Chaperoning Third-Parties to the Prom

Demystifying third-party risk management in a world of possible suitors

August 5, 2025

Amy Feldman

Get to know me!

Geography

Charleston, South Carolina

Background

I am cybersecurity professional with over 12 years of experience helping clients assess and build their cybersecurity programs.

I am passionate about third-party risk management and serve as RSM's third-party risk management leader for Risk consulting. I help clients evaluate their third-party risk management programs, taking a broad lens to the program to evaluate the end-to-end relationship lifecycle & consider multiple areas of risk. I help our clients build mature and scalable third-party risk management programs, specializing in policy & procedure development, risk identification and mitigation techniques, and technology enablement.

Credentials

CTPRA, CISSP, PMP

Learning objectives

- Define high-level third-party risk management principles in line with industry leading practices
- Recap third-party related risks and trends from the last year
- Adequately prepare your third-party risk management programs to reduce risks from your external third-party partners

Let’s talk about your TPRM program

RSM

According to Gartner, Inc.[1], third-party risk management is one of the **most pressing challenges** for **compliance leaders**. Organizations are increasingly dependent on third-parties to do business, provide goods and services, & improve operational efficiency. However, **only 16%** of organizations say they effectively manage third-party risks, & only **28%** of organizations continuously monitor third-parties throughout the engagement lifecycle.

[1](2022). Third Party Risk Management Governance and Technology Investments: A Gartner Trend Insight Report. *Gartner, Inc.* https://doi.org/2/10/2022

RSM

Third-parties in healthcare

Medical equipment

Claims processing

Medical billing & coding

Pharmacy Benefit Managers

Customer service

Medication distribution

Telehealth

IT support

EHR Management

Diagnostic services

Cybersecurity tools

Implicit trust

(noun, adjective)

Inherent trust placed in vendors until proven otherwise, often providing levels of access to critical systems and processes outside of normal controls.

Exploring the risks of third-party relationships

Holistic risk management principles are critical to reducing risks associated with third-party relationships.

Operational risk

Vendor failure to meet service level agreements (SLAs) can lead to operational downtime and reduced service quality.

Failure to meet production timelines could result in delays or decreased product quality.

Cybersecurity risk

Poor data handling hygiene may lead to unauthorized access, or data loss of ePHI, incurring regulatory penalties and financial costs.

Inappropriate vendor access to IT systems increases the risk of insider threats, data theft, or operational sabotage.

Financial risk

Vendor's financial instability may disrupt services or necessitate costly alternatives, affecting the organization's operations and budgets.

A vendor's failure to perform could lead to unbudgeted replacement needs.

Strategic risk

Dependence on a few critical vendors heightens the potential impact of any single vendor's failure (concentration risk).

Ignoring joint ventures or affiliates could lead to misalignment of strategic goals or alignment to shared policies.

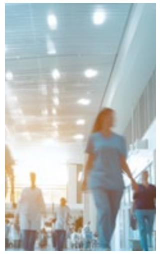
Reputational risk

A data breach at a third-party provider could leak company or customer data.

Statements or posts on social media from your third-party providers could present backlash from customers as the public could associate the vendor with your organization.

Risks in real time

What did we see in 2024?



Change Healthcare

February 2024

- Responsible for between 1/3 –1/2 of all US health transactions
- Prescription backlogs, inability to process claims, bill patients, or receive payments
- Up to $100M/a day in lost revenue for some providers

CrowdStrike

July 2024

- Botched software update
- Affected millions of Windows based systems
- Estimated cost for Fortune 500 Companies $5.4 billion

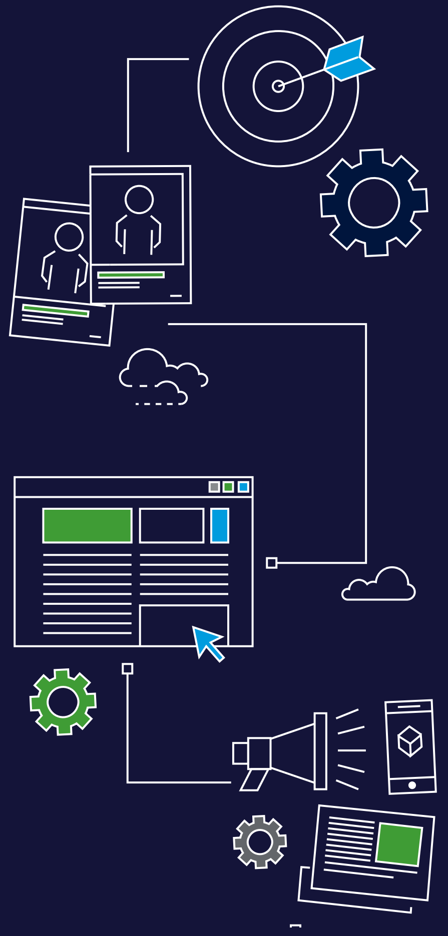
Ascension

May 2024 - Ransomware

- EHR systems down in 14 states

December 2024 - Vulnerability exploited in third-party software

- 437,329 patient records affected, but no breach of systems.



Emerging trends in 2025

We are keeping a close eye on these trends impacting third-party risk management this year.

TPRM Ownership

Demands for operational resiliency

Changes in administration

"nth" party management

Automation and AI

Evolution to continuous monitoring

Demystifying third-party risk management

The “prom” lifecycle…

An effective TPRM program includes the following components:

Planning

- Find a prom date!

Due diligence

- Make sure your prom outfit fits
- Do you like your prom date’s friends?

Contracting

- Buy your prom tickets and make a dinner reservation

Ongoing monitoring

- Attend the prom
- Plan for an after prom party

Termination

- Remain friends (or not) with your prom date

Governance: Decide if you're going alone, or in a group

Building and maintaining a third-party risk management program requires defined risk ownership and roles and responsibilities. The following risk management governance models set risk posture, program goals and objectives, and management/board reporting requirements.

Functional model (Decentralized)

Individual functions are responsible for specific risk identification. There is some visibility between functions, but little central enterprise visibility.

Federated model

There is a centralized oversight of third-party risk activities, with distributed or functional risk identification.

Centralized model

Centralized oversight of third-party risks and centralized risk identification. There is little regular involvement from functions or business units.

Enterprise Risk Management (ERM) reporting ⟷ **Governance. Risk management and Compliance (GRC) objectives**

Sourcing
- Ethical Social, Governance (ESG)
- Strategic Initiative Prioritization
- Strategic Sourcing Performance Monitoring

Procurement
- Tactical Sourcing
- Spend Management/ rebates
- Contract Execution

Contract management
- Service agreements standards
- Contract management
- Golbal compliance

Project Management	Accounting/ Finance	Vendor Relationship Owners (VRO)	IT Asset Management (ITAM)	Legal	Information Security	IT Service Delivery	Regulatory/ Compliance	Human Resource (Contactors))

Governance model

Risk Takers
Management
1st Line

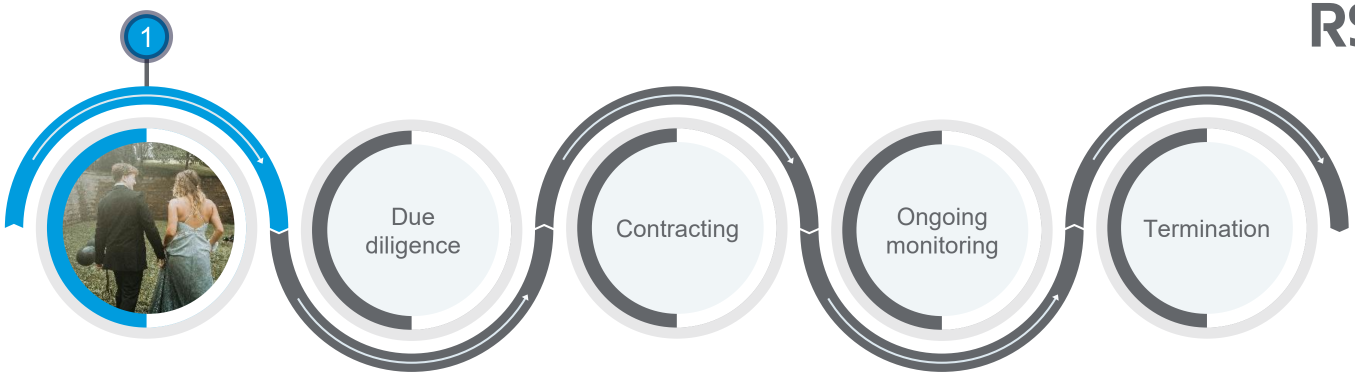
Risk Monitors
Compliance
2nd Line

Risk Assurers
IA
3rd Line

Operations | **Support** | **Oversight** | **Assurance**

Third-Party Risk Management Toolset

- AP SOPs / Controls
- Defined & Monitored KPIs & KRIs
- Policy Audits
- Delegation of Authority
- Contract Management Tool
- ESG Strategy
- Procurement Audit
- Third-Party Inventory
- Contract Reviews
- Security & Control Questionnaire
- AP Audit
- Procurement Policy
- Business Continuity & Disaster Recovery Policy
- TPRM Audit
- Risk Management Committee
- ESG Audit
- Conflicts of Interest Policy
- Third-Party Risk Management Policy
- Code of Ethics
- Enterprise Risk Management Policy



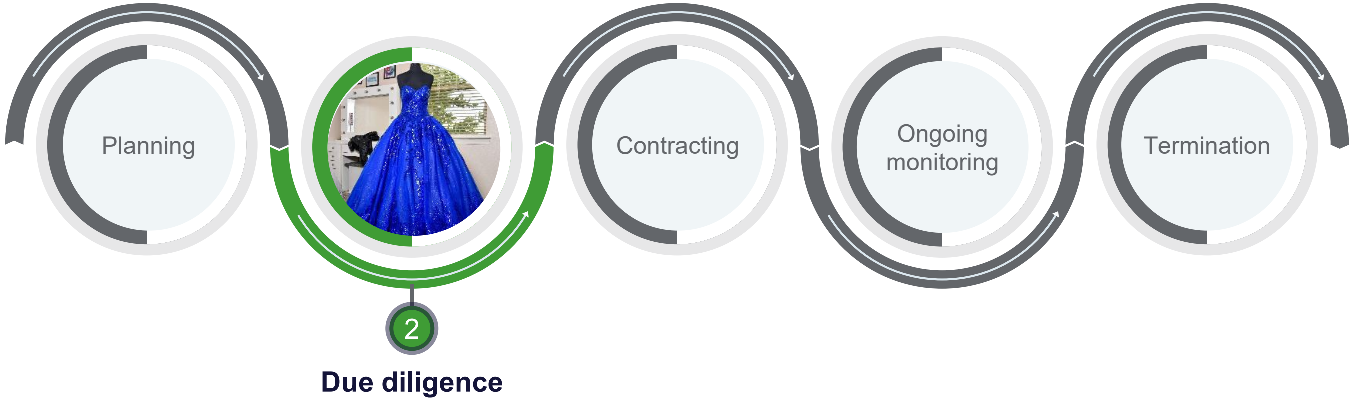
Step 1: Find a prom date

Shop the service to understand the competitive landscape of the product/offering and ensure you are receiving a fair price for services, and evaluate features across suppliers/products.

Analyze whether an existing vendor is already providing similar services?

Evaluate and tier vendors based on inherent risk
- Supporting critical business processes/activities.
- Access to critical data sets
- Spend

Step 2: Make sure your outfit fits



Assess individual third parties

- Risk types
- Questionnaires
- Evidence (Trust but verify)
- Evaluate third-party attestations (i.e. SOC 2, HITRUST, ISO, PCI, etc.)

Document risks and identify any items for remediation or tracking

Assign residual risk score

Collaborate with other stakeholders

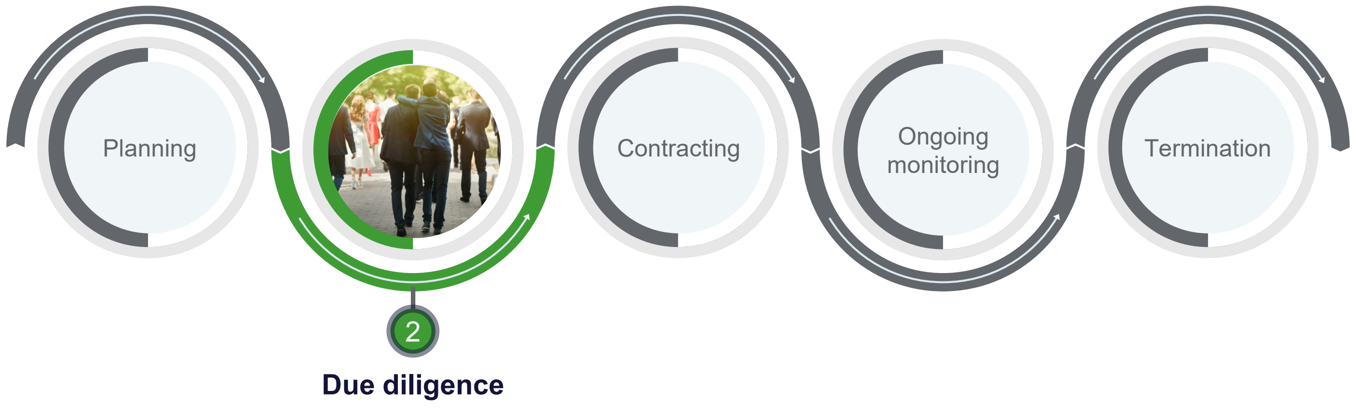
Step 2 (cont.): Do you like your date's friends?

Understanding your supplier ecosystem, and monitoring "nth" dependencies, is becoming increasingly more important as organizations are outsourcing now more than ever.

Third Party
Vendors, suppliers, and relationships you have directly contracted with.
Ex: Your Software as a Service (SaaS provider)

Fourth Party (nth party)
A supplier that your supplier is dependent on to deliver a service or product to you. Your third-party supplier has a direct contract with them, but you do not.
Ex: Your SaaS provider's cloud supplier.

RSM



Managing "Nth" Party Risks

Follow these steps to better manage your supplier ecosystem.

1. Create an Inventory

- Ask your third parties to identify fourth parties they depend on to provide your services.
- Start with critical and high-risk suppliers.
- Document within your supplier inventory.

2. Understand Access

- Will the fourth party have access to your data, systems or network?
- Will the fourth party have physical access to your building/offices?
- Will the fourth party interface with your customers?

3. Address Concentration Risk

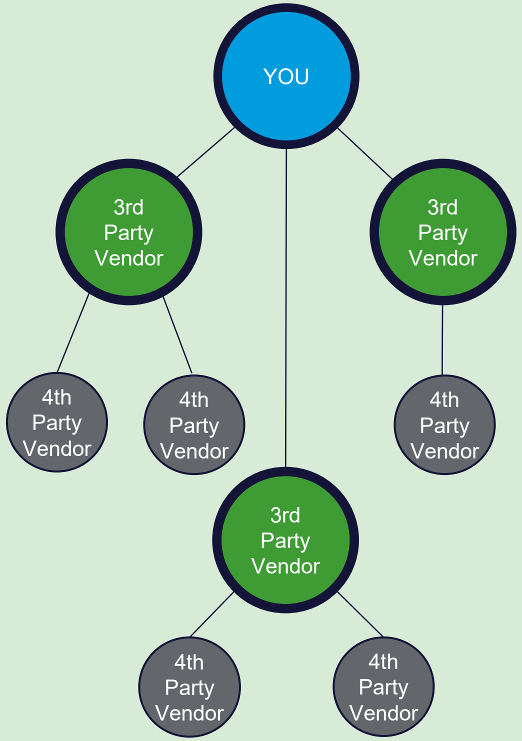
Analyze fourth parties to evaluate for concentration risks:

- Same fourth party
- Similar geographic areas
- Operational reliance

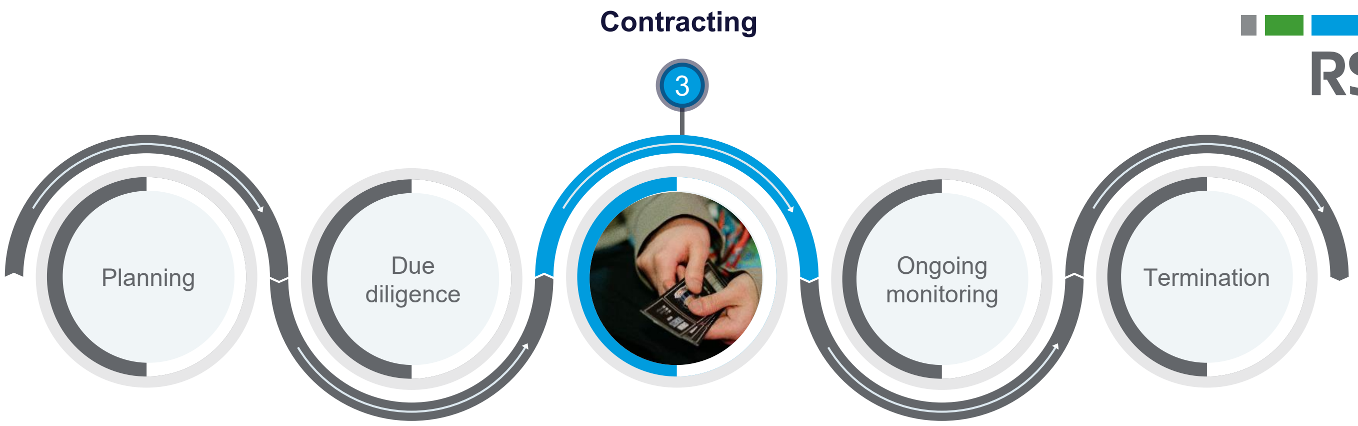
4. Understand how your suppliers manage their suppliers

Understand how your suppliers manage *their* suppliers

Note: The goal is not to evaluate the maturity of their TPRM program, but to ensure proper due diligence was completed on critical fourth party suppliers.



Step 3: Buy your prom tickets and make a reservation



- Ensure a formal contract is prepared and properly reviewed by legal against a standard set of requirements. (i.e Right to audit clause, notification of outsourcing or subcontractors, requirements for destruction or return of data, termination terms, SLAs/KPIs, etc.)
- Require a Business Associate Agreement (BAA) be executed. This should include the permitted and required uses and disclosures of PHI by the business associate.
- Maintain contracts in a central repository & ensure appropriate people are aware of terms & requirements.

Step 4: Attend prom…and did someone say after prom??

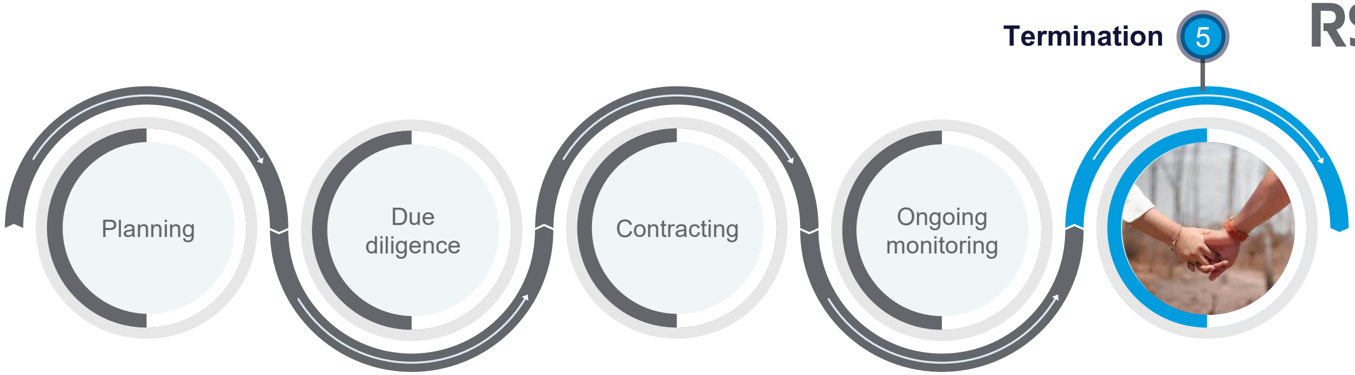
Attend the prom

- Implement repeatable onboarding procedures to ensure vendors are receiving proper training in alignment with your organization’s policies (security awareness, regulatory & compliance, role-based access training, etc.)
- Ensure proper access is granted and managed.

Plan for an after-prom party

- Report out and up
- Review long-term contracts to ensure contractual provisions are still appropriate and don’t need to be reevaluated
- Evaluate the vendor’s performance against SLAs and KPIs
- Enact the right to audit clause.
- Implement tools for ongoing monitoring

Step 5: Remain friends… or not



Track renewals or identify the appropriate time to exit the relationship.

Plan third-party relationship succession.

Create a termination checklist
- Deprovision access
- Proof of data destruction
- Invoice reconciliation
- Return hardware

Why do TPRM programs fail?

01 Lack of ownership and cohesive risk management strategy (alignment to ERM).

02 Ignoring vendors with smaller spend.

03 Failure to align with resilience efforts and protecting core business processes.

04 Lack of risk classification tiering to prioritize risk management strategies.

05 Inconsistent follow up with vendors, resulting in incomplete assessments or lack of remediation.

06 Insufficient or outdated contractual terms.

07 Lack of performance monitoring and SLA management.

08 Reliance on point in time assessments rather than continuous monitoring.

09 Improper termination of third-party access.

10 Failure to use technology, resulting in manual processes.

Looking at your program on a maturity scale

Just as prom dates are not one size fits all, neither are TPRM programs.

Weak

- Ad-hoc processes
- Problem driven
- Inconsistent outcomes
- Rework
- Reactive
- Individual effort

Sustainable

- Basic process
- Processes follow a regular pattern
- Repeatable practices
- Reduced rework
- Processes not standardized

Mature

- Documented processes
- Standard approval processes
- Proactive and reactive
- Request driven
- Technology utilized
- Improve productivity

Integrated

- Stable processes
- Proactive
- Accountable
- Effective monitoring
- Formal change management process
- Service level agreements
- Continuous improvement
- Strong business relationships
- Predictability
- Quality driven

Advanced

- Proactive
- Optimizing costs and quality
- Agile
- Fully automated
- Complete integration
- Enterprise-wide knowledge
- Planned innovations
- Change management fully implemented
- Strategic performance metrics

You can outsource services, but you can’t outsource the risk.

Appendix

RSM

RSM capabilities and expertise

Program evaluation
Ensuring alignment to regulatory requirements, internal policy, and/or Leading practices.

Design, build, & optimize
Developing repeatable and scalable programs with automation and efficiencies.

Managed services
Aligning your risk appetite with a turnkey solution for managed success.

Capabilities

Maturity assessment
Assess the maturity of your program's controls across the third-party risk management lifecycle.

Policy & procedure development
Build foundational program-level documentation to ensure repeatability and scalability.

Vendor risk assessments
Expertise and resources to complete vendor risk assessments.

Program audit
Evaluate the design and operating effectiveness of the third-party risk management program across the engagement lifecycle.

Technology enablement
Subject matter expertise to help you select or implement a new third-party risk management tool.

Managed program
A turnkey solution to ensure successful completion of third-party risk analysis.

<<<Full Program Development & Customizable Services Are Available>>>

Third-party risk management experience

RSM

Did you know?

270+
Certified professionals to help ensure subject matter expertise during vendor risk analysis.

TPRA
THIRD PARTY RISK ASSOCIATION

Preferred assessor for
Microsoft
Supplier Security and Privacy Assurance third-party validations.

Microsoft

RSM professionals hold **Certified Third Party Risk Assessor (CTPRA)** credentials.

Our third-party risk management practice

- Delivers custom-tailored solutions that empower our clients to operate more efficiently
- Combines broad business insight with industry knowledge
- Aligns with regulatory requirements for managing third-party risks within the healthcare industry (i.e., HIPAA, HITRUST, etc.)
- Keeps clients informed through white papers and insight articles
- Hosts conferences, webcasts and roundtables with your industry peers
- Contributes to thought leadership and industry forums to the Third-Party Risk Association as an active professional member
- Has strong relationships with various technology providers specializing in third-party risk management tools

When seeking a professional services provider, organizations deserve to work with a firm that knows how to address your unique challenges.

We have helped many organizations mature their third-party risk management programs in alignment with industry standards & compliance requirements.

Our proven track record of success includes:

- Developing vendor management procedures for an organization that integrates stakeholders across a complex organizational chart and evaluates a breadth of risk variables across the relationship lifecycle.
- Auditing hundreds of third-party risk management programs, including the procure to pay process, contract compliance and IT due diligence.
- Providing co-sourced due diligence assistance for many organizations, reviewing vendor assessments and supporting evidence (i.e. SOC reports, penetration testing, etc.), to provide risk-based decisions.

Amy Feldman

216.927.8236

Amy.feldman@rsmus.com

www.linkedin.com/in/amybfeldmanTPRM

RSM

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING