

A vibrant, circular collage of legal and business-related icons. The design features a variety of symbols such as scales of justice, magnifying glasses, briefcases, folders, documents, and checklists, all rendered in a clean, line-art style. The color palette is bright and varied, including shades of orange, green, blue, and red. The icons are interspersed with decorative elements like stars, diamonds, and plus signs, creating a dynamic and professional visual composition.



Agenda

- Importance of third-party risks to overall business risks
- Third-Party risk management procedures to collect and analyze data to inform specific risk profiles
- Mitigation strategies tied to risk profiles
- Continuous risk updating and compliance program improvement



-
- An aerial, top-down view of a massive container yard. The yard is filled with thousands of intermodal containers stacked in neat, dense rows. The containers come in a wide variety of colors, including blue, red, yellow, green, and white, creating a vibrant, multi-colored mosaic. Several large, blue gantry cranes are positioned throughout the yard, their long horizontal beams spanning over the stacks of containers. The perspective is from directly above, showing the layout of the yard and the scale of the operations. The lighting is bright, casting sharp shadows that emphasize the three-dimensional nature of the stacked containers.

Business Continuity & Third-Party Procedures



Business Justification



Due Diligence



Contract



Risk Mitigation

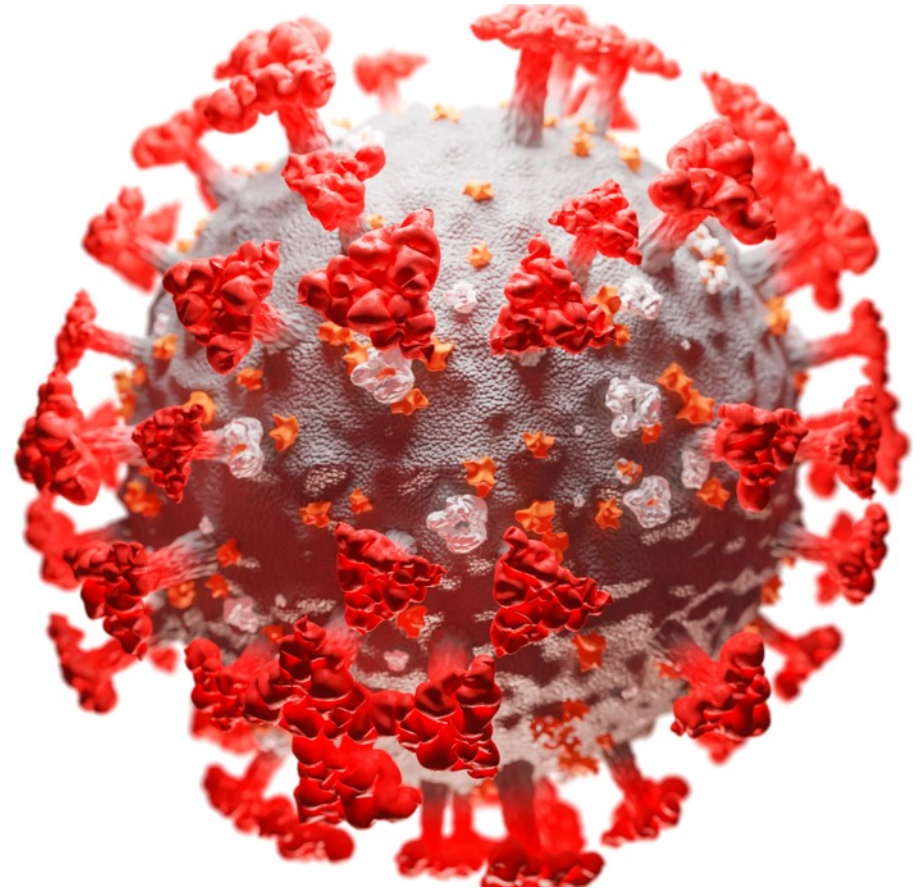


Monitoring, Testing and Audits



What COVID-19 Exposed

- COVID-19 introduced a sudden disruption to operations
- Firms were unable to find new suppliers in a timely manner
- Firms had to adjust sales distribution channels and logistics
- The onboarding of replacement suppliers and distributors occurred in a haphazard way



Supply Chain: Defining “Risk”

- Supply risks rise from a variety of sources:
 - Political
 - Legal
 - Logistics
 - Climate
 - Financial
 - Economic (e.g. sole supplier?)
- Holistic approach considers all of these risks together
 - Impact on business
 - Likelihood of occurrence



Developing a Holistic Risk Model

- What risks would be considered?
 - Data that would be used (supply quantity, price and value)
 - Impact of disruption
 - Training on model
 - Metrics on success of risk management
 - Maintaining supply, reducing costs, and overall measurement of procurement function



What Role Should Compliance Play ?

- Shares considerable overlap with enterprise risk
- Plays an important role in locating and onboarding substitutes.
- Offers a “line of sight” across the organization.
- Balances competing distribution, supply chain and fiscal management priorities.



DOJ and Regulatory Expectations

- Third-Party Risk Management Expectations
- Monitoring, Updating and Continuous Improvement



DOJ Revises Its Compliance Evaluation Guidance



June 1, 2020



Access to and use of data



Real-time monitoring



Continuous updating of program



Measure, Monitor and Review

It is a good idea and government says so

DOJ's Evaluation of Corporate Compliance Programs	Continuous Improvement; Periodic Testing and Review; Control Testing; Evolving Updates
Federal Sentencing Guidelines	"Reasonable steps to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct; and to evaluate periodically the effectiveness of the organization's compliance and ethics program"
DOJ and SEC's Resource Guide to the FCPA	"DOJ and SEC evaluate whether companies regularly review and improve their compliance programs and not allow them to become stale."
OIG Compliance Program Guidance	"The use of audits and/or other evaluation techniques to monitor compliance and assist in the reduction of identified problem areas."

Compliance Vision



Compliance industry is moving fast



Technology and innovation

Data analytics

Artificial Intelligence



Machine learning



Sophisticated strategies for monitoring, testing and auditing



Replacing reactive – e.g., classic audit retrospective testing



Proactive monitoring and risk management

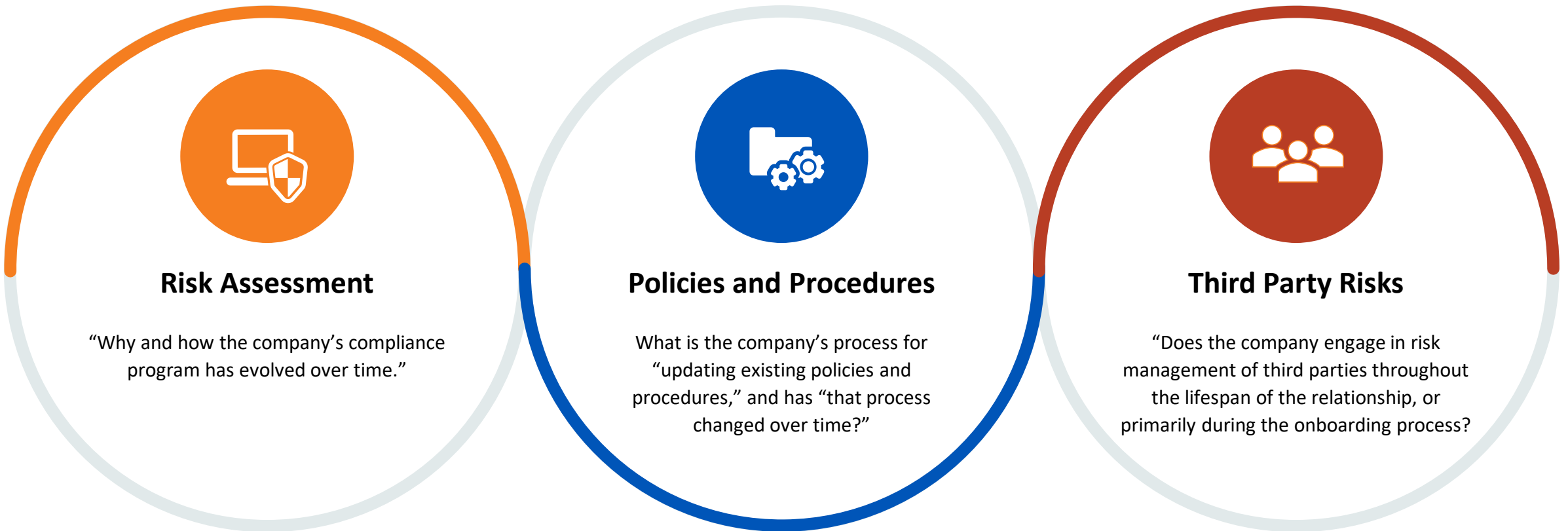


DOJ Evaluation Guidance Expectations

- Data-driven reviews
- Disfavor “snapshot” in time
- Favor “continuous” based on access to operational data and information across functions
- DOJ expects this information to be used to update compliance and business operations:
 - Risk assessments
 - Policies and procedures
 - Financial controls



DOJ Emphasis on Real-Time Monitoring and Continuous Improvement



Automation is Imperative

- Effective risk identification requires gathering and analyzing more and more information
 - Gathering information is time consuming!
 - Analyzing information is time consuming!
- Automation is an effective strategy to manage information flow
- Intelligent automated systems provide efficient information presentation



The background of the slide is a complex, abstract composition. It features a grid of binary digits (0s and 1s) in various colors, including red, blue, and white. Overlaid on this grid are several mathematical expressions and formulas, such as $x=0$, $1+x+y+2a$, $(3a+3g+x)$, and $1+x+y+2a+21$. The overall aesthetic is high-tech and digital.

Artificial Intelligence & Machine Learning

- New technology for faster and more efficient database searches
- Some due diligence data service providers offer platforms with this capability
- Artificial intelligence = increased computer storage and processing capabilities
- Artificial intelligence = more efficient and faster search



Third-Party Data

- Classifying Third Parties
- Assessing Risk
- Collecting Data
- Mitigation Strategies



Third Parties – Who Are They?



Due Diligence Data and Analysis



Collect during onboarding process



Create risk profile









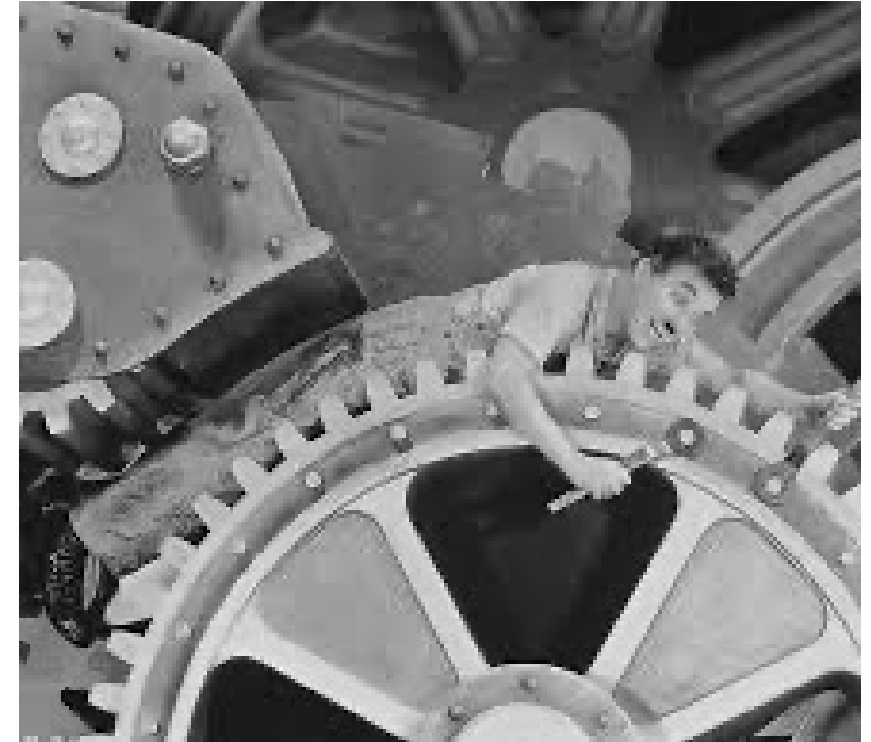
Refresh and collect additional data
(internal and external sources)



Incorporate monitoring and refresh
data to reassess risk profile and
mitigation strategies

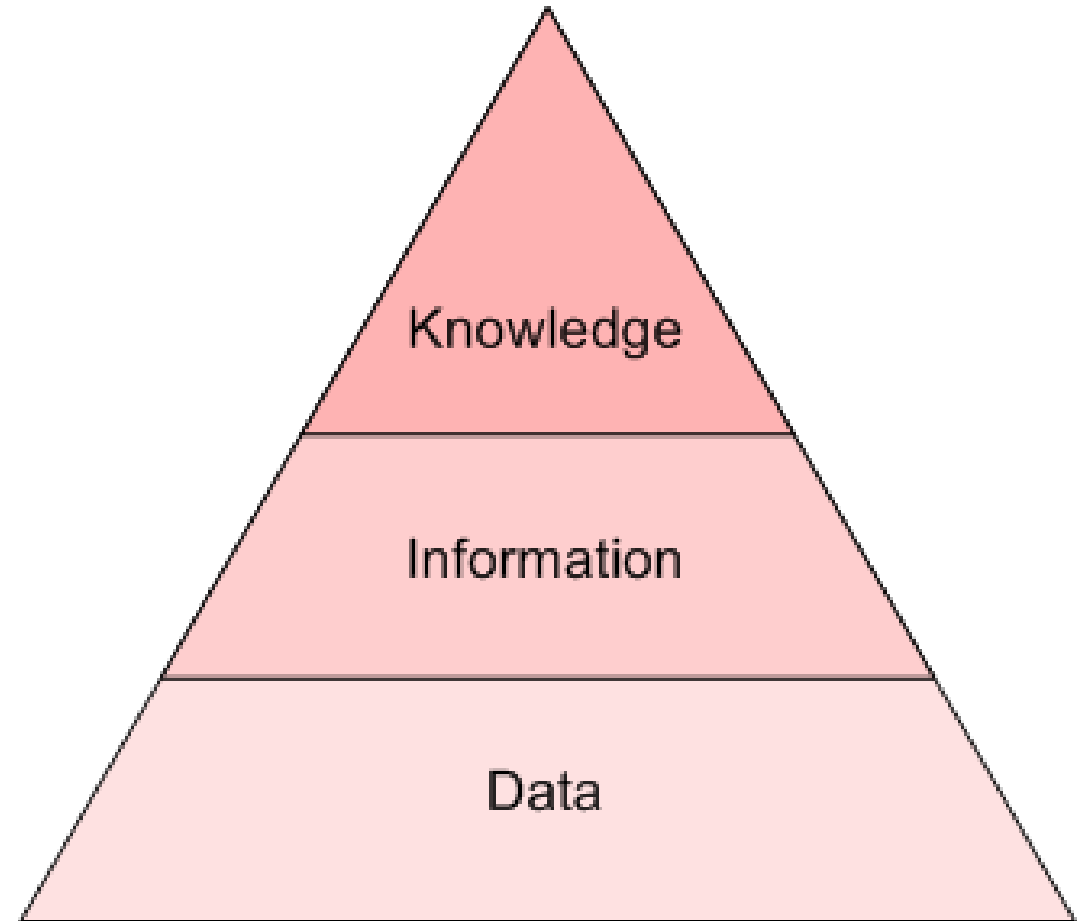
Data Sources: Automation

-  **Third-party onboarding and monitoring**
-  **Continuous refresh of due diligence data**
-  **Financial transactions and controls
(e.g. discounts, rebates, tender offers)**
-  **Transaction monitoring**
-  **Testing financial and compliance controls
via sampling**
-  **Training**

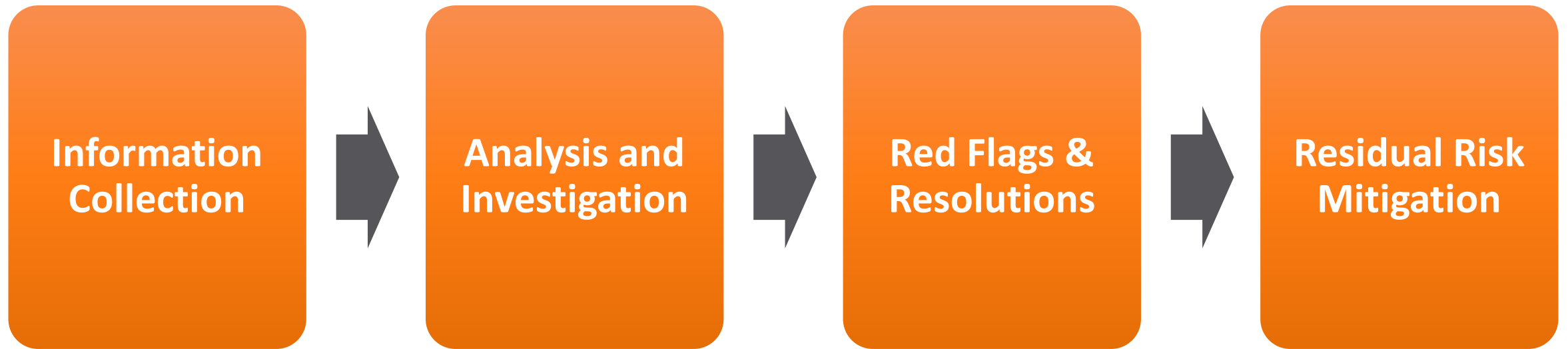


Due Diligence Information Collection: Onboarding

- Country of operation
- Board members
 - Government official or former official
 - Close family member foreign official
- Qualifications
- Financial status
- Payment arrangements and bank account(s)
- Professional background
 - Prior or ongoing litigation
 - Criminal record
- Licenses and authorizations
- Adverse media reports



4 Required Steps For Minimizing Risk



Third-Party Data: Ongoing Operations



Financial transactions



Unusual transactions, payees or payments



Purchases or sales trends



Unusual business activity



**Changes in ownership, board members,
management**



Nature of ongoing interactions



Adverse media reports



Third-Party Information: Testing and Auditing



Focus on high-risk



Sample financial transactions



Look for high-risk sources: rebates, discounts, tenders



Customer end-users



Financial anomalies



Red flags of change in ownership, operations or unusual business patterns



Supplement “traditional” audit plan



Understanding Third-Party Risks

- Anti-Corruption
- Sanctions
- Money Laundering
- Cyber and data breach



Sophisticated System for Determining Risk Profile

- Identify and weigh your risks:
 - Anti-corruption
 - Foreign official interactions and potential ownership interests
 - Export controls
 - Trade sanctions
 - Anti-Money laundering
 - Cyber-security and data



Classify Your Third Parties

- Representation
 - Agents and sub-agents
 - Distributors and sub-distributors
 - Customs/immigration
 - Regulatory
 - Professionals
- Government-owned (any amount)
- Professionals
- Vendors/suppliers
- Nominees



Sanctions Risk Assessment

- Risk Assessment must consist of a “holistic review of the organization from top-to-bottom and asses its touchpoints to the outside world.”
- Required elements
 - Clients and customers
 - Products and services
 - Supply chain
 - Intermediaries and counter-parties
 - Transactions
 - Locations
 - Potential mergers and acquisitions, particularly non-US companies



Distributor and Agent Sanctions Risks

- Specially Designated Nationals
- Sectoral sanctions
- 50 percent rule
- Beneficial ownership
- Sub-distributors and liability
- Prohibited end customer or country



OFAC Supply Chain Risks: The New Frontier

- Supply chain audits (akin to conflict minerals compliance)
- Parties that are not in direct privity
- Liability extends to unknown sourcing from prohibited parties
- Contractual provisions need to “flow down” OFAC compliance
- Geographic and product/service risks evaluated (e.g., North Korea -- China, Iran -- Dubai)



Anti-Money Laundering Third-Party Risks



Trade-based risks



Large and unexplained purchases



Third-party payments



Accounts receivable



Due Diligence and Beneficial Ownership

Customers/Clients

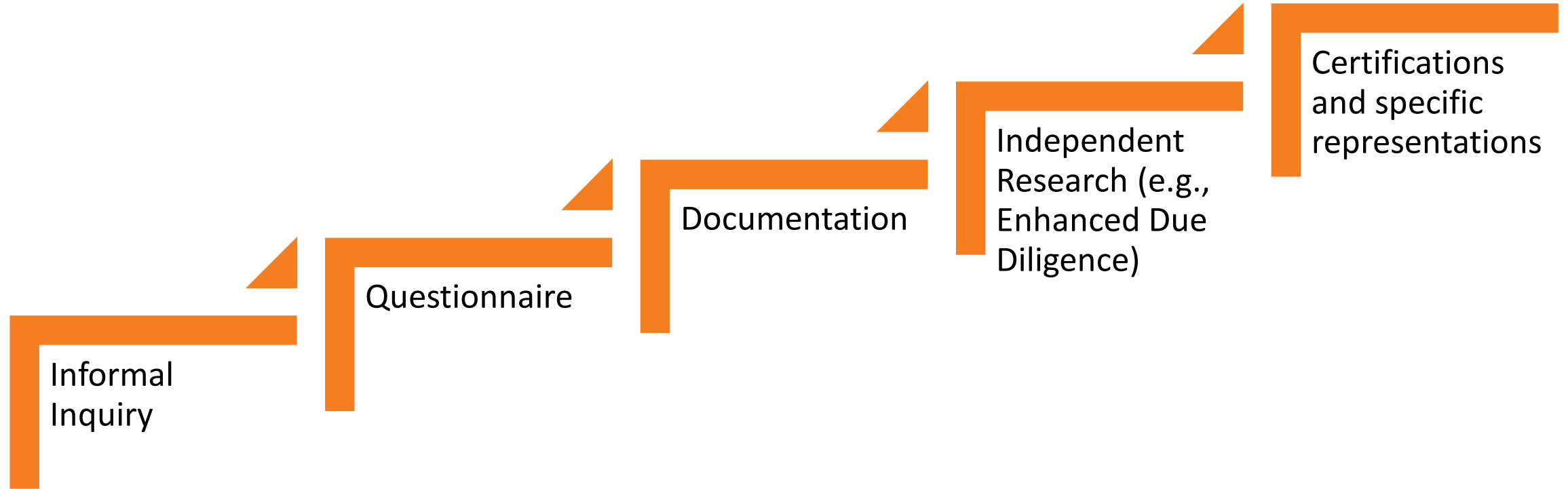
- Lack of due diligence of organization's **ownership** and ***business dealings***
- Customers
- Supply chain
- Intermediaries
- Counter-parties

Due Diligence Factors

- Various OFAC enforcement actions involve improper or incomplete due diligence:
 - **Ownership**
 - Geographic locations
 - Counter-parties
 - Transactions
 - Knowledge and awareness of OFAC sanctions



Ownership Verification



Cybersecurity Threats: An Evolving Set of Risks

- Primary threats today:
 - Phishing and malware attacks
 - Ransomware (growing)
 - Denial of service (DDoS) against high-profile companies by attacking Internet of Things (IoT) devices (service disruptions to Twitter, Airbnb, Android devices)
- Ransomware attacks circumvent encryption and rely on tried-and-true phishing campaigns.
- Point of sale attacks have declined because of advent of chip technology
- Focus on corporate data – financial and personal data



Third Parties and Cyber Risks

- Third parties back door to circumvent cybersecurity (e.g., Target)
- IoT risks: Expanding network of physical devices, vehicles, home appliances that contain software, sensors and network connectors to transmit and exchange data
- Businesses connect as many as 3 billion objects to the existing network and are expanding past network devices
- IoT devices are generally unsecured and lack basic protections
- Only one quarter of companies assess, manage and monitor third-party cyber risks
- Global companies will have to add cybersecurity and data risks to due diligence and impose cybersecurity standards (e.g., encryption)



Data Breach and Response

- Legal requirements vary across U.S. states and countries
- Countries are gravitating toward EU framework
- GDPR has imposed strict 72-hour and documentation requirements
- GDPR definition of “breach” is broad
- Legal and compliance have to prepare a response protocol and define responsibilities for each actor



Determining Risk Profile

- Based on factors outlined above, companies identify and assess risks
- For many third parties, country (CPI and proximity to OFAC embargoed countries), type of third party and projected annual revenues/sales will drive determination of high, medium or low risk
- Stratify risks based on these three factors
- Additional factor for cybersecurity and privacy
- Designation of category will trigger applicable controls and monitoring, testing and auditing practices



Apply “Rules” to Each Class



**Onboard to
Contract**



**Information
Updates**



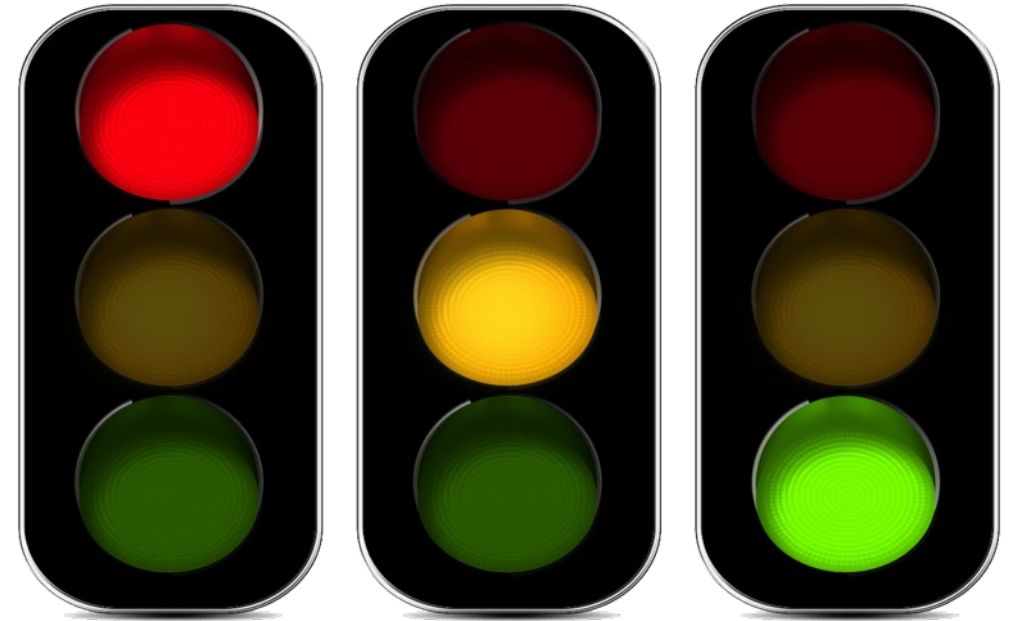
**Audits and
Testing**



**Monitoring
Program**



Investigations



Define High, Medium and Low Risk Categories

High

- Representatives (agents, consultants and distributors)
- Government ownership or control
- Interact with government entity (state-owned entities)

Medium

- Vendor or supplier
- Above spend threshold
- Operates in higher risk countries
- < 50 CPI

Low

- Vendor or supplier
- Below spend threshold
- Operates in lower risk countries
- > 50 CPI

Mitigation Strategies

- Screening
- Monitoring
- Testing, Sampling
- Audits



Database Requirements

Selection

Which solutions did you consider and why did you select the specific solution?

Calibration

What settings did you implement in the screening software and how does this incorporate your risk assessment and profile?

Routine Testing

How often do you test your solution to ensure that your results are accurate and reliable?

Risk Management: The Three Essential Functions

Due Diligence Onboarding

Monitoring

Audit and Testing

Should Your Recalibrate Onboarding, Monitoring and Auditing Functions?



Due Diligence

Screen

Research

Document

Focus on High-Risk (10%)

Standard Mitigation Package



Monitoring

Intensive Red-Flag Program
(Contact, Interview,
Transaction Testing)

Update Notices

Sampling of Medium Risk



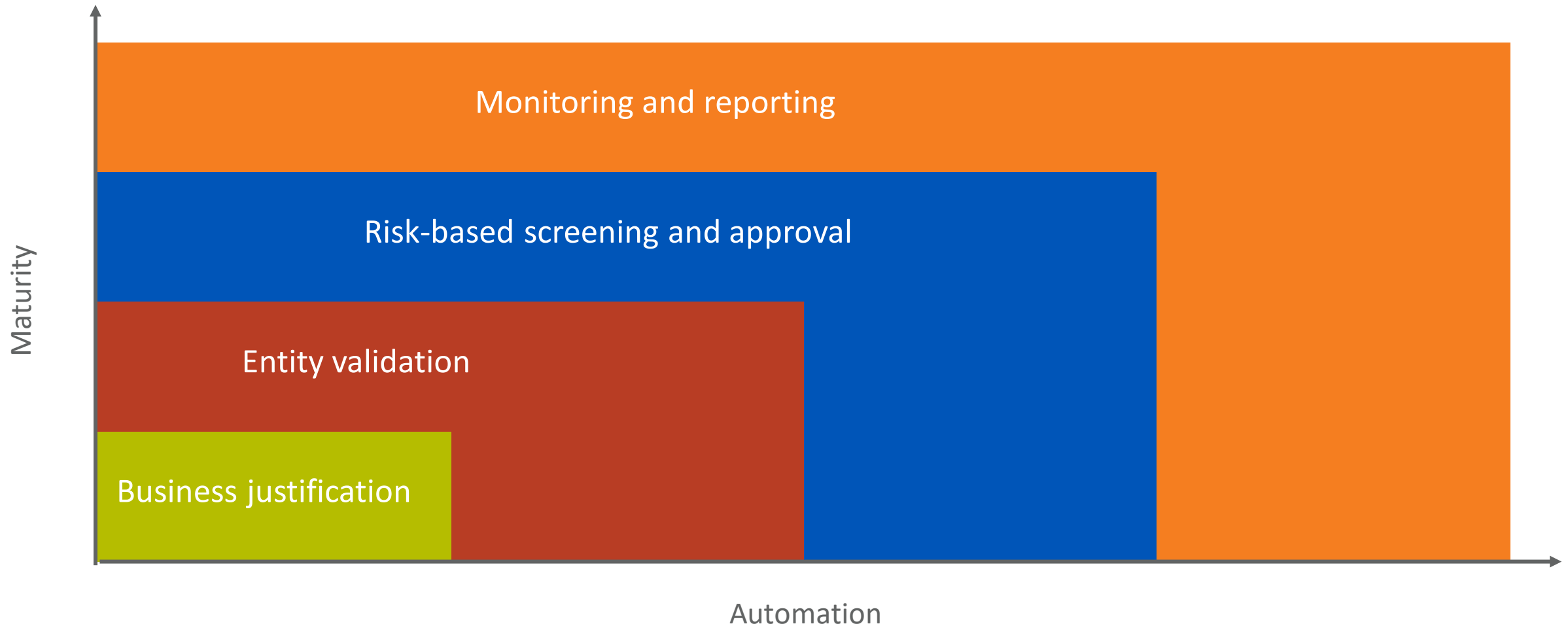
Testing/Audit

High-Risk Audits

Sample Medium Risk

Training Evaluation

Building & Scaling your Third-Party Program



Monitoring & Third-Party Data

- Changes in ownership, directors or management
- New adverse information
- Change in business activity
- Sampling of transactions
- Due diligence refresh
- Invoice to payment issues
- Third-party payments



Proactive Sampling of Third-Party Transactions

- Focus is immaterial transactions
- Search for anomalies in high-risk accounts
- Strategy for sampling is:
 - Risk rank financial operations by region, country or product/service
 - Identify high-risk accounts in these categories
- Sampling protocol



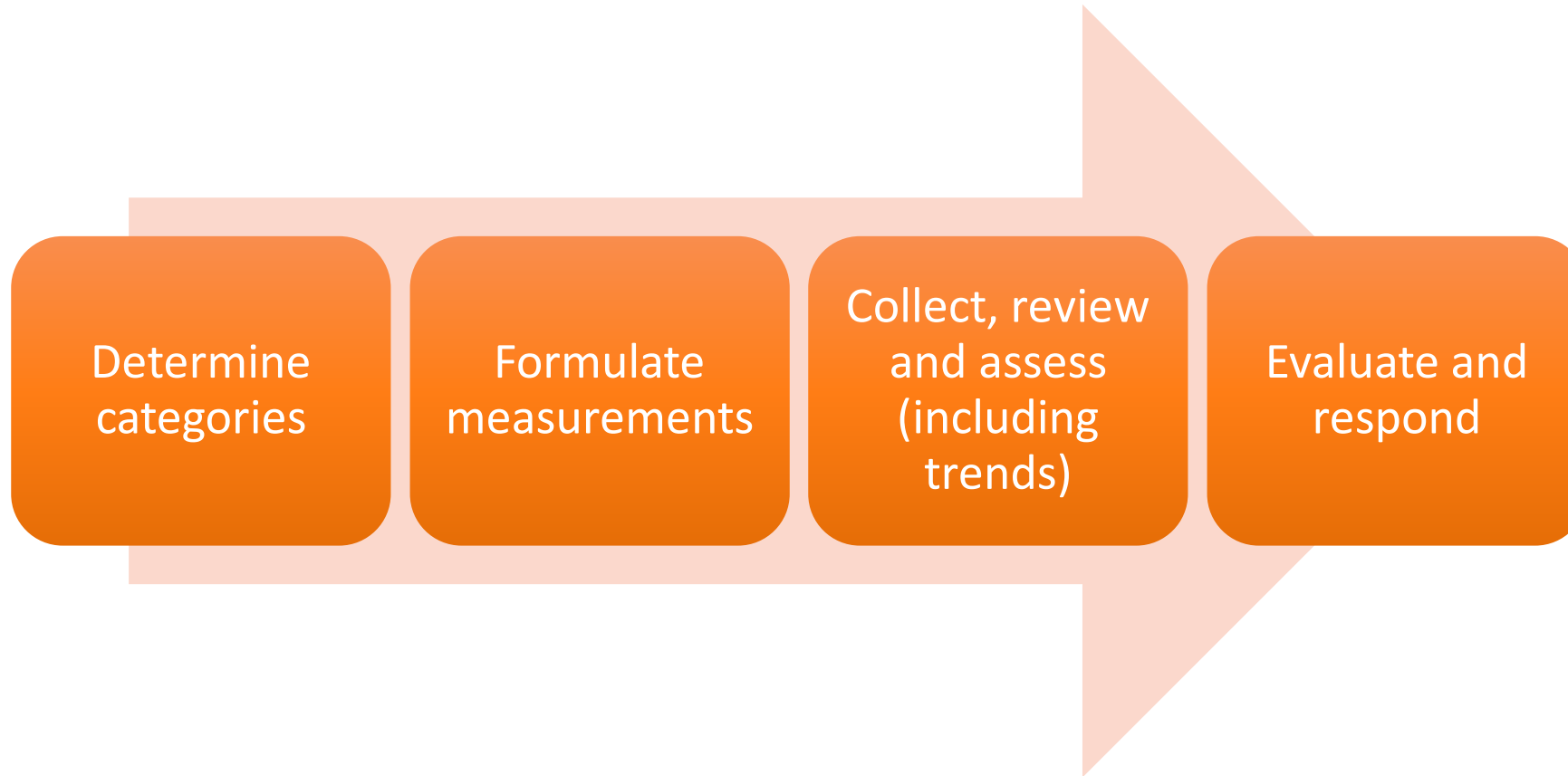
Transaction Analytics and Sampling Focus

- Apply forensic analytic tools to search for “anomalies” or “suspect” transactions
- Depends on trial balance account labels
- Difficult if transactions outside of ERP system and on spreadsheets
- If ERP system, transaction testing can be conducted remotely
- Adequate documentation
- Duplicate transactions
- Proper justification
- Compliance with controls
- Comparison of vendor data with employees, agents or distributors data
- Emails and surrounding communications if necessary

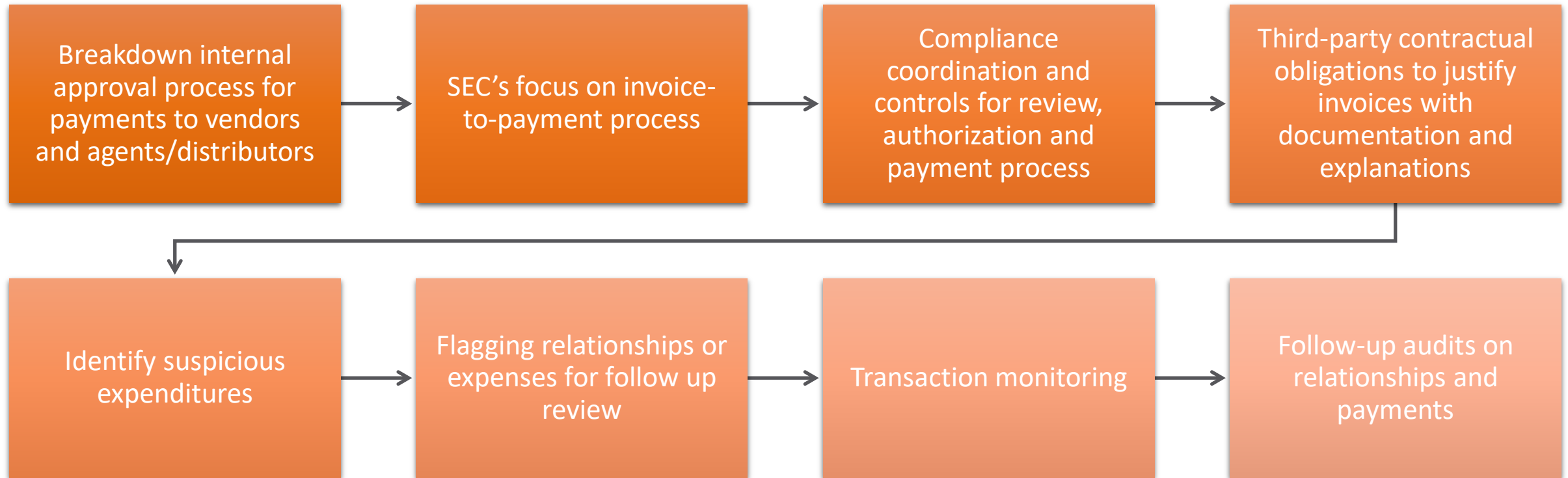


The Big Picture for Data and Monitoring

4 Key Steps in the testing and review process:



Financial Controls



High-Risk Monitoring Program

- Design high-risk 3P partnership program (compliance and business)
- Build ongoing check-ins, transaction review and business input/meetings
 - Consider survey form
 - Key to initial date and quarterly check-ins
- Identify risks and follow-up issues based on continuous monitoring of business
 - Business opportunities, bidding and tender
 - Invoices, statement of services and payments
 - Suspicious or unusual compensation (high commission or fees)
 - Diversion risks (marketing fund allowance, discounts)
 - Transaction sampling



Auditing Plan and Cadence

Audit Subjects and Schedule

- Customer verification and documentation
- Pricing and discounts
- Discounts and rebates
- Product samples
- Annual plan

Means

- Sampling of transactions
- Risk-based ranking
 - Sanctions locations
 - FCPA red flags
- Control compliance audits
 - Rate of compliance with controls for discounts, rebates
- Substantive review of population or samples



Continuous Risk Monitoring: Information

- Risk assessment is the **foundation** of your compliance program
- Update risk assessment from regional and local sources
- Conduct targeted surveys: divide as needed to update information annually
- Focus on specific risk factors
 - FCPA (foreign official interactions)
 - Antitrust: Interactions with competitors
 - Healthcare fraud: Billing, quality of care, reimbursement
 - Sanctions: Geographic and customer risks
 - AML: If non-financial institution, 3P payments
- Identify and update risk profile
- Implement regular update process



The Volkov Law Group

- Anti-corruption due diligence, compliance, enforcement defense and internal investigations
- The Volkov Law Website: <http://volkovlaw.com>
- Follow Corruption, Crime & Compliance
<http://corruptioncrimecompliance.com>

Michael Volkov:

Mvolkov@volkovlaw.com

(240) 505-1992



Michael Volkov
CEO

mvolkov@volkovlaw.com

(p) 240.505.1992

(f) 831.298.0838

Licensed in Virginia and the District of Columbia

The Volkov Law Group

1940 DUKE STREET • ALEXANDRIA, VA 22314

www.volkovlaw.com

blog: www.corruptioncrimecompliance.com



www.volkovlaw.com





Thank You!

