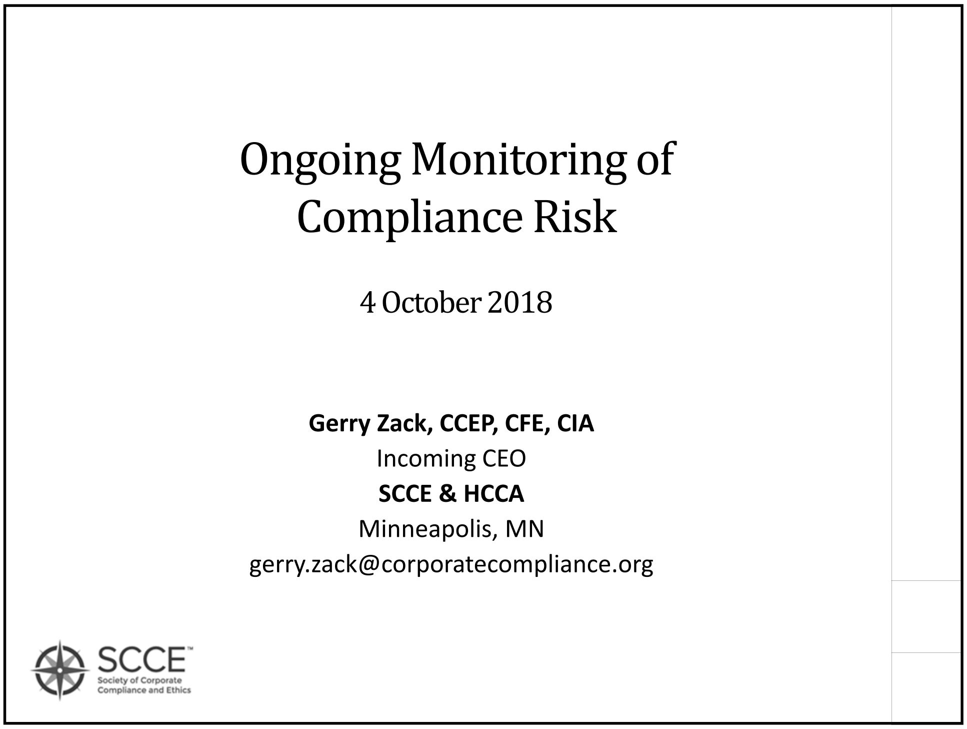
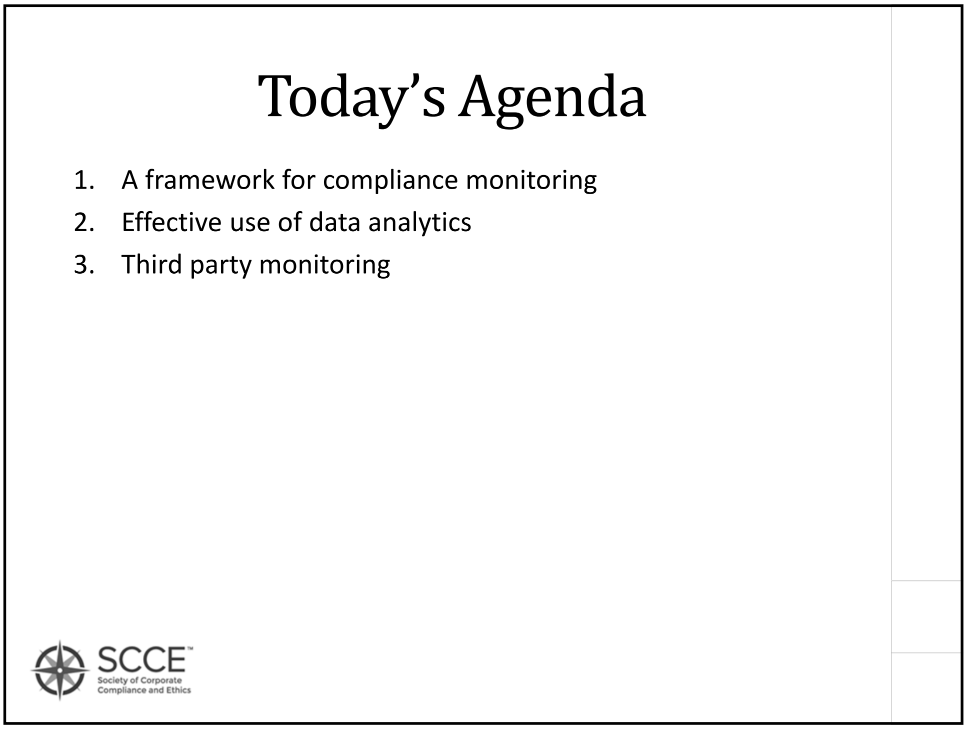


Ongoing Monitoring of Compliance Risk

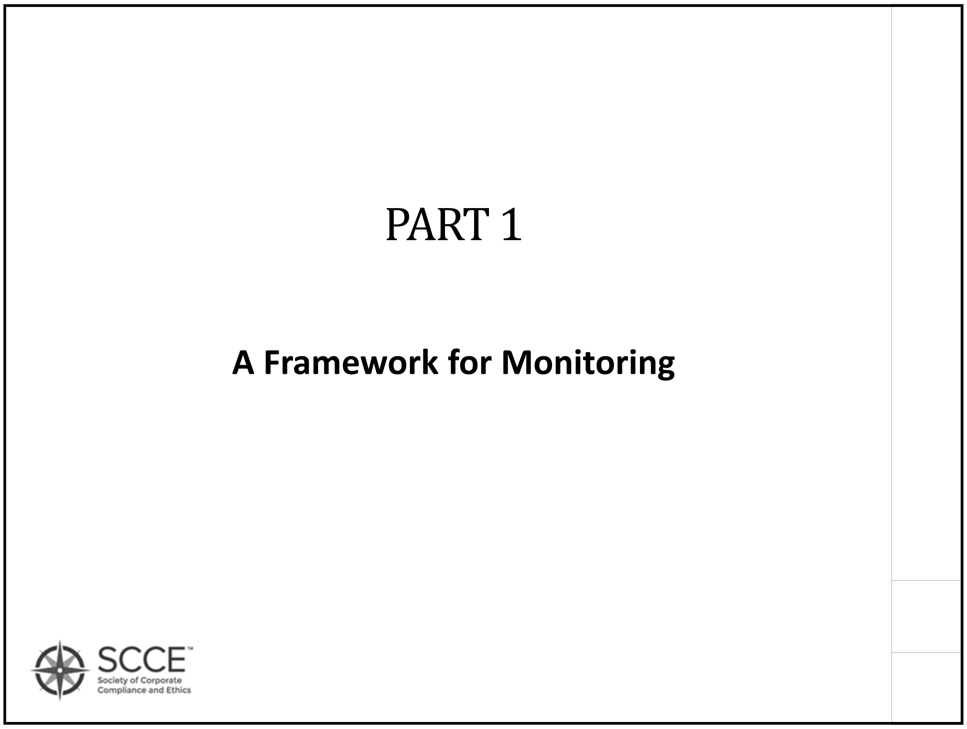
4 October 2018

Gerry Zack, CCEP, CFE, CIA
Incoming CEO
SCCE & HCCA
Minneapolis, MN
gerry.zack@corporatecompliance.org



Today's Agenda

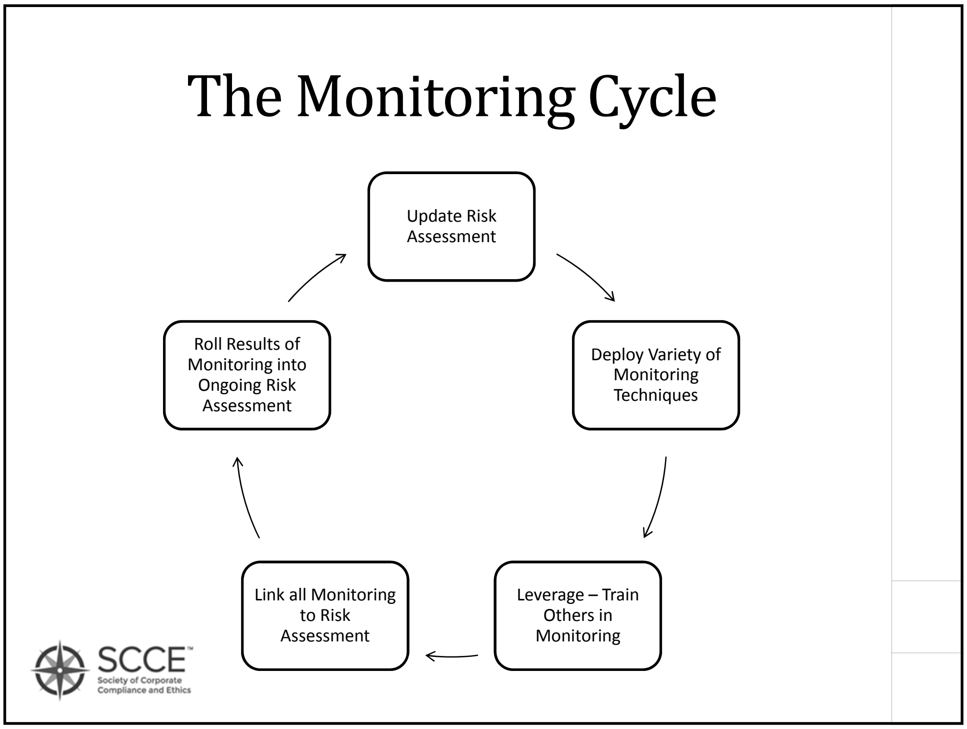
1. A framework for compliance monitoring
2. Effective use of data analytics
3. Third party monitoring



PART 1

A Framework for Monitoring

SCCE Society of Corporate Compliance and Ethics



The Monitoring Cycle

Update Risk Assessment

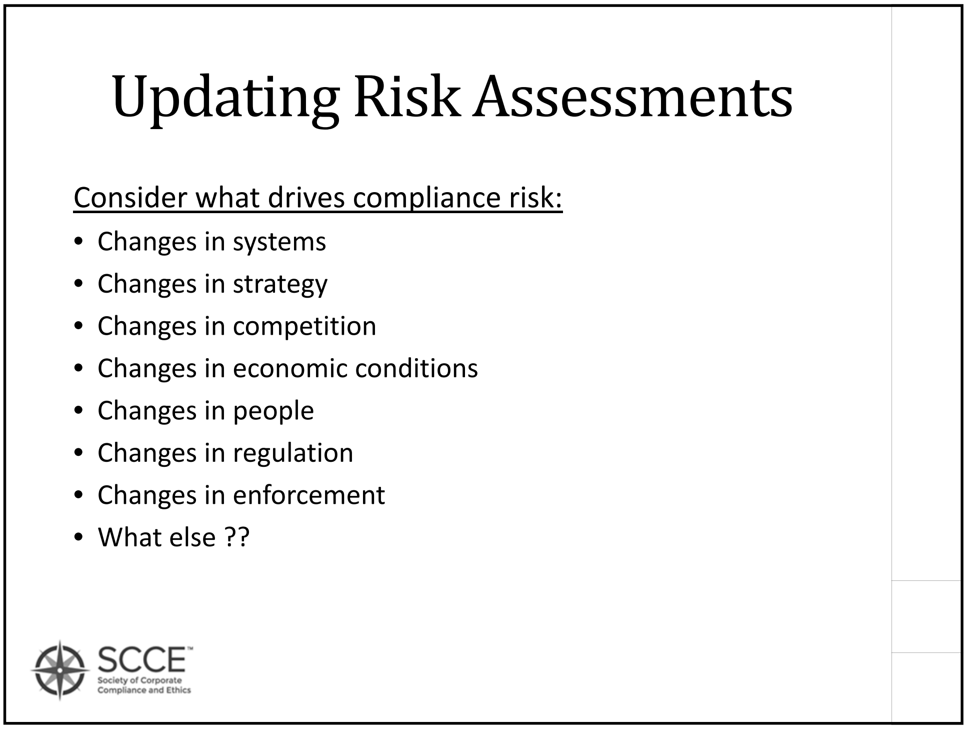
Deploy Variety of Monitoring Techniques

Leverage – Train Others in Monitoring

Link all Monitoring to Risk Assessment

Roll Results of Monitoring into Ongoing Risk Assessment

SCCE Society of Corporate Compliance and Ethics

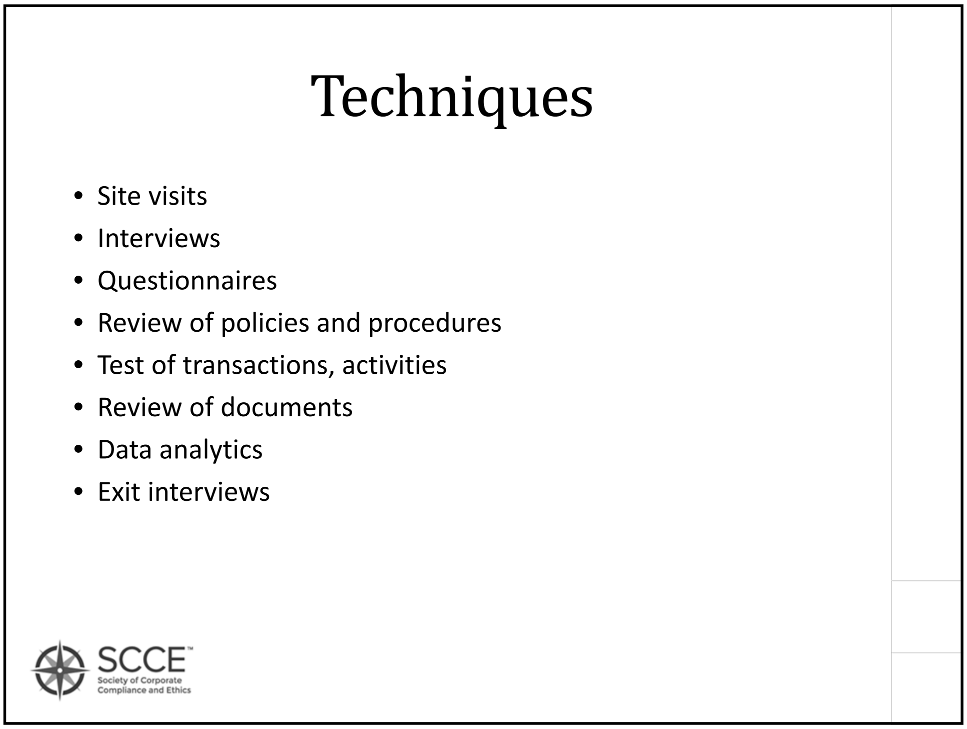


Updating Risk Assessments

Consider what drives compliance risk:

- Changes in systems
- Changes in strategy
- Changes in competition
- Changes in economic conditions
- Changes in people
- Changes in regulation
- Changes in enforcement
- What else ??

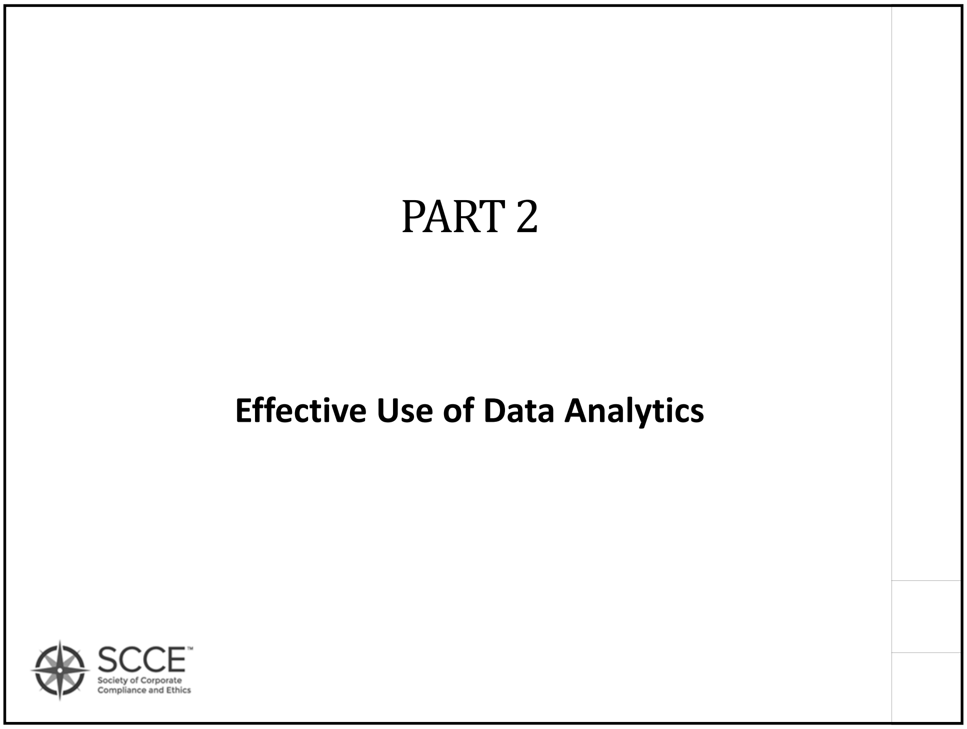
SCCE™ Society of Corporate Compliance and Ethics



Techniques

- Site visits
- Interviews
- Questionnaires
- Review of policies and procedures
- Test of transactions, activities
- Review of documents
- Data analytics
- Exit interviews

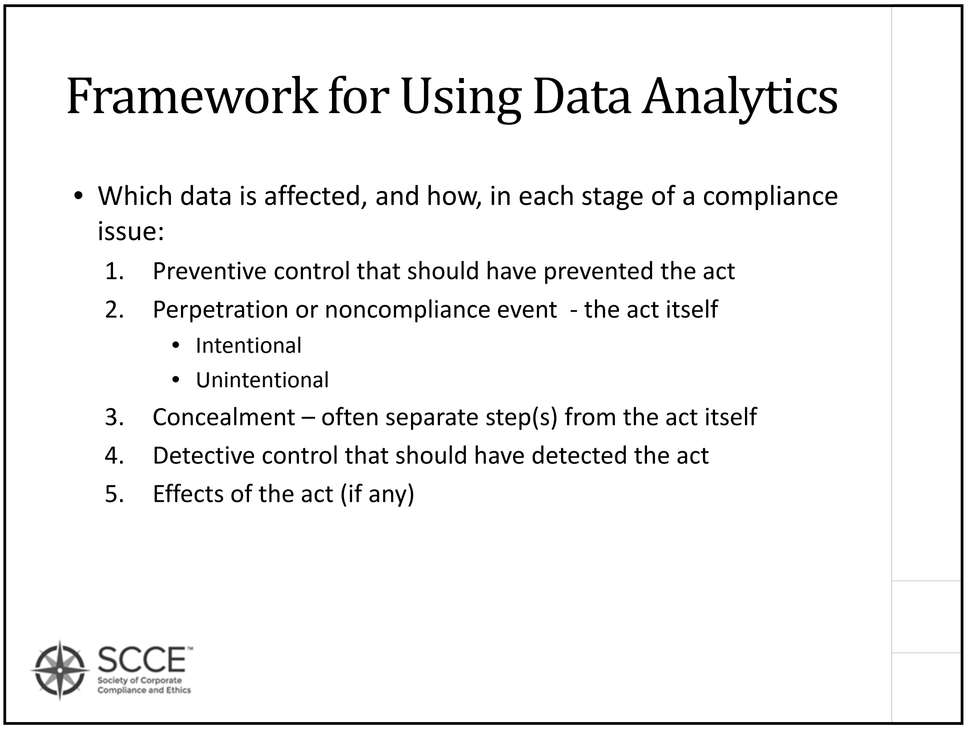
SCCE™ Society of Corporate Compliance and Ethics



PART 2

Effective Use of Data Analytics

SCCE™
Society of Corporate
Compliance and Ethics



Framework for Using Data Analytics

- Which data is affected, and how, in each stage of a compliance issue:
  1. Preventive control that should have prevented the act
  2. Perpetration or noncompliance event - the act itself
     - Intentional
     - Unintentional
  3. Concealment – often separate step(s) from the act itself
  4. Detective control that should have detected the act
  5. Effects of the act (if any)

SCCE™
Society of Corporate
Compliance and Ethics

Types of Data

Structured

- Accounting/financial
- Inventory
- Sales/purchases
- Payroll/H.R./timekeeping
- Security
- Customer service
- System access/use
- Travel, asset use, etc

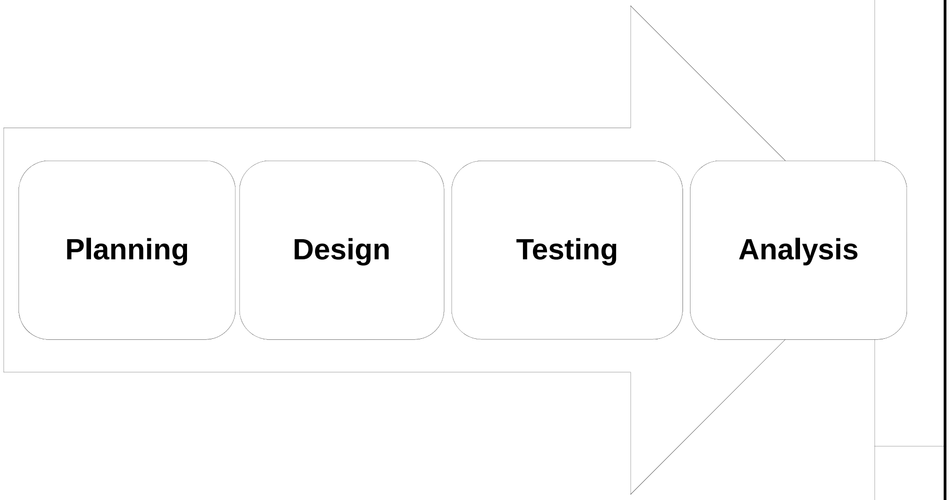
Unstructured

- Journal entry explanations
- Purchase descriptions
- P.O. explanations
- Variance explanations
- E-mails, IMs, etc
- Photo, video, audio files

The Devil's in the Data

- When fraud or corruption is involved, concealment leaves a digital trail:
    - Deleting electronic records
    - Altering electronic records
    - Adding electronic records
- Sometimes, unintentional noncompliance still leads to concealment
- Don't overlook "the curious incident of the dog in the night-time"
    - Sometimes the lack of a record is important

The Data Analysis Process



SCCE™ Society of Corporate Compliance and Ethics

Identifying Records and Data Needed

- Develop process map of the transaction/activity cycle(s) involved in the target area
  - MUST understand how the transaction cycle operates in order to identify relevant records/people needed
- Based on this process map, identify:
  - People involved in each step
  - Internal controls
    - Preventive
    - Detective
  - Documents and forms
    - Received
    - Created
  - Electronic records
  - Systems and databases affected

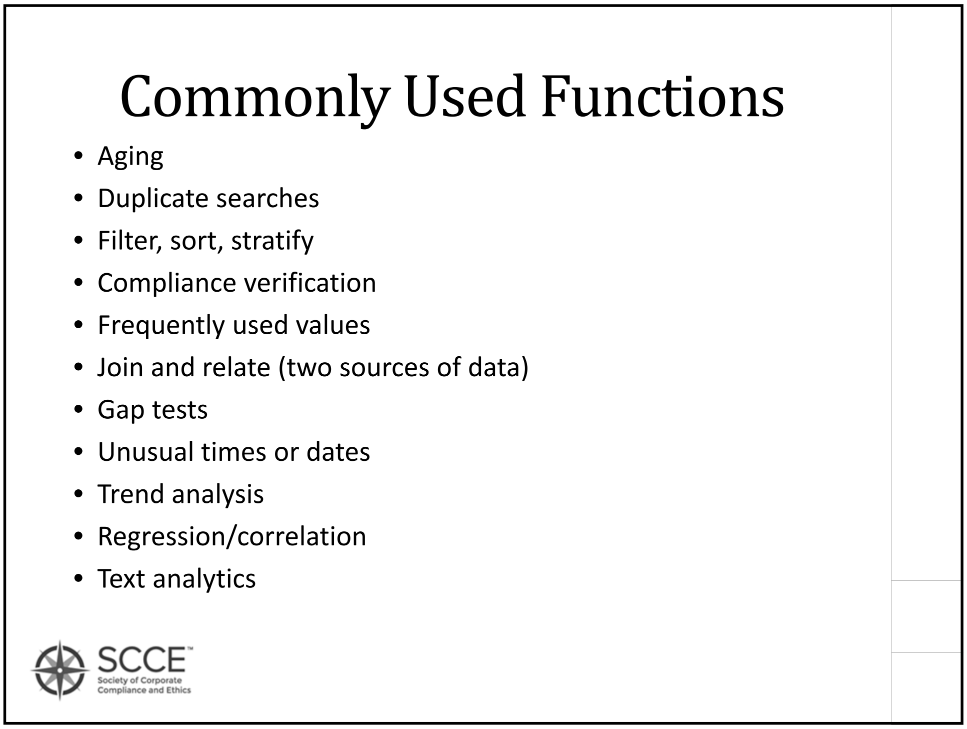
SCCE™ Society of Corporate Compliance and Ethics

Identifying Records and Data Needed

- **Example** – For corruption risk in the purchasing cycle:
  - Identification and documentation of need
  - Development of specifications, if necessary
  - Solicitation of bids or negotiation with alternative vendors
  - Selection of vendor
  - Contract, statement(s) of work, etc
  - Purchase orders
  - Change orders, subcontracts, etc
  - Receipt of goods or services
  - Submission, review and approval of invoice
  - Payment
- In addition, what other internal records would we expect along the way? E-mails, electronic approvals, etc.

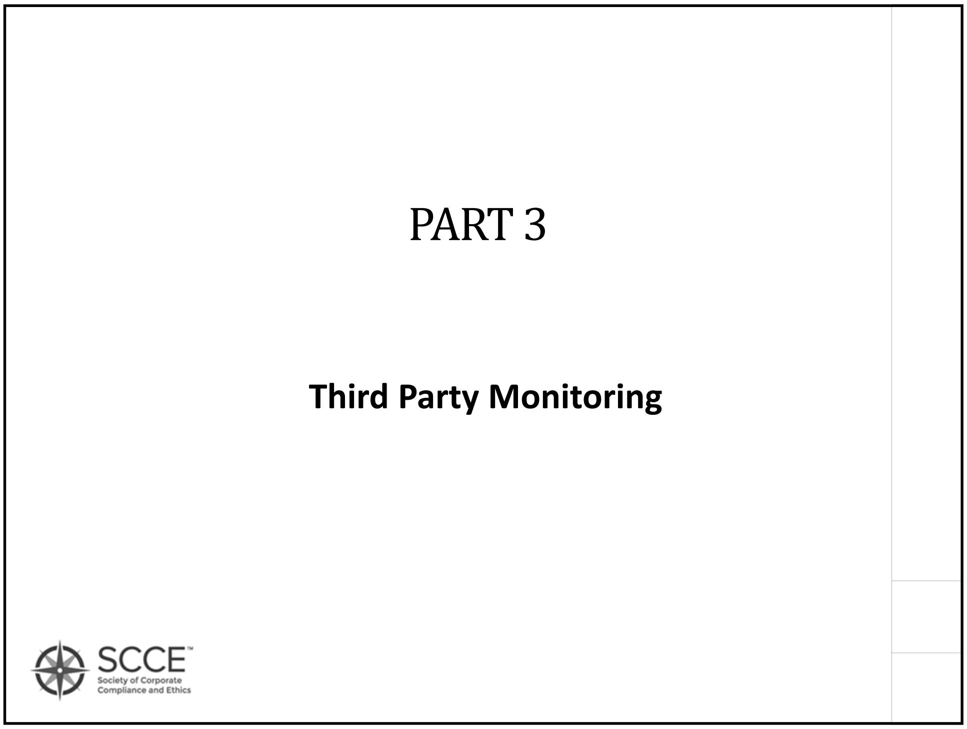
Example Data Sources: Bribery Payment Schemes

SOURCE	USES
Vendor master file	Identifies all approved vendors
Accounts payable ledger	Lists when and to whom payments are due
Cash disbursements journal	Lists all cash disbursements
Purchases journal	Reports requests for purchases
Selected GL accounts • Charity/donations • Agent/consulting payments • Marketing expenses	Identifies accounts where payment of a bribe could be hidden
Travel and entertainment	Itemized T&E submissions



Commonly Used Functions

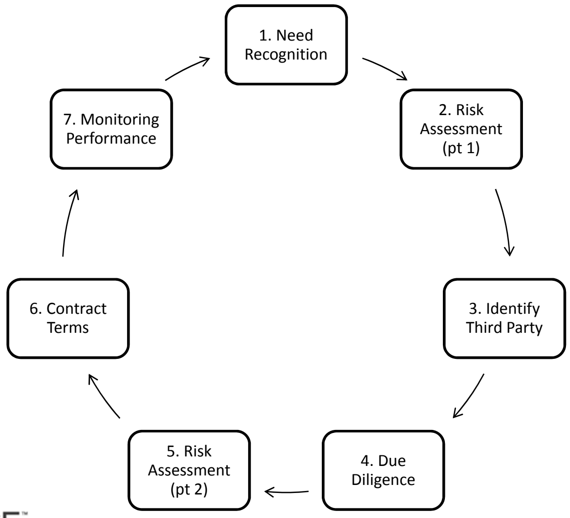
- Aging
- Duplicate searches
- Filter, sort, stratify
- Compliance verification
- Frequently used values
- Join and relate (two sources of data)
- Gap tests
- Unusual times or dates
- Trend analysis
- Regression/correlation
- Text analytics



PART 3

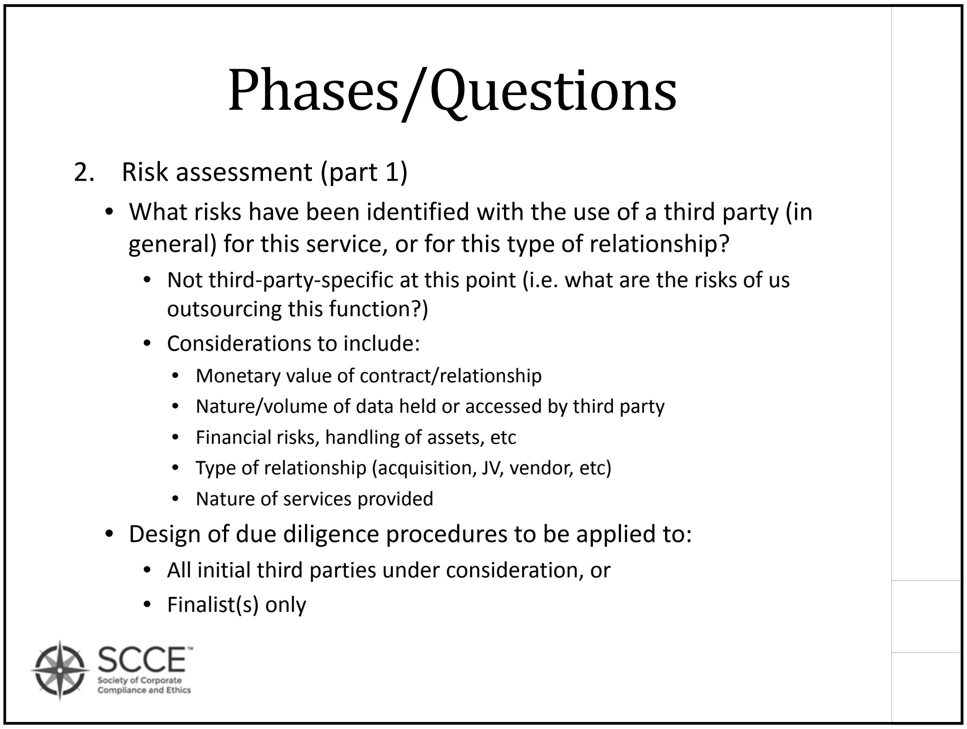
Third Party Monitoring

Third-Party Management Life Cycle


1. Need Recognition
2. Risk Assessment (pt 1)
3. Identify Third Party
4. Due Diligence
5. Risk Assessment (pt 2)
6. Contract Terms
7. Monitoring Performance

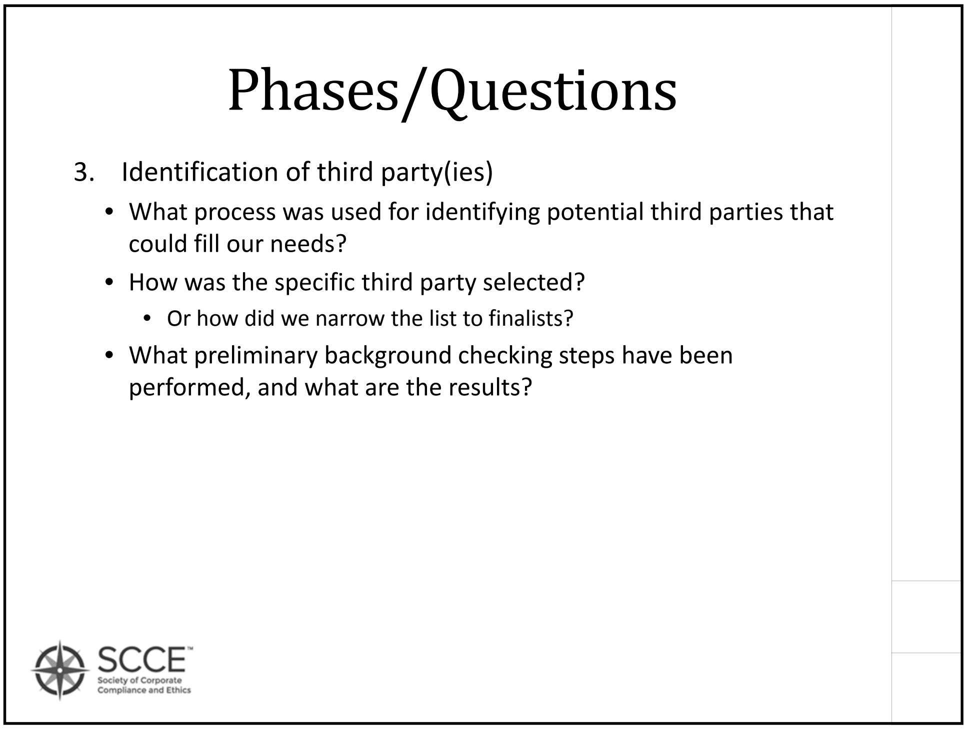
Phases/Questions

1. Need recognition
   - Is there a legitimate business need for a third party?
   - What business purpose would the third party serve?
   - Can we clearly articulate the scope of what the third party will do?
     - Scope of work



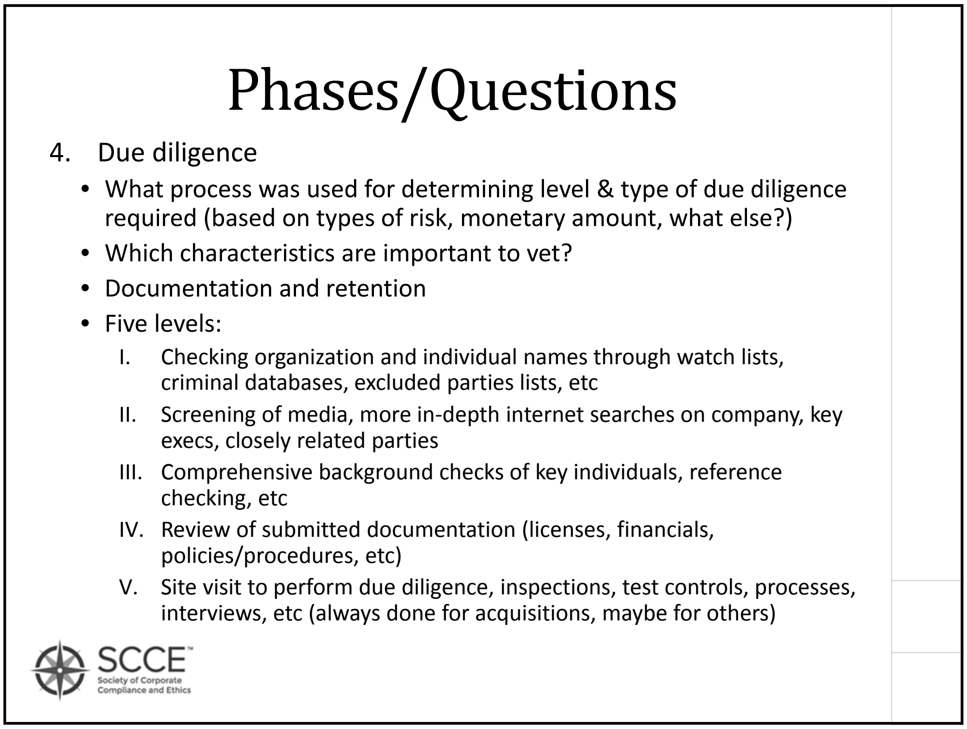
Phases/Questions

2. Risk assessment (part 1)
   - What risks have been identified with the use of a third party (in general) for this service, or for this type of relationship?
     - Not third-party-specific at this point (i.e. what are the risks of us outsourcing this function?)
     - Considerations to include:
       - Monetary value of contract/relationship
       - Nature/volume of data held or accessed by third party
       - Financial risks, handling of assets, etc
       - Type of relationship (acquisition, JV, vendor, etc)
       - Nature of services provided
   - Design of due diligence procedures to be applied to:
     - All initial third parties under consideration, or
     - Finalist(s) only



Phases/Questions

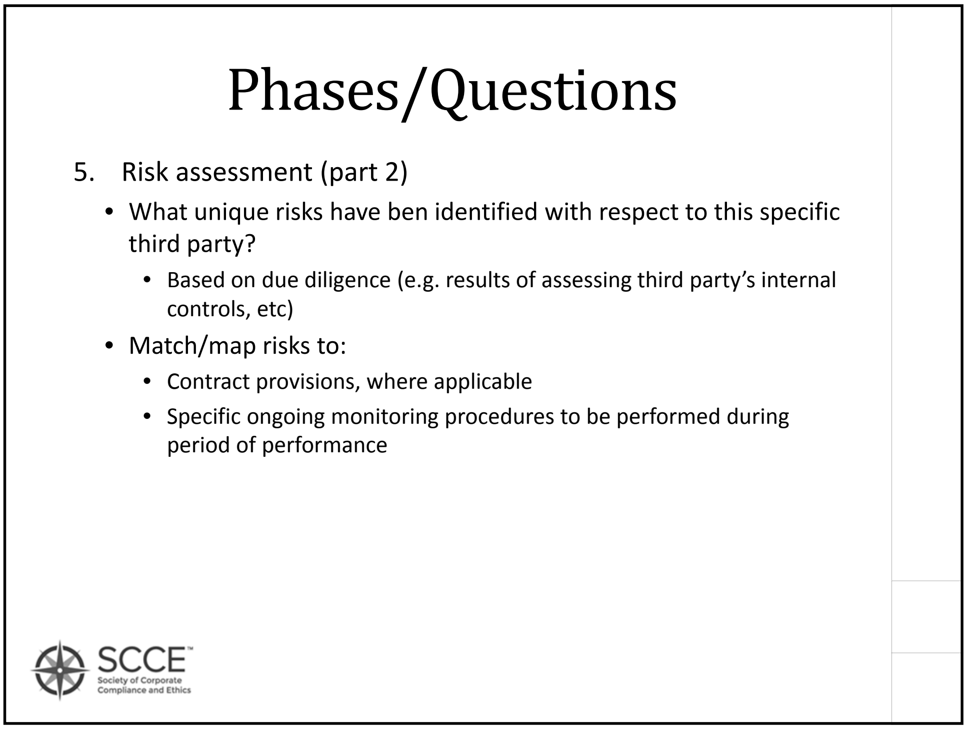
3. Identification of third party(ies)
   - What process was used for identifying potential third parties that could fill our needs?
   - How was the specific third party selected?
     - Or how did we narrow the list to finalists?
   - What preliminary background checking steps have been performed, and what are the results?



Phases/Questions

4. Due diligence
   - What process was used for determining level & type of due diligence required (based on types of risk, monetary amount, what else?)
   - Which characteristics are important to vet?
   - Documentation and retention
   - Five levels:
     - I. Checking organization and individual names through watch lists, criminal databases, excluded parties lists, etc
     - II. Screening of media, more in-depth internet searches on company, key execs, closely related parties
     - III. Comprehensive background checks of key individuals, reference checking, etc
     - IV. Review of submitted documentation (licenses, financials, policies/procedures, etc)
     - V. Site visit to perform due diligence, inspections, test controls, processes, interviews, etc (always done for acquisitions, maybe for others)

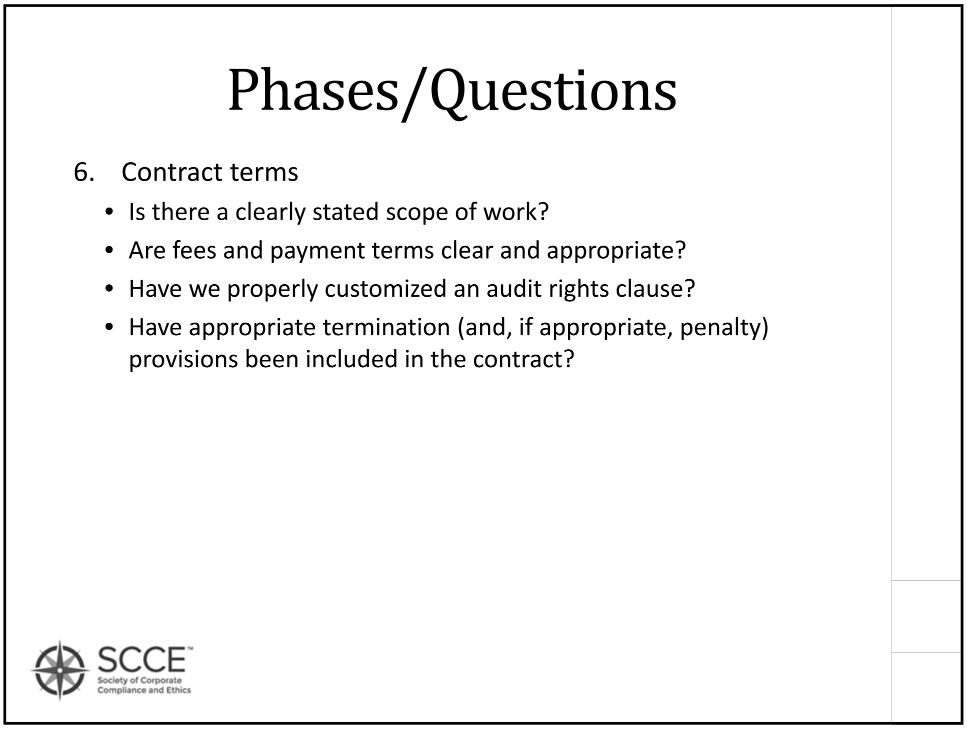
SCCE™ Society of Corporate Compliance and Ethics



Phases/Questions

5. Risk assessment (part 2)
   - What unique risks have ben identified with respect to this specific third party?
     - Based on due diligence (e.g. results of assessing third party's internal controls, etc)
   - Match/map risks to:
     - Contract provisions, where applicable
     - Specific ongoing monitoring procedures to be performed during period of performance

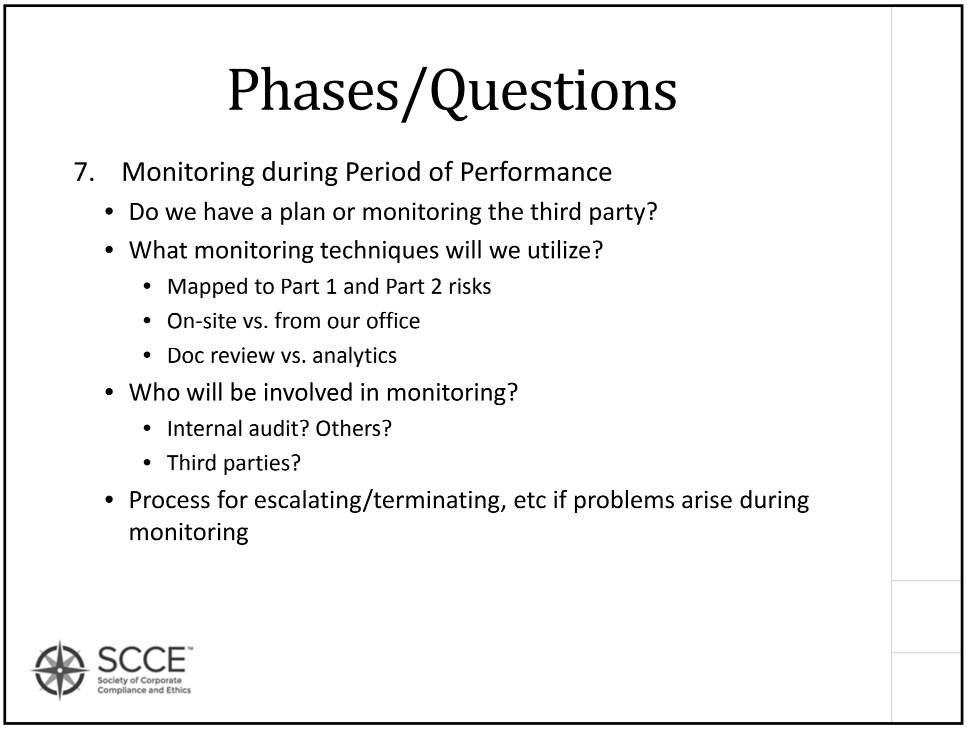
SCCE™ Society of Corporate Compliance and Ethics



Phases/Questions

6. Contract terms
   - Is there a clearly stated scope of work?
   - Are fees and payment terms clear and appropriate?
   - Have we properly customized an audit rights clause?
   - Have appropriate termination (and, if appropriate, penalty) provisions been included in the contract?

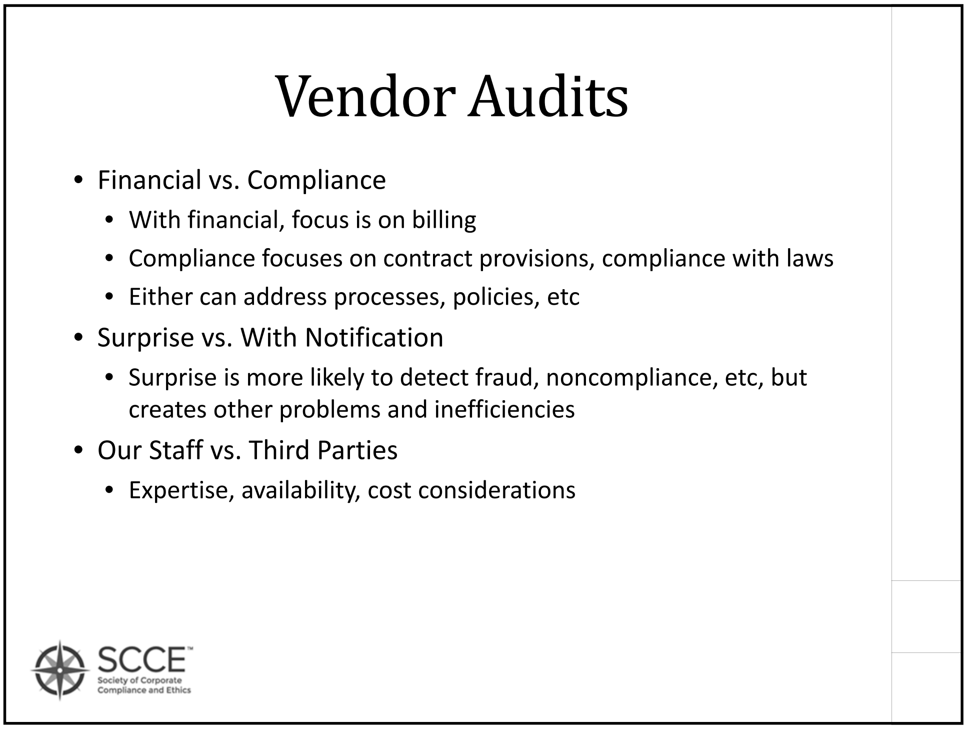
SCCE™ Society of Corporate Compliance and Ethics



Phases/Questions

7. Monitoring during Period of Performance
   - Do we have a plan or monitoring the third party?
   - What monitoring techniques will we utilize?
     - Mapped to Part 1 and Part 2 risks
     - On-site vs. from our office
     - Doc review vs. analytics
   - Who will be involved in monitoring?
     - Internal audit? Others?
     - Third parties?
   - Process for escalating/terminating, etc if problems arise during monitoring

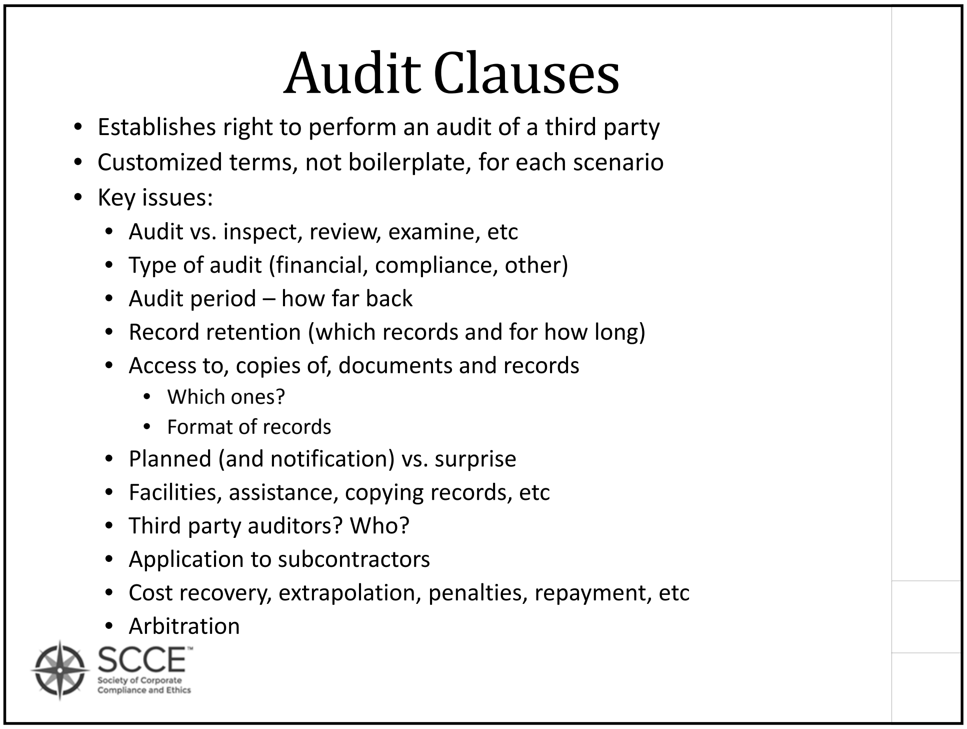
SCCE™ Society of Corporate Compliance and Ethics



Vendor Audits

- Financial vs. Compliance
  - With financial, focus is on billing
  - Compliance focuses on contract provisions, compliance with laws
  - Either can address processes, policies, etc
- Surprise vs. With Notification
  - Surprise is more likely to detect fraud, noncompliance, etc, but creates other problems and inefficiencies
- Our Staff vs. Third Parties
  - Expertise, availability, cost considerations

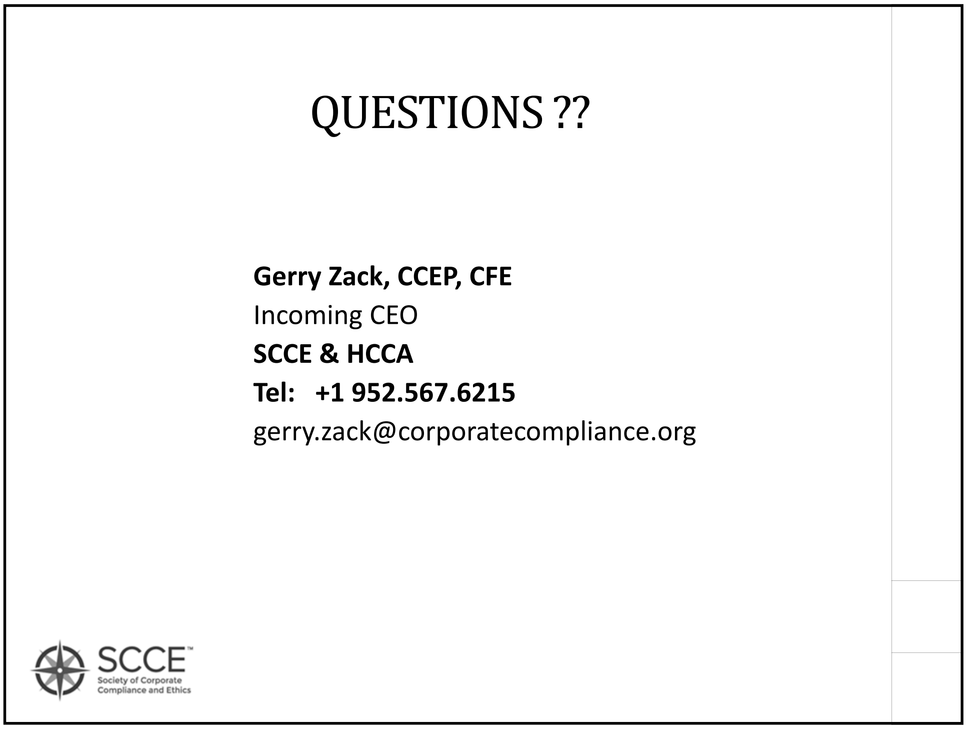
SCCE™ Society of Corporate Compliance and Ethics



Audit Clauses

- Establishes right to perform an audit of a third party
- Customized terms, not boilerplate, for each scenario
- Key issues:
  - Audit vs. inspect, review, examine, etc
  - Type of audit (financial, compliance, other)
  - Audit period – how far back
  - Record retention (which records and for how long)
  - Access to, copies of, documents and records
    - Which ones?
    - Format of records
  - Planned (and notification) vs. surprise
  - Facilities, assistance, copying records, etc
  - Third party auditors? Who?
  - Application to subcontractors
  - Cost recovery, extrapolation, penalties, repayment, etc
  - Arbitration

SCCE™ Society of Corporate Compliance and Ethics



QUESTIONS ??

Gerry Zack, CCEP, CFE
Incoming CEO
SCCE & HCCA
Tel: +1 952.567.6215
gerry.zack@corporatecompliance.org

SCCE™
Society of Corporate
Compliance and Ethics