onetrust

Staying vigilant: 7 practical tips for ongoing third-party risk monitoring

This presentation includes statements relating to the business, technology, products, services and development activities of OneTrust LLC and its affiliates ("OneTrust"). While OneTrust makes these statements based on current understandings and expectations, there is no guarantee that the statements included in this presentation will remain true after the date of this presentation, nor does OneTrust make any representation, warranty or guaranty, express or implied, regarding anticipated or future technology, products, services and development activities.

August 2nd 2023

Agenda

01 Understanding the new third-party landscape

02 Seven tips for ongoing monitoring

Shea Hanson
Senior Solutions Engineer
OneTrust

Understanding the new third-party landscape

Companies rely on third parties more than ever

60% of organizations surveyed by Gartner work with over 1,000 third parties

Gartner

Third parties are causing disruption and value loss

73% of organizations have experienced a significant disruption, caused by a third party, in the last three years

KPMG

Third parties are inadequately managed

16% of organizations say they effectively manage third-party data risks

Gartner

Fundamental shifts in the business landscape are reshaping how we engage third parties

Operational

Data-driven mindset focused on trust across critical domains

Cross-team information sharing with focus on breaking down siloes

System alignment becoming a necessity across technologies

Regulatory

Increasing global privacy laws and impactful legal rulings

Cybersecurity threats leading to government action

Emerging Ethics and ESG regulations taking center stage

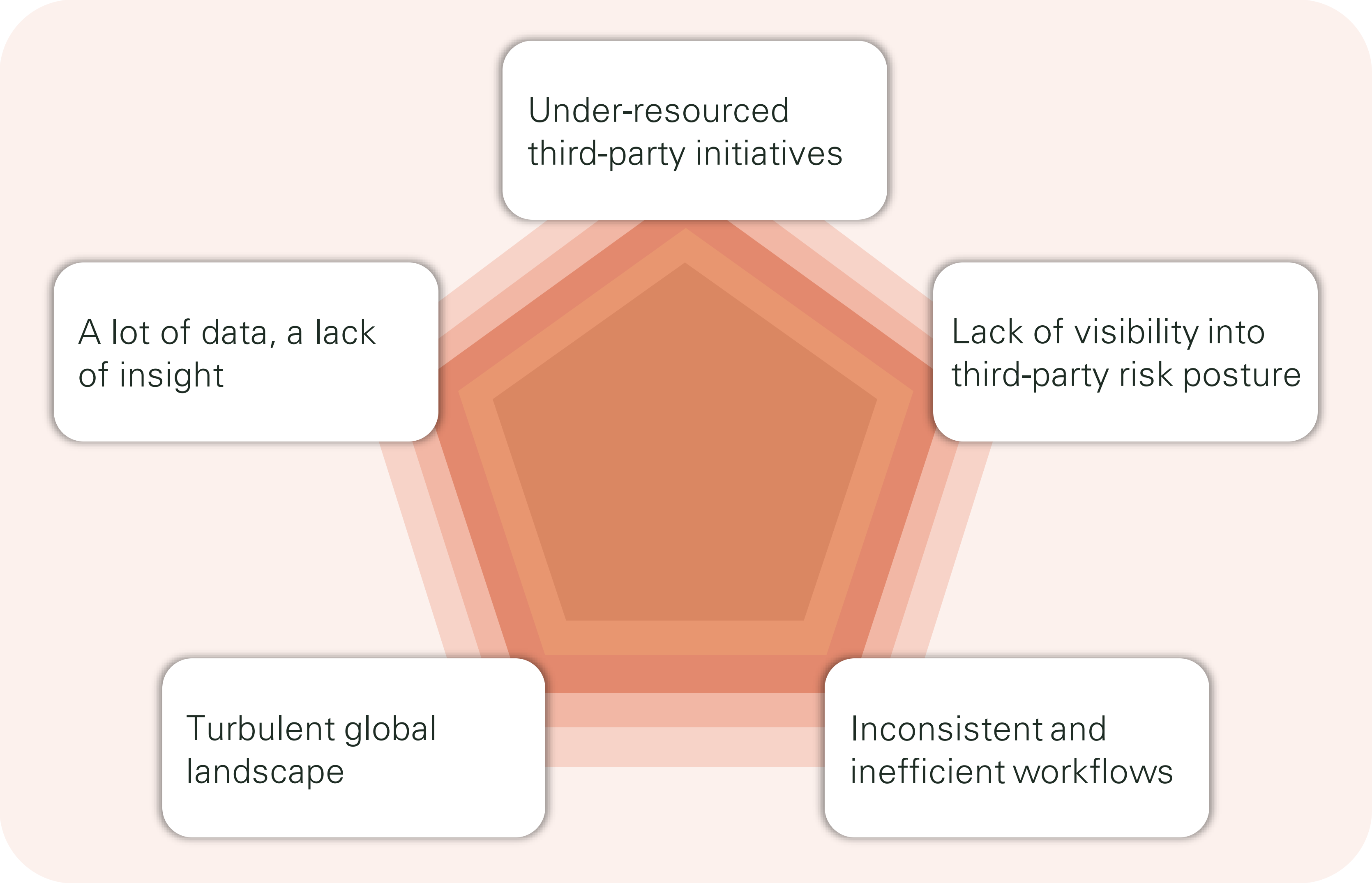
Monitoring

Board-level scrutiny on resilience of third-party ecosystem

Ongoing monitoring of reputational risks associated with third parties

Management of nth parties introducing complexities and resilience issues

Expanding third-party ecosystems are increasing the complexity of management programs



Under-resourced third-party initiatives

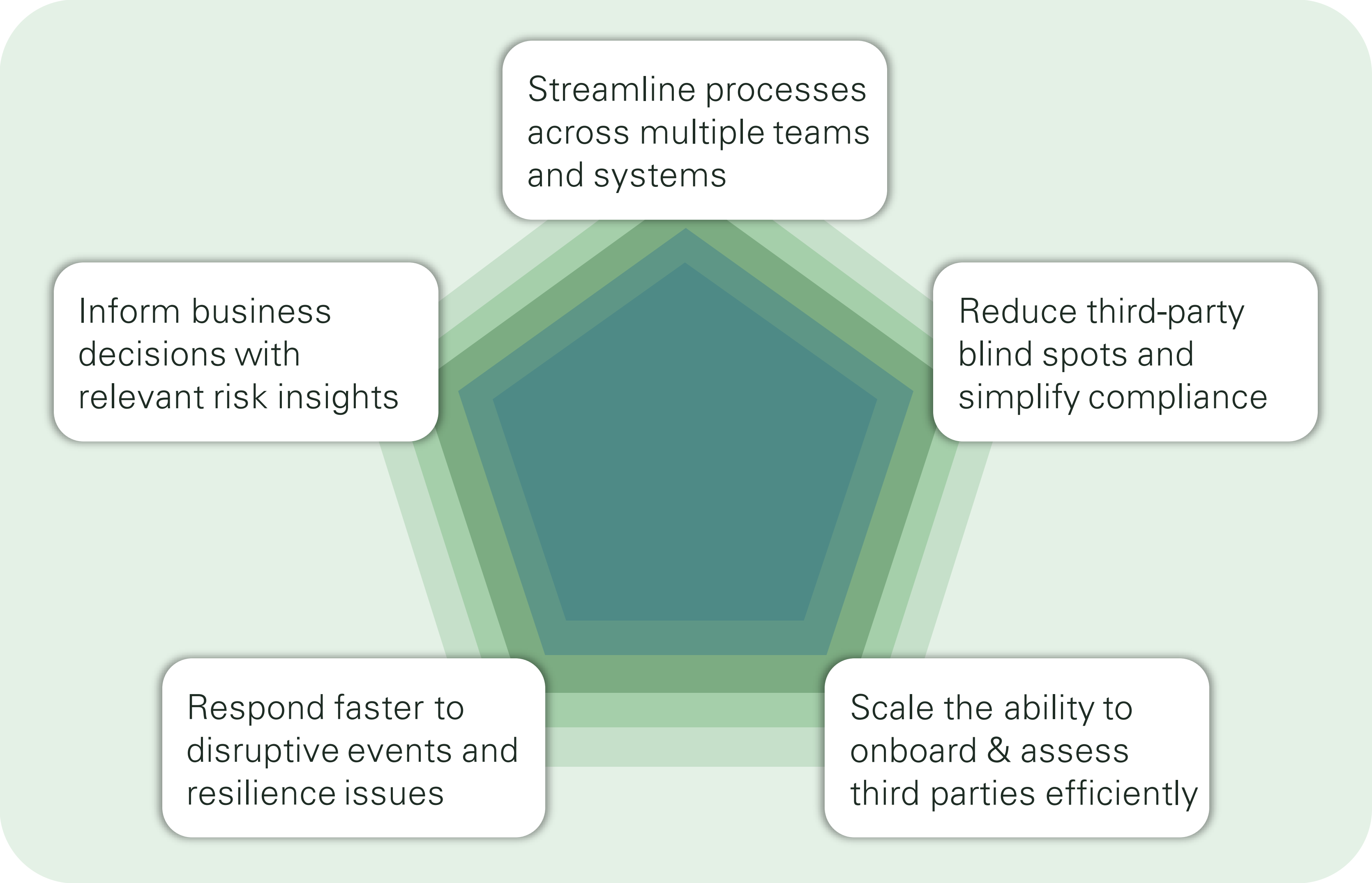
A lot of data, a lack of insight

Lack of visibility into third-party risk posture

Turbulent global landscape

Inconsistent and inefficient workflows

A fit-for-purpose third-party management program is centered on clear outcomes



Streamline processes across multiple teams and systems

Inform business decisions with relevant risk insights

Reduce third-party blind spots and simplify compliance

Respond faster to disruptive events and resilience issues

Scale the ability to onboard & assess third parties efficiently

7 tips for ongoing third-party risk monitoring

Tip One

Create a comprehensive risk assessment framework

Develop a risk assessment framework that categorizes third-party vendors based on their criticality and potential impact on your organization. This will help prioritize monitoring efforts and allocate resources effectively.

Tip Two

Establish Key Performance Indicators (KPIs)

Define and track KPIs related to third-party risk management, such as response times to security incidents, patch management compliance, and adherence to contractual obligations.

Tip Three

Establish clear contractual obligations

Ensure that all third-party contracts include specific security and data protection requirements, compliance standards, incident response plans, and access controls. Regularly review and update contracts to address changing risks and regulatory requirements.

Tip Four

Enhance monitoring with external data and risk ratings

Assessments are singular, point-in-time, evaluations of a third party’s risk posture and it is difficult to track meaningful risk metrics that change over time. External data sources and risk ratings can help to fill in the gap and keep you apprised of what your third parties are up to.

Tip Five

Automate responses to changes in risk scoring

Automate response actions as risks arise by listening for data changes and creating triggers to notify stakeholders, flag risks, and kick-off dynamic reassessments.

Tip Six

Re-think when a traditional risk assessment is necessary

Triage third parties and automate evaluation procedures by leveraging risk data to tailor evaluation and assessment depth. In some cases, bypass assessments altogether or send assessments that are specific to distinct issues.

Tip Seven

Use monitoring data to validate assessment responses

When a third party responds to a risk assessment, compare monitoring data and insights against there responses and flag inconsistencies for further examination and follow up.

Bonus Tips

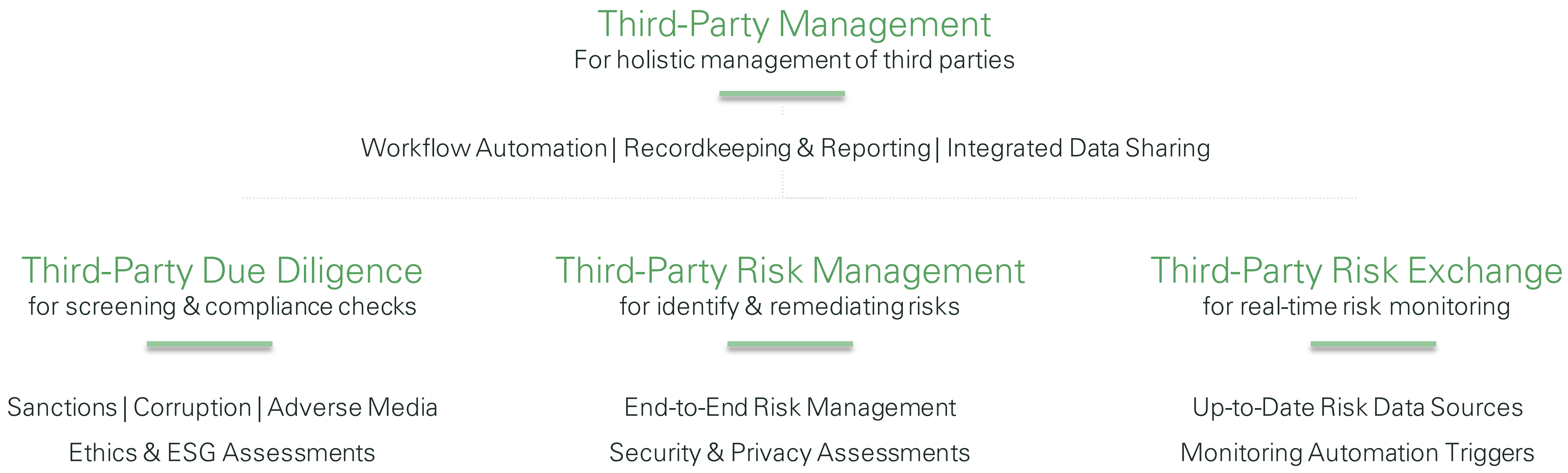
Encourage collaboration and communication

Establish open lines of communication with third-party vendors and encourage transparency. Regularly discuss security concerns, updates, and changes in risk profiles.

Promote a culture of risk awareness

Foster a risk-aware culture within your organization. Train employees to recognize and report potential risks associated with third-party relationships. Encourage open communication and reporting of concerns.

OneTrust Third-Party Management Solutions



Third-Party Management

For holistic management of third parties

Workflow Automation | Recordkeeping & Reporting | Integrated Data Sharing

Third-Party Due Diligence

for screening & compliance checks

Sanctions | Corruption | Adverse Media

Ethics & ESG Assessments

Third-Party Risk Management

for identify & remediating risks

End-to-End Risk Management

Security & Privacy Assessments

Third-Party Risk Exchange

for real-time risk monitoring

Up-to-Date Risk Data Sources

Monitoring Automation Triggers

onetrust

Questions?

Need to be updated with a CTA- Thoughts?

onetrust

Thank you!

Visit OneTrust's Third Party Management Academy to stay tuned! Scan the QR now

2024