TPRM | Looking Beyond The Handshake

Anticipating Vendor Risks Before They Strike

Webinar by PwC Netherlands
3 March 2026

Agenda

1 **Introduction** – *What is Third-Party Risk Management and why now?*

2 **Cyber & Business Perspective** – IT Landscape, Dependencies and Risks

3 **Legal & Regulatory Perspective** – What is the minimum you need to have in order?

4 **Auditor's expectations and TPRM Operating Models** – How to organise

5 **Wrapping Up & Q&A**

Welcome & Introduction
Insight and control over risks in your chain.

Casper Ruizendaal

Risk
casper.ruizendaal@pwc.com

Lean Besseling

Compliance
lean.besseling@pwc.com

Peter Avamale

Cyber Risk
peter.avamale@pwc.com

Ilse van Wendel de Joode

Legal
ilse.van.wendel.de.joode@pwc.com

Ariana Lopez

Risk
ariana.lopez@pwc.com

- You can ask your questions directly via the chat function
- For other questions, please contact your PwC adviser
- Webcast and presentation will be made available afterwards
- Evaluation form afterwards

1

Introduction – What is Third-Party Risk Management and why now?

The urgency for sound third party risk management (TPRM) in an ever more complex and volatile world is increasing…

The Guardian

Stock markets stumble as global trade faces more Trump tariff uncertainty

FINANCIAL TIMES

ME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HOW TO SPEND IT

Aggressive reshoring of supply chains risks significant GDP loss, warns OECD

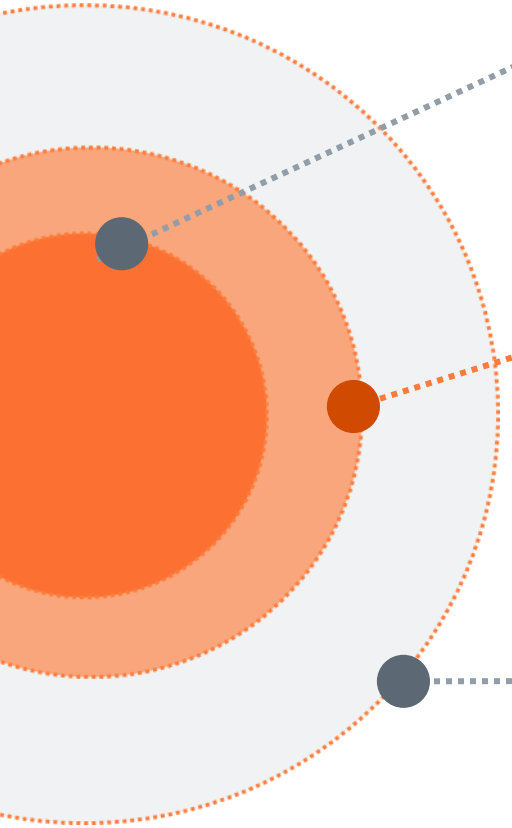
- Armed conflict
- Trade friction
- Supply chain disruptions
- Political uncertainty
- Cyber incidents
- Fracturing world

- Executive liability

38% of Dutch CEOs
believe they are highly or extremely exposed to the threat of geopolitical conflict in the next 12-months

Q: How exposed do you believe your company will be to the following key threats in the next 12 months? (Only highly or extremely exposed)

… Amidst all turmoil, effective TPRM has moved beyond contract control into ongoing management of third-party relationships



Sphere of Control

The organisation can directly act and has relatively the most options to do so, but is also closest to impact

Sphere of Influence

The ecosystem around the organisation, i.e. where there are still direct ties to the firm itself and a measure of influence can be exerted, depending on relations, positions, and agreements

Sphere of Concern

Macro-developments that an organisation has no control or influence over in any way. Acting can still be proactive, e.g. in scenario preparation.

Influence (?)

- **Financial Risks**
- **Regulatory Compliance Risks**
- **Concentration Risk**
- **Business continuity Risk**
- **Geopolitical Risk**

State of play: where are organisations in their TPRM journey?

Key survey data on TPRM

75% Of surveyed organisations indicate to not have a **single inventory** of all their third parties

83% Of surveyed organisations does not conduct **ongoing due diligence** on third parties

69% Of surveyed organisations does not manage for concentration risks

Data on third parties

150 - 250 Estimate of **legally required data points** for an EU financial institution

70 - 150 Estimate of **legally required data points** for non-financials

TPRM Challenges

- Know-how of set-up and application
- Resources
- Establishing scale, speed, change
- Establishing regulatory requirements
- Commitment and enterprise buy-in

2

Cyber & Business Perspective – IT Landscape, Dependencies and Risks

Supply chain cybersecurity incidents are on the rise..

50-60%

of organisations report having experienced a security or data incident caused by a third-party in the recent 12-24 months*

30%

of data breaches now involve a third-party, a 100% increase from the 15% reported previously*

€ 4.15 million

In 2024-2025, Supply chain compromise surged to become the second most prevalent attack vector (15%), and second costliest (EUR 4.15 million)**

*TPRM Global Forecast **IBM Cost of Breach Report

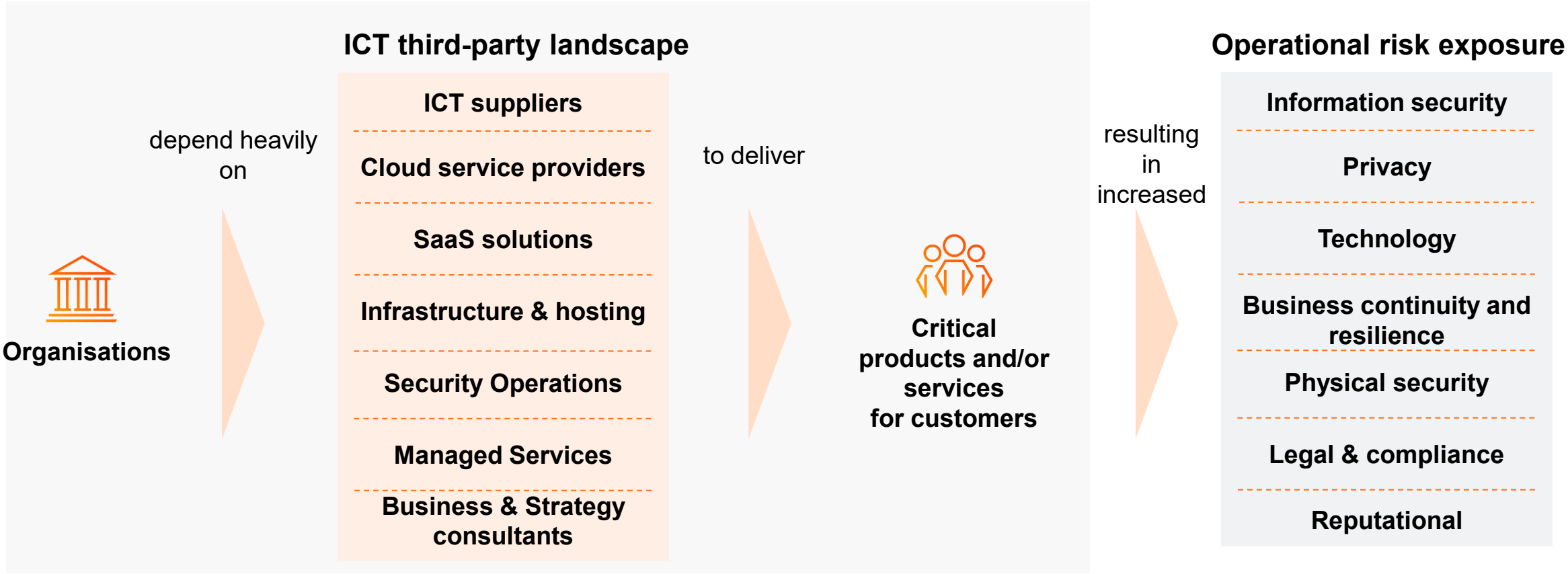
Incidents examples:

Salesloft data breach

Major cloud incidents

Jaguar Land Rover cybersecurity incident

Increasing complexity in the third-party landscape



Risk exposure doesn’t necessarily (always) originate at the third-parties

Hidden application integrations and add-ons

Reliance on 4th party external cloud and hosting providers

Team owned applications purchased informally

Treating sub-contractor risk is equally an important aspect:

- **Identify relevant fourth-parties or nth parties**
- **Determine cross-border risk exposure**
- **Ensure contractual requirements flow down**
- **Update playbooks to manage cyber incidents**

Retaining digital sovereignty by minimising dependencies on Big Tech

“AFM and DNB warn of systemic risks in the financial sector from digital independence”

“ACM is concerned about the decline in competition and extreme dependence on several large non-European companies”

KEY CONCERNS:

- Concentration risk
- Systemic risk
- Impact on business operations

NEXT STEPS:

- Rehearse risk scenarios
- Identify alternative measures
- Prepare to diversify IT dependencies

Dependencies examples

Solvinity. DigiD Microsoft Google

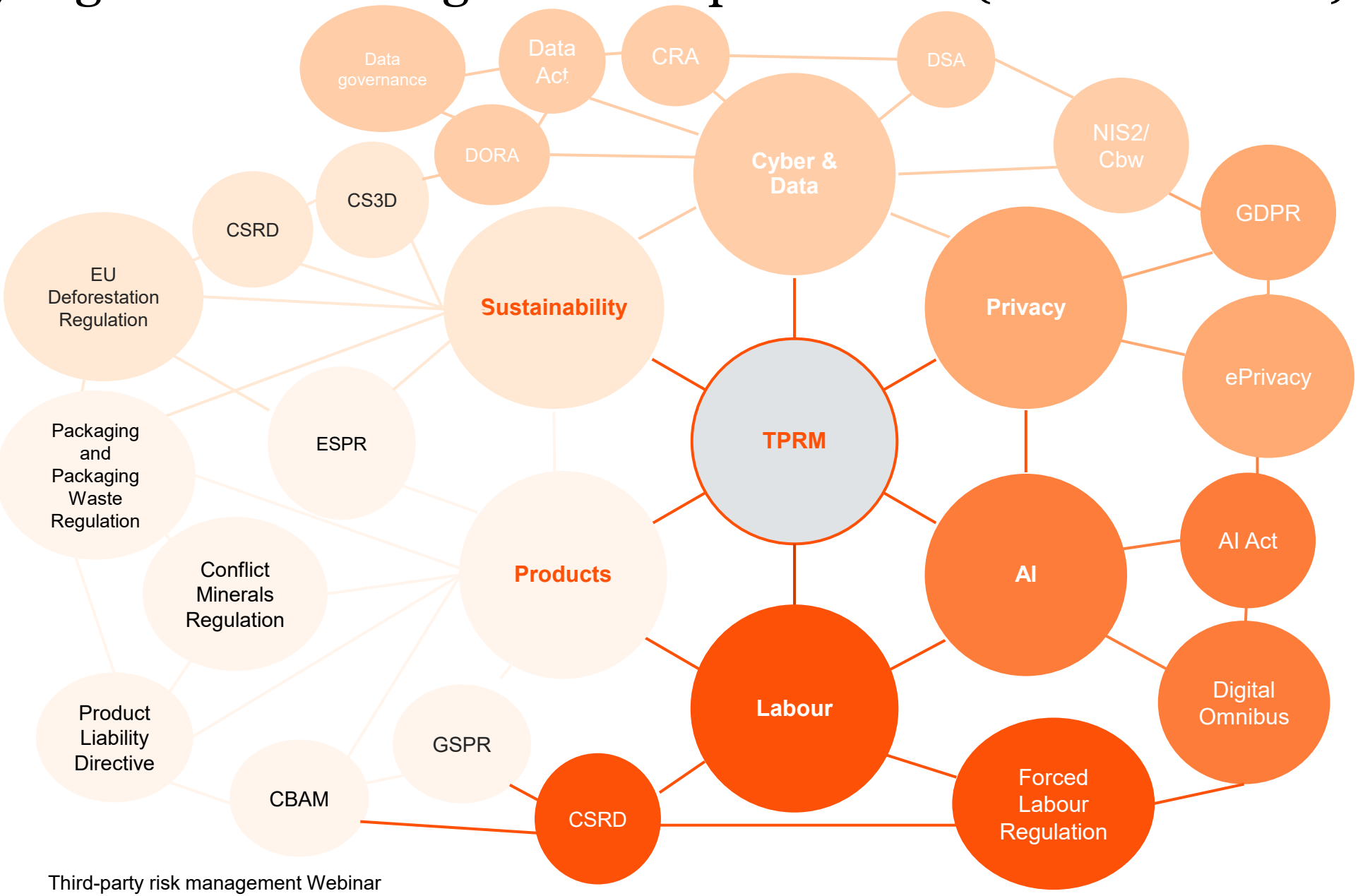
3

Legal & Regulatory Perspective – What is the minimum you need to have in order?

Transforming the framework: the regulatory evolution of the EU

Supervision	Static compliance (periodic audits)	Sectoral rules	Siloed responsibility	Voluntary best practices
				
Full supply chain traceability	Continuous monitoring and proactive resilience	Horizontal integration	Integrated governance and demonstratable outcomes	Mandatory multi-dimensional risk frameworks

Key regulations driving TPRM requirements (not exhaustive)



From compliance gap to headline risk: the growing wave of value chain infringements in cyber, data, and product liability

Headphones removed from sale as a precaution after investigation into harmful substances

Programmer accidentally peeks into thousands of homes through poorly secured robot vacuum cleaners

Board held liable for EUR 140 million

Canada calls OpenAI to account for not warning about shooter

Fines up to 6% of the annual world wide turnover

Reputation and credibility

Service disruption

Board liability

Product recalls

Integrated legal involvement across the TPRM lifecycle

00

Due diligence

Systematic research into the third party in advance (including financial, security, compliance) to determine the risk profile.

01

Contract Terms

Clear agreements in the contract about security, compliance, service levels, liability and rights/obligations.

02

Audit rights

The contractual right to review the third party (or through a third party), for example through audits or reports (SOC, ISAE).

03

Monitoring

Continuously monitor and evaluate performance, risks and incidents at the third party throughout the contract term.

04

Reporting

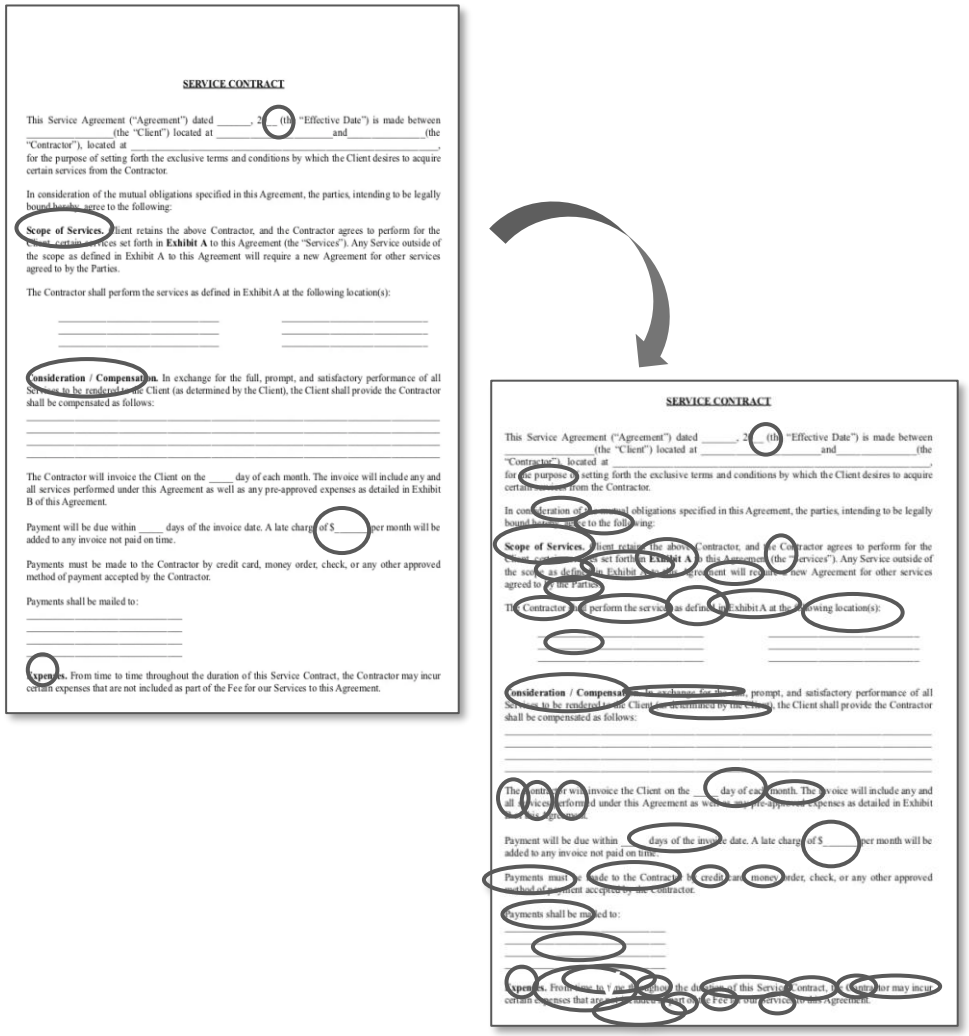
Structured reporting on the status of third parties, risks and incidents to management and relevant stakeholders.

05

Exit strategies

Predetermined agreements and plans to terminate the cooperation in a controlled manner and to transfer services safely.

Beyond the basics: how contract review expanded from 10 to 110 Data Points



SERVICE CONTRACT

This Service Agreement ("Agreement") dated _____, 2__ (the "Effective Date") is made between _____(the "Client") located at _____and_____(the "Contractor"), located at _____, for the purpose of setting forth the exclusive terms and conditions by which the Client desires to acquire certain services from the Contractor.

In consideration of the mutual obligations specified in this Agreement, the parties, intending to be legally bound hereby, agree to the following:

Scope of Services. Client retains the above Contractor, and the Contractor agrees to perform for the Client certain services set forth in **Exhibit A** to this Agreement (the "Services"). Any Service outside of the scope as defined in Exhibit A to this Agreement will require a new Agreement for other services agreed to by the Parties.

The Contractor shall perform the services as defined in Exhibit A at the following location(s):

_____ _____
_____ _____
_____ _____

Consideration / Compensation. In exchange for the full, prompt, and satisfactory performance of all Services to be rendered to the Client (as determined by the Client), the Client shall provide the Contractor shall be compensated as follows:

_____
_____
_____
_____

The Contractor will invoice the Client on the _____ day of each month. The invoice will include any and all services performed under this Agreement as well as any pre-approved expenses as detailed in Exhibit B of this Agreement.

Payment will be due within _____ days of the invoice date. A late charge of $_____ per month will be added to any invoice not paid on time.

Payments must be made to the Contractor by credit card, money order, check, or any other approved method of payment accepted by the Contractor.

Payments shall be mailed to:

_____
_____
_____
_____

Expenses. From time to time throughout the duration of this Service Contract, the Contractor may incur certain expenses that are not included as part of the Fee for our Services to this Agreement.

SERVICE CONTRACT

This Service Agreement ("Agreement") dated _____, 2__ (the "Effective Date") is made between _____(the "Client") located at _____and_____(the "Contractor"), located at _____, for the purpose of setting forth the exclusive terms and conditions by which the Client desires to acquire certain services from the Contractor.

In consideration of the mutual obligations specified in this Agreement, the parties, intending to be legally bound hereby, agree to the following:

Scope of Services. Client retains the above Contractor, and the Contractor agrees to perform for the Client certain services set forth in **Exhibit A** to this Agreement (the "Services"). Any Service outside of the scope as defined in Exhibit A to this Agreement will require a new Agreement for other services agreed to by the Parties.

The Contractor shall perform the services as defined in Exhibit A at the following location(s):

_____ _____
_____ _____
_____ _____

Consideration / Compensation. In exchange for the full, prompt, and satisfactory performance of all Services to be rendered to the Client (as determined by the Client), the Client shall provide the Contractor shall be compensated as follows:

_____
_____
_____
_____

The Contractor will invoice the Client on the _____ day of each month. The invoice will include any and all services performed under this Agreement as well as any pre-approved expenses as detailed in Exhibit B of this Agreement.

Payment will be due within _____ days of the invoice date. A late charge of $_____ per month will be added to any invoice not paid on time.

Payments must be made to the Contractor by credit card, money order, check, or any other approved method of payment accepted by the Contractor.

Payments shall be mailed to:

_____
_____
_____
_____

Expenses. From time to time throughout the duration of this Service Contract, the Contractor may incur certain expenses that are not included as part of the Fee for our Services to this Agreement.

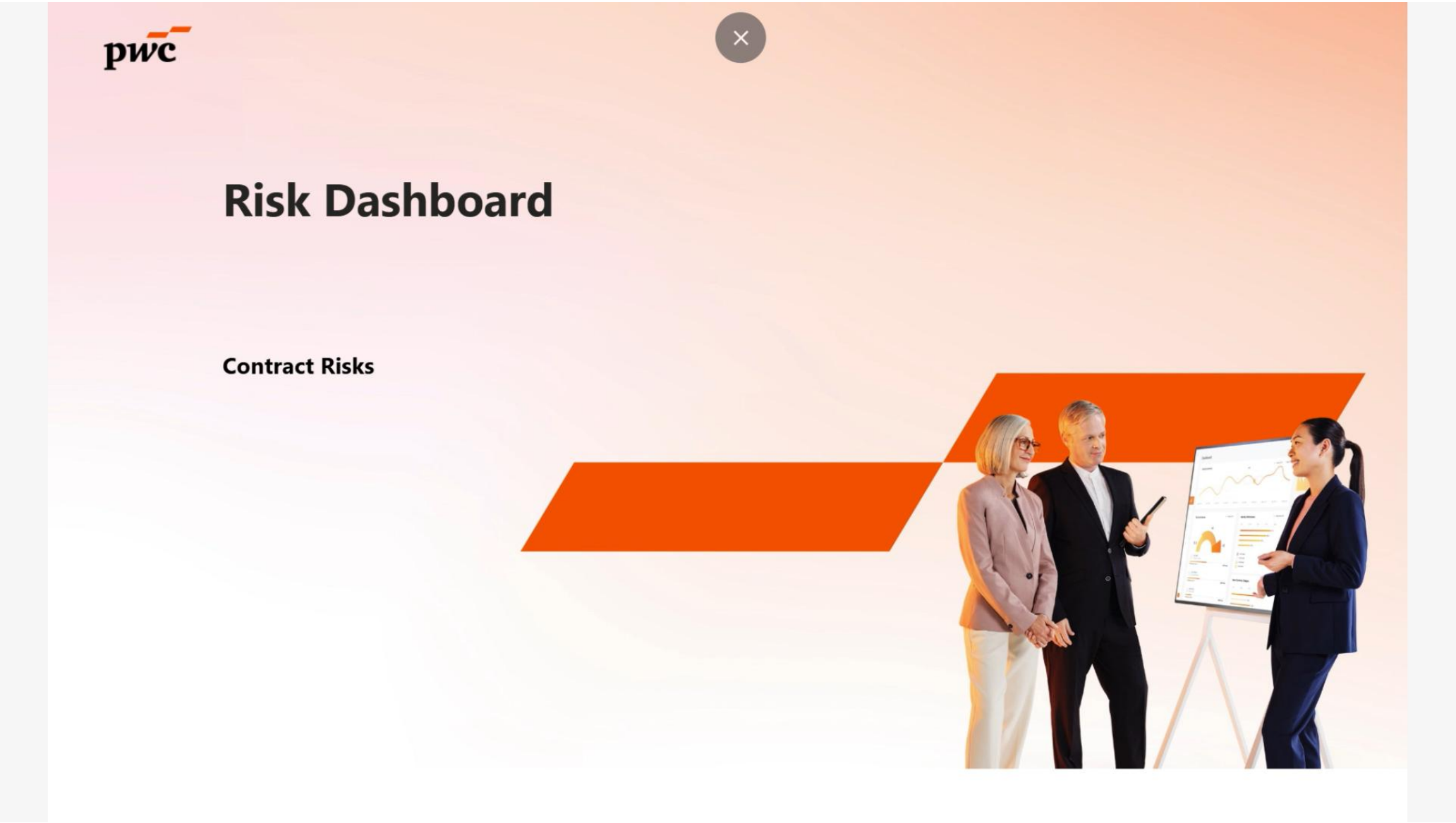
Data Points

- *Term and termination*
- *Payment terms*
- *Penalties*
- *Limitation of liability*
- *Governing law*
- *Insurance requirements*
- *Notice rights*
- *Assignment and change of control*

- Subcontracting provisions and approval requirements
- Audit and access rights for the (financial) entity and regulators
- Exit strategies and termination provisions
- Data location and processing requirements
- Service level descriptions and performance targets
- Security measures and incident reporting obligations
- Business continuity and disaster recovery provisions
- Cooperation with competent authorities
- Enhanced requirements for contracts supporting critical functions
- Notification obligations for material changes
- Specific exit planning and transition assistance terms
- Incident reporting timelines and procedures
- Notification thresholds and escalation paths
- Root cause analysis and remediation commitments
- Participation in threat-led penetration testing
- Access to test results and remediation plans
- Ongoing resilience testing cooperation

- Data category
- Role identification
- Processing activities
- International transfer
- Security measures
- Compliance certifications and commitments (ISO)
- Reporting obligations
- Carbon footprint or emissions reduction commitments
- Labor and human rights standards compliance
- Penetration testing and vulnerability assessment obligations
- Business continuity and disaster recovery provisions
- Product quality standards and specifications
- Warranty provisions and limitations
- Product liability and indemnification clauses
- Recall and defect notification procedures
- Regulatory compliance certifications (e.g., CE, FDA approval)
- Intellectual property ownership and licensing terms
- Supply chain transparency and subcontractor requirements
- Data retention and deletion obligations
- Sub-processor notification and approval requirements
- Privacy impact assessment obligations

Contract Remediation with AI: addressing third-party risk at scale



4

Auditor’s expectations and TPRM Operating Models

IIA Third-Party Requirements

Topical requirement

Third-Party topical requirement

- Internal auditors must apply Topical Requirements in conformance with the Global Internal Audit Standards when providing assurance services on the topics released if they are included in IA's plan. Topical Requirements are recommended but not required for advisory services.
- The Third-Party Topical Requirement was released on September 15, 2025, with an effective date of September 15, 2026.

What it is:

- Required when providing assurance in a specific area related to third-party risk (e.g., third-party program risk management program audit, third-party audit)
- Covers third-party 1) governance, 2) risk management and 3) control processes
- Includes a supplemental user guide with optional documentation tool
- Subject to external quality assessment

What it's not:

- Requiring internal audit to specifically audit third-parties
- Comprehensive third-party work program (consider any local laws and regulations specific to third party risks in your territory)

Assessment Areas

Governance

- Policies and procedures for defining, assessing, contracting and managing third-party risks across the lifecycle
- Roles and responsibilities for third-party management
- Communication protocols related to third-party management

Risk Management

- Defined processes to manage third-party risks across key categories (e.g., strategic, reputational, ethical, operational, financial, compliance, IT/cyber, legal, sustainability and geopolitical)
- Risk assessment process ranking/prioritizing third parties
- Monitoring and escalation process for issues related to third parties

Control Processes

- Onboarding processes over third parties (including an inventory or listing)
- Due diligence processes for third-party sourcing, selection, etc.
- Contracting and approval process
- Ongoing monitoring processes over third parties
- Corrective action and escalation process for performance issues
- Renewal, expiration and offboarding processes

Where does the TPRM Function sit?

There is not one "right" place that TPRM functions should sit within the organisation.

Where do we frequently see the "owners" of TPRM within organisations?

Procurement

Enterprise Risk Management (ERM)

Data Security / Information Security

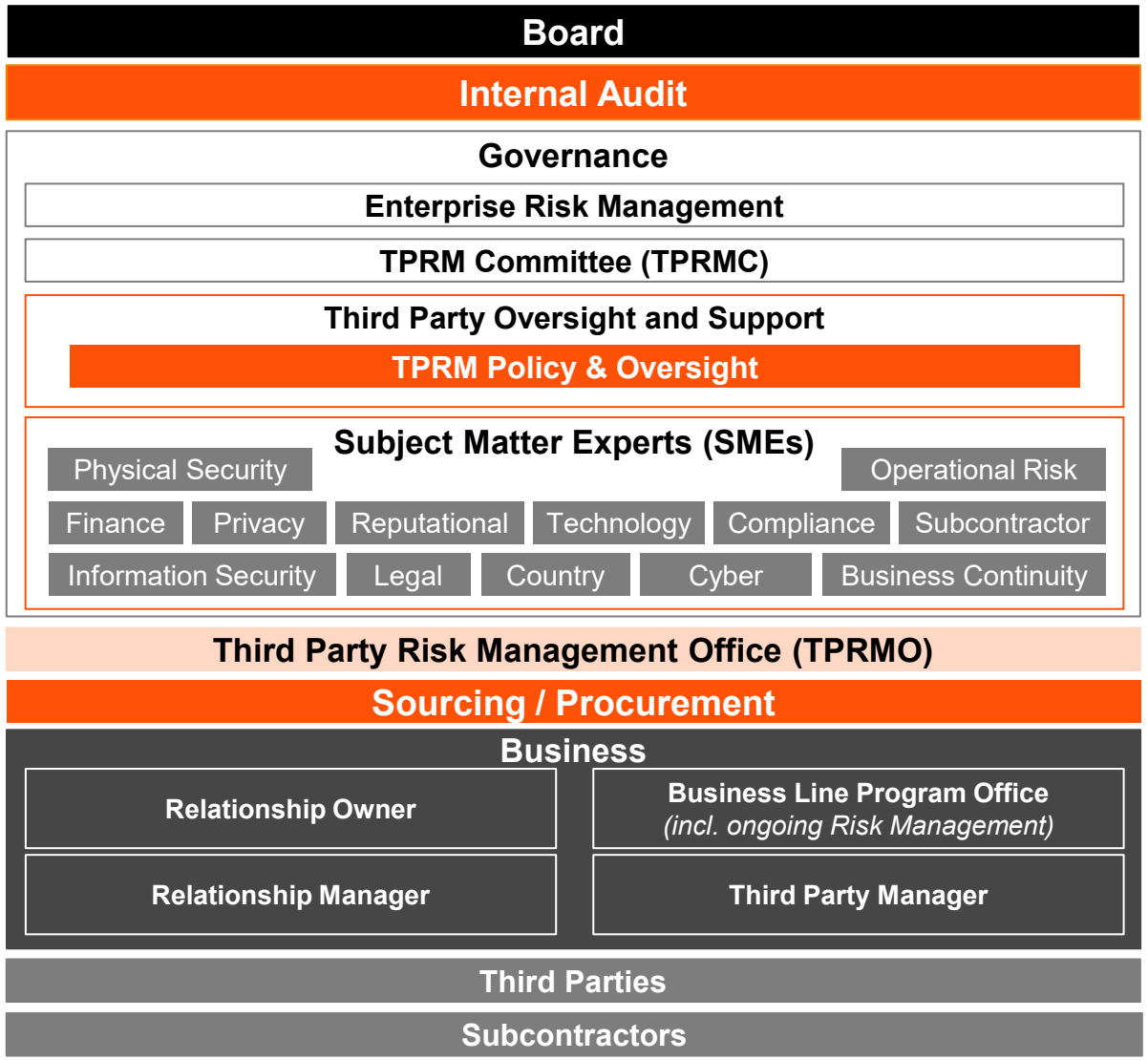
Stand Alone TPRM Function

Compliance

Legal

- ***Essential that Procurement and TPRM are well coordinated and aligned***
- *Procurement serves as the "entry" or "kick off" point for the Businesses to request a new third party product / service and the TPRM activities will be completed concurrently while Procurement drives the selection and negotiation processes.*
- ***Procurement as the "gatekeeper" to ensure that contracts are not signed until required risk assessment activities are performed.***

Operating model: three lines of defense



Purpose

Third Line

- Independently test the design and operating effectiveness of third party risk management policies and controls across the lifecycle as well as the effectiveness of second line and oversight activities and report on effectiveness of the program

Second Line

- Define TPRM policy requirements including various regulatory specifications / requirements
- Design and assist in implementing company-wide risk framework
- Perform quality assurance reviews and other targeted oversight practices to ensure that the line of business is compliant with internal policies and external regulations
- Review effectiveness of the Governance Framework

First Line

- Execution of the program based on TPRM policies and standards
- Business relationship managers and third party relationship owners are responsible for identifying, assessing and mitigating risk associated with their business
- Implement internal controls and practices consistent with company-wide policies and procedures

Key Considerations:

- Specialist resources ("SMEs") are used to support due diligence activity and can be drawn from both 1st and 2nd line functions. **Typically 2nd line SMEs define requirements for 1st line SME execution**
- Procurement is positioned as a 1st line function reflecting the operational nature of its activities
- Variability between what components of TPRMO stay in the 1st line or appear as part of TPRM Policy and Oversight (e.g., testing and reporting)

Advancing TPRM to the next level with AI embedded throughout the TPRM lifecycle

Risk Planning

- Submit request/ intake form
- Create business case
- Conduct inherent risk profiling/ assessment
- Measure inherent risk and criticality
- Trigger due diligence requirements
- Initiate third party registration
- Execute third party verification

Due Diligence

- Distribute due diligence requests
- Conduct risk intelligence analysis
- Execute control assessments
- Measure due diligence results and residual risk
- Generate remediation action plans
- Generate risk summary reports
- Determine business decision (remediate/ accept)
- Select third party / award contract

Contract Negotiation

- Draft third party contract
- Establish clauses, provisions, and SLAs (risk/performance)
- Negotiate contractual terms
- Evaluate contract risk and legal/ regulatory alignment
- Generate contract risk summary
- Sign, execute and link contract
- Generate contingency and exit plans
- Complete onboarding activities

Ongoing Monitoring

- Set/trigger ongoing monitoring activities
- Oversee and manage third party engagement
- Continuously monitor third parties
- Execute alert triage and incident/event processes
- Conduct performance reviews
- Perform periodic risk profiling
- Execute periodic due diligence assessments
- Simulate/update contingency and exit plans

Termination

- Determine business decision to terminate/exit
- Generate termination checklist
- Initiate exit plan/transition
- Complete termination activities
- Source alternative third parties

AI-enabled **Traditional automation** **Manual activity/control**

TPRM service offerings

- PwC is a global leader in designing, implementing, and operating Third Party risk management programs.
- Our team leverages innovative approaches and technologies to help our clients expand risk coverage, drive process consistency and reduce their overall cost of operations.
- Our goal is help you protect your operations, brand and reputation.

A snapshot of PwC services

TPRM Program (Current) Assessment

TPRM Assessment Support

Program Design & Build

TPRM Managed Services

Technology Selection, Implementation & Optimization

TPRM Internal Audit

5

Wrapping up & Q&A

Summary of key messages

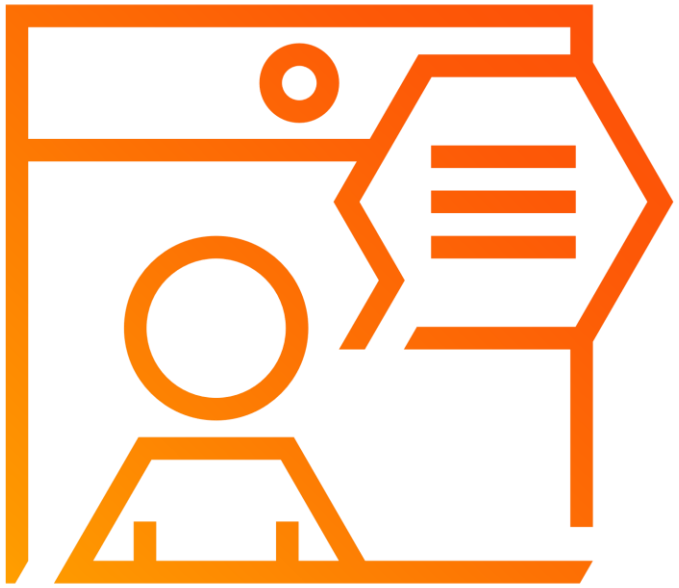
Third-party risk management (TPRM) is the process of identifying, assessing, and mitigating risks associated with outsourcing tasks or engaging external vendors to ensure operational, regulatory, and cybersecurity resilience.

TPRM is essential due to chain dependencies

Regulation and supervision are increasing

A structured approach provides insight and control

Start with overview, risk-based choices and clear governance



Q&A

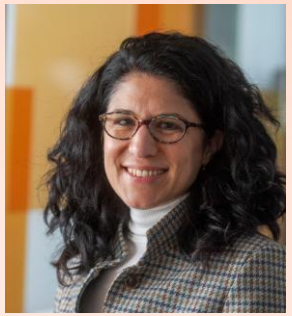
Questions?
Ask them in the chat
or live

Let’s talk

Thank you for attending!

Casper Ruizendaal

Partner
casper.ruizendaal@pwc.com



Seda Foppen

Partner
seda.foppen@pwc.com

Bram van Tiel

Partner
bram.van.tiel@pwc.com

Mimoent Haddouti

Partner
Mimoent Haddouti@pwc.com

Lean Besseling

Director
lean.besseling@pwc.com

Ilse van Wendel de Joode

Director
ilse.van.wendel.de.joode@pwc.com

Peter Avamale

Director
peter avamale@pwc.com

Marco Valkenburg

Senior Manager
marco.valkenburg@pwc.com