RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART4-R02**

Securing the Supply Chain: What Does Compliance Look Like?

Justin Henkel

Head of CISO Center of Excellence
OneTrust

Adam Topkis

Enterprise and Operational Risk
Program Leader
PayPal

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

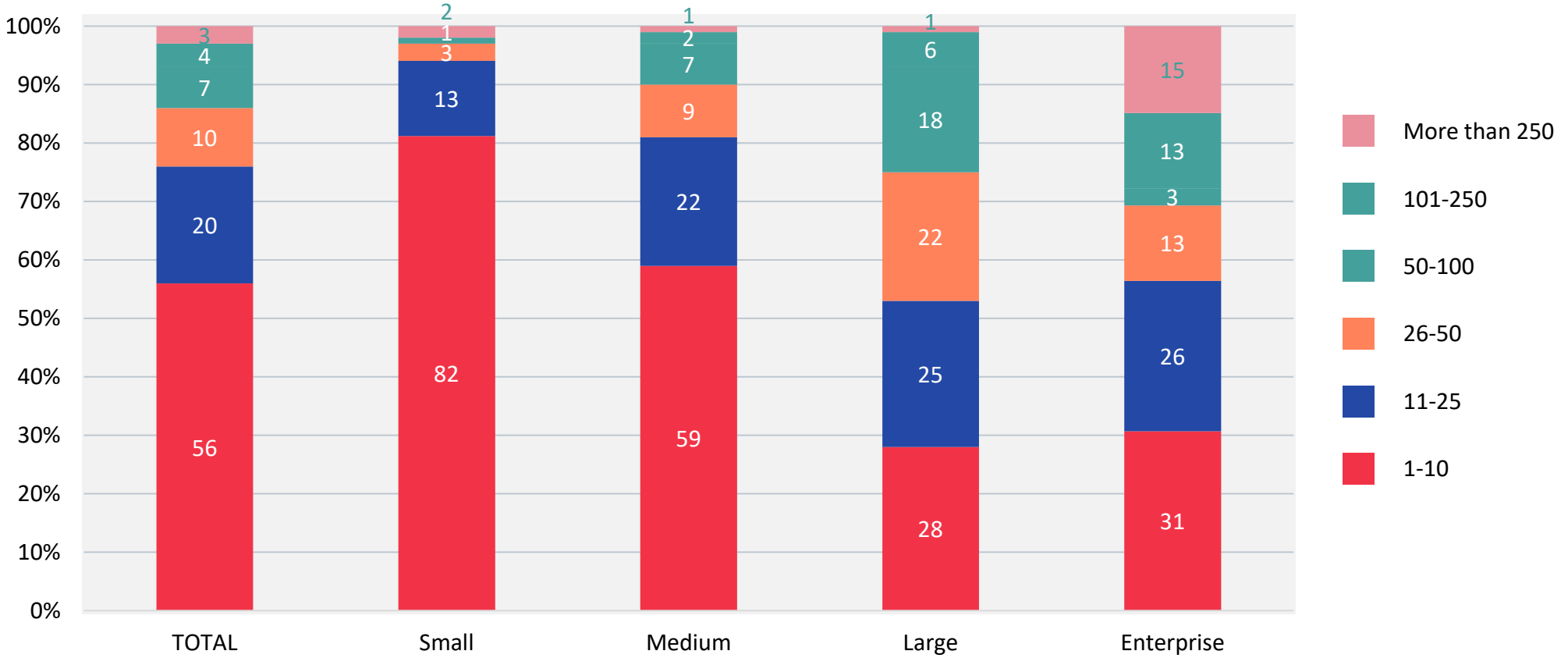
- What's Going on Down There?
- The Evolution of Risk
- On the Supply Chain Horizon

RSAConference2022

The Supply Chain Slippery Slope

What's Going on Down There?

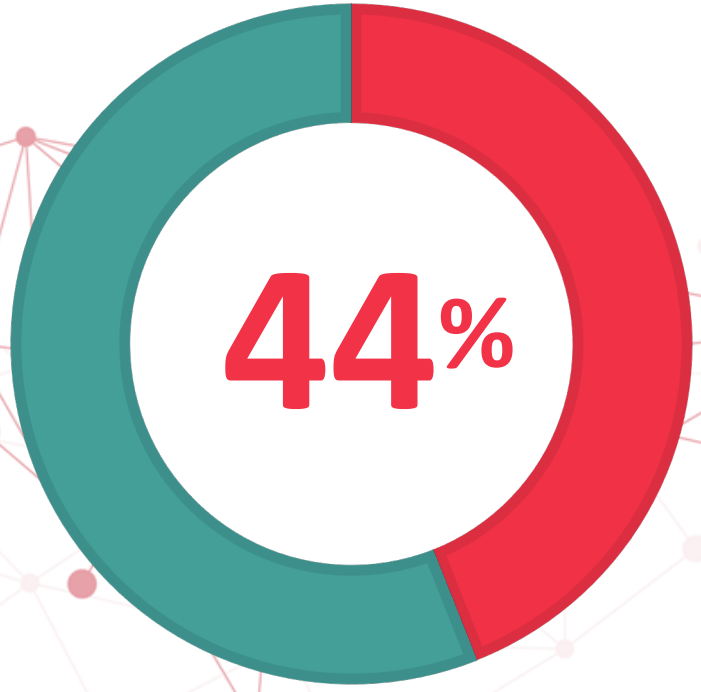
Scale of Third-Party Partners



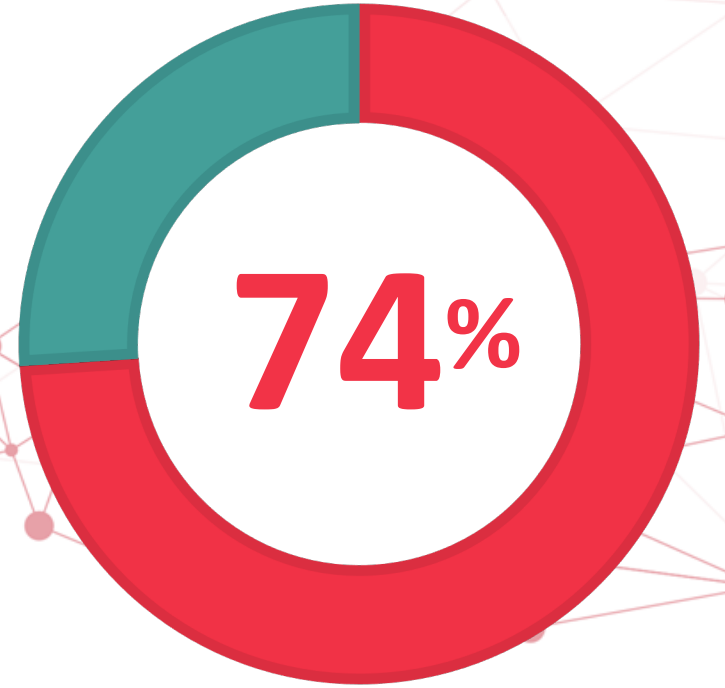
22% of all companies work with more than 250 third parties

Source: 2022, CyberRisk Alliance + OneTrust study of 301 IT professionals

Third Parties and Data Breaches Are Often Intertwined



of organizations have experienced a breach within the last 12 months



of organizations say it was the result of giving too much privileged access to third parties

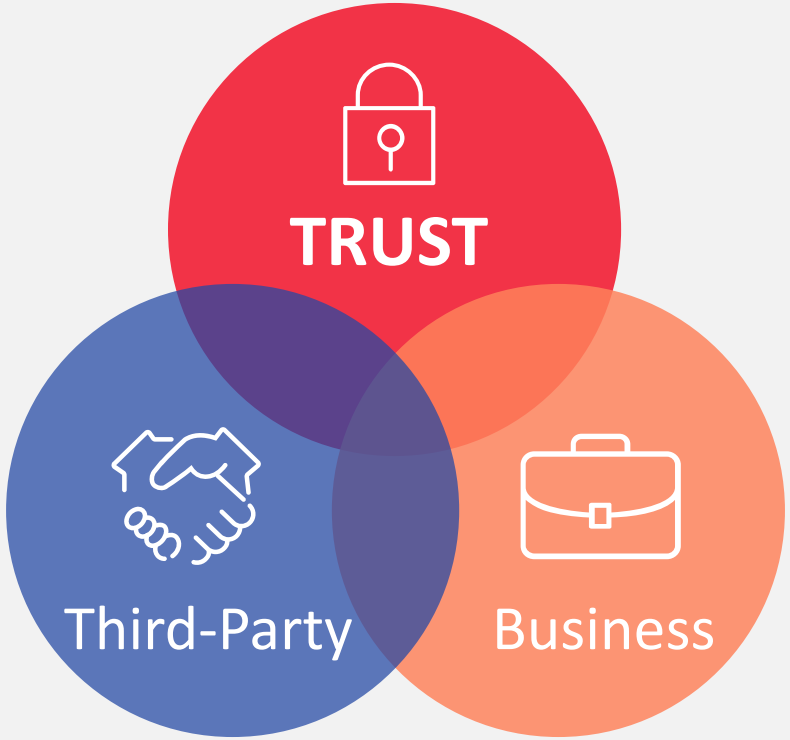
2021, Ponemon Institute Survey of 627 individuals with involvement in their organization's approach to managing third-party risks

Third-Party Visibility

Third-Party Risk

Third-Party Impact on Cybersecurity Risk

Major Supply Chain Attacks take advantage of the inherent trust in third-party relationships



RSAConference2022

The Evolution of Risk

Risk Definitions

ECONOMIC

Likelihood that **macroeconomic conditions** may affect an investment or a company's prospects domestically or abroad.

COMPLIANCE

is an **organization's potential exposure to legal penalties, financial forfeiture and material loss**, resulting from its failure to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

SECURITY & FRAUD

impact **trust and reputation**, but a company is also financially liable for any data breaches or identity theft, loss of intellectual property.

FINANCIAL

May involve credit extended to customers or your **own company's debt load.**

REPUTATIONAL

Risk that an unhappy customer, product failure, negative press or lawsuit can adversely impact a **company's brand reputation**.

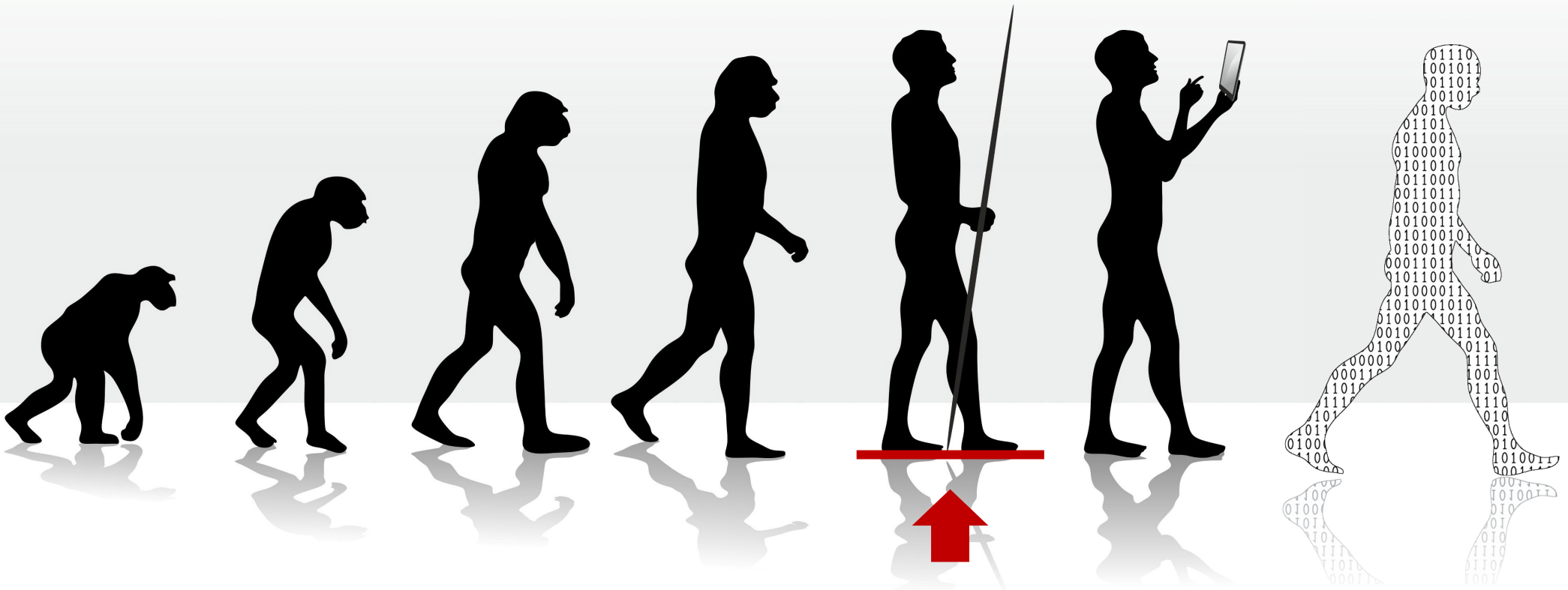
OPERATIONAL

business risk can happen internally, externally or involve a combination of factors that causes you to **lose business continuity**.

COMPETITIVE

Businesses so comfortable with their **success and the status quo** that they don't look for ways to pivot or make continual improvements.

Evolution of Risk



RSAConference2022

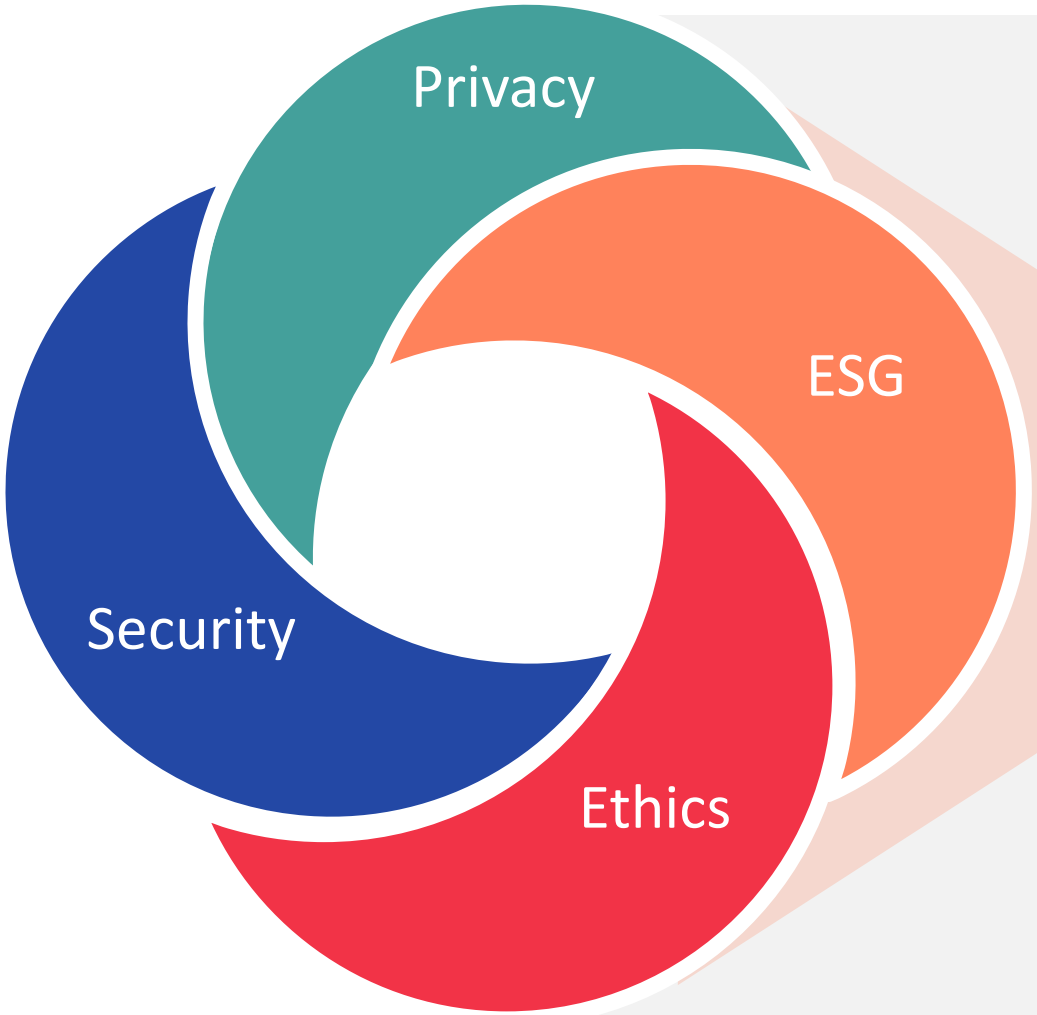
On the Supply Chain Horizon

What Is the German Supply Chain Due Diligence Act?

- Companies with any footprint in Germany and headcount of 3,000 employees*
- Establish risk management system
- Implement due diligence with regard to indirect suppliers (4th, Nth level)

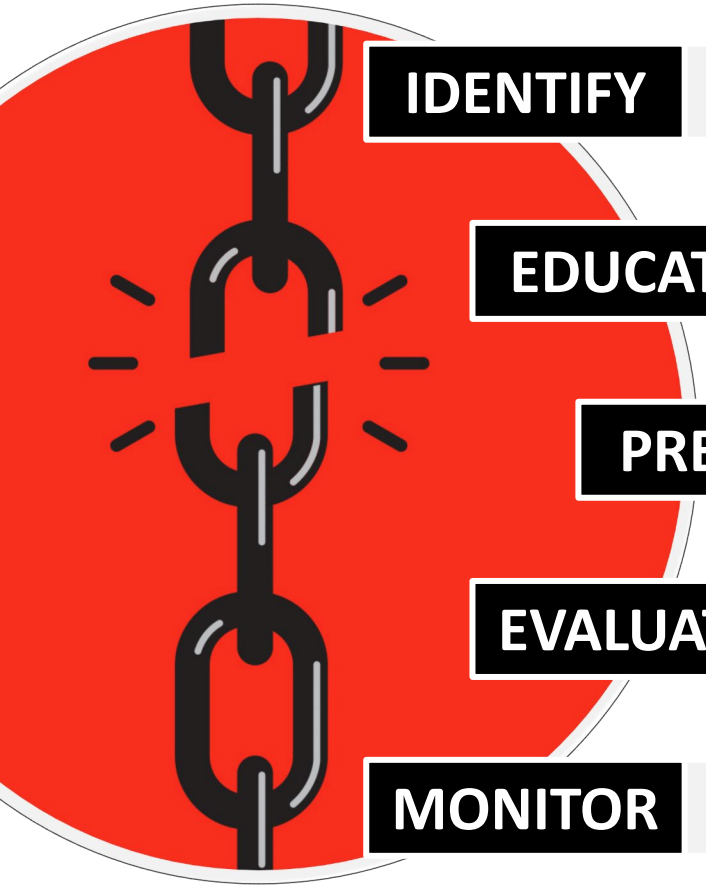
*Includes temporary agency workers on the rolls for more than six months; lowers to 1,000 employees in 2024

What Incentive Do We Have to Work Together?



Reduce Risk and
Enable the Business

Addressing Cyber Supply Chain Risk



IDENTIFY	Critical assets, their location and who has privileged access
EDUCATE	Internal stakeholders on their roles and responsibilities
PREPARE	Vendors on their security program and compliance practices
EVALUATE	A plan with vendors to coordinate incident response and recovery
MONITOR	Vendors through re-assessments and compliance checks

Future-Proof Your Third-Party Risk Program

Commit to Grow Your Program and Awareness

Build **Broad Management Skillset** Across Your GRC Team

Engage Leadership to Make Strategic Decisions

Collaborate Across Your Team and Your Third Parties

Establish Maturity with Standardized Processes

Identify Core Business Competencies, and Business Continuity Processes

Key Takeaways / Apply

Gauge your company's internal visibility: Are risk management processes in place across all departments?

Apply

Create a trust-based process to bring all departmental risk programs under one umbrella

How big is your company's third-party network, and where are the blind spots?

Apply

Streamline and automate risk assessments for the company's entire third-party network

The German Supply Chain Due Diligence Act adds another layer of compliance regulations that will impact nearly any international business by 2024.

Apply

Implement a holistic third-party management platform to remain in compliance and have a proactive security posture.

Thank You!

RSAConference2022

Questions?

Visit Us Online

OneTrust.com

Visit OneTrust
Booth #4334

@OneTrust