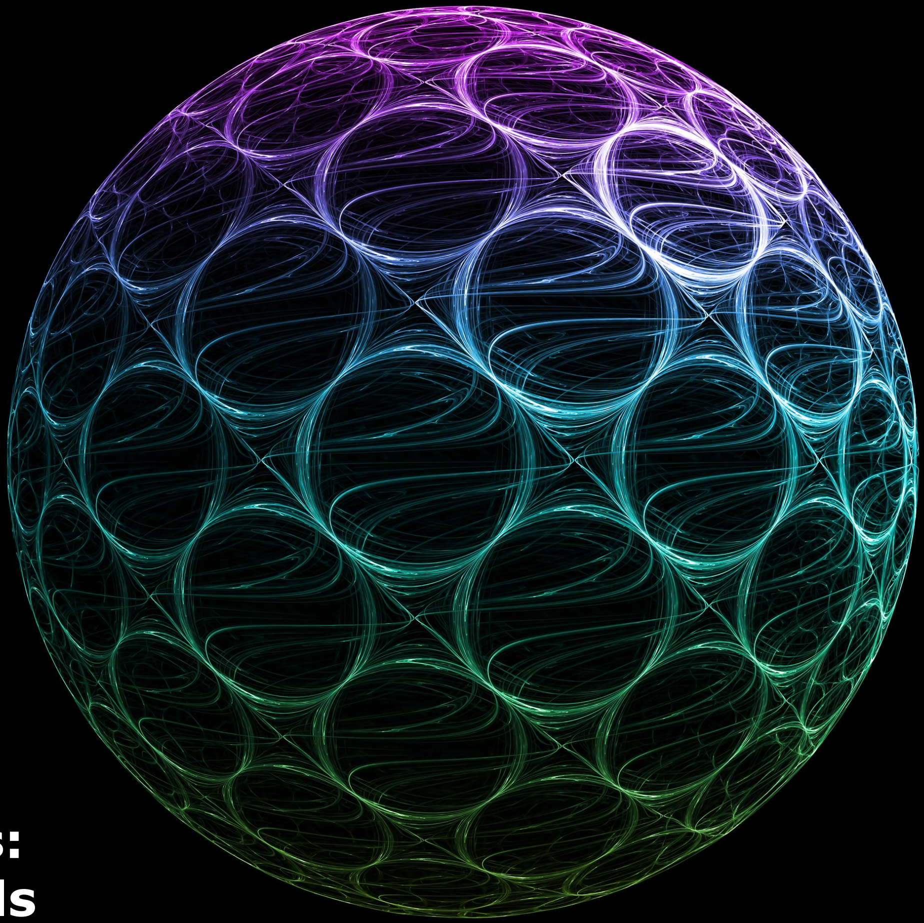
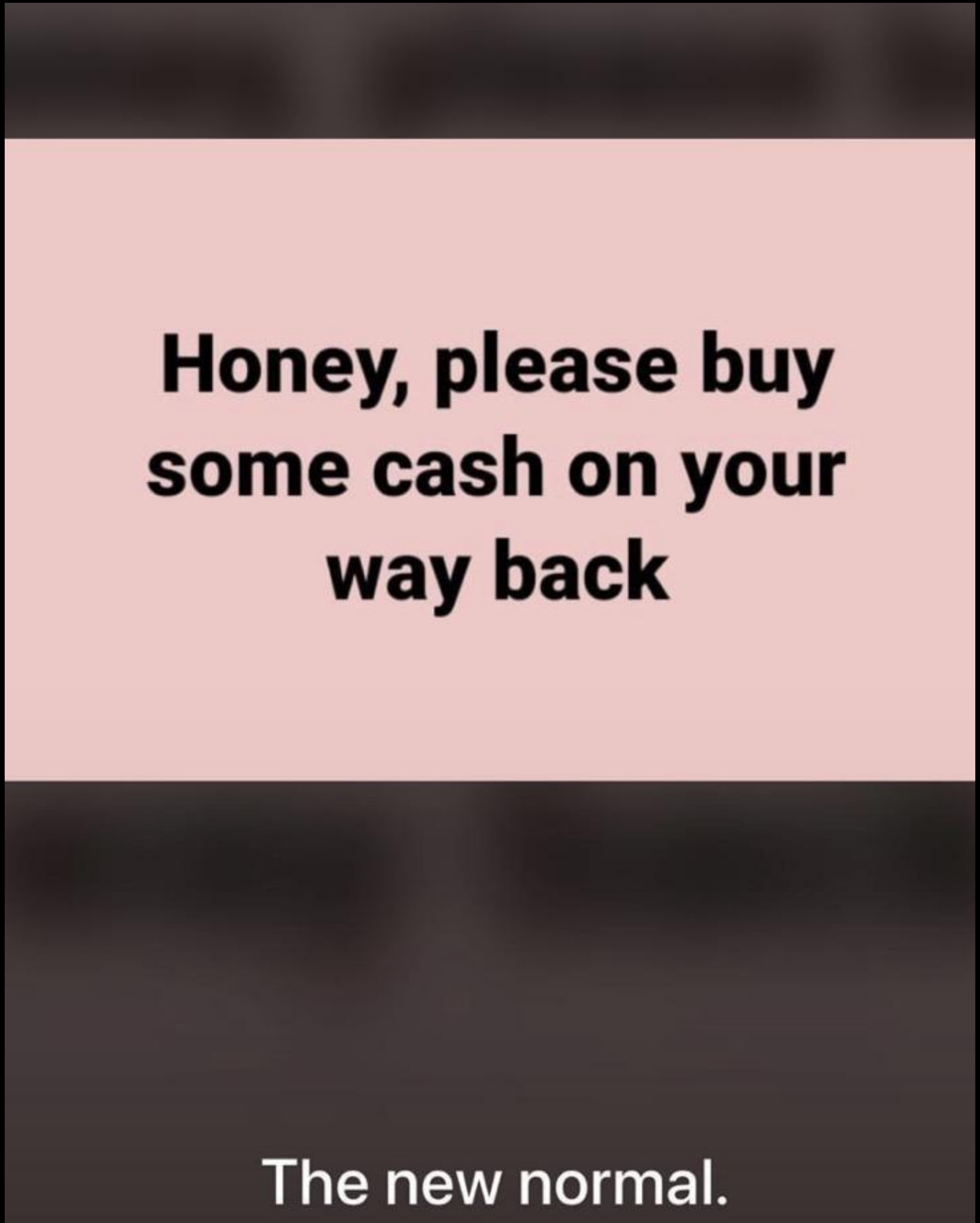


Embracing Emerging Risks: 3rd Party Risks and Controls

Funmilola Odumuboni
CISA, CISSP, CDPSE, CHFI, ISO 27001 LA
COBIT5 LI, OCP, ITIL V3

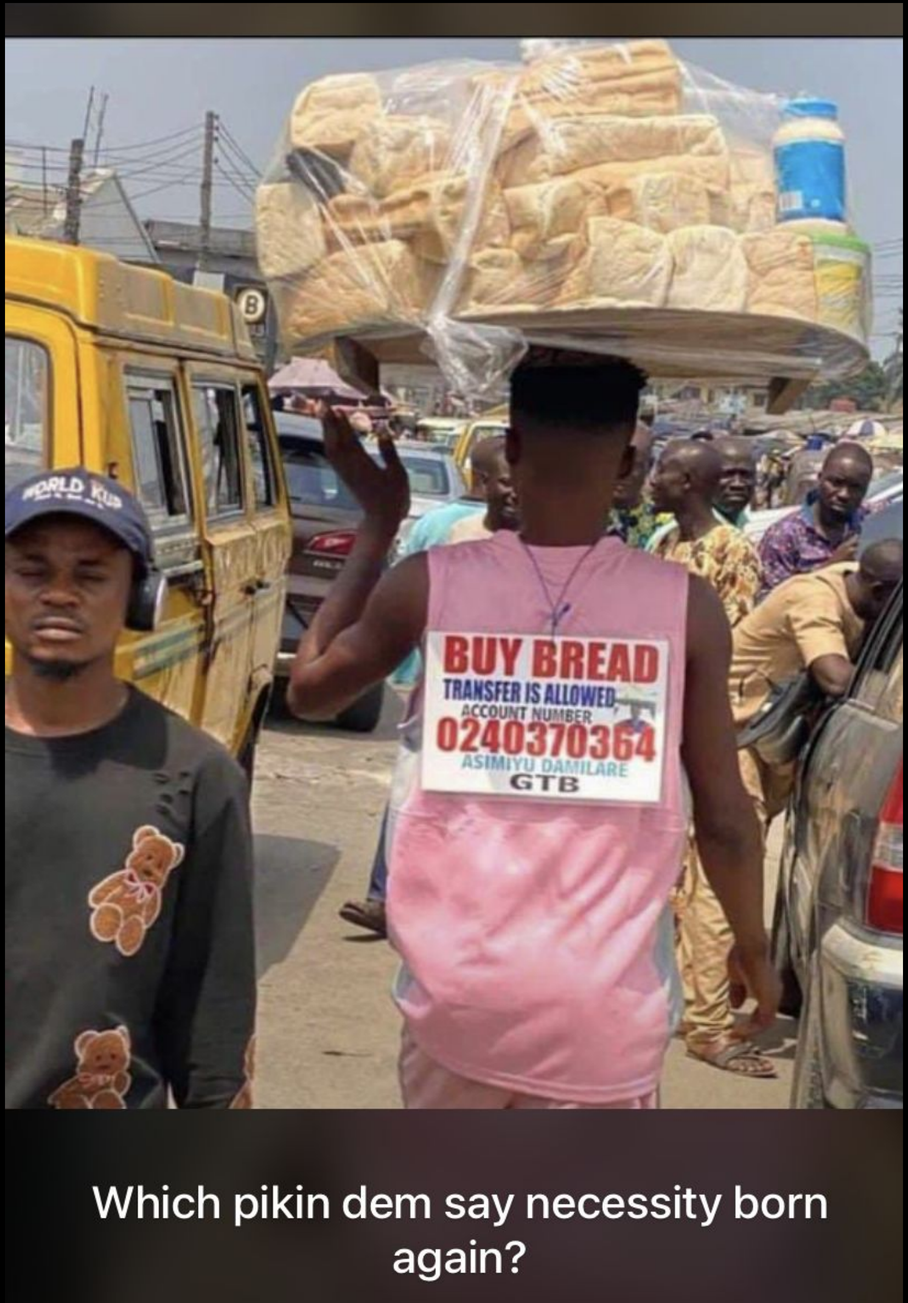
ACAEBIM AGM, March 2023

The New Normal



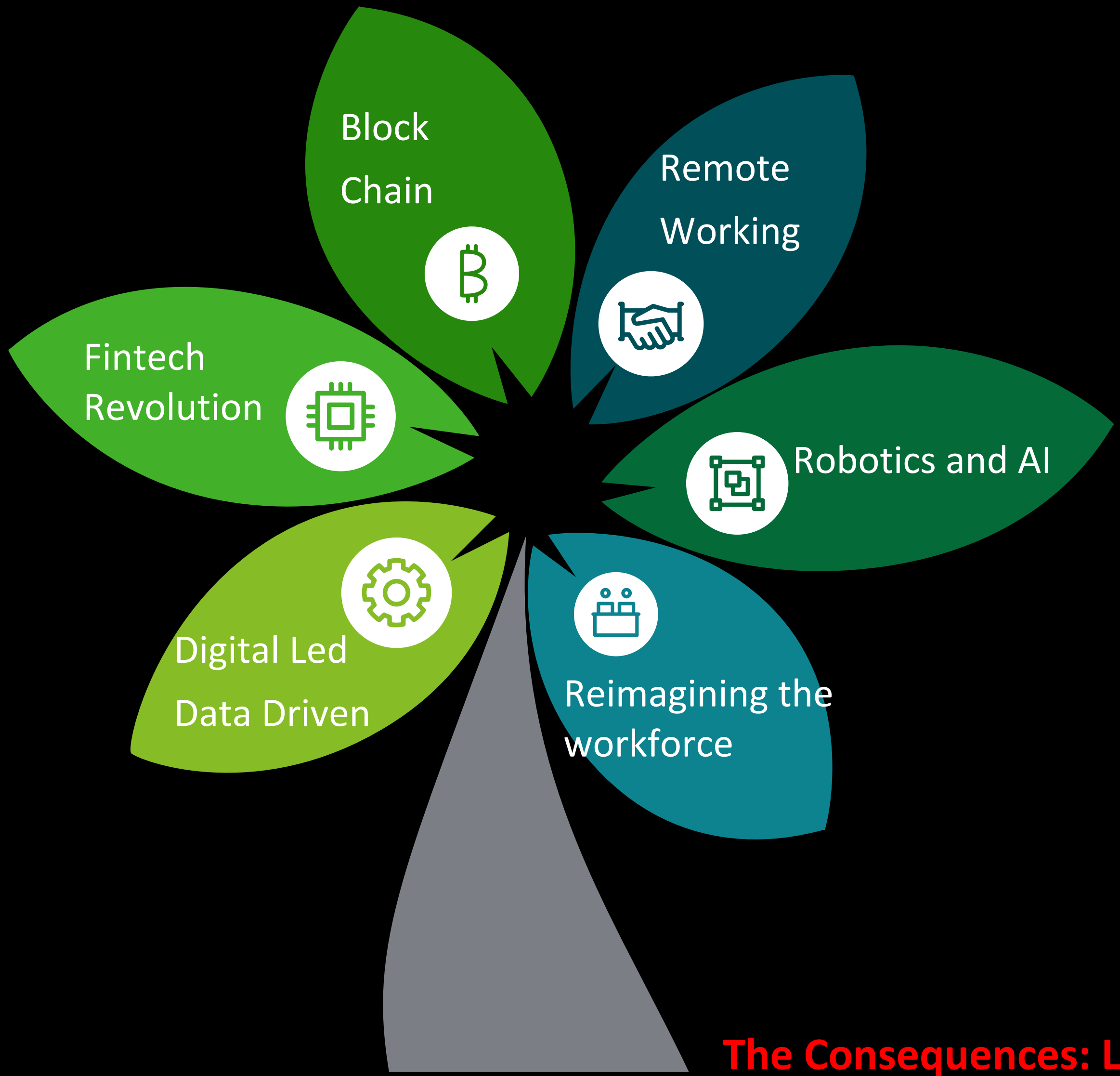
Honey, please buy some cash on your way back

The new normal.



Which pikin dem say necessity born again?

The Business Environment has Changed Forever…



Digital Led, Data Driven:
Shift to Technology centric products and solutions with proper customer orientation, using Data as new Oil

Fintech Revolution:
Need to collaborate to provide services to clients

Blockchain:
Adopt blockchain to drive digital currency, identity management, fraud management, investment etc

Remote working:
COVID-19 led to the deployment of technology across several companies to support remote working

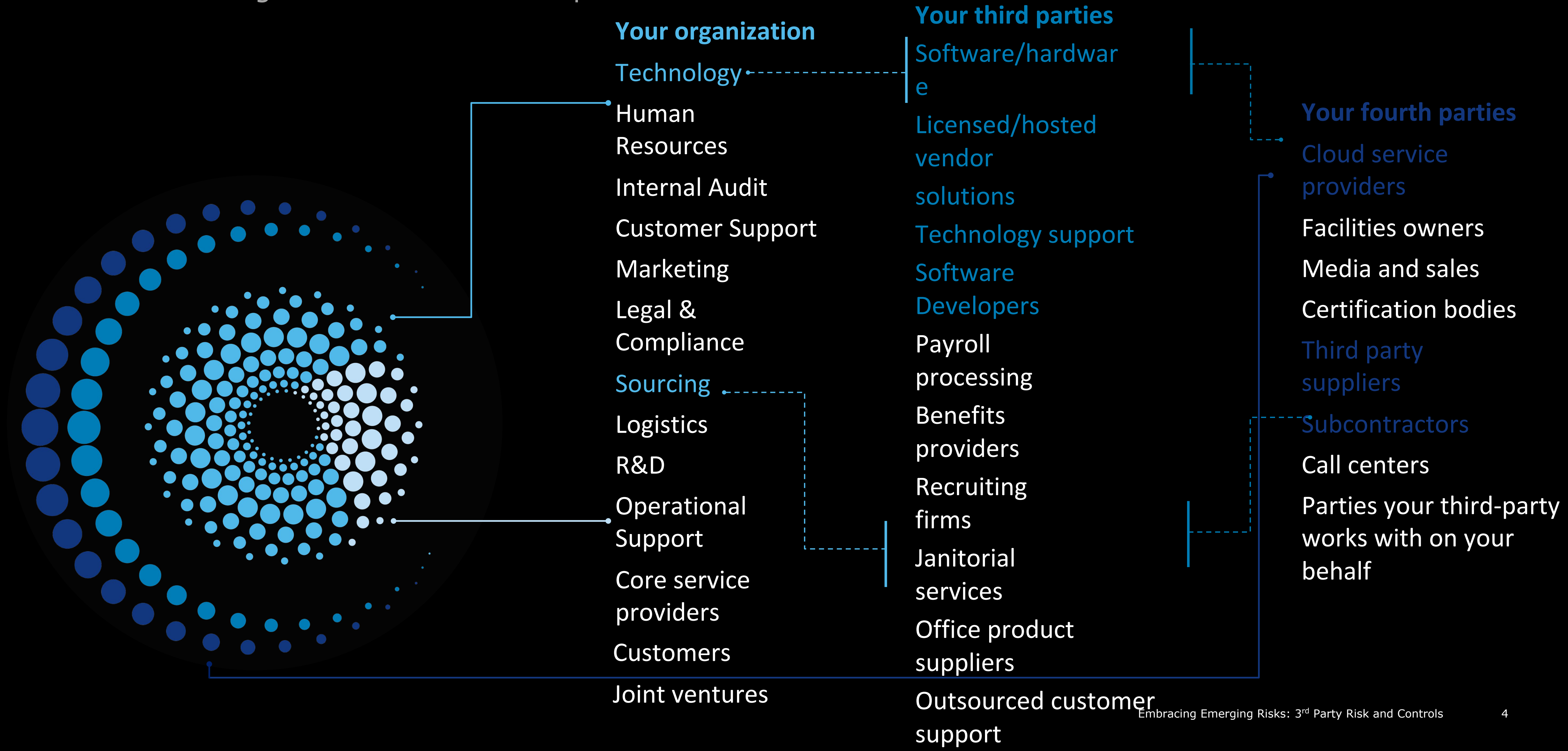
Robotics and AI:
Leverage AI-enabled back-office operations; drive customer loyalty

Reimagining the workforce:
Rethink future talent in line with expanding automation and diversity; balance between Humans and Machines

The Consequences: Larger Risk Landscape

The rising importance of third-party risk management

Third parties are no longer just managing ancillary activities, but driving critical activities in core parts of the business—extending the walls of the enterprise



Your organization

- Technology
- Human Resources
- Internal Audit
- Customer Support
- Marketing
- Legal & Compliance
- Sourcing
- Logistics
- R&D
- Operational Support
- Core service providers
- Customers
- Joint ventures

Your third parties

- Software/hardware
- Licensed/hosted vendor solutions
- Technology support
- Software Developers
- Payroll processing
- Benefits providers
- Recruiting firms
- Janitorial services
- Office product suppliers
- Outsourced customer support

Your fourth parties

- Cloud service providers
- Facilities owners
- Media and sales
- Certification bodies
- Third party suppliers
- Subcontractors
- Call centers
- Parties your third-party works with on your behalf

Foundational third-party risks span multiple domains

When considering 3rd party risks it is important to look at it wholistically

Cyber/Information Security

Resiliency

Compliance

Anti-bribery and Corruption

Spectrum of Risks

Environmental

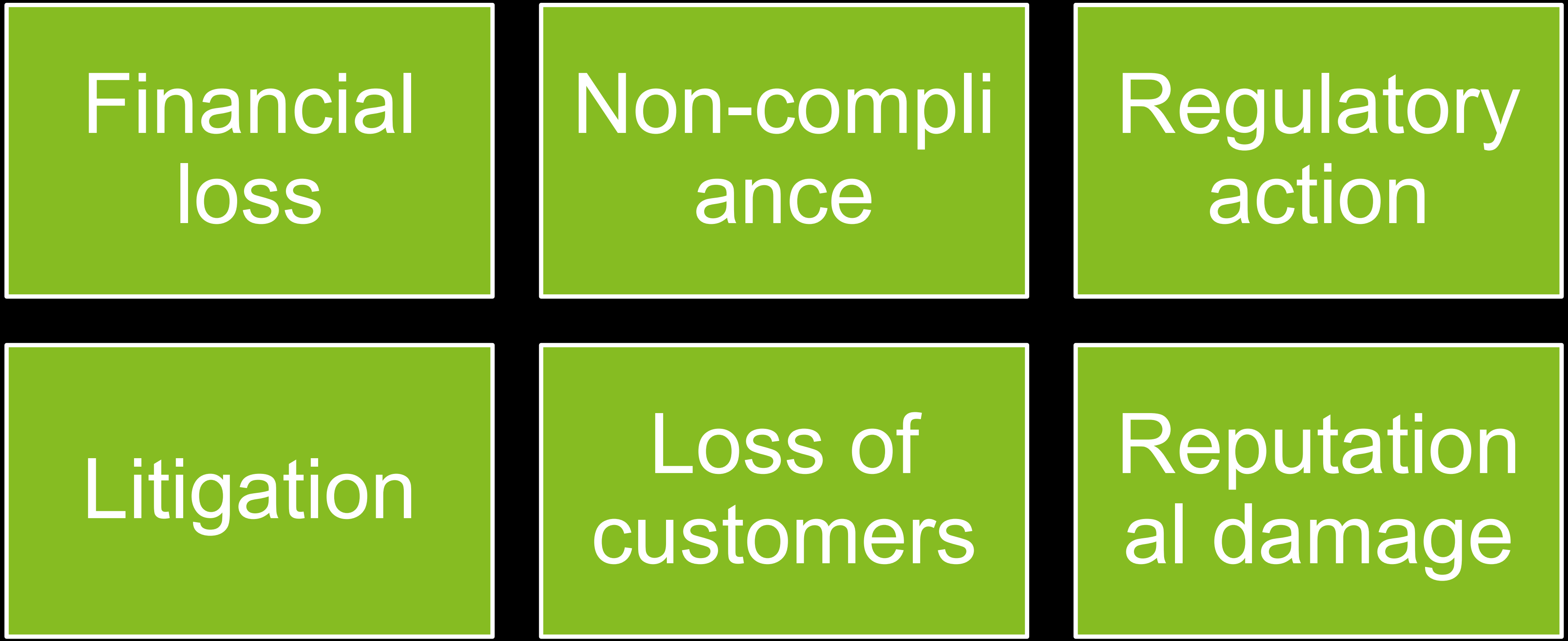
Fourth Parties

Reputation and Conduct

Financial Viability

Consequences of poorly managed 3rd party risks

Third-party arrangements may reduce management’s direct control. If not properly managed, third-party arrangements may result in several issues for the enterprise.



Financial loss

Non-compliance

Regulatory action

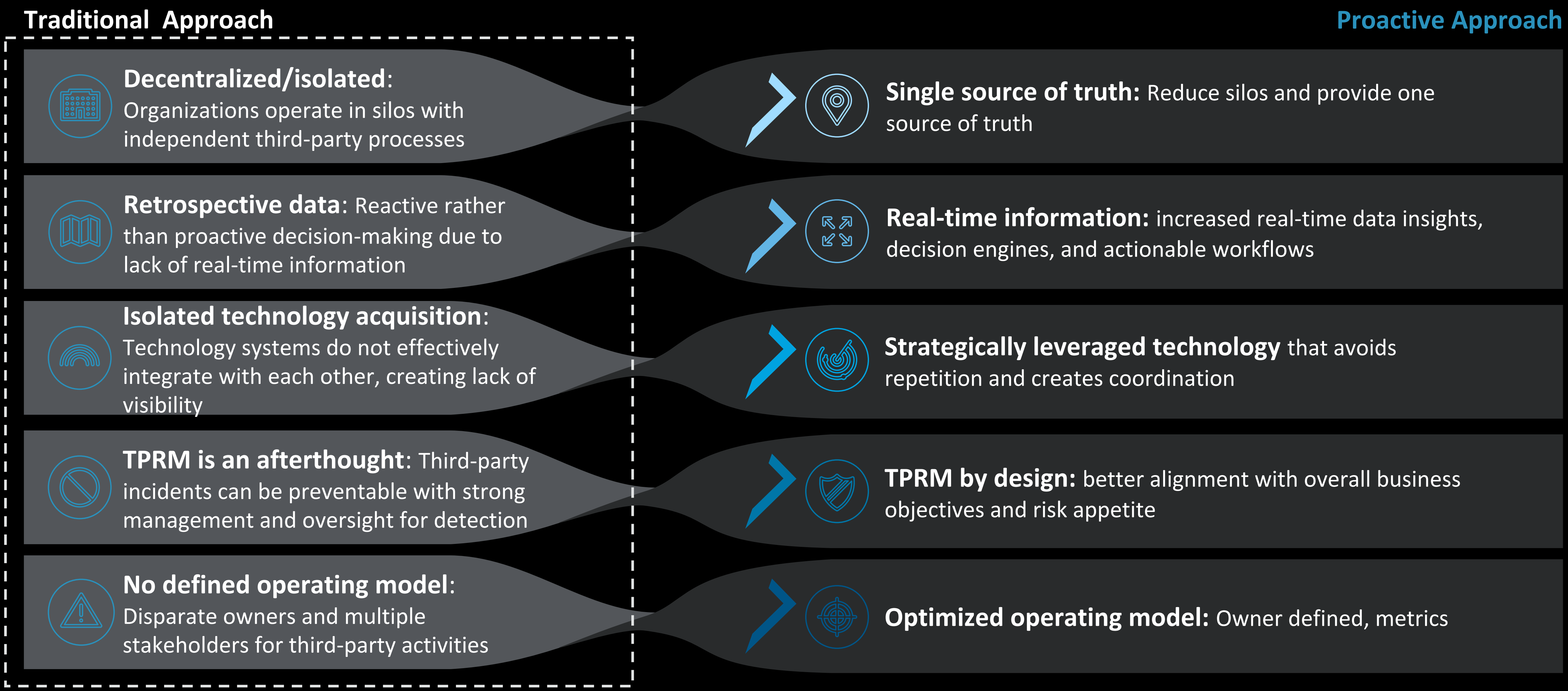
Litigation

Loss of customers

Reputational damage

Traditional third-party risk management may not be effective for emerging risks

In order to prevent third-party incidents, organizations should shift their perspective to developing integrated and proactive programs



Traditional Approach

Decentralized/isolated: Organizations operate in silos with independent third-party processes

Retrospective data: Reactive rather than proactive decision-making due to lack of real-time information

Isolated technology acquisition: Technology systems do not effectively integrate with each other, creating lack of visibility

TPRM is an afterthought: Third-party incidents can be preventable with strong management and oversight for detection

No defined operating model: Disparate owners and multiple stakeholders for third-party activities

Proactive Approach

Single source of truth: Reduce silos and provide one source of truth

Real-time information: increased real-time data insights, decision engines, and actionable workflows

Strategically leveraged technology that avoids repetition and creates coordination

TPRM by design: better alignment with overall business objectives and risk appetite

Optimized operating model: Owner defined, metrics

Common challenges to the traditional approach

What is preventing organizations from getting what they want out of their current programs?

Inadequate risk management

Inadequate third-party attestations and traditional check-the-box assessments can create a **limited understanding** of the **nature and criticality** of an organization's third-party relationships.

Limited legal means

Limited contractual and legal means to perform third-party oversight exposes organizations to **risk, lost value**, and can **inhibit proper monitoring** of critical business activities.

Lack of data

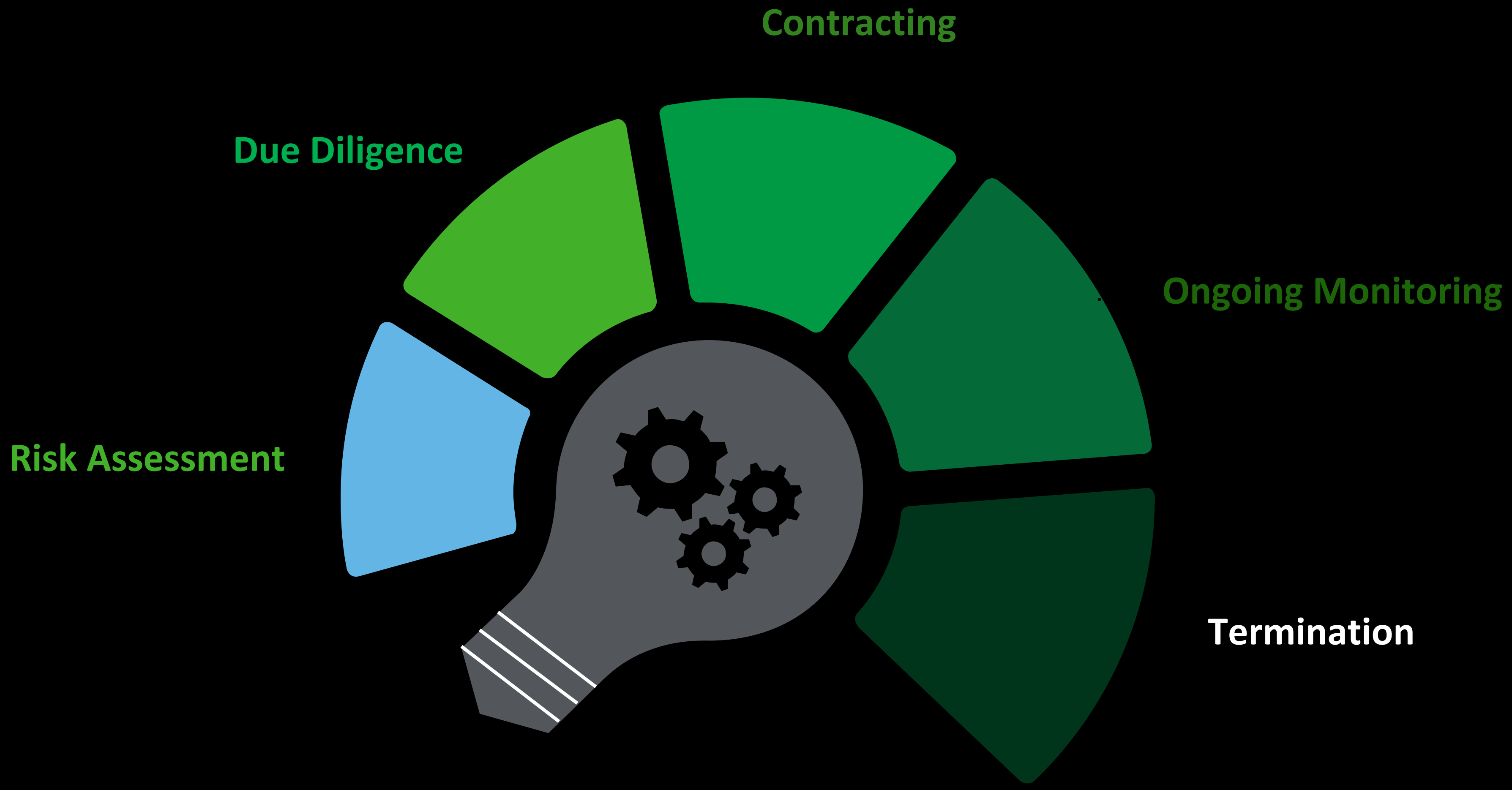
Many organizations lack transparent, detailed, **aggregated sources of data** that help them manage risk in real time. Insufficient access to real-time, decision-making data and analytics can **increase third-party engagement costs** across the enterprise.

External customer requests

Requests for information from customers coming through various channels at **increasing speeds** and levels of **complexity** are placing pressure on organizations without visibility into their third-party activities.

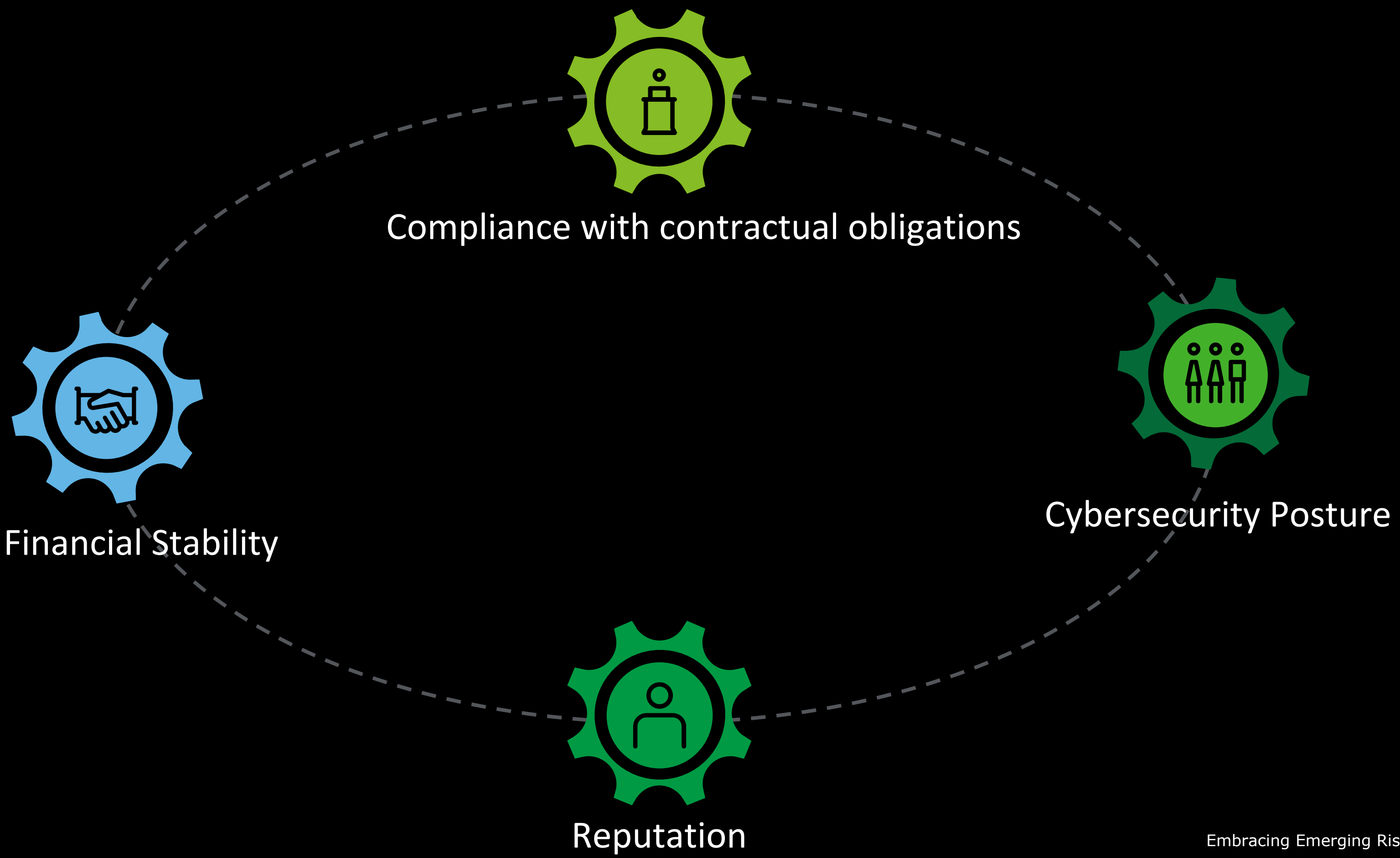
Comprehensive framework for managing third-party risk

A comprehensive framework for managing third-party risk includes several key components, which can help organizations identify, assess, monitor, and mitigate third-party risks. Here are some of the essential elements of a comprehensive third-party risk management framework:



Ongoing Monitoring - Metrics to Monitor Third-party Performance

A very essential part of a third-party relationship is continuous performance monitoring. Some of the major metrics for third-party monitoring are:


Compliance with contractual obligations

Financial Stability

Cybersecurity Posture

Reputation

Third-party risk management framework:

Termination

Reasons for having a Detailed Plan for Terminating Third-party Relationships

To mitigate risks and protect the organization's interests.

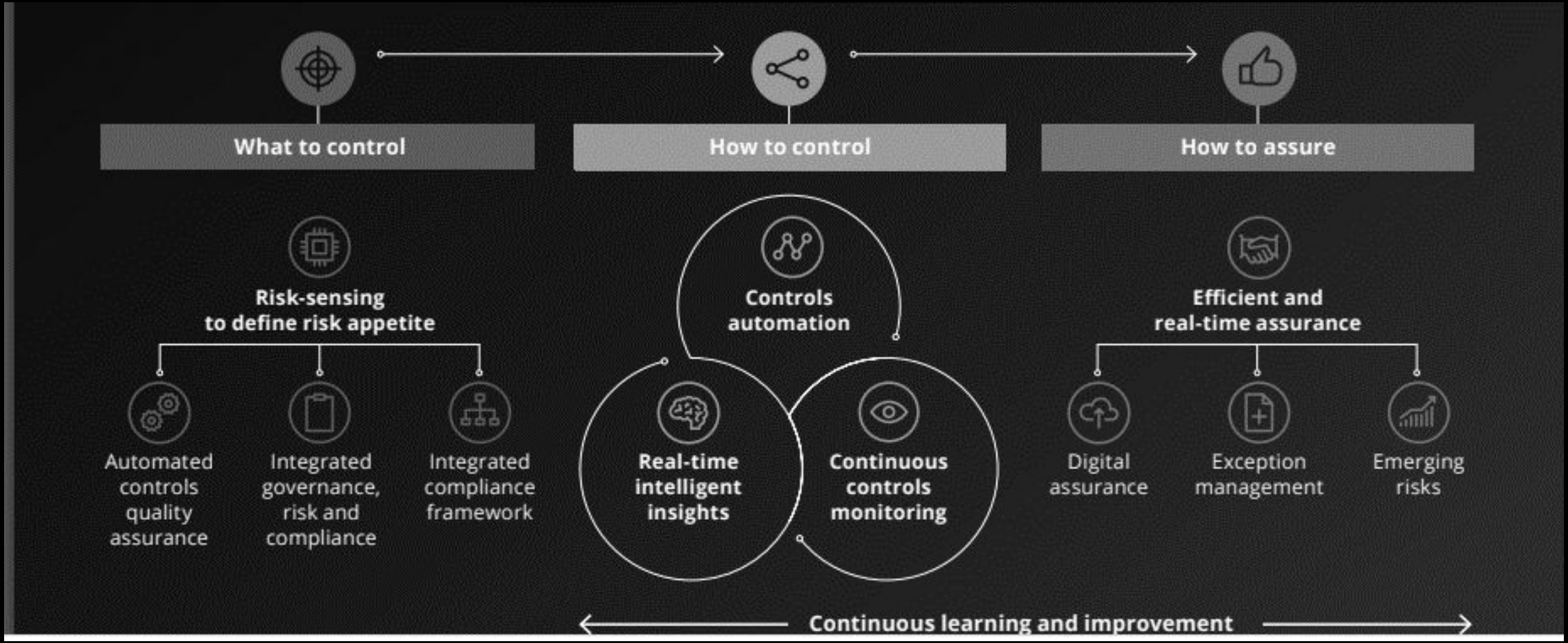
Compliance Requirements

To minimize costs associated with termination process

To have a transparent process that can help build trust and credibility.

Role of Audit – Are today’s controls up to the task?

There needs to be a fundamental change in the way technology is used in the operation, assurance and monitoring of controls. Whereas today, technology is being used for tactical solutions, technology will be at the heart of the future control environment.



What to control
How to control
How to assure
Risk-sensing to define risk appetite
Automated controls quality assurance
Integrated governance, risk and compliance
Integrated compliance framework
Controls automation
Real-time intelligent insights
Continuous controls monitoring
Efficient and real-time assurance
Digital assurance
Exception management
Emerging risks
Continuous learning and improvement

Leveraging Technology

To have an effective third party risk management program, there is the need to have a solution designed to increase the performance of the extended enterprise and help your organization improve decisions around risk management and achieve its strategic business objectives.

Point in time assessments

Assessments based on checklists aligned to internal and external compliance requirements

- customised assessments
- Risk profiling
- Onsite and / or Remote
- Integrated risk management

Continuous controls monitoring

Solutions to continuously assess third parties and proactively sense and respond to extended enterprise risks and opportunities

- Risk sensing
- Framework aligned to risk assessment
- Proactive compliance reporting
- Embedded service

Technology enablement

Solutions to transform and continuously enhance extended enterprise risk management by designing, implementing and deploying technology solutions

- Usage of tools
- Preventive controls
- Technology integration
- Shared assessment platform

Technology is the foundation for effective third-party risk management programs

Managing third parties can be complex, involving several activities typically performed by different groups across a variety of tools/platforms. Technology solutions should support in three primary ways to establish a single source of truth:

Technology elements

Inventory engagements and relationships

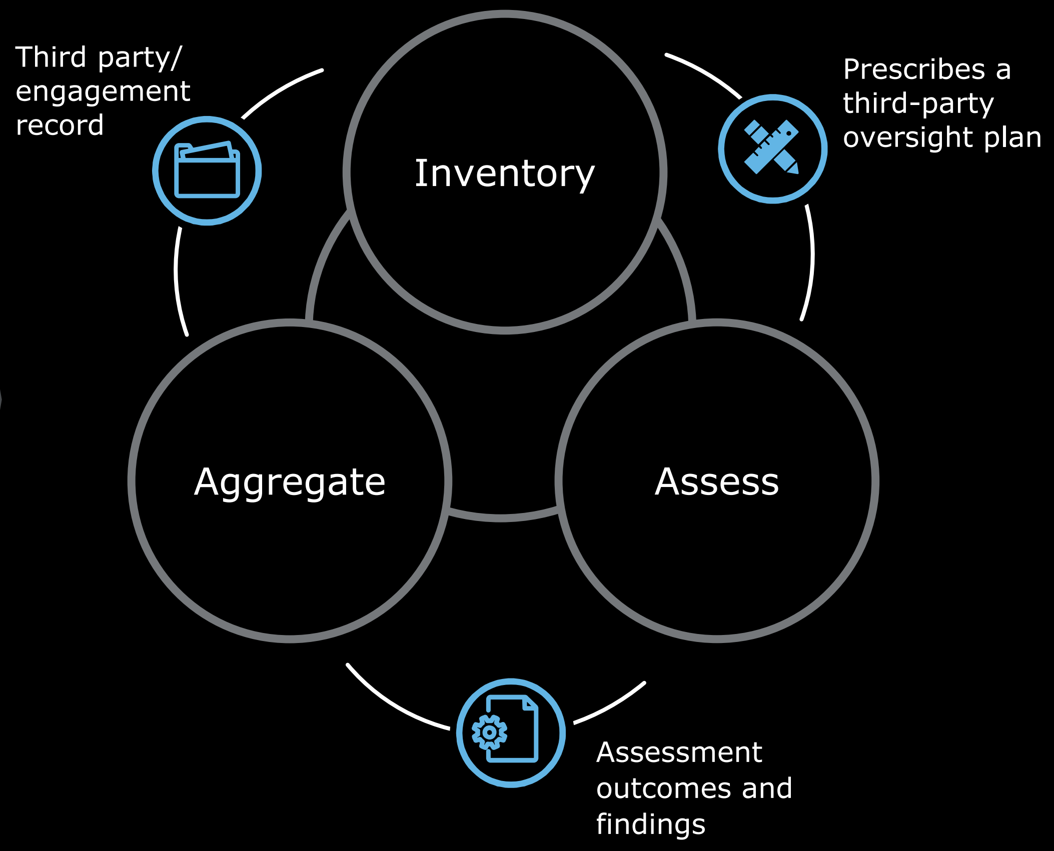
- Serves as the single inventory for third-party relationship and engagement records
- Used to identify the third parties leveraged by the organization. The tool determines what oversight practices are required and delegates this workload to the appropriate stakeholders
- Produce a relationship/engagement risk profile and a prescribed **oversight plan**
- Typically, a single tool completes this activity

Perform assessments

- Allows for different control assessments to be performed as prescribed based on a specific risk domain area (i.e., compliance, IT, reputation)
- Creates an assessment outcome (usually an objective score) and identifies adverse findings/ outcomes
- Multiple tools can typically conduct these assessments

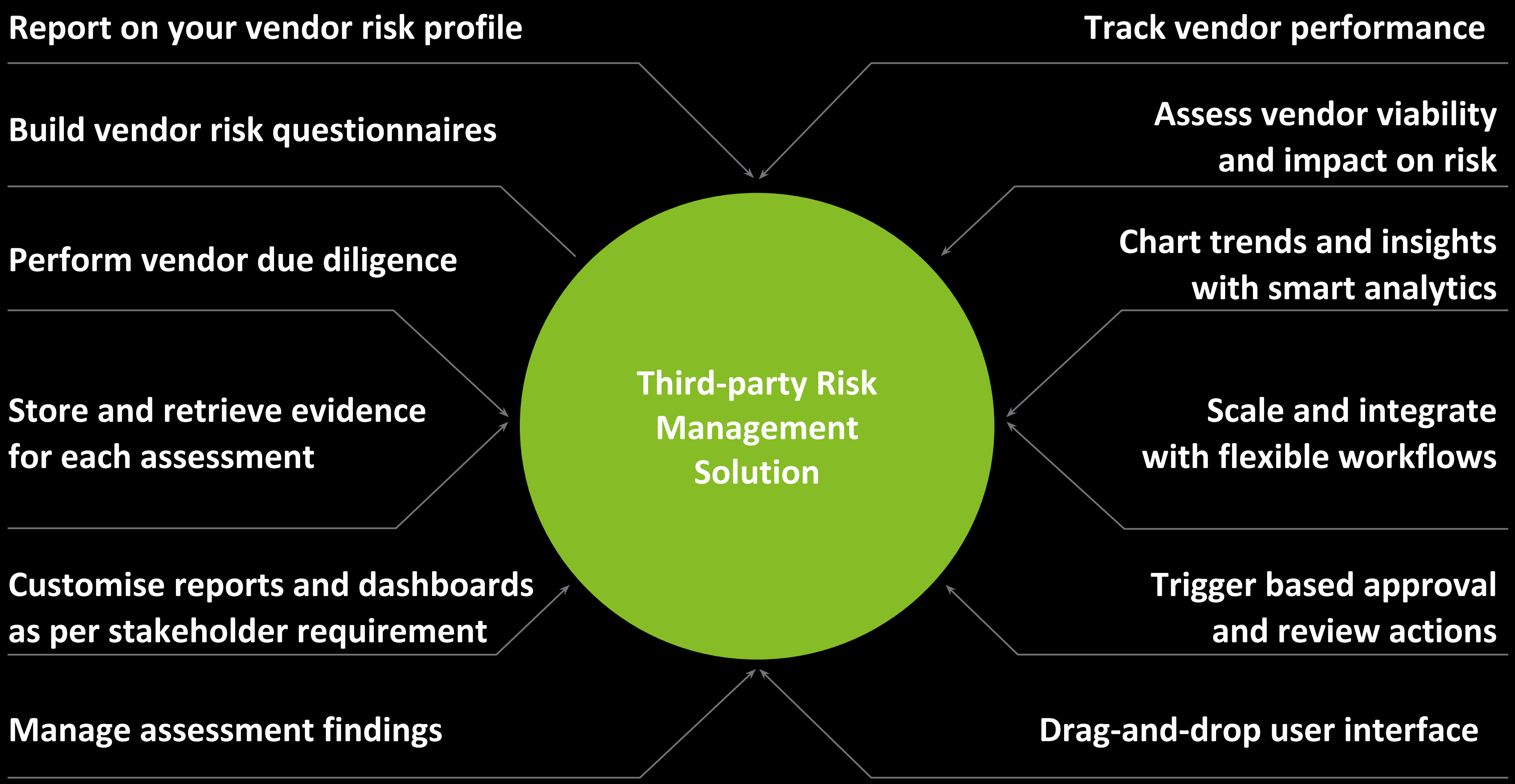
Aggregate risk data

- Takes the third-party relationship/engagement record created and adds information collected along the third-party lifecycle through the completion of various execution activities
- The objective is to create a **third-party risk profile** for each record that shows:
    - Inherent and residual risk summaries
    - An oversight plan
    - Assessment outcomes
    - Performance metrics
    - Open findings & risk acceptance
- Third-party risk profile data is then compiled to create third-party reports and analytics
- Typically, a single tool completes this activity



Third Party Risk Management

Automation – Modules and functionality



Third-party Risk Management Solution

Report on your vendor risk profile

Build vendor risk questionnaires

Perform vendor due diligence

Store and retrieve evidence for each assessment

Customise reports and dashboards as per stakeholder requirement

Manage assessment findings

Track vendor performance

Assess vendor viability and impact on risk

Chart trends and insights with smart analytics

Scale and integrate with flexible workflows

Trigger based approval and review actions

Drag-and-drop user interface

Conclusion

To manage the evolving third party risk, you need to propel your organization into more real-time monitoring and less reactive remediations

Novel ongoing monitoring methods and practices leveraging innovative processes, new data sets, AI technology, and refreshed skill sets

Tools that focus on ‘post-contract’ monitoring as opposed to ‘due-diligence’ and pre-contract

Programs that invest more time in inherent risk analysis enable organizations to make more informed investments and can assist with a higher ROI

THANK YOU

The views and opinions expressed in this presentation are those of the author and do not in any way represent the views of the author’s employer. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication. The author does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Contact Information

fodumuboni@deloitte.com.ng

+234 807 054 8472