DEMYSTIFYING THE ENTERPRISE RISK MANAGEMENT (ERM) AND THIRD-PARTY RISK MANAGEMENT (TPRM) PROCESS

KEY COMPONENTS, BUILDING BLOCKS, CHALLENGES, MOVE TOWARDS INTEGRATED RISK MANAGEMENT

Wolfspeed® | SANJIV SHARMA | AUGUST 17, 2023

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

SANJIV SHARMA

PROFILE

Sanjiv Sharma

Vice President and Chief Audit Executive (CAE) at Wolfspeed Inc.

❑ **Education:** Certified Public Accountant (CPA), Certified Internal Auditor (CIA), and Certified Information Systems Auditor (CISA).

❑ **Current Responsibilities:** Enterprise Risk Management, Internal Audit, and SOX Compliance.

❑ **Past Experience:** NXP Semiconductor, Freescale Semiconductor, and Motorola in various leadership roles in Finance, Internal Audit, SOX Compliance, and Pricing in the US, Malaysia, China, and India.

❑ **Key Interests:** Environment, Social, and Governance (ESG) framework, Third-party Risk Management (TPRM) , and Cybersecurity frameworks and leveraging Enterprise Risk Management (ERM) for optimization.

❑ **Presentations:** Regular Presenter at National & International Conferences on various topics

AGENDA

Demystifying the Enterprise Risk Management (ERM) and Third-party Risk Management (TPRM) Process

Key Components, Building Blocks, Challenges, Move Towards Integrated Risk Management

ENTERPRISE RISK MANAGEMENT (ERM)

- Why ERM Is Important?
- Industry Standards
- Alignment Of Risks And Controls With Objectives
- ERM Governance Structure
- ERM Framework – Key Components & Activities
- Challenges and Learning Opportunities

THIRD PARTY RISK MANAGEMENT (TPRM)

- Third-party Threat Landscape and Associated Risks
- Building Blocks of the TPRM Framework
- Governing Frameworks and Regulations
- Leveraging Internal Audit to Optimize the TPRM
- Journey to TPRM Maturity
- Challenges and Learning Opportunities

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

DEMYSTIFYING THE ENTERPRISE RISK MANAGEMENT (ERM) PROCESS

ENTERPRISE RISK MANAGEMENT (ERM)

WHY IS IT IMPORTANT?

Helps Managing Change

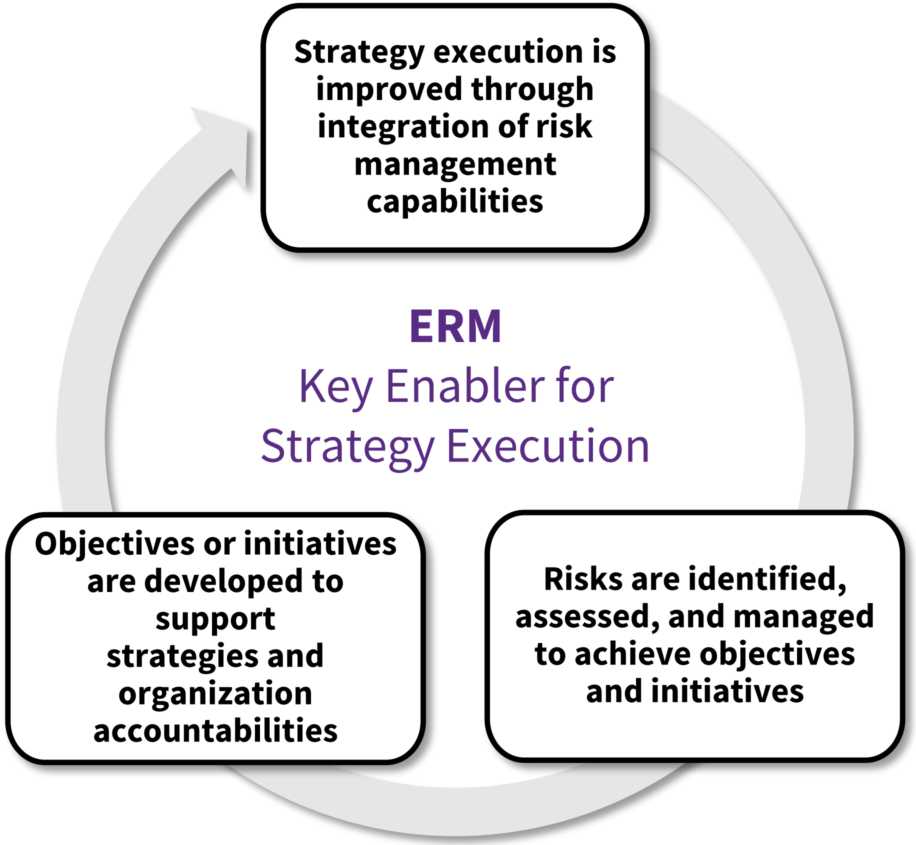
- Changes in competition, technology innovation, customer expectations, digital capabilities, supply chain and channel management.

Reducing Uncertainty

- Structured approach to better understand the alignment between business objectives, enterprise-wide risks, and management capabilities.
- Increase the likelihood of achieving objectives and reducing surprises

Meeting Stakeholder Expectations

- Standard-setting organizations like COSO, ISO and NACD provide guidance for ERM program development



ERM

Key Enabler for Strategy Execution

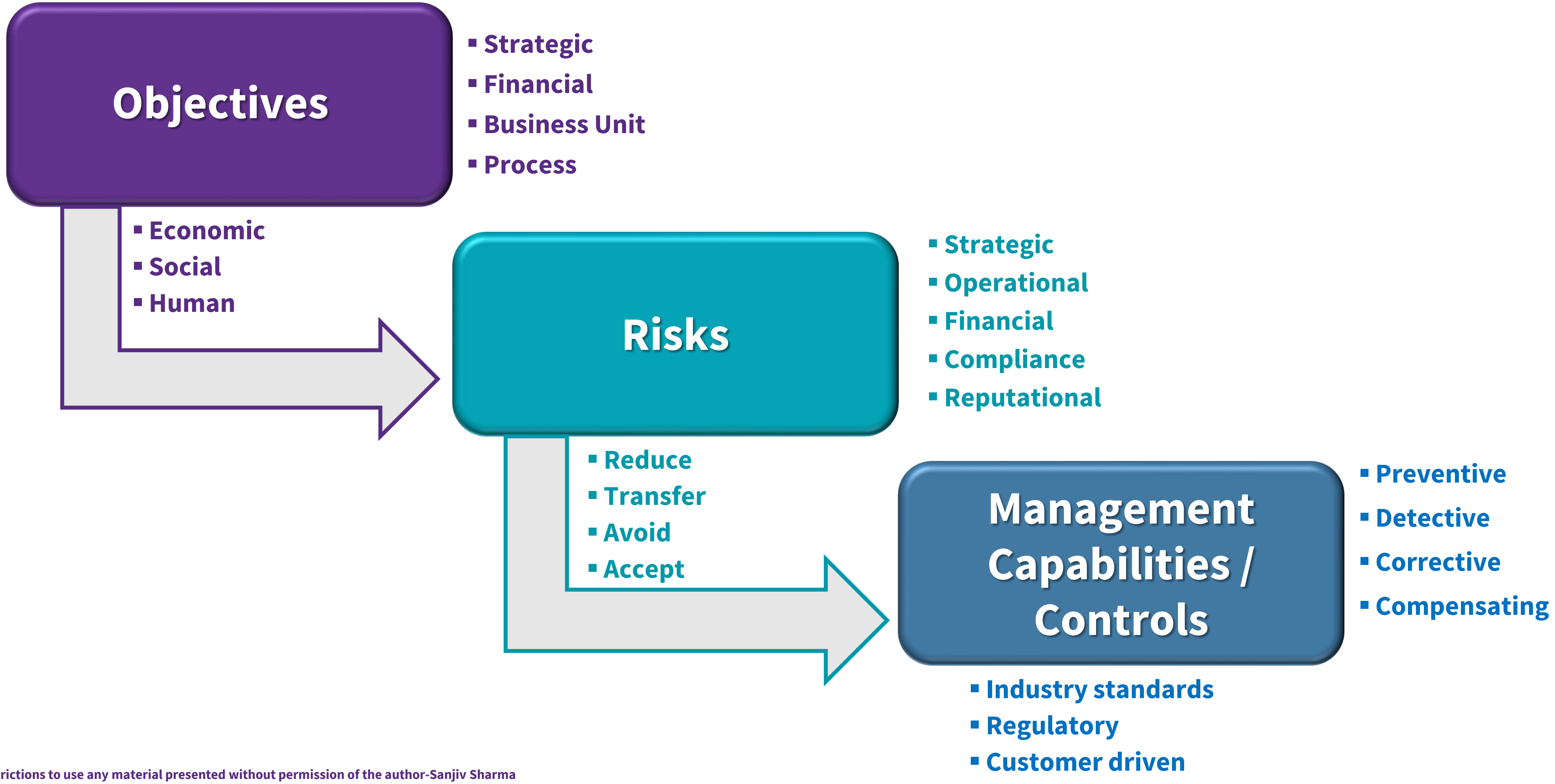
Strategy execution is improved through integration of risk management capabilities

Risks are identified, assessed, and managed to achieve objectives and initiatives

Objectives or initiatives are developed to support strategies and organization accountabilities

ALIGNMENT OF RISKS AND CONTROLS WITH OBJECTIVES

KEY ELEMENTS



Objectives

- Strategic
- Financial
- Business Unit
- Process

- Economic
- Social
- Human

Risks

- Strategic
- Operational
- Financial
- Compliance
- Reputational

- Reduce
- Transfer
- Avoid
- Accept

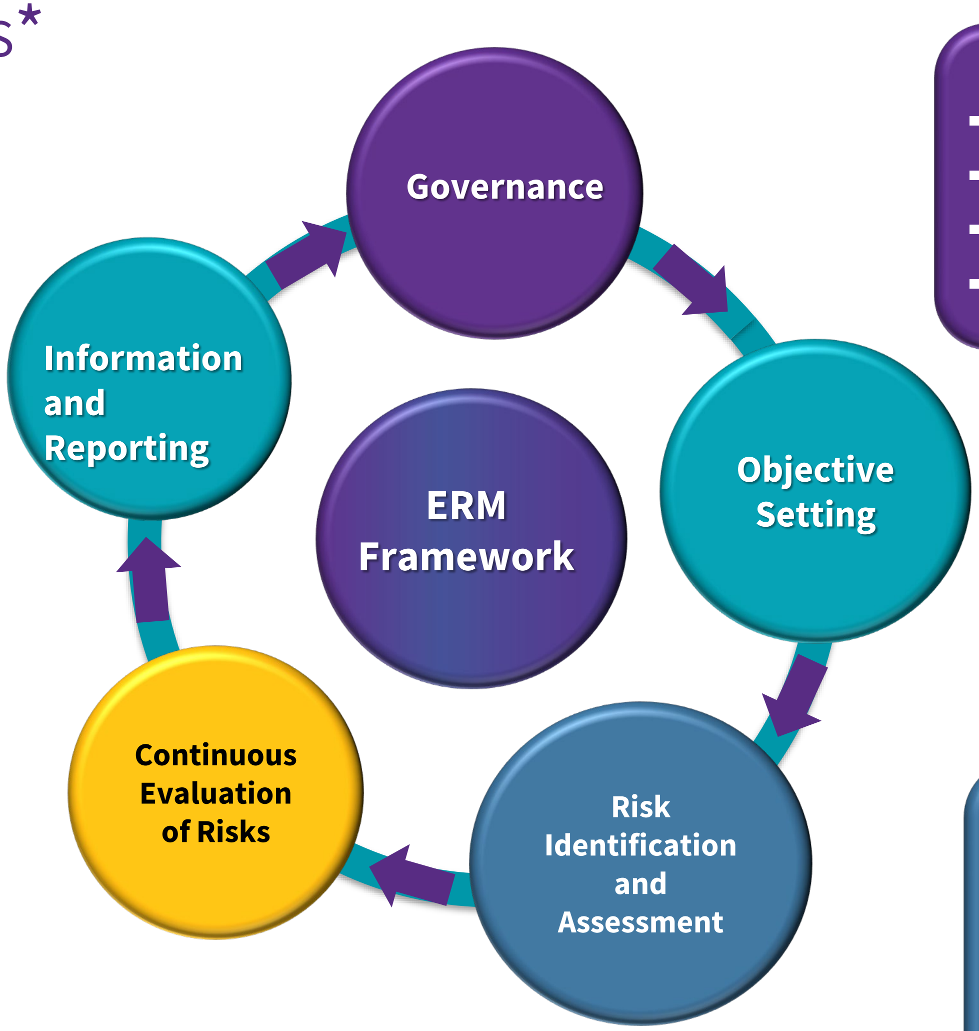
Management Capabilities / Controls

- Preventive
- Detective
- Corrective
- Compensating

- Industry standards
- Regulatory
- Customer driven

ERM FRAMEWORK

BEST PRACTICES/STANDARDS*


Governance
Objective Setting
Risk Identification and Assessment
Continuous Evaluation of Risks
Information and Reporting
ERM Framework

Governance

- Risk oversight structure
- Define Risk-aware culture
- Commitment to core values
- Attract, develop, and retain talent

Objective Setting

- Define strategy & objectives
- Analyze business environment
- Define risk appetite

Risk Identification and Assessment

(survey/interview)

- Identify risk
- Assess severity of risks
- Prioritize risks
- Implement risk plan

Continuous Evaluation of Risks

- Assess key changes
- Review risk and performance
- Pursue improvements

Information & Reporting

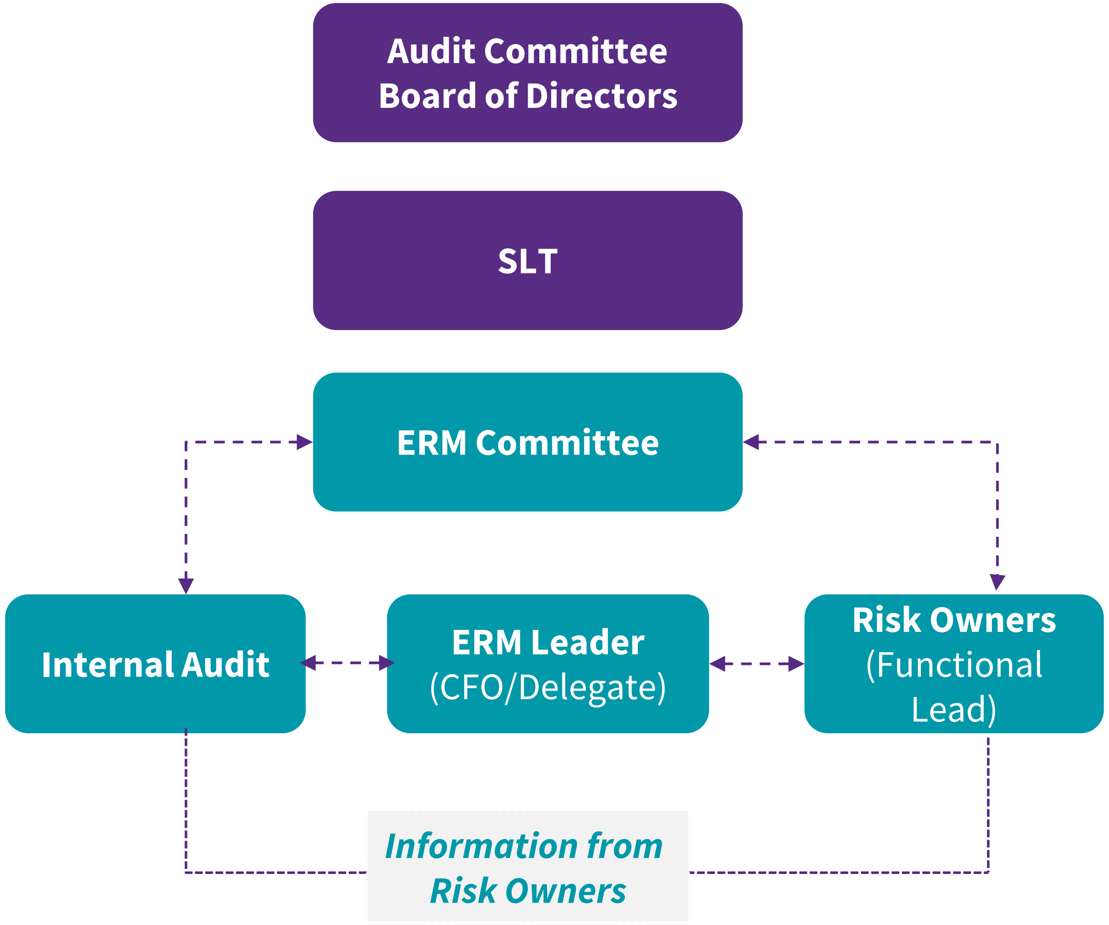
- Communicate risk information
- Reports on Risk
- Leverage technology

*Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Framework-Integrating with Strategy and Performance

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

ERM GOVERNANCE STRUCTURE

RISK OVERSIGHT



Note: Arrows above indicate communication flow rather than organizational reporting

Roles and Responsibilities

- **Audit Committee:** Oversee the alignment between Wolfspeed's strategic objectives and risk framework

- **SLT:** Direct resource allocation for the management of key risks to meet strategic objectives

- **ERM Committee:** Oversee the execution of the ERM Program *(identification, assessment, analysis, and reporting of key enterprise risks).*

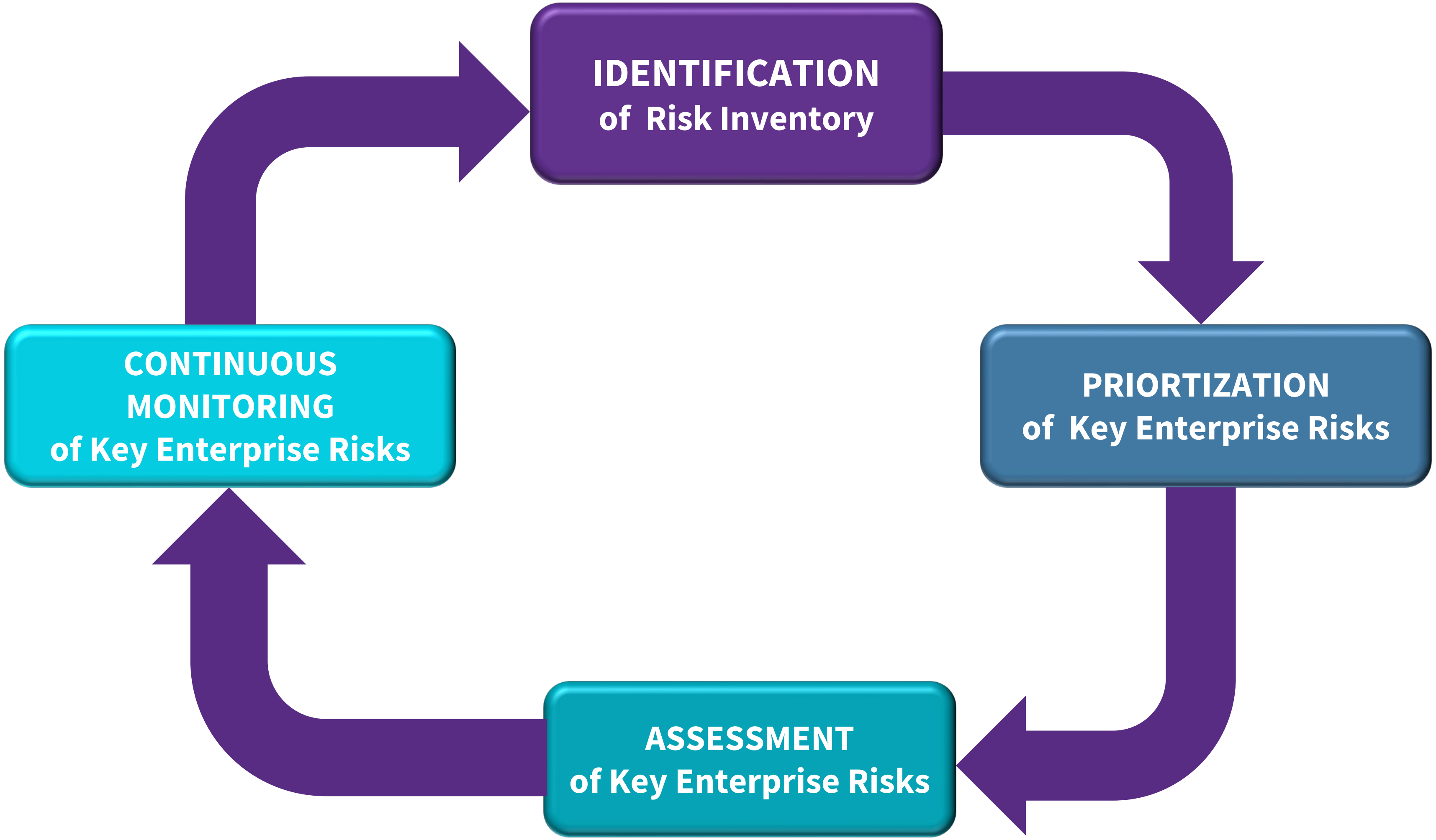
- **ERM Leader:** Facilitate ERM Program activities including risk assessments, risk plan development, risk reporting and education.

- **Risk Owners:** Manage respective enterprise risks, perform risk assessments and risk plans, and close gaps. Communicate with senior management about current and emerging risks.

- **Internal Audit:** Facilitate ERM program; Develop Risk-based Internal Audit Plan aligned with the Key ERM risks. Perform independent evaluation of risks and controls.

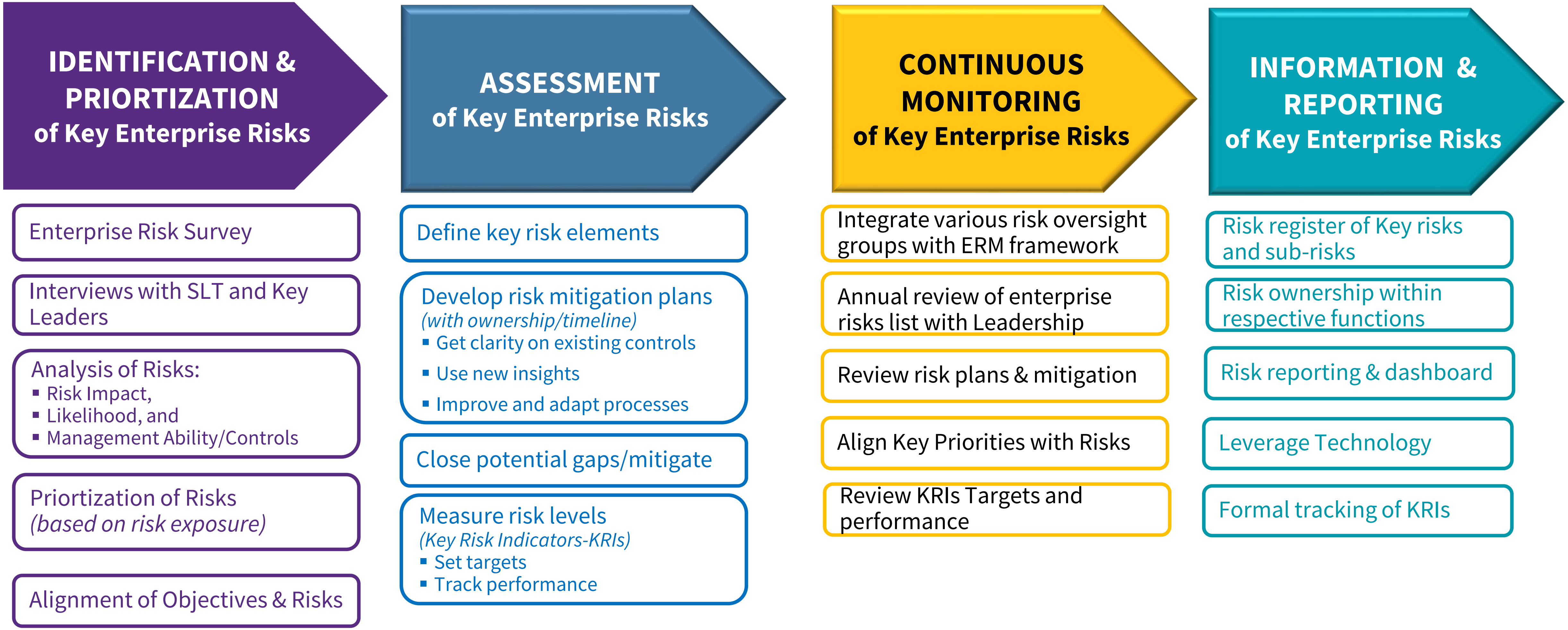
Restrictions to use any material presented without permission of the author-Sanjiv Sharma

ERM PROCESS
KEY COMPONENTS


IDENTIFICATION of Risk Inventory
PRIORTIZATION of Key Enterprise Risks
ASSESSMENT of Key Enterprise Risks
CONTINUOUS MONITORING of Key Enterprise Risks

ENTERPRISE RISK MANAGEMENT PROCESS

KEY PROCESS ELEMENTS



IDENTIFICATION & PRIORTIZATION of Key Enterprise Risks

- Enterprise Risk Survey
- Interviews with SLT and Key Leaders
- Analysis of Risks:
  - Risk Impact,
  - Likelihood, and
  - Management Ability/Controls
- Priortization of Risks *(based on risk exposure)*
- Alignment of Objectives & Risks

ASSESSMENT of Key Enterprise Risks

- Define key risk elements
- Develop risk mitigation plans *(with ownership/timeline)*
  - Get clarity on existing controls
  - Use new insights
  - Improve and adapt processes
- Close potential gaps/mitigate
- Measure risk levels *(Key Risk Indicators-KRIs)*
  - Set targets
  - Track performance

CONTINUOUS MONITORING of Key Enterprise Risks

- Integrate various risk oversight groups with ERM framework
- Annual review of enterprise risks list with Leadership
- Review risk plans & mitigation
- Align Key Priorities with Risks
- Review KRIs Targets and performance

INFORMATION & REPORTING of Key Enterprise Risks

- Risk register of Key risks and sub-risks
- Risk ownership within respective functions
- Risk reporting & dashboard
- Leverage Technology
- Formal tracking of KRIs

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

ERM PROCESS
KEY ACTIVITIES SUMMARY

RISK IDENTIFICATION AND PRIORITIZATION

Risk Inventory

- Evaluate Enterprise Risk Inventory and Profile

Inventory of risks in key categories

Enterprise Risk Prioritization

- Survey Inputs of Key Stakeholders
- Interviews with Management

To identify and prioritize risks

Review and Validation

- ERM Committee
- CFO and CEO

Agree on the results and next steps

RISK ASSESSMENT

Risk Plan

(Top XX Risks)

- Confirm owners of risks/sub-risks
- Define Preliminary Risk mitigation plans
  (Risk elements, management capability/ controls, Mitigation plans, and Key Risk Indicators etc.)
- Present to Risk Committee

Risk Plan Tracking

(Top XX Risks)

- Update Final Risk Mitigation Plans
  (Risk elements, management capability/ controls, Mitigation plans, and Key Risk Indicators etc.)
- Final Risk Plan presentation to ERM Committee

Final Risk Plan

(Top XX Risks)

- Presented to Audit Committee

RISK INVENTORY

SAMPLE RISKS

ENTERPRISE RISK INVENTORY		
I. EXTERNAL	**II. STRATEGIC**	**III. OPERATIONS**
E1. Competition E2. Technology Innovation & Customer Preferences E3. Economic and Geopolitical Conditions	S1. Strategy & Growth Plan Execution S2. Organizational Design S3. Industry & Customer Concentration S4. Product Development S5. Intellectual Property Management	O1. Plant Expansion O2. Product Quality O3. Business Continuity & Crisis Management O4. Operational Planning & Forecasting O5. Supply Chain Management
IV. PEOPLE	**V. INFORMATION TECHNOLOGY**	**VI. FINANCIAL AND COMPLIANCE**
P1. Culture P2. Integrity & Ethical Values P3. Health & Safety P4. Employee Recruitment & Retention	I1. IT Infrastructure & Digital Platform I2. Systems Implementation I3. Information Security	F1. Financial Liquidity F2. Shareholder Management F3. Currency & Interest Rate Management F4. Financial, Legal, and Regulatory Compliance

NAVIGATING THE CHALLENGES OF THIRD-PARTY RISK MANAGEMENT (TPRM)

DEFINITELY MORE THAN A CHECKBOX EXERCISE

CONTENTS

1 THIRD-PARTY THREAT LANDSCAPE AND ASSOCIATED RISKS

2 BUILDING BLOCKS OF THE TPRM FRAMEWORK

3 GOVERNING FRAMEWORKS AND REGULATIONS

4 LEVERAGING INTERNAL AUDIT TO OPTIMIZE THE TPRM

5 JOURNEY TO TPRM MATURITY

6 CHALLENGES AND OPPORTUNITIES

Third-Party Threat Landscape and Associated Risks

Third-Party Extended Enterprise

Understanding the Universe

What are Third Parties?

- Any external associate with which a company carries out its business activities.
- This includes both sales and supply channels [2]

Nature of Relationship

- Growing from the basic products or services to specialized services
- Extending beyond cafeteria or security services to business analytics, cloud services, and technology development etc.

Complexity of Arrangements

- Going beyond 3rd party to, 4th, or nth party *(sub-contractors)*
- Increasingly complex third-party landscape is also expanding the risk threats associated with it

"**81%** of organizations[1] had their **third-party network increase** in the past 3 years"

"Sales intermediaries (such as agents or distributors) may be more frequently abused than suppliers in order to relay corrupt" [2]

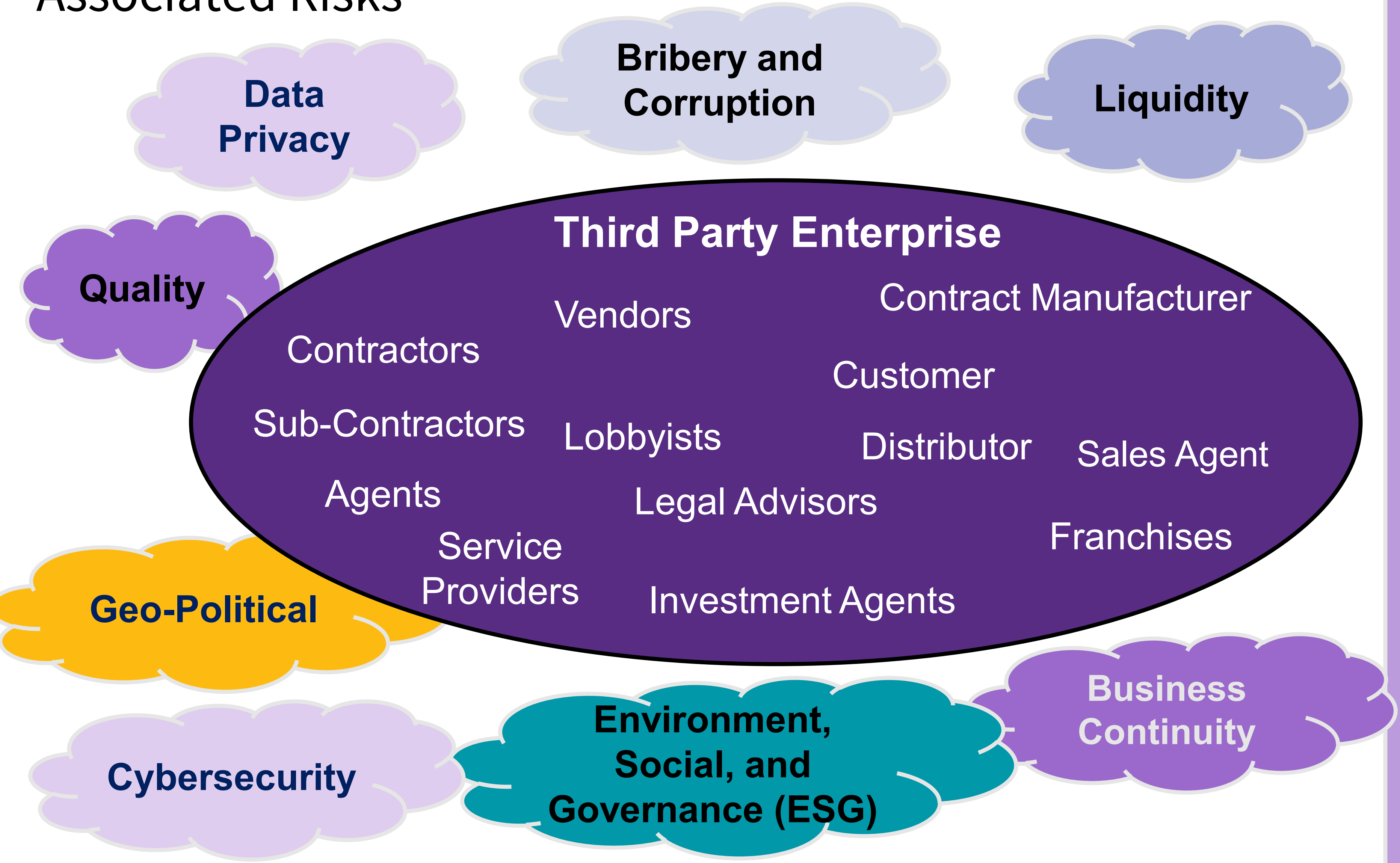
Source:

[1] 2022 Gartner Third-Party Risk Management Governance, Activities and Technology Survey

[2] Good Practice Guidelines on Conducting Third Party Due Diligence (Geneva: WEF, 2013)

Third Party Landscape

Associated Risks



Data Privacy

Bribery and Corruption

Liquidity

Quality

Third Party Enterprise

Vendors

Contract Manufacturer

Contractors

Customer

Sub-Contractors

Lobbyists

Distributor

Sales Agent

Agents

Legal Advisors

Service Providers

Franchises

Investment Agents

Geo-Political

Cybersecurity

Environment, Social, and Governance (ESG)

Business Continuity

Expanding Third-party Landscape is Bringing in Significant Risk Threats

- Margin pressures are driving explosion in growth
- More complex risks are emerging
- Risk threats are expanding beyond management controls

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

Key Third-Party Breaches

Reported in Recent Years

Gartner to pay $2.5M to settle alleged FCPA violations in South Africa

SITA Supply Chain Breach Hits Multiple Airlines

71% of Employees Globally Admit to Sharing Sensitive and Business-Critical Data Using Instant Messaging and Business Collaboration Tools,

A Casino Gets Hacked Through a Fish-Tank Thermometer

New type of supply-chain attack hit Apple, Microsoft and 33 other companies

How the SolarWinds hack and COVID-19 are changing cybersecurity spending

In 2022, third-party risks such as regulatory, compliance, business disruptions, and security incidents more than doubled over 2021

41% of companies experienced an impactful third-party data breach in the last 12 months, but rely on multiple overlapping tools and manual processes for incident response

(2023 Third Party Management Study by Prevalent)

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

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

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

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

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

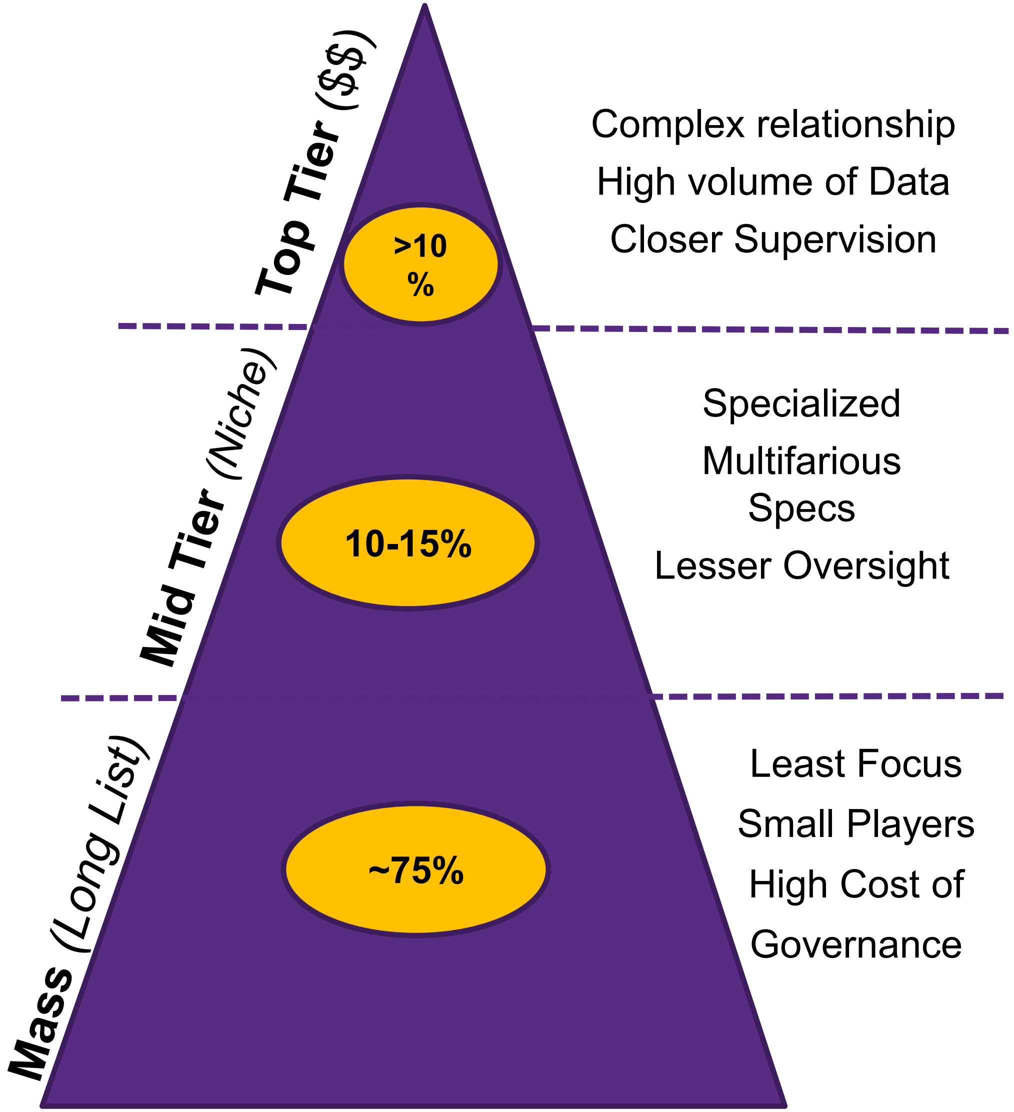
"Inadequate formal mechanism to assess or prioritize **ESG risks in the xtended enterprise"**. Deloitte's 2022 lobal Third-Party Risk Management Survey

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

What is Causing Third-Party Breaches and Risks ?

Possible Reasons

- Complexity of Arrangement of Relationships
- Lack of Adequate oversight over for 3rd and nth Parties
- Unchartered Privileged Access to the Third Parties
- Not Keeping pace with Changing Regulations



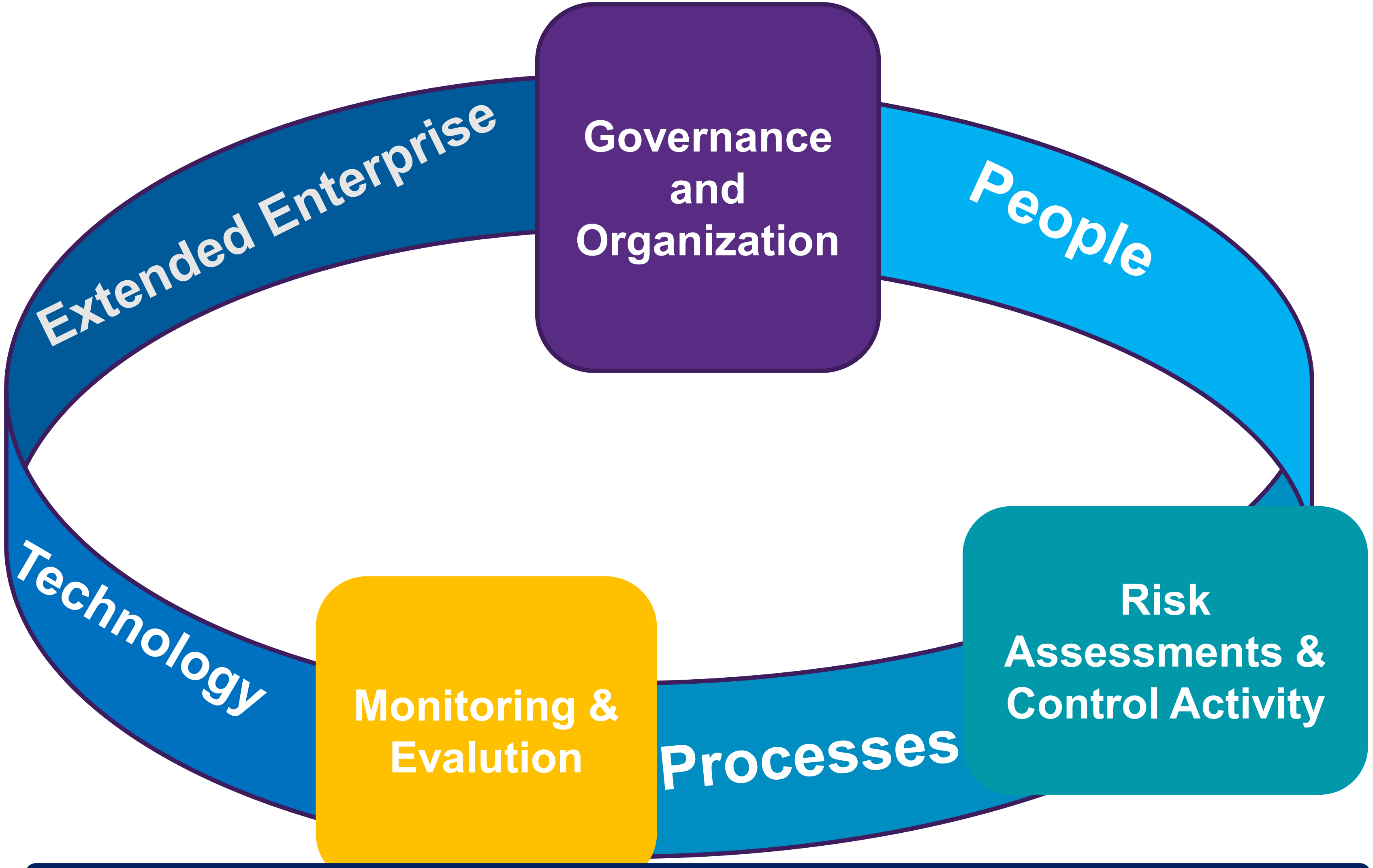
Third Party Base (*Numbers in %*)

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

Building Blocks of Third-Party Risk Management Framework

Establishing a Tailored TPRM Framework

Integrated with Business Processes



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

Deloitte's Global Third-party risk management survey 2022*

70% felt that an integrated TPM will increase efficiency by avoiding duplication and exploiting synergies

61% say that their priority is to simplify, standardize and integrate technology solutions to improve efficiency and reduce cost

* *1,309 responses from a wide range of organizations from about 38 countries*

Key Building Blocks for Success of TPRM

Critical Components

Governance and Organization

- Management Support
- Roles & Responsibilities
- Scope and Model
- Repeatable Processes

Risk Assessment and Control Activity

- Third-Party Inventory
- Risk-based Tiering*
  - Critical Third-Party
  - Non-Critical Third-Party
  - Unrated
- Risk Stratification
  - High Risk
  - Moderate Risk
  - Low Risk
- Iterative Risk Review in Contracting Life Cycle

  (see next slide for details)

Monitoring and Evaluation

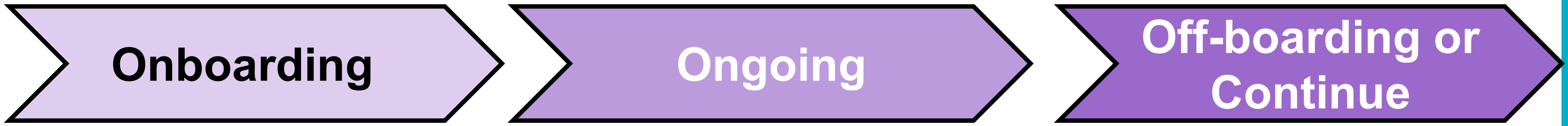
- Metrics and Scorecards
- Continuous Monitoring
- Issue Management
- Gap Identification and Required Actions

***Criticality Is Not a Risk Rating; Criticality indicates the impact on your operations**

Risk ratings or levels identify the types and amounts of risk present in the product or service and the relationship

Third-Party Contracting Life Cycle

Assessing Risks and Taking Charge



Onboarding

- Expectations
- Identify Risks
- Due diligence & Contract

Ongoing

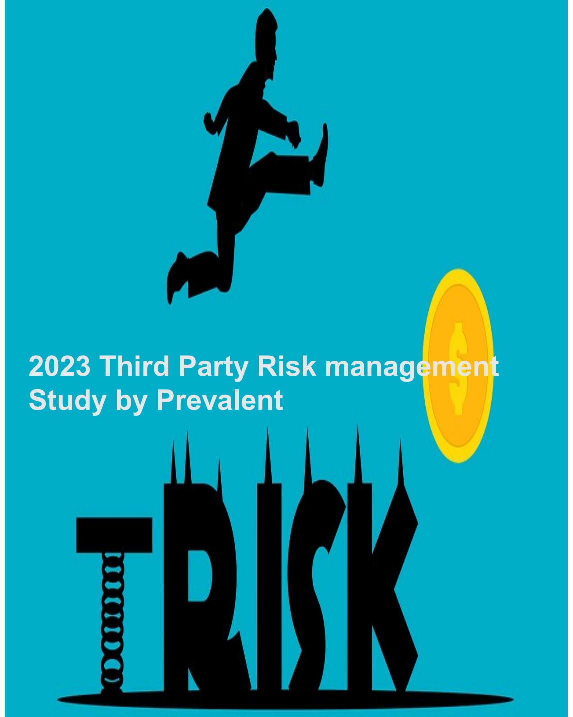
- Risk Tiering and Stratification
- Manage Relationships and Risks
- Regular On-site or Off-site assessments

Off-boarding or Continue

- Monitor Risks
- Assess Impact
- Renew or Terminate

~48% use spreadsheets to assess third parties.

~Only 47% track offboarding and 38% remediate risks, and 39% do nothing



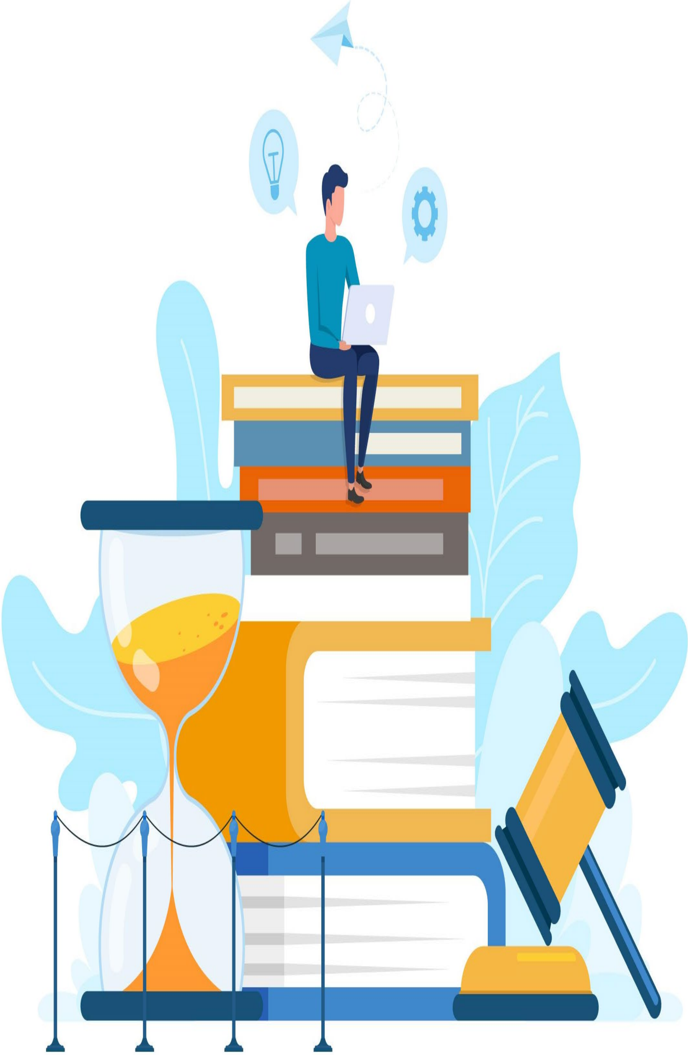
2023 Third Party Risk management Study by Prevalent

Move towards an “Iterative approach” from a traditional “Point of Time Review”

Navigating The Challenges of Third-Party Risk Management (TPRM)

Definitely More Than a Checkbox Exercise

Industry Standards and Regulations



Key Industry Standards and Regulations*

Governing Third-Parties

Industry Standards

ISO 27001 & 27036

Information Security for Supplier Relationships

NIST-SP 800-37 & 800-161

Risk Management Framework

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 some guidance

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):

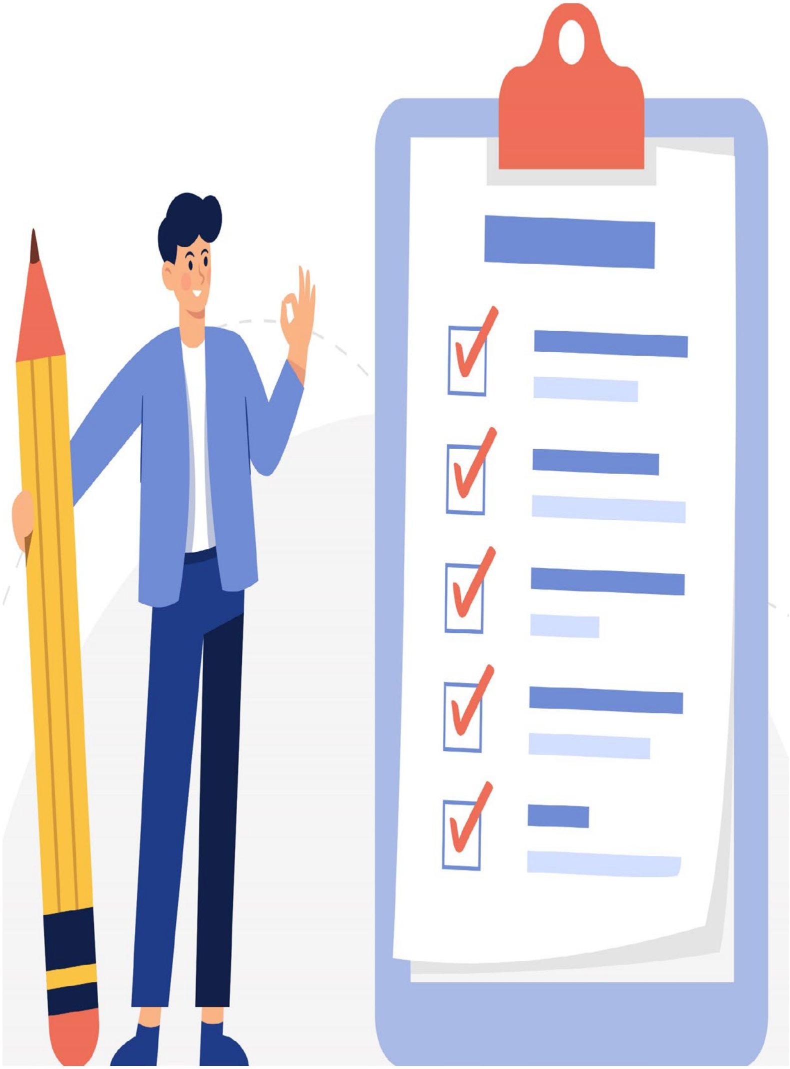
Various new legislations on governance of Third-parties are being formulated

** This is not an exhaustive list*

Navigating The Challenges of Third-Party Risk Management (TPRM)

Definitely More Than a Checkbox Exercise

Leverage Internal Audit



Leverage The Strengths Of Internal Audit

Assist in Identification and Ongoing Review and Monitoring

Review Governance of Third-Party Risk Framework

- Review Framework Governance
- Assess adherence to standards
- Identify regulatory compliance gaps
- Evaluate Classification of Risks of Parties

Contract Review of Third-Parties

- Review the Contracting Process
- Review contract terms to cover 4th and nth parties
- Ensure that following are included in the Contracts with Rights to:
  - Adherence to Company policies
  - Compliance to Code of Conduct
  - Completion of Required Trainings
  - Right to Audit
  - Right to Terminate

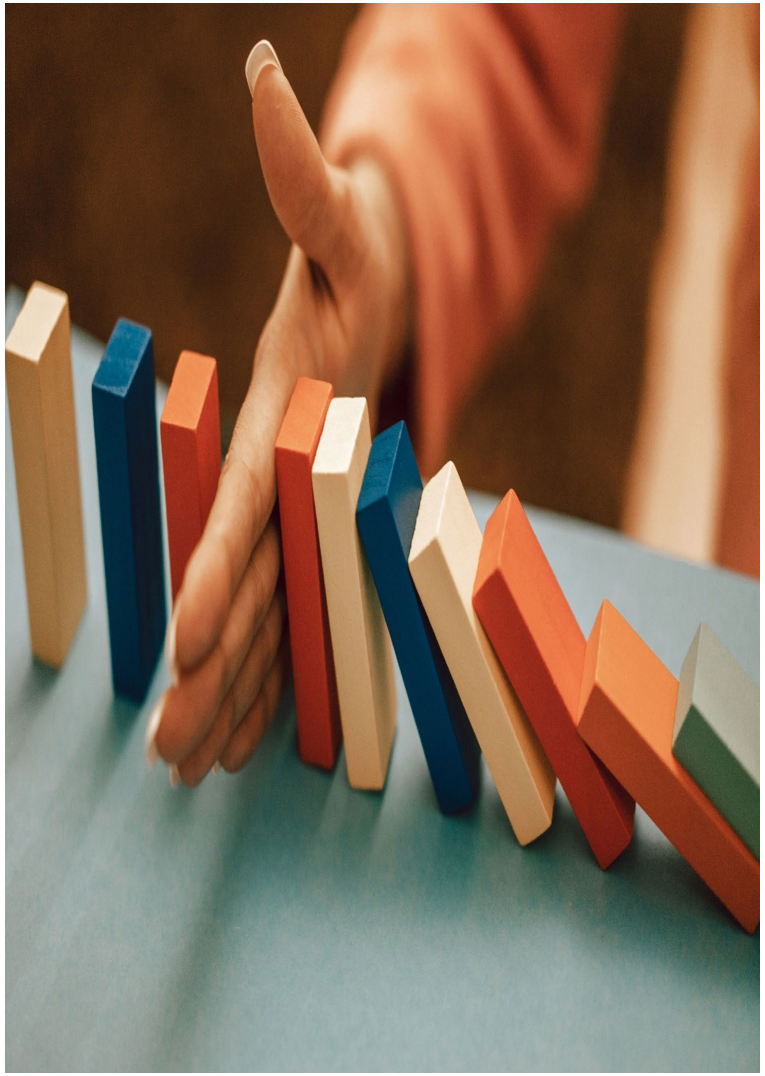
Audit of Third-Parties

- Conduct Audits based on Risks
  - 6 Months/More frequent audits
  - Annual Audits
  - Every 2-3 years
  - Checklist Review (no audit)
- Review the level of Continuous Monitoring of Third Parties
- Assess Third-Party Data and Access Management Risks
- Review SOC Reports & Compliance

Independent Review Of The Framework, Contracting Process, and Ongoing Conduct of Third-parties

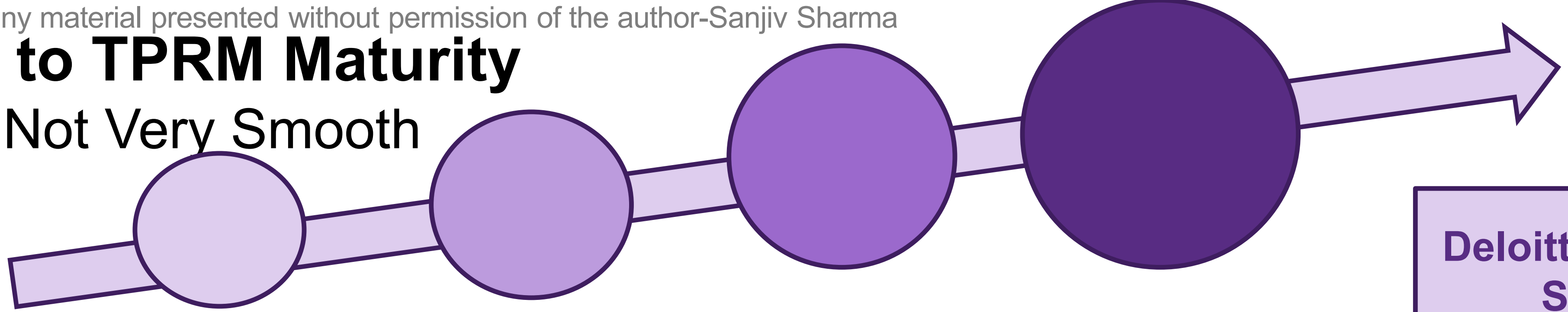
Restrictions to use any material presented without permission of the author-Sanjiv Sharma

Journey to TPRM Maturity



Journey to TPRM Maturity

Definitely Not Very Smooth



Area	Initial	Developing	Managed	Optimized
Governance	No formal governance	Limited Local Governance	Governance in some areas	Global Integrated Governance
Policies & Standards	No formal policies in place	Some local policies in place	Global policies but not fully integrated with processes	Global policies integrated with business processes
Business Processes	Few activities defined *(Fire fighting)*	Processes in silos. *(Reactive mode)*	Coordinated processes with some integration	Fully integrated process. Proactive
Tools & Technology	No use of technology	Limited use of technology	Adapted tools for reporting/monitoring	Customized & integrated tools for real time decisions
Risk Metrics & Reporting	No defined metrics or reporting	Limited/ad-hoc metrics and reporting	Business unit level metrics	Well defined Risk metrics and reporting KPIs in all areas
People & Organization	Low management input	Scattered Support	Invested executive support in silos	Executive support aligned with goals

Deloitte's TPRM Global Survey 2021*

~26% believed they were "Optimized" in TPRM maturity

49% believe need to enhance risk management processes

~53% want to improve real-time information, risk metrics and reporting

** 1,170 responses from TPRM associates from over 30 countries*

Pain Points and Opportunities in ERM or TPRM Framework Implementation

Key Challenges and Plans to Address the Gaps

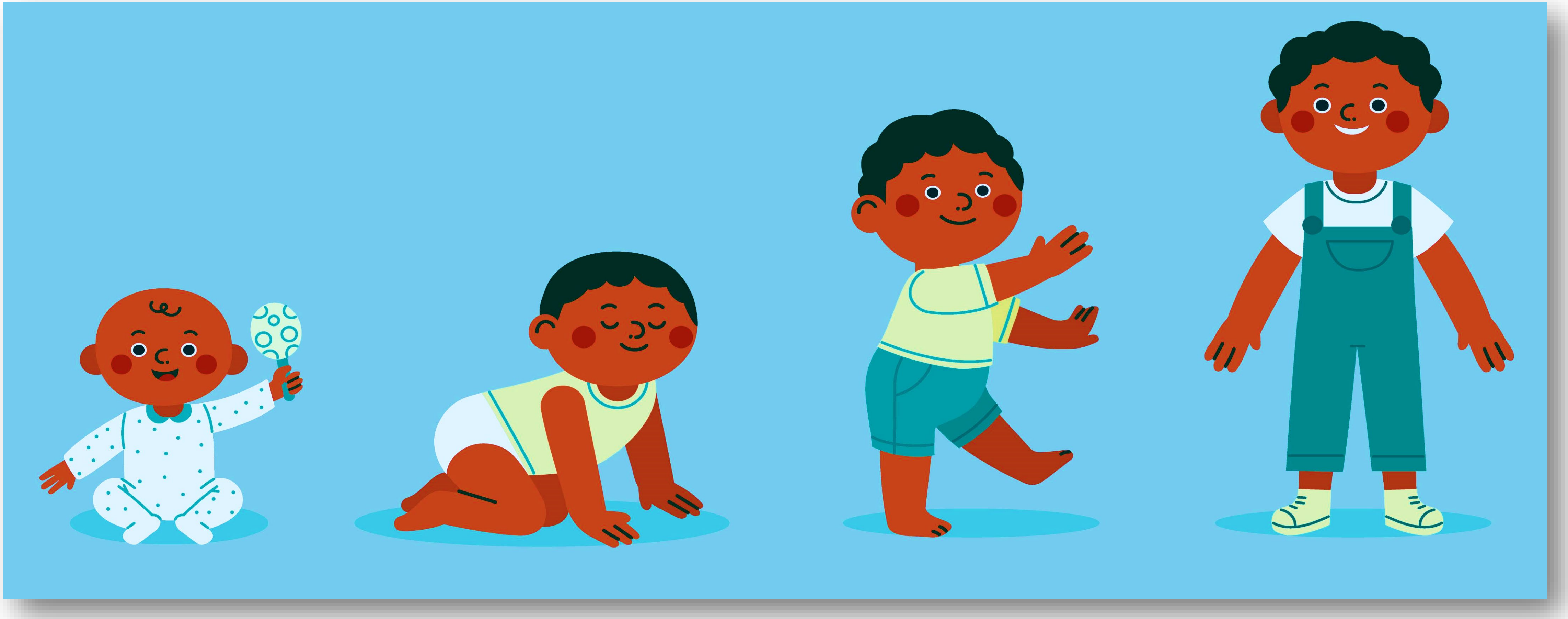
Area	Challenges	Opportunities
Tone at the Top	Lack of buy-in from Senior Leadership	Get early Management Buy-in
Risk Assessment Processes	Ad-hoc business process or no framework/inconsistency	Integrated business processes with functions leads to consistency
Standards and Regulations	Insufficient compliance to standards and regulations (as applicable)	Defined structure to comply with applicable standards and legal compliance
Stakeholder Interaction	Silo based implementation with poor coordination	Alignment across various function for end-to-end relationship life cycle
Risk Metrics and Quantification	Undefined risk metrics and poor Quantification. No use of Qualitative	Critical to define key risk metrics for tracking progress. Use of both Quantitative & Qualitative
Integrity of Data	Not a Check the Box Exercise	Need to ensure consistent compliance to guided instructions
Technology	Ad-hoc tools used with no integration	Integrated with business processes for consistent real time information
Monitoring	Risk of non-compliance	Fool proof the process adherence

Integrated Enterprise Risk Management

- Another important trend in ERM is the shift from a siloed and fragmented approach to a more holistic and integrated one.
- Integrated Enterprise risk management (IERM) is a framework that aims to connect and align the different risk functions, such as governance, compliance, audit, security, resilience, and sustainability, across the organization and its stakeholders.
- IERM enables a more comprehensive and consistent view of the risks and opportunities that affect the organization's objectives and performance, as well as a more coordinated and efficient response to them.
- IERM also supports the integration of risk management with other strategic functions, such as planning, budgeting, decision making, and reporting.
- ERM professionals need to embrace the IERM framework and foster a culture of collaboration and communication among the various risk actors and stakeholders.

Demystifying the Enterprise Risk Management (ERM) and Third-party Risk Management (TPRM) Process

Key Components, Building Blocks, Challenges, Move Towards Integrated Risk Management



Crawl, Walk, and Run

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

Demystifying the Enterprise Risk Management (ERM) and Third-party Risk Management (TPRM) Process

Key Components, Building Blocks, Challenges, Move Towards Integrated Risk Management

Q&A/ Open Discussion

Restrictions to use any material presented without permission of the author-Sanjiv Sharma

THANK YOU

Restrictions to use any material presented without permission of the author-Sanjiv Sharma