Own Expert Personal Opinion



RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – CATEGORIZE AND ASSESS YOUR RISKS

- Categorize risks within your framework (and note which specific risks have not been integrated)
- Measure risks
  - 2 parameters for measurement
    - Impact (Severity of Occurrence); and
    - Frequency (Probability of Occurrence)
  - Holistic review: should understand relative legal, financial, operational, or reputational damage
- Assess the adequacy of existing mitigation strategies
- Document, and focus resources on, the greatest "residual risks"

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS – EXAMPLES OF COMPLICATING ENVIRONMENTAL FACTORS OBTAINING INFORMATION

- Language barriers
- Cultural environments
- Geographical issues
- Access to information
- Availability of electronic documentation
- Availability of internet and consistent energy supply
- Government controls on information transfers
- Availability of paper records
- Enforcement authority (or other government agency) obligations
- War zone or unstable country risks

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

RISK ASSESSMENTS –EFFECTIVE COMMUNICATION OF FINDINGS / OBSERVATIONS

Unfortunately, you'll likely need to draft a "short" and "long" version of the results.

- Senior management and the Board will likely want specific findings, overall risks, and recommended remediation.
- Your function will need to retain a detailed overview of:
  - How you scoped and then performed the risk assessment; and
  - How you analyzed the results and determined remediation.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

MATERIAL FINDINGS: SELF-REPORTING TO THE AUTHORITIES?

- Are you required to do so (e.g., under your DPA)?
- Will it be discovered anyway?
- Do you wish to avail yourself of potential leniency or reductions based on voluntary disclosure?

Regardless of whether your self-report:

1. Stop the bleeding (hold notices; terminations; shifting of reporting lines; modifications of DOAs; etc.)
2. Preserve evidence.
3. Document mitigation activity.

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

MATERIAL FINDINGS: THE NECESSITY OF PROMPT REMEDIATION

- Regulators consider short lags in implementing audit recommendations—as brief as eight months—to be evidence of faulty internal procedures
  - General Cable – rebuke for taking 8 months of inaction
  - Biomet – criticism for not following up on concerns from a draft report
- Speedy implementation of audit recommendations and mitigation strategies is viewed favorably (Nortek, Anheuser-Busch InBev)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

MATERIAL FINDINGS: ACT REASONABLY, DILIGENTLY, AND ETHICALLY

- Regulators will take note if the same issues arise in repeated audits but remain unaddressed (Qualcomm, Bristol-Myers Squibb)
  - Consider whether a problem is a one-time aberration or more systematic (GlaxoSmithKline)
- Regulators are particularly critical of intentional doctoring or destroying records of audits (Och-Ziff, Avon Products)

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

THE END

THANK YOU!

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

APPENDIX A: SAMPLE COMPLIANCE CATEGORIES (INTERNATIONAL COMPANY)

- Business with State-Owned Entities
- Licensing and Permitting
- Regulatory Audits / Examinations
- Dealings with Government Officials / PEPs
  - As vendors/consultants
  - With reference to employment (e.g., internships)
- Dealings with Local Regulators (Police, Military)
- Customs
- Immigration
- Sponsors
- Intermediary Agents
  - Distributors (with specific focus on clients who are not the ultimate end user)
  - Sanctions concerns
  - Discounts that could create a slush fund
- Sanctions and Boycott Risks
- Data Protection / GDPR Risks

RISK ASSESSMENTS, EVALUATIONS, MONITORING AND AUDITING:

APPENDIX A: SAMPLE COMPLIANCE CATEGORIES (INTERNATIONAL COMPANY)

- Disbursements:
  - Travel and Hospitality Expenses
  - Facilitating Payments
  - Expense Reports
  - Petty Cash
- Charitable Contributions and Donations
- Joint Ventures
  - Note, e.g., shell JV partners who contribute negligibly
  - Assess both "control" elements and "compliance protections"