Conducting Defensible Supply Chain Due Diligence

Having the right supply chain can be a competitive advantage but failing to control supplier risk can have devastating effects. With thousands of suppliers in play, due diligence requires more than a shallow review of readily available information at the time of onboarding. Real risk-based supply chain management demands ongoing due diligence with advanced methods and readily auditable supplier records. Records must not only enable oversight of each supplier but also should support reports and views of risk across the entire supply chain to enable true governance.

1. Start with Effective Governance

Establish a supply chain governing body to set "tone at the top", oversee critical risk identification and drive establishment of a unified data management capability.

RISKS TO THE BUSINESS

IDENTIFY HIGH LEVEL RISKS
Evaluate each area of risk in relation to business operations, products and services to identify those with the highest potential impact. Consider each type of risk and limitations established by leadership and by legislation/regulation. Determine level of importance for addressing each risk or risk category.

POLICY DEVELOPMENT
- Supplier selection
- Risk assessment
- Continuous monitoring
- Supplier reporting
- Templates

ESTABLISH POLICIES AND TEMPLATES
Use the organization's established guidance for development of policies including assignment of roles for authoring and management, templates and specific limitations for supplier use established by leadership. Provide policies for each stage of the due diligence process.
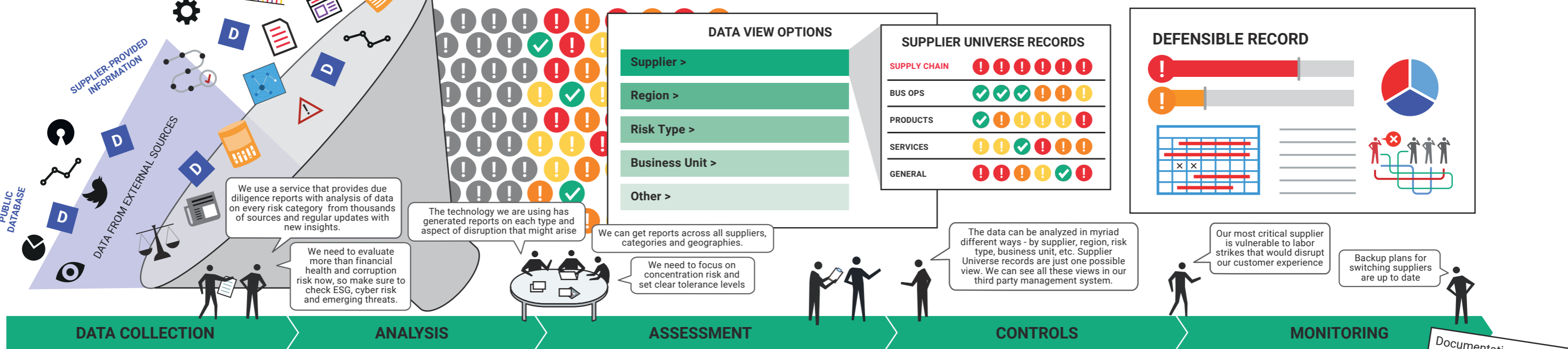
DEFINE DATA INTEGRATION
Provide guidance and resources to enable integration of internal and external data sources for use in due diligence, single system of record for each supplier, reporting and audit trail of due diligence process.

2. Apply Advanced Methods of Data Collection and Analysis

- Use information providers that provide consolidated data
- Ensure timely updates with ongoing monitoring
- Assess and monitor each supplier's risk
- Establish records of all data and analyses

3. Maintain Supplier Records and Audit Trail

- Identify categories of information for the supplier record
- Update record as changes are identified through data monitoring
- Enable views for different needs per record and across supplier universe
- Maintain historic records for audit needs

4. Manage Integrated Assessment, Controls and Monitoring

- Conduct risk assessments with scope based on initial analysis of need
- Apply controls based on identified risk levels for each supplier
- Revisit the process when changes in supplier information are flagged
- Integrate technology-supported assessment, controls and monitoring to support timely revisions and a defensible record of due diligence

SUPPLIER-PROVIDED INFORMATION

DATA FROM EXTERNAL SOURCES

PUBLIC DATABASE

DATA VIEW OPTIONS
- Supplier >
- Region >
- Risk Type >
- Business Unit >
- Other >

SUPPLIER UNIVERSE RECORDS

SUPPLY CHAIN	!	!	!	!	!	!
BUS OPS	✓	✓	✓	!	!	!
PRODUCTS	✓	!	!	!	!	!
SERVICES	!	!	✓	✓	!	!
GENERAL	!	!	!	!	✓	!

DEFENSIBLE RECORD

> We use a service that provides due diligence reports with analysis of data on every risk category from thousands of sources and regular updates with new insights.

> We need to evaluate more than financial health and corruption risk now, so make sure to check ESG, cyber risk and emerging threats.

> The technology we are using has generated reports on each type and aspect of disruption that might arise

> We can get reports across all suppliers, categories and geographies.

> We need to focus on concentration risk and set clear tolerance levels

> The data can be analyzed in myriad different ways - by supplier, region, risk type, business unit, etc. Supplier Universe records are just one possible view. We can see all these views in our third party management system.

> Our most critical supplier is vulnerable to labor strikes that would disrupt our customer experience

> Backup plans for switching suppliers are up to date

DATA COLLECTION → **ANALYSIS** → **ASSESSMENT** → **CONTROLS** → **MONITORING**

Today, the best supplier due diligence is managed in a technology-driven system supported by AI and automation. Data collection, risk analysis and assessment is ongoing. Controls are established and monitored and are revisited as risk assessments change because of new data. When issues are detected, corrective action plans are triggered.

Documentation of Decisions

Actions Taken

Monitoring Key Risks
Each vendor may have different risks but these are common across supply chains. Each risk requires monitoring of different data sources. Here are a few examples you may not have thought about:

POLITICAL INSTABILITY
- Regime changes
- Political upheaval
- Uncertainty in government policy
- Civil unrest

OPERATIONAL DISRUPTION
- Extreme weather events
- Concentration risks
- Border disruptions
- Resource shortages

CYBER ATTACKS
- Network security
- DNS Health
- Patching cadence
- Data breaches

BRIBERY AND CORRUPTION
- Sanctions
- Enforcement Actions
- Politically Exposed Persons (PEPs)
- Beneficial Ownership

MODERN SLAVERY/TRAFFICKING
- Product/materials
- Location
- Labor practices
- Enforcement actions

FINANCIAL HEALTH
- Profitability
- Operating Efficiency
- Z-score
- Liquidity