KY3P®

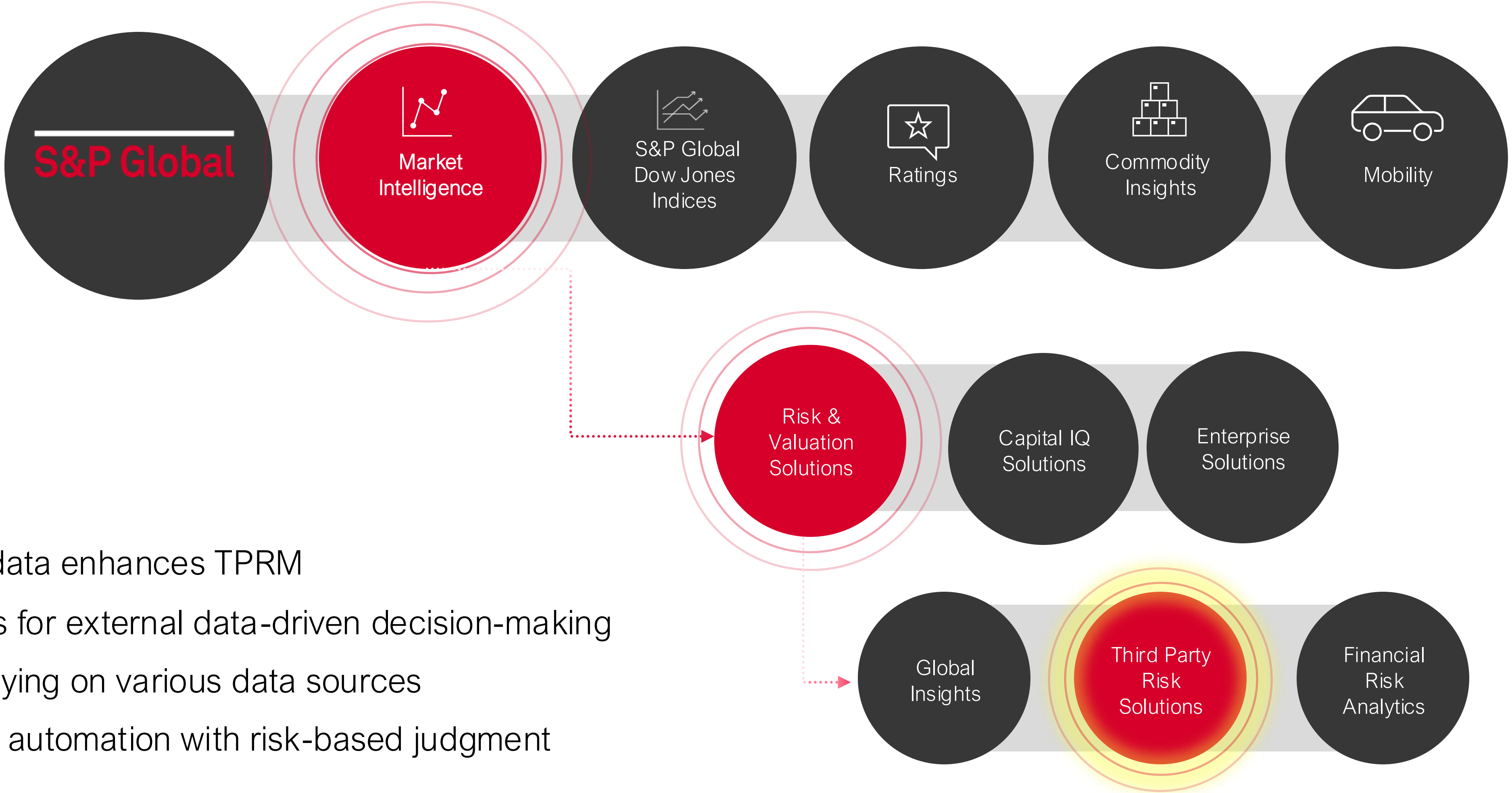
S&P Global

Leveraging External Data for Compliant Third-Party Risk Management

March 2025

S&P Global | Introduction and Objectives

The growing complexity of third-party risk

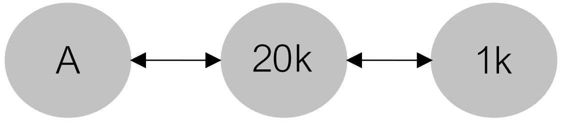


- Understand how big data enhances TPRM
- Explore best practices for external data-driven decision-making
- Identify key risks in relying on various data sources
- Learn how to balance automation with risk-based judgment

S&P Global | The Challenge of Third-Party Risk Today

Current approach to Third Party Risk Management is becoming unsustainable

Sole reliance on bilateral data exchange becomes untenable as scale and scope increases



A ↔ 20k ↔ 1k

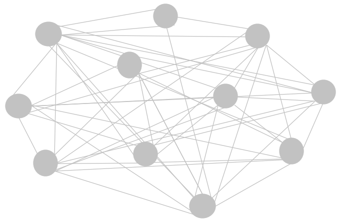
- Company A has 20k Third Parties
- Each of those have 1k Third Parties

Up to 50m

Information requests

Up to 1Bn

data points



- 330mn companies globally
- 380k large companies (>250 employees)
- Other organisations (non-companies) incremental

An inefficient model which struggles to deliver the required outcomes

Bilateral, in-consistent

Point in time view or no view

Manual and siloed

Inaccurate, incomplete

Qualitative

- ✗ Lack of visibility of risk, risk of non-compliance
- ✗ Unable to provide quality answers to basic stakeholder questions e.g. Boards/regulators
- ✗ Resource intensive focus on data collection
- ✗ Difficult to report and derive insight
- ✗ Suppliers are overwhelmed and pushing back
- ✗ Admin heavy - inability to attract / retain talent

S&P Global | What is Big Data in Third-Party Risk

Big data in TPRM includes structured and unstructured sources

In the coming years, many facets of Third-Party Risk Management will pivot towards reliance on data, rules, and AI. Advancing technology and enhanced information quality will propel this transformation.

- Internal: Assessments, contract history, audit results
- External Domain Specific: Cybersecurity ratings, financial stability, ESG scores, negative news
- External Broad Sourcing: Location Risk, Macro-economic scenario modeling, cross-domain analytics.
- Regulatory & Market: Sanctions lists, compliance breaches

One-to-many data exchange

Real-time insights

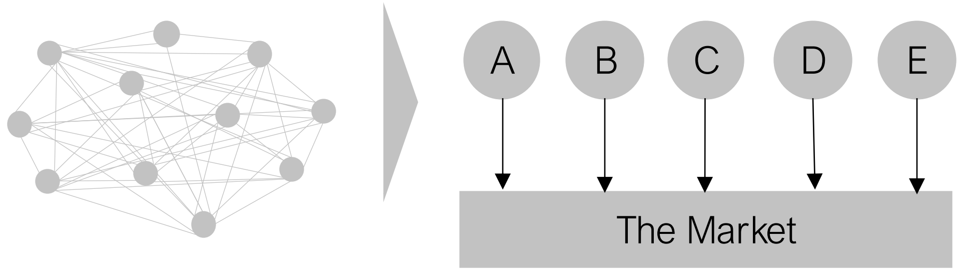
Automated

Dynamic

More quantitative and standardised

Risk data exchanged bi-laterally between companies

Company risk data available centrally as a one to many



✓ Enables clear reporting and insight and drives risk decision making

✓ Third parties are engaged and incentivised to contribute

✓ Resources focussed on response and mitigation

✓ Clarity to stakeholders e.g. Boards/regulators

S&P Global | Big Data Insights

Supply Chain Risk

Hold for S&P Global Research to be added before event

S&P Global | How Big Data Enhances TPRM Programs

Leveraging Data-Driven Insights for Smarter Risk Management

CYBER RISK INSTITUTE

GLOBAL RESILIENCE FEDERATION

Big data powers real-time risk monitoring, AI-driven assessments, and regulatory alignment, strengthening Resilience and general TPRM while optimizing supply chain oversight.

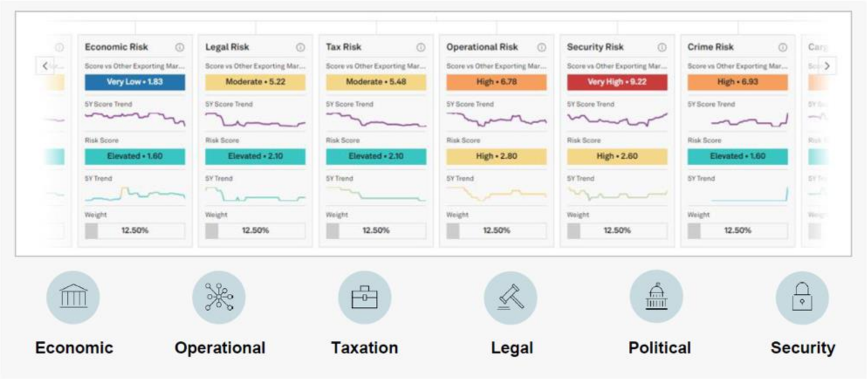
Key Use Cases:

- **Private & Public Data Sharing & Benchmarking:** Leverage industry-wide insights to improve resilience and cyber risk assessments and enhance decision-making.
- **Vendor Profiling & Ratings:** Utilize external data for automated oversight, risk correlation, and third-party matching.
- **Automated Due Diligence & Monitoring:** Combine profile data with validated assessments to proactively identify risks and recommend mitigation strategies.
- **Streamlined TPRM Processes:** Optimize efficiency and cost-effectiveness, ensuring speed, quality, and a sharper competitive edge.
- **Supply Chain Optimization & Risk Management:** Enhance visibility across supplier networks, predict disruptions, and ensure business continuity.

COUNTRY RISK AND ECONOMICS

Country Risk Analytics

Robust methodology reveals the full global risk profile.



	Economic Risk	Legal Risk	Tax Risk	Operational Risk	Security Risk	Crime Risk
Score vs Other Exporting Mar...	Very Low • 1.83	Moderate • 5.22	Moderate • 5.48	High • 6.78	Very High • 9.22	High • 6.93
Risk Score	Elevated • 1.60	Elevated • 2.10	Elevated • 2.10	High • 2.80	High • 2.60	Elevated • 1.60
Weight	12.50%	12.50%	12.50%	12.50%	12.50%	12.50%

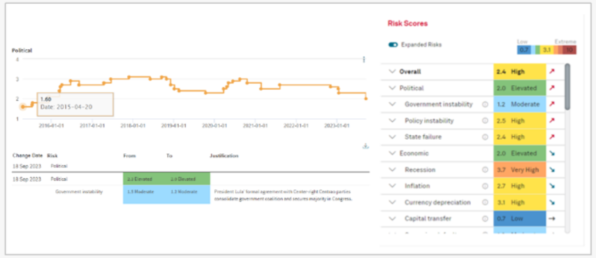
COUNTRY RISK AND ECONOMICS

Country Risk Data

Identify which markets are the best fit and have the most attractive sourcing environment with 12-month, forward-looking data.

Understand the evolution of potential risks to the business. Use risk as a key decision driver or consideration in sourcing and expansion decisions.

Uncover the economic and political risks in potential expansion markets or regions and factor them into decision-making.



Change Date	Risk	From	To	Justification
18 Sep 2023	Political			
18 Sep 2023	Political	2.3 Elevated	2.0 Elevated	
	Government instability	1.5 Moderate	1.2 Moderate	President Lula' formal agreement with Center-right Centrao parties consolidate government coalition and secures majority in Congress.

Risk Scores

Overall	2.4	High	↗
Political	2.0	Elevated	↗
Government instability	1.2	Moderate	↗
Policy instability	2.5	High	↗
State failure	2.4	High	↗
Economic	2.0	Elevated	↘
Recession	3.7	Very High	↘
Inflation	2.7	High	↘
Currency depreciation	3.1	High	↘
Capital transfer	0.7	Low	→

S&P Global | Benefits of Big Data in TPRM

Leveraging Data-Driven Insights for Smarter Risk Management

Big data enhances Third-Party Risk Management (TPRM) by improving risk visibility, accelerating decision-making, and optimizing compliance and cost efficiency.

Key Benefits:

- Improved Risk Visibility: Real-time monitoring and alerts provide proactive risk identification.
- Timely Decision-Making: Automated risk scoring and AI-driven insights enable quicker, data-backed decisions.
- Compliance & Audit Readiness: Standardized, data-driven documentation ensures regulatory alignment and audit preparedness.
- Cost Efficiency: Reduces reliance on manual assessments, optimizing resources and lowering operational costs.
- Supply Chain Resilience: Predictive analytics help anticipate disruptions and strengthen third-party risk mitigation.

S&P Global | Risk of Over-Reliance on External Data and Vendor Scores

*“Everybody wants scores, but nobody uses them”**

While big data enhances Third-Party Risk Management (TPRM), overreliance on data and automated scoring can introduce challenges and risks that must be carefully managed.

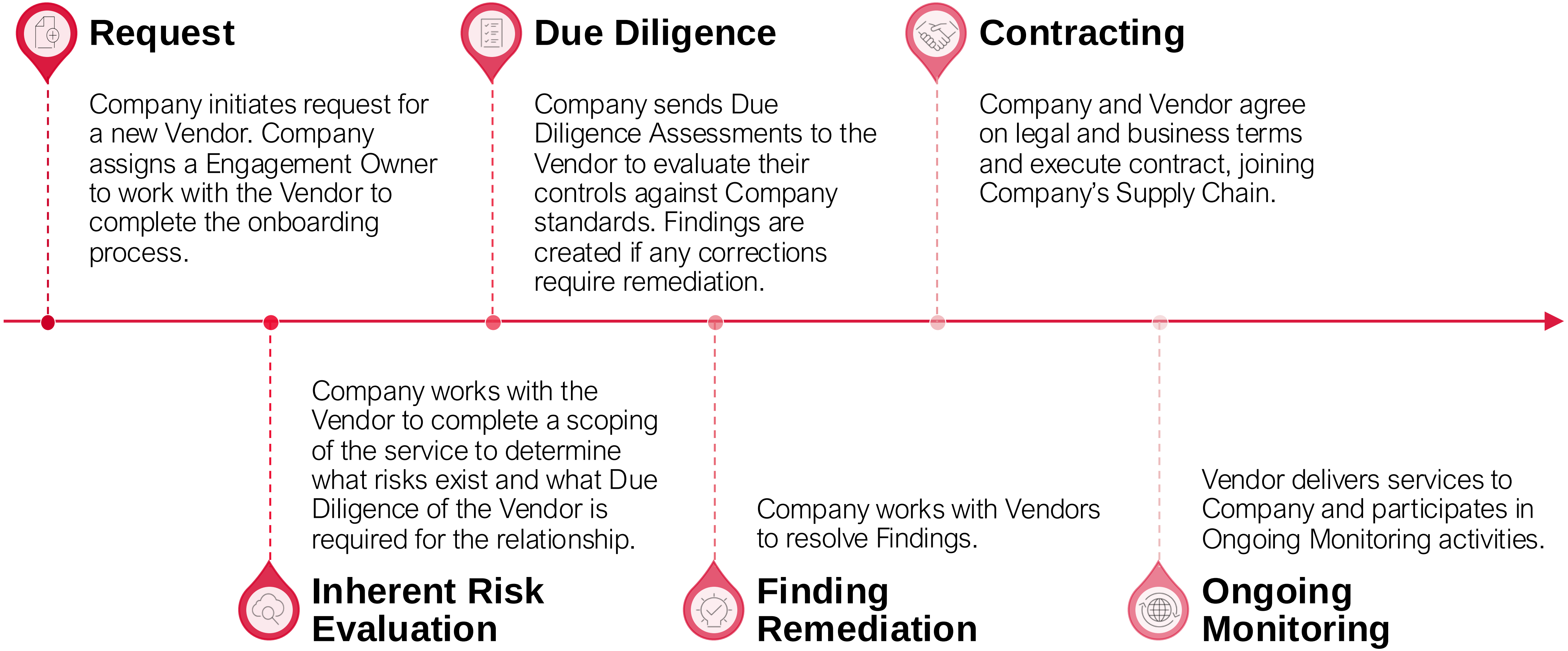
Key Risks:

- Data Quality Challenges: Not all sources are equally reliable, and outdated or incomplete data can skew assessments.
- Unclear Modeled vs. Validated Data: Relying on vendor-provided data without recognizing it may be modeled (not independently validated) can introduce blind spots and misinformed risk decisions.
- False Positives/Negatives: Algorithmic risk scoring isn’t always accurate, leading to misclassified risks.
- Regulatory Misalignment: Compliance expectations vary across jurisdictions, requiring tailored risk frameworks.
- Risk Decision Trade-Offs: Determining the right weight for each data source is critical to ensuring balanced, defensible decisions.

*Unknown philosopher at a recent conference

S&P Global | Case Study – Data-Driven TPRM in Action

Before



Request

Company initiates request for a new Vendor. Company assigns a Engagement Owner to work with the Vendor to complete the onboarding process.

Inherent Risk Evaluation

Company works with the Vendor to complete a scoping of the service to determine what risks exist and what Due Diligence of the Vendor is required for the relationship.

Due Diligence

Company sends Due Diligence Assessments to the Vendor to evaluate their controls against Company standards. Findings are created if any corrections require remediation.

Finding Remediation

Company works with Vendors to resolve Findings.

Contracting

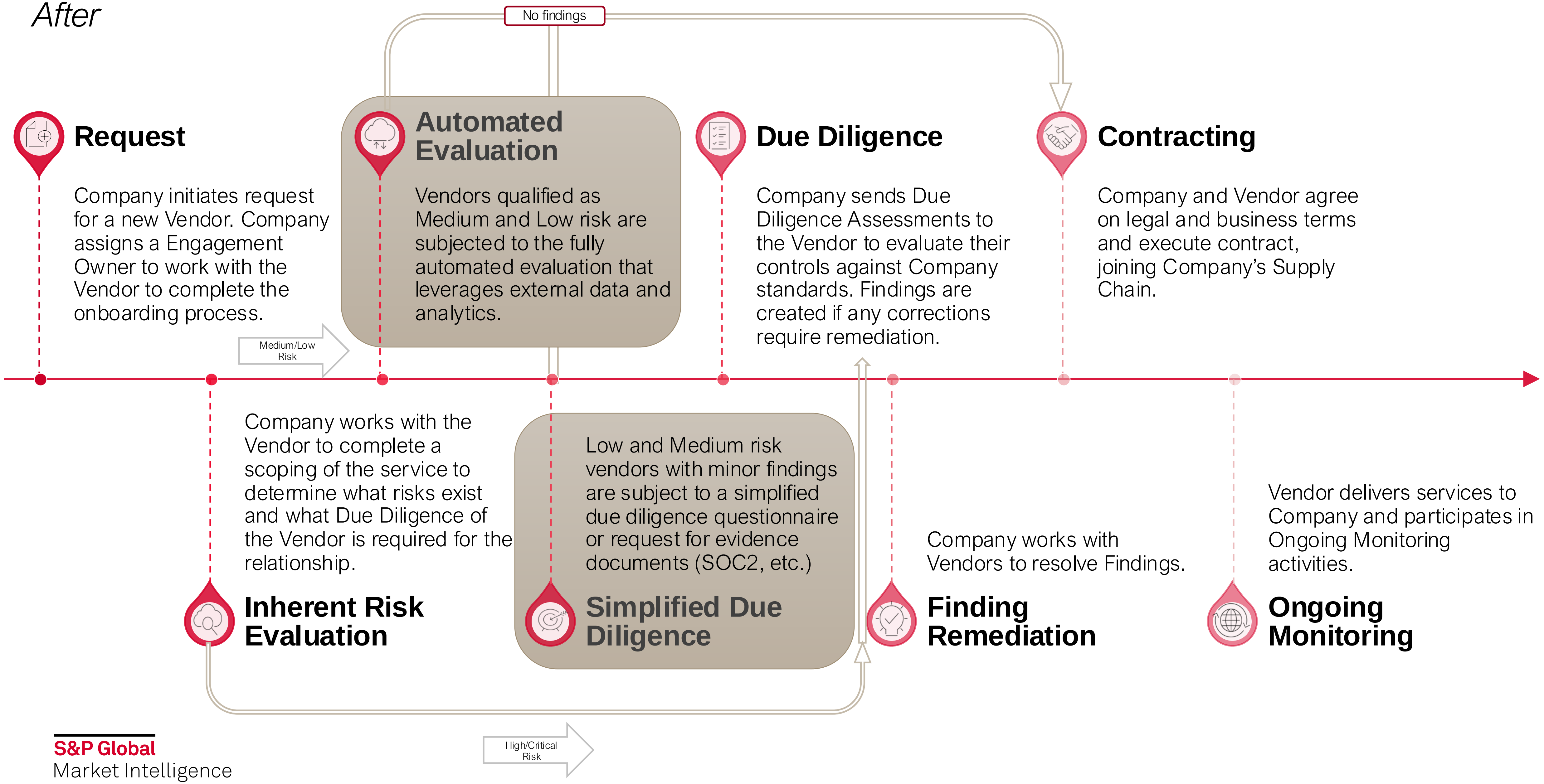
Company and Vendor agree on legal and business terms and execute contract, joining Company's Supply Chain.

Ongoing Monitoring

Vendor delivers services to Company and participates in Ongoing Monitoring activities.

S&P Global | Case Study – Data-Driven TPRM in Action

After



Request

Company initiates request for a new Vendor. Company assigns a Engagement Owner to work with the Vendor to complete the onboarding process.

Inherent Risk Evaluation

Company works with the Vendor to complete a scoping of the service to determine what risks exist and what Due Diligence of the Vendor is required for the relationship.

Automated Evaluation

Vendors qualified as Medium and Low risk are subjected to the fully automated evaluation that leverages external data and analytics.

Simplified Due Diligence

Low and Medium risk vendors with minor findings are subject to a simplified due diligence questionnaire or request for evidence documents (SOC2, etc.)

Due Diligence

Company sends Due Diligence Assessments to the Vendor to evaluate their controls against Company standards. Findings are created if any corrections require remediation.

Finding Remediation

Company works with Vendors to resolve Findings.

Contracting

Company and Vendor agree on legal and business terms and execute contract, joining Company's Supply Chain.

Ongoing Monitoring

Vendor delivers services to Company and participates in Ongoing Monitoring activities.

S&P Global
Market Intelligence

Real-Life Applicability for External Data Usage

💬 *“We get the data, but how do we know when it’s enough to skip a full assessment?”*

💬 *“I trust continuous monitoring for alerts, but how do I turn that into a decision?”*

💬 *“I have a SOC 2, a DDQ, and a risk rating—but how do I justify that is enough to onboard this vendor.”*

💬 *“Leadership wants faster onboarding, but I don’t want to cut corners on due diligence.”*

💬 *“We’ve invested in external data, but it’s hard to show how it reduces our effort.”*

S&P Global | Best Practices for Using External Data in your Assurance Program

Maximizing Data-Driven Insights for Effective Risk Management

Define data reliability levels

- Weigh internal vs. external sources (e.g., self-assessments vs. independent audits)

Develop a Data Reliance Framework

- How much trust to place on each data type?

Combine human judgment with AI-driven insights

- Automated scoring should inform, not replace, expert analysis

Establish governance for risk-based decisions

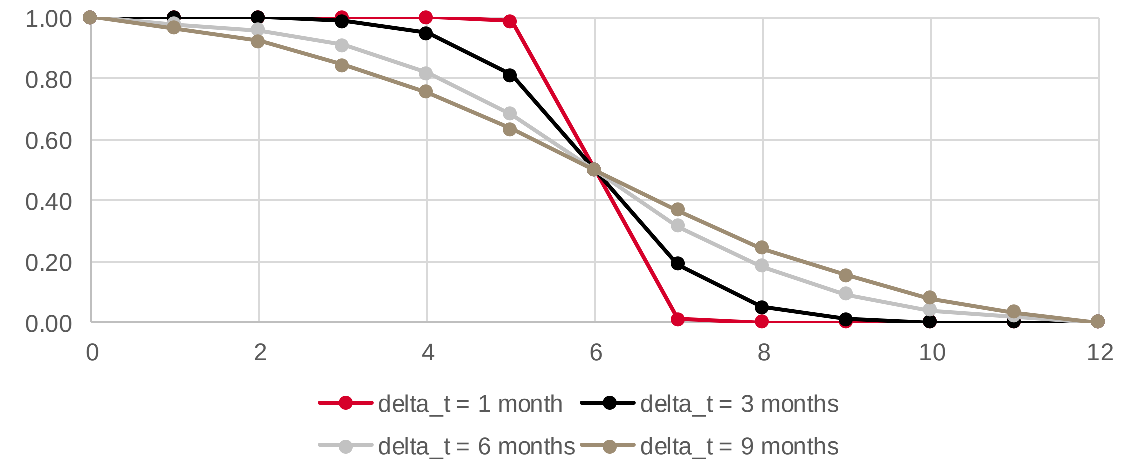
- Ensure transparency in risk calculations

Score Adjustments: Handling quality, conflicts, and timeliness of data

Source Confidence: Impact of 4th party data, positive vs. negative modifiers

Scope Consistency: Example: Aligning audit reports and network scans (Apples vs. Oranges)

Example: Assigning and scaling information value between [0,1] $t = 0$ & $t = max$ based on timeliness



S&P Global | Best Practices for Using External Data in your Assurance Program

Understanding Data Shelf Life: Ensuring Timely & Reliable Insights

Analogy

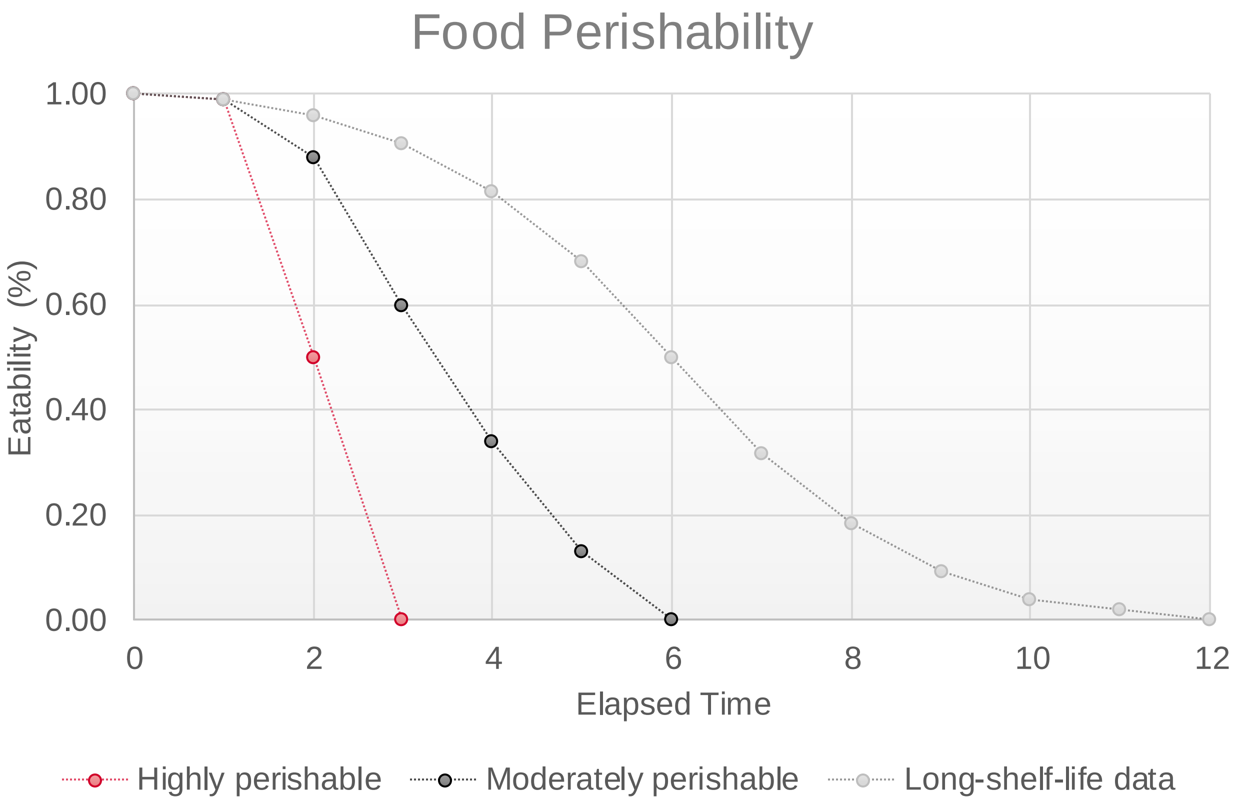
Just like different supermarket products have varying expiration dates, different types of supplier assurance data have different 'shelf lives' when it comes to usefulness and reliability.

Variables

❖ Highly perishable (dairy, fruits) → Needs immediate use (e.g., real-time risk scores, cyber alerts).

❖ Moderately perishable (bread, eggs) → Requires periodic validation (e.g., compliance checks, operational metrics).

❖ Long shelf life (canned goods, pasta) → Stays valid longer - needs occasional review (e.g., P&P, foundational risk assessments).



S&P Global | Best Practices for Using External Data in your Assurance Program

Step 1: Mapping Data Sources to Internal Requirements

Objective:

Organizations must align third-party risk data sources with their internal risk assessment frameworks. This ensures that each data type contributes appropriately to risk evaluations, enabling better decision-making.

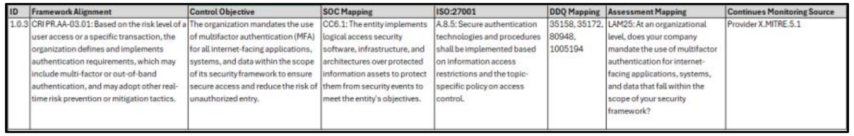
Consider:

- Assess Internal Expertise – Do we have the skills and resources to map third-party data to our risk framework?
- Evaluate Vendor Mapping – Has the data provider already mapped sources to key risk categories, or do we need to do it?
- Validate Accuracy & Fit – Does the mapped data align with our internal assessment methodology and risk priorities?

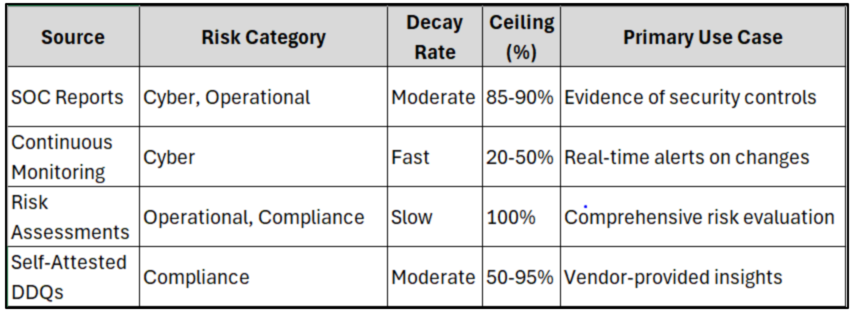
Steps

- ❖ Identify Key Risk Categories and Map Data Sources to internal TPRM Requirements:
  - ❖ Cybersecurity Risk (SOC Reports, Continuous Monitoring)
  - ❖ Operational Risk (Assessments, Incident Reports)
  - ❖ Regulatory Compliance (DDQs, Audit Findings)
- ❖ Define Internal Requirements & Weightings
  - ❖ Set decay rates for each data source based on frequency and relevance.
  - ❖ Assign ceilings (maximum contribution) to ensure balance.

Example



ID	Framework Alignment	Control Objective	SOC Mapping	ISO:27001	DDQ Mapping	Assessment Mapping	Continues Monitoring Source
1.0.3	CRI PR.AA-03.01: Based on the risk level of a user access or a specific transaction, the organization defines and implements authentication requirements, which may include multi-factor or out-of-band authentication, and may adopt other real-time risk prevention or mitigation tactics.	The organization mandates the use of multifactor authentication (MFA) for all internet-facing applications, systems, and data within the scope of its security framework to ensure secure access and reduce the risk of unauthorized entry.	CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A.8.5: Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	35158, 35172, 80948, 1005194	LAM25: At an organizational level, does your company mandate the use of multifactor authentication for internet-facing applications, systems, and data that fall within the scope of your security framework?	Provider X.MITRE.5.1



Source	Risk Category	Decay Rate	Ceiling (%)	Primary Use Case
SOC Reports	Cyber, Operational	Moderate	85-90%	Evidence of security controls
Continuous Monitoring	Cyber	Fast	20-50%	Real-time alerts on changes
Risk Assessments	Operational, Compliance	Slow	100%	Comprehensive risk evaluation
Self-Attested DDQs	Compliance	Moderate	50-95%	Vendor-provided insights

S&P Global | Best Practices for Using External Data in your Assurance Program

Step 2: Mapping Data Sources to Internal Requirements (Ex: SOC Report) -- Sigmoidal Model

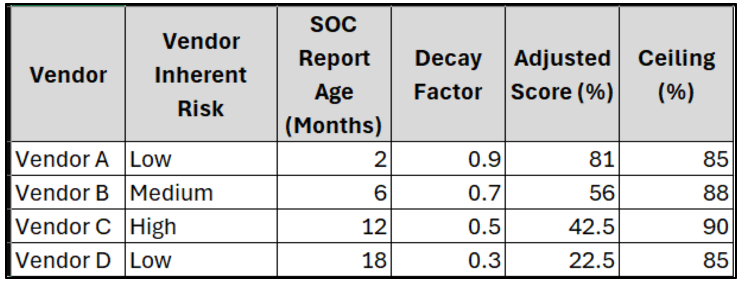
Objective:

Analyze SOC reports from multiple suppliers to assess their reliability over time.

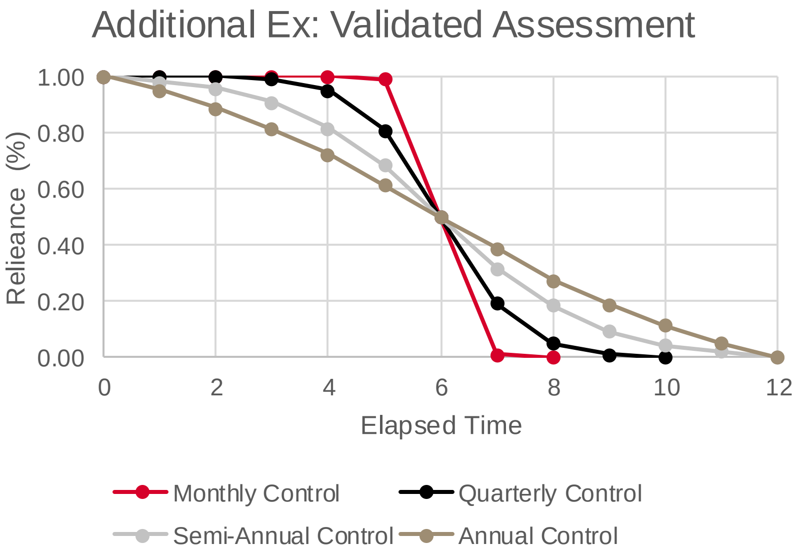
Note: This approach can be applied to any data source mapped in Step 1.

Steps

- ❖ SOC reports degrade in influence as they age.
- ❖ Apply logistic decay function to adjust scores.
- ❖ Compare age-based adjusted scores.



Vendor	Vendor Inherent Risk	SOC Report Age (Months)	Decay Factor	Adjusted Score (%)	Ceiling (%)
Vendor A	Low	2	0.9	81	85
Vendor B	Medium	6	0.7	56	88
Vendor C	High	12	0.5	42.5	90
Vendor D	Low	18	0.3	22.5	85



Key Insights

- ❖ Inherent risk determines the SOC Report ceiling (%):
  - ❖ Low Risk vendors are capped at 85% reliance.
  - ❖ Medium Risk vendors at 88%.
  - ❖ High Risk vendors at 90%.
- ❖ Recent SOC reports (2-6 months) retain significant weight.
- ❖ Older reports (12+ months) contribute far less to risk assessment.
- ❖ Using decay-adjusted scoring ensures reliance on fresh, relevant data.

$$f(x) = \frac{1}{1 + e^{-x}}$$

S&P Global | Best Practices for Using External Data in your Assurance Program

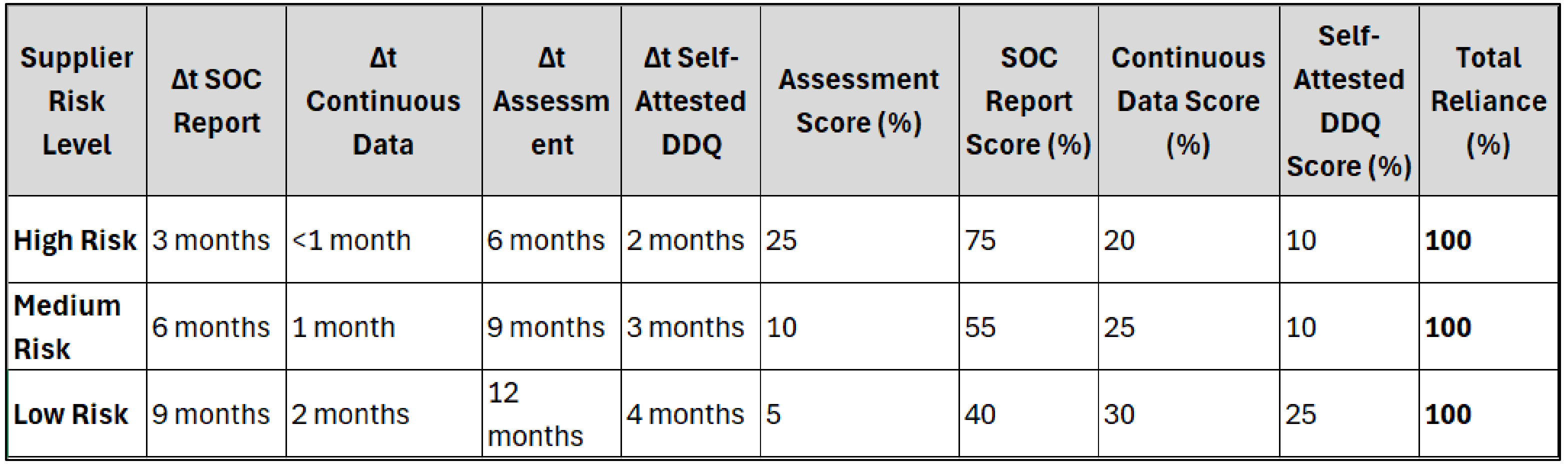
Scenario 1: All Risk Levels Reach Theoretical 100% Reliance

Objective:

To demonstrate how risk level affects total reliance score and how reliance shifts across data sources.

Key Takeaways

- ❖ All risk levels can reach a theoretical 100% reliance when data is well-distributed across sources. SME judgement should be a "tie-breaker"
- ❖ High Risk suppliers depend more on SOC reports & assessments.
- ❖ Low Risk suppliers rely more on continuous data & DDQs.



Supplier Risk Level	Δt SOC Report	Δt Continuous Data	Δt Assessment	Δt Self-Attested DDQ	Assessment Score (%)	SOC Report Score (%)	Continuous Data Score (%)	Self-Attested DDQ Score (%)	Total Reliance (%)
High Risk	3 months	<1 month	6 months	2 months	25	75	20	10	**100**
Medium Risk	6 months	1 month	9 months	3 months	10	55	25	10	**100**
Low Risk	9 months	2 months	12 months	4 months	5	40	30	25	**100**

S&P Global | Best Practices for Using External Data in your Assurance Program

Scenario 2: Exceeding and Falling Short of Reliance Thresholds

Objective:

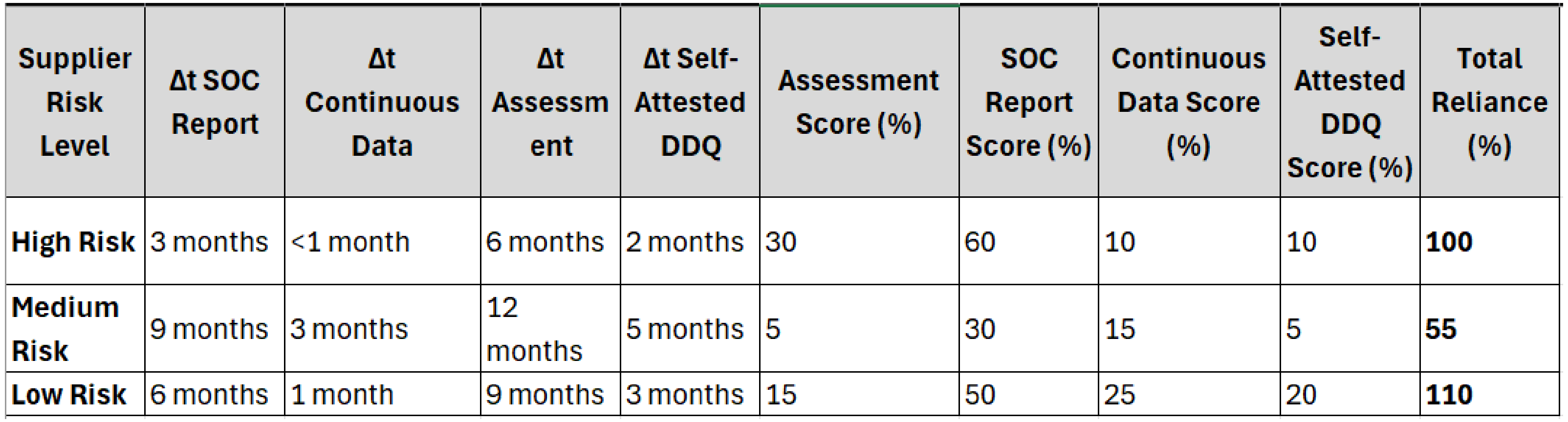
To demonstrate how risk level affects total reliance score and how reliance shifts across data sources.

Key Takeaways

❖ Low Risk supplier exceeds theoretical 100% reliance (110%) due to strong continuous data and DDQ scores. Consider reducing effort.

❖ High Risk supplier remains at theoretical 100%, with balanced reliance on SOC reports and assessments.

❖ Medium Risk supplier falls short at 55%, as older SOC reports and assessments reduce its weight. Direct due diligence may be necessary.



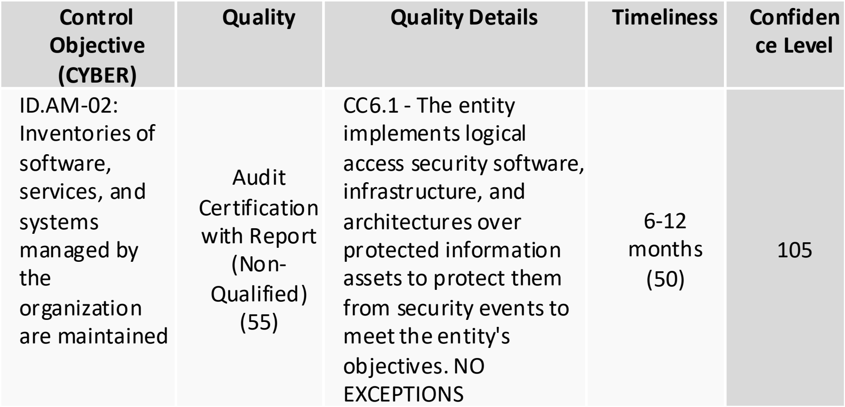
Supplier Risk Level	Δt SOC Report	Δt Continuous Data	Δt Assessment	Δt Self-Attested DDQ	Assessment Score (%)	SOC Report Score (%)	Continuous Data Score (%)	Self-Attested DDQ Score (%)	Total Reliance (%)
High Risk	3 months	<1 month	6 months	2 months	30	60	10	10	**100**
Medium Risk	9 months	3 months	12 months	5 months	5	30	15	5	**55**
Low Risk	6 months	1 month	9 months	3 months	15	50	25	20	**110**

S&P Global | Best Practices for Using External Data in your Assurance Program

Control Level Example

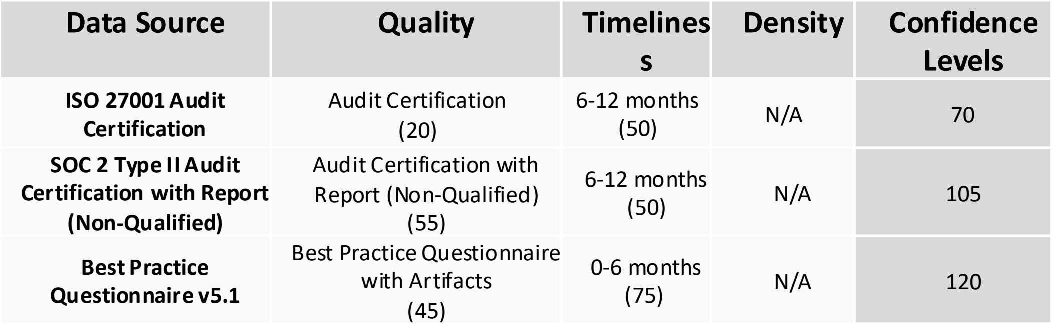
Composite “Scoring”: ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained

1 Map Sources to Control



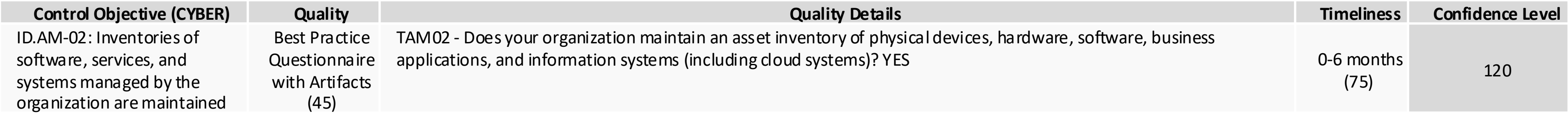
Control Objective (CYBER)	Quality	Quality Details	Timeliness	Confidence Level
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	Audit Certification with Report (Non-Qualified) (55)	CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. NO EXCEPTIONS	6-12 months (50)	105

2 Determine Confidence Levels of Data Sources



Data Source	Quality	Timelines s	Density	Confidence Levels
ISO 27001 Audit Certification	Audit Certification (20)	6-12 months (50)	N/A	70
SOC 2 Type II Audit Certification with Report (Non-Qualified)	Audit Certification with Report (Non-Qualified) (55)	6-12 months (50)	N/A	105
Best Practice Questionnaire v5.1	Best Practice Questionnaire with Artifacts (45)	0-6 months (75)	N/A	120

3 Determine Confidence Level at the Control Level



Control Objective (CYBER)	Quality	Quality Details	Timeliness	Confidence Level
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	Best Practice Questionnaire with Artifacts (45)	TAM02 - Does your organization maintain an asset inventory of physical devices, hardware, software, business applications, and information systems (including cloud systems)? YES	0-6 months (75)	120

S&P Global | Key Takeaways

- Big data is a powerful tool, but risk decisions must be strategic
- Best practice: Use a mix of internal, external, and independent sources
- Avoid over-reliance on automated scores—human oversight is key
- Build a structured framework for weighing data in risk decisions

Thank you