Addressing Today's Third-Party Risk Management (TPRM) Challenges

Sanjiv Sharma- CPA, CIA, & CISA

Vice President and Chief Audit Executive, Wolfspeed Inc.

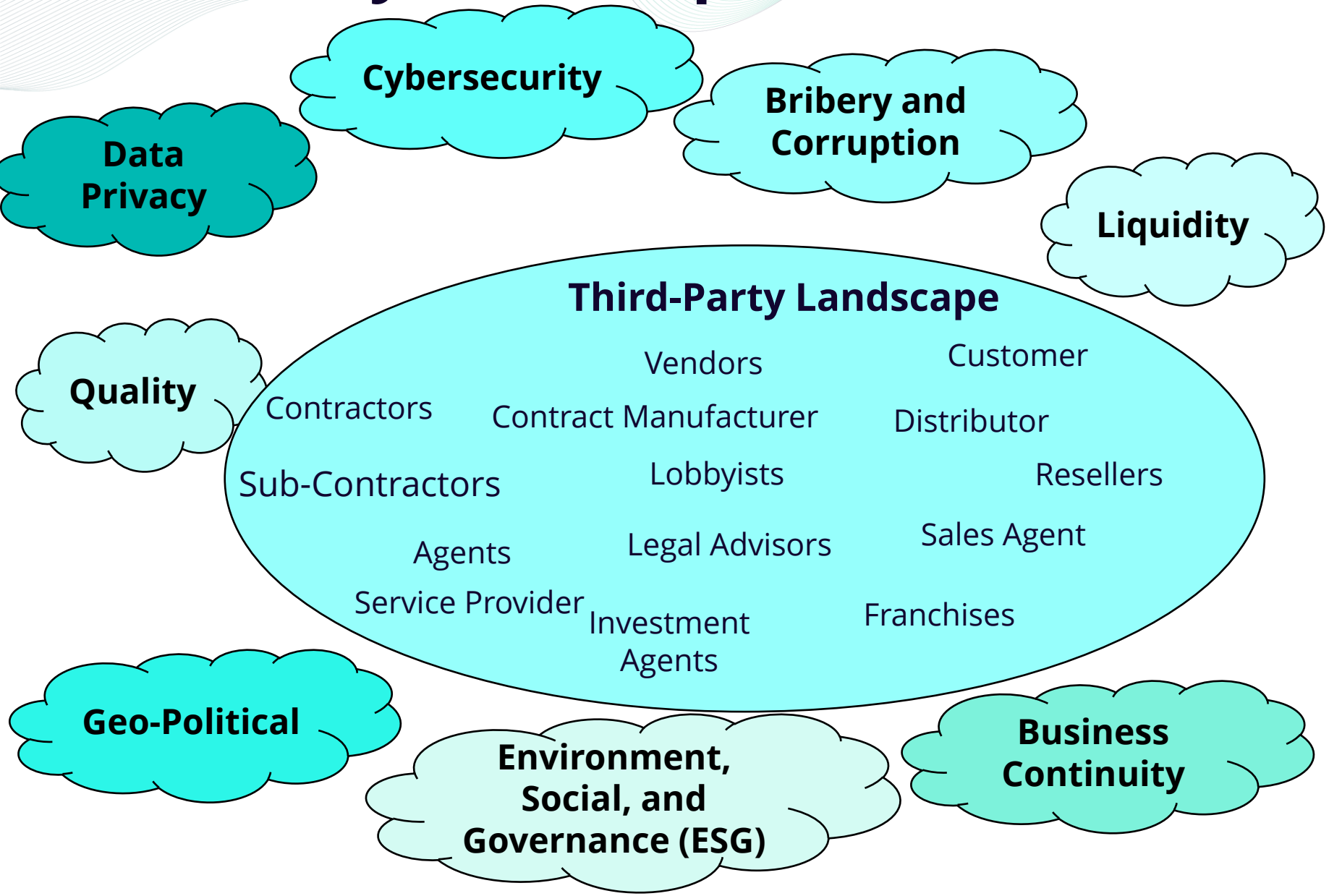
Agenda

- Why is TPRM Critical to Survival?
- Key Components of TPRM
- Governing Frameworks and Regulations
- Challenges and Leading Practices
- Q&A/ Open Discussion

Why is TPRM Critical to Survival?

metricstream
thrive on risk™

Third Party Landscape and Associated Risks



Expanding Third-party Landscape is Bringing in Significant Risk Threats

- Includes both sales and supply channels
- Margin pressures are driving explosion in growth
- Moving beyond outsourcing of physical security to cloud, and Tech development
- Risk threats are expanding beyond management controls

The Business Case of Third-party Risk Management **is** Becoming **more Important Than Ever**

Third-Party Risk Incidents

Personal details of patients at the Cancer Centers of Southwest Oklahoma were **exposed in a data breach of their server partner**.

"Inadequate formal mechanism to assess or prioritize **ESG risks in the extended enterprise"**. Deloitte's 2022 Global Third-Party Risk Management Survey

Facebook **improperly shared data of 87 million users with third-party app developers,** causing public mistrust and a market cap loss of ~$80 billion

Over 1 million Wells Fargo customers charged unnecessary auto insurance partly due to vendors (Insufficient 3rd-party oversight). Fines of $1 billion

"The **top 10 FCPA settlements** have all involved bribery ***channeled through third parties*** including consultants, agents and joint venture partners."
Transparency International, UK

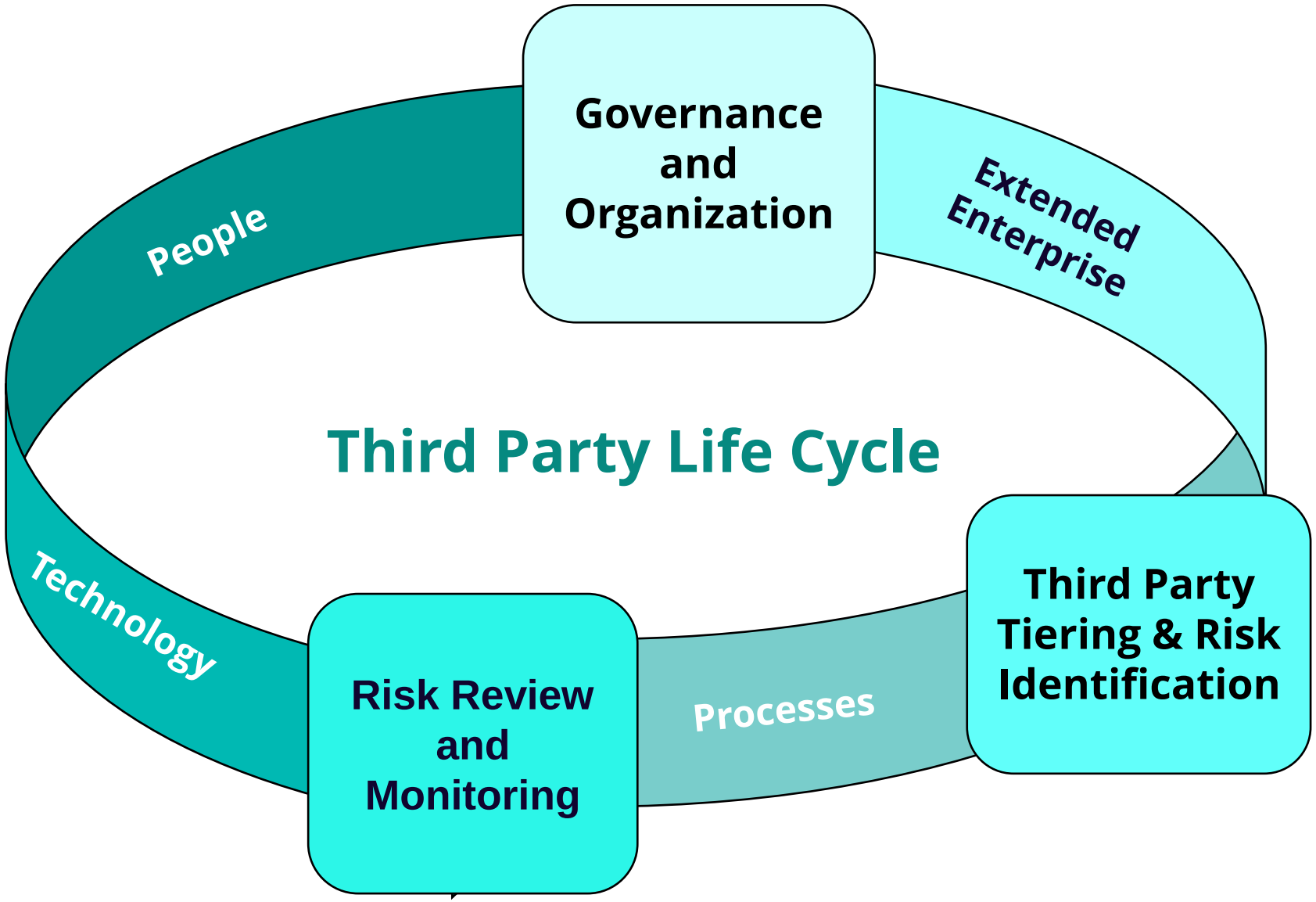
Goldman Sachs charged **$3.3 billion for FCPA** violations for payments through **Third party intermediary** in Malaysia and Abu Dhabi

More than reputational risk, third-party risks could impact the survival

Key Components of TPRM

metricstream
thrive on risk™

Integrated Third-Party Risk Management Framework



What is on Offer?

✓An **End-to-End** managed service

✓Broad **View of Risks and Performance** across the extended enterprise

✓**Real-time Identification of Risks and Mitigation** responses

Integrated Response to Risks

Need to Customize Based on the Risk profile. No One size Fits All

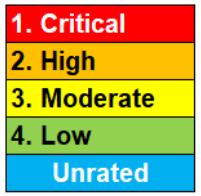
Key Components of TPRM

Governance

- Roles & Responsibilities
- Standards & Regulations
- Repeatable Processes

Tiering and Risk Identification

- Inventory of 3rd Party (nth party)
- Risk Identification
- Risk-Based Tiering
  -Questionnaire based or Manual



Risk Review and Monitoring

- Iterative Risk Review
- Informed Decision Making
- Monitoring

Third-Party Life Cycle Management

Onboarding

- Expectations
- Identify Risks
- Due diligence & Contract

Ongoing

- Risk Tiering and Stratification
- Manage Relationships and Risks
- Regular On-site or Off-site assessments

Off-boarding or Continue

- Monitor Risks
- Assess Impact
- Renew or Terminate

Governing Frameworks and Regulations

metricstream
thrive on risk™

Governing Frameworks and Regulations

Industry Standards

- ISO 27001 & 27036

  Information Security for Supplier Relationships

- NIST-SP 800-37

  Risk Management Framework

- SP 800-161

  Supply Chain Risk Management

- PCI-DSS Standards

  Third Party Security Standards for Safe Payments

- COBIT

  Framework by ISACA for governance and management of enterprise IT

No specific standard for 3rd parties; Various standards provide guidance to govern 3rd parties

Legal Regulations

- Office of the Comptroller of the Currency Guidance
- Federal Financial Institutions Examination Council Guidance
- Federal Deposit Insurance Corporation Guidance (FDIC)
- European Banking Authority Guidance
- Monetary Authority of Singapore (MAS) Guidelines
- UK Bribery Act
- The US Foreign Corrupt Practices ACT (FCPA):

Various new legislations on governance of Third-parties are being formulated

Challenges in Implementation and Leading Industry Practices

metricstream
thrive on risk™

Challenges and Leading Practices

Challenges	Leading Practices
Inadequate Management Support and Resources	**Established Tone at the Top** ▪ Board level oversight and buy-in from Senior Leadership ▪ Integrated Resource Support: In-house or Outsourced
No Formally Defined Policies and Procedures	**Effective Policies, Program, and Procedures** ▪ Well Defined Guidance with Roles & Responsibilities ▪ Aligned With Industry Standards and Regulations
Inadequate Awareness of Third Parties and Risks	**Risk Linkage with Critical Third Parties** ▪ Accurate Inventory of Third-party and Risk-based Tiering ▪ Risk Stratification
Point of Time Risk Assessment	**Iterative and Ongoing Risk Assessment** ▪ Life-cycle-Onboarding, Ongoing, and Off-boarding ▪ Regular Interaction and Oversight
Manual Processes (Excel) for Assessments and Metrics	**Technology Integrated with Business Process** ▪ Customized Software for Tracking and Assessment ▪ Metrics and KPIs on a Real-time Dashboard
Ineffective Evaluation	**Self-assessment and Independent Evaluation** ▪ Leverage Internal Audit to perform objective review ▪ Assess the capability and effectiveness

Q&A/ Open Discussion

metricstream
thrive on risk™