

# **Transforming Third-Party Risk Management**

*Building Resilience and Integrity in the Extended Enterprise*

PRESENTATION


---

Governance, Risk Management & Compliance Insight



**The Modern Organizations is the Extended Enterprise**



A world map is overlaid on a background of blue shipping containers. The map features several glowing blue nodes connected by thin, curved lines, representing a global network. The nodes are located in North America, South America, Europe, Africa, Asia, and Australia. The background shows a perspective view of stacked shipping containers, with a crane visible in the distance.

**Businesses must take reasonable steps to ensure they manage risks and maintain ethical environments and relationships across the extended enterprise**





**Navigating Chaos of Risk, Regulation & the Extended Enterprise**





A Tale of Two Futures, is Our Future a . . .

- Blade Runner Future?
- Star Trek Future?





”

The more we study the major problems of our time, the more we come to realise that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent.

- Physicist Fritjof Capra

# Range of Third-Party Risks



# Supply Chain Laws/Regulations with Global effect

## USA:

- SEC Climate Disclosure (proposed)
- Dodd Frank Act - Section 1502 (Conflict Minerals) (2009)
- Foreign Corrupt Practices Act (1977)
- Federal Acquisition Regulation (1947)
- Trade Enforcement Act (2015)
- Uyghur Forced Labor Prevention Act (2022)

## California:

- Transparency in Supply Chains Act (2010)
- California Consumer Privacy Act (2018)
- California climate disclosure bills (2023)

## Canada:

Transparency In Supply Chains Act

## Netherlands:

Child labour law (2020)

## Norway:

Transparency Act (2021)

## UK:

- Modern Slavery Act (2015)
- UK Bribery Act (2010)

## France:

- Duty of care (2017)
- Sapin II (2017)

## Belgium

Duty of care

## Austria

Supply Chain Legislation

## Switzerland:

Responsible Business Initiative (counter proposal) (2022)

## European Union:

- > GDPR (2018)
- > Conflict Minerals Regulation (2021)
- > Non-Financial Reporting Directive (2018)
- > Timber Regulation (2013)
- > Corporate sustainability due diligence directive (CSRD)
- > Corporate sustainability reporting directive (CSDDD)
- > Regulation to Ban Products Made with Forced Labor

## Germany:

LkSG due diligence law "Supply Chain Act" (2021)

## China:

- Chinese Guidelines for Mineral Supply Chains (2015)
- Restricted Use of Hazardous Substances (2019)

## Japan:

- The Act on Promoting Green Procurement (2001)
- The Clean Wood Act (2017)

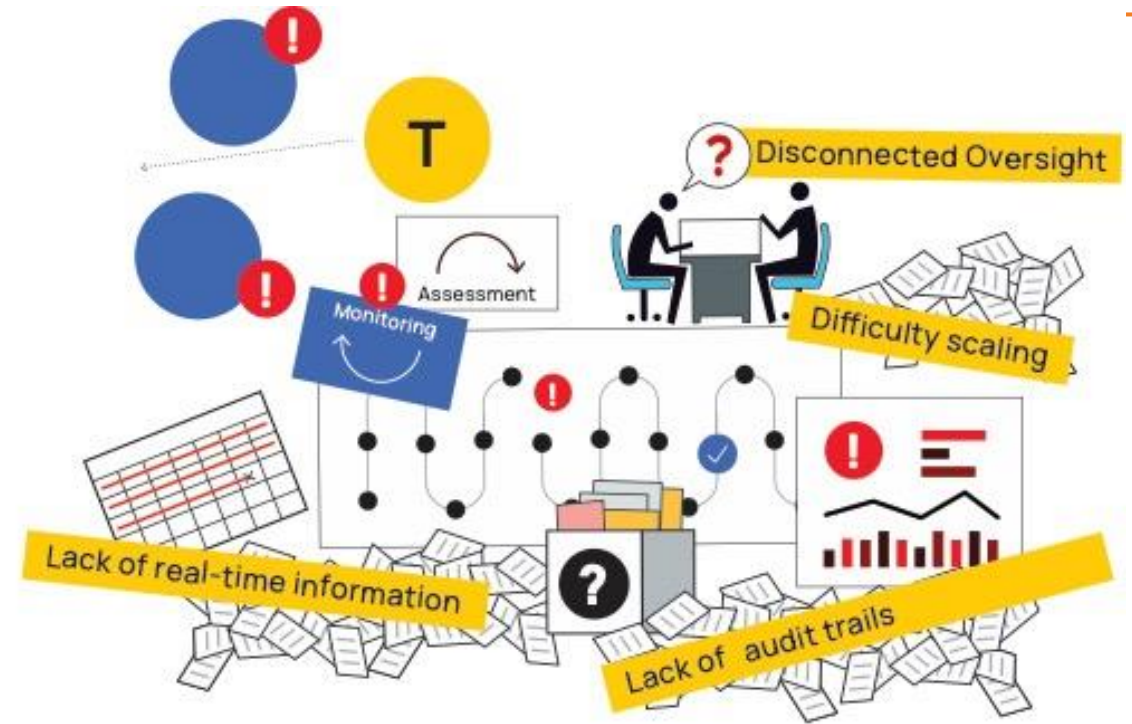
## Australia:

- Australia Modern Slavery Act (2018)
- New South Wales Modern Slavery Act (2018)



# Top 10 Challenges Companies Face

- Siloed Information and Processes
- Inadequate Resources for Third-Party Management
- Disconnected Third-Party Risk Oversight
- Inefficiency and Redundancy in Manual Processes
- Lack of Real-Time Information
- Inadequate Change Management
- Poor Third-Party Performance Evaluations
- Lack of Comprehensive Audit Trails
- Scattered and Non-Integrated Technologies
- Difficulty in Scaling



Address these challenges by transitioning to an integrated Third-Party GRC solution that provides a unified view of third-party objectives, risks, and activities, streamlines workflows and automation, and delivers greater efficiency, effectiveness, resilience, and agility to the organization.

Contact [info@oceg.org](mailto:info@oceg.org) for comments, reprints or licensing requests ©2024 OCEG for additional GRC illustrations and resources visit [www.oceg.org/resources](http://www.oceg.org/resources)

# Inevitability of Failure . . .



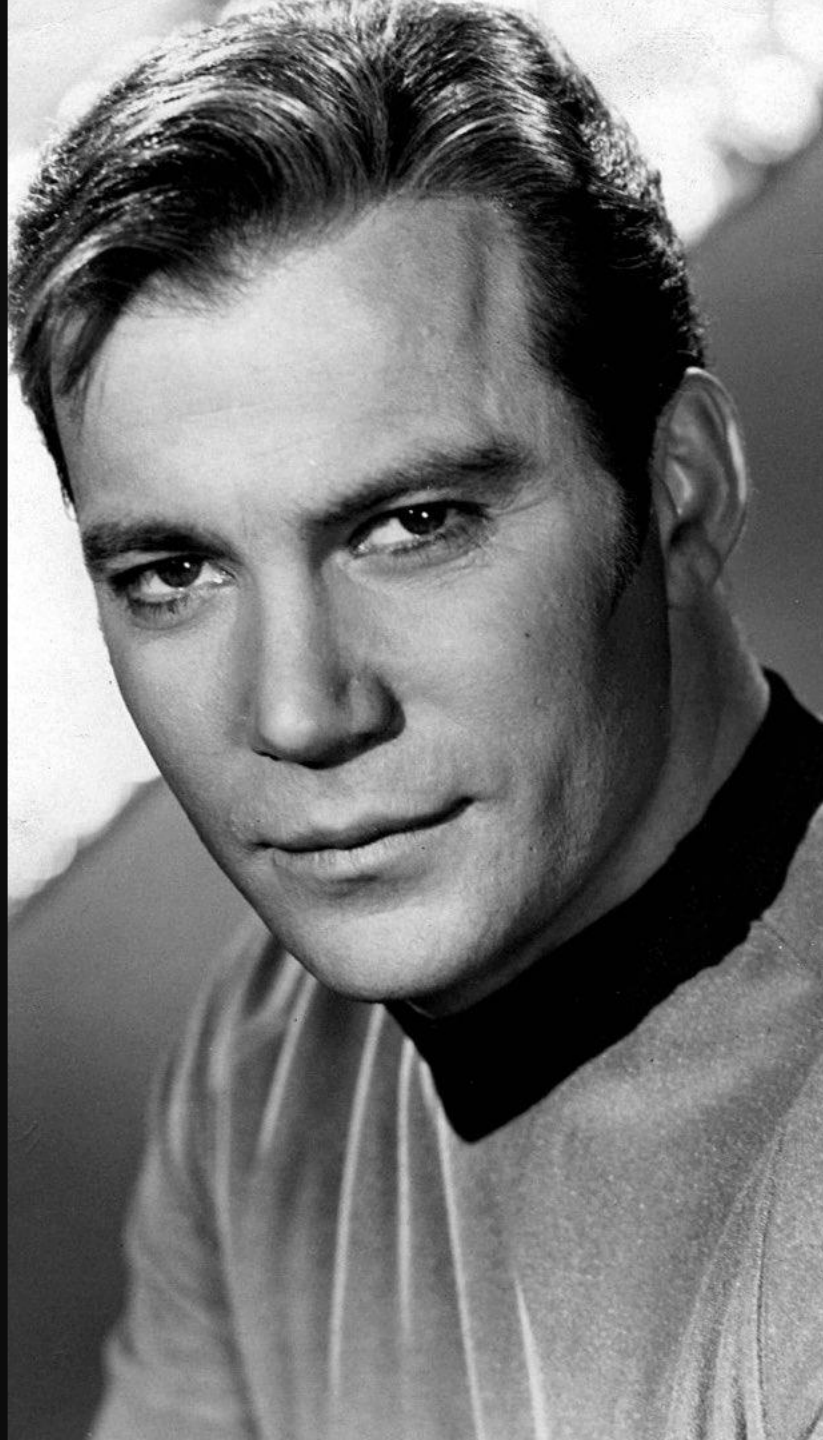


# Third-Party Management Mystery House

- 160 rooms
- 47 fireplaces
- 6 kitchens
- 10,000 windows
- 65 doors to blank walls
- 13 staircases abandoned
- 25 skylights – in floors
- 147 builders/no architects
- Built without a blueprint
- \$5.5 million over 38 years



**“RISK... RISK IS  
OUR BUSINESS.  
THAT’S WHAT THIS  
STARSHIP IS ALL  
ABOUT. THAT’S  
WHY WE’RE  
ABOARD HER.”  
-CAPTAIN  
JAMES T. KIRK**





# Third Party Risk Management = NO SURPRISES!





# Resilience: Ability to Recover from Events and Get Back in the Game





# Agility: Navigate and Leverage Your Environment





# Integrity: Across the Extended Enterprise



*“Doing the right thing is never the wrong thing.”*

- Ted Lasso





# The Official Definition of GRC . . .



GRC is a capability that enables an organization to:

**G)** reliably achieve objectives

**R)** address uncertainty and

**C)** act with integrity.

SOURCE: OCEG GRC Capability Model



3<sup>rd</sup> party risk management is a capability that enables an organization to:

G) reliably achieve objectives

R) Address uncertainty and

C) act with integrity

in and across its 3<sup>rd</sup> party relationships.





## Governance

### Governance of 3<sup>rd</sup> Parties

So the organization may reliably achieve objectives in the relationship and align those with the overall objectives of the organization.



## Risk Management

### Manage & Mitigate Uncertainty

To understand risk exposure and mitigate uncertainty, issues, and loss in 3<sup>rd</sup> party relationships that impact the organization.



## Compliance

### Act With Integrity

To ensure that 3<sup>rd</sup> parties align and meet the values, ethics, policies, regulatory, and contractual obligations of the organization.

# 3<sup>rd</sup> Party Risk Management: a Top Down Approach



3<sup>rd</sup> Party GRC Management Strategy



3<sup>rd</sup> Party GRC Management Process



3<sup>rd</sup> Party GRC Management Information



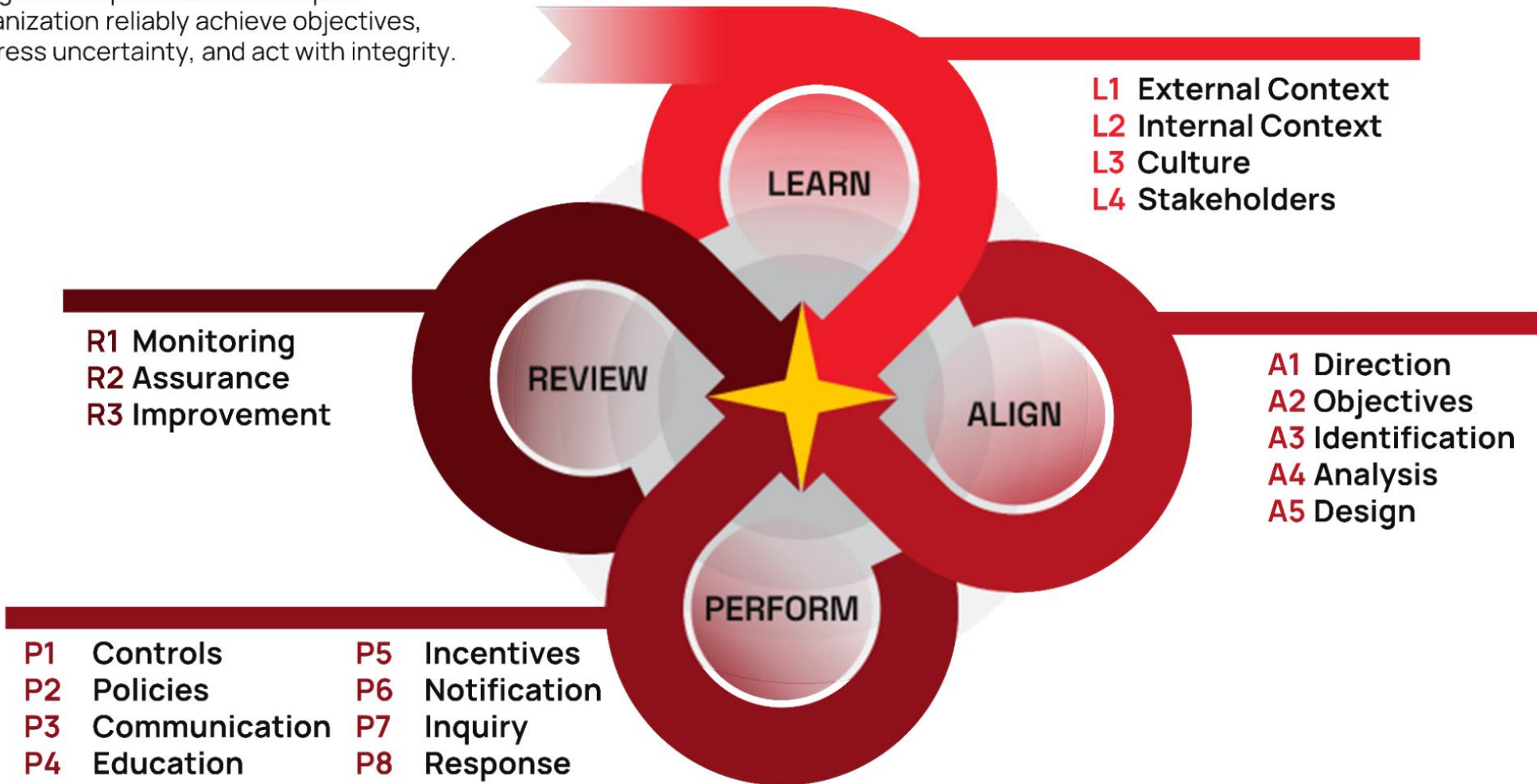
3<sup>rd</sup> Party GRC Management Technology



# GRC Capability Model in Context of Third-Party Risk/GRC

## GRC Capability Model 3.5

integrated capabilities that help an organization reliably achieve objectives, address uncertainty, and act with integrity.







**TREND: Third-Party Risk Orchestration**



# Third-Party GRC Program Management

Third-Party GRC Program Management involves establishing a comprehensive and integrated framework to govern, assess, and monitor third-party relationships throughout their lifecycle.

This includes developing strategies, policies, and processes to ensure that third-party engagements align with organizational objectives, manage risks effectively, and maintain compliance with regulatory requirements.



Contact [info@oceg.org](mailto:info@oceg.org) for comments, reprints or licensing requests ©2024 OCEG for additional GRC illustrations and resources visit [www.oceg.org/resources](http://www.oceg.org/resources)

# Core Components: 3<sup>rd</sup> Party GRC Management Program



## GOALS

Define specific 3rd party management goals and strategies in context of governance, risk and compliance.



## MEASUREMENT

Decide on the metrics for each phase of the 3rd party management process.



## AUDIENCE

Define 3rd parties and and who within those 3rd party relationships do we communicate with.



## ALIGNMENT

Align 3rd party management strategies with the corporate culture and Code of Conduct.



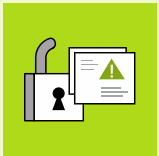
## RESOURCES

Assign the appropriate people, budget and other resources to ensure 3rd party management goals are met.



## INTERNAL STAKEHOLDERS

Collaborate with and enlist the support of internal stakeholders across the business.



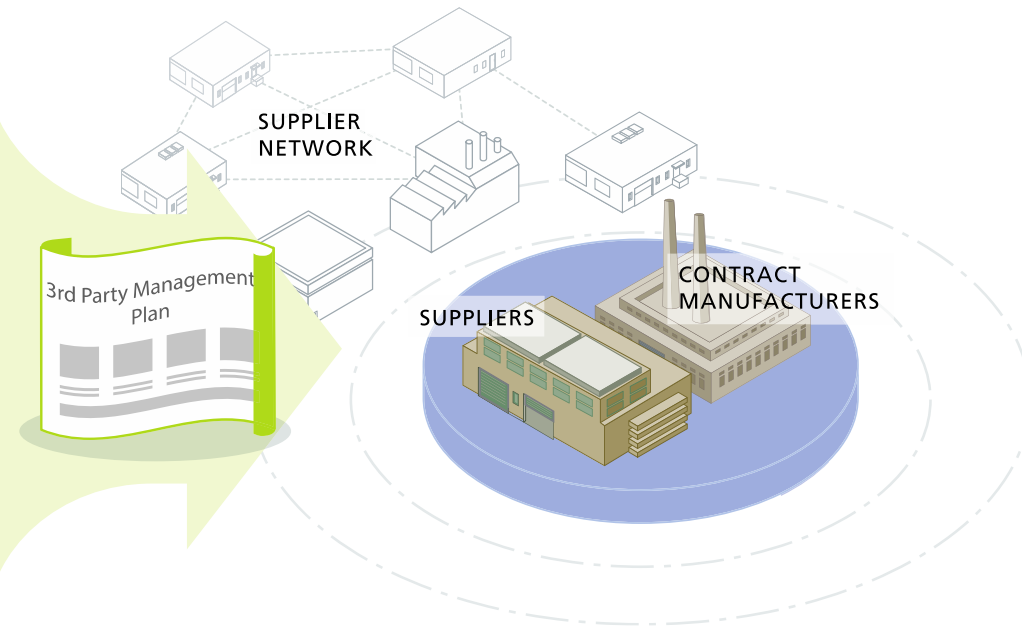
## ACCESSIBILITY

Ensure that 3rd party communications are be accessible, understandable and actionable by all groups regardless of education level, geography, culture, language, ethnic group or disability status.



## EXECUTIVE SUPPORT

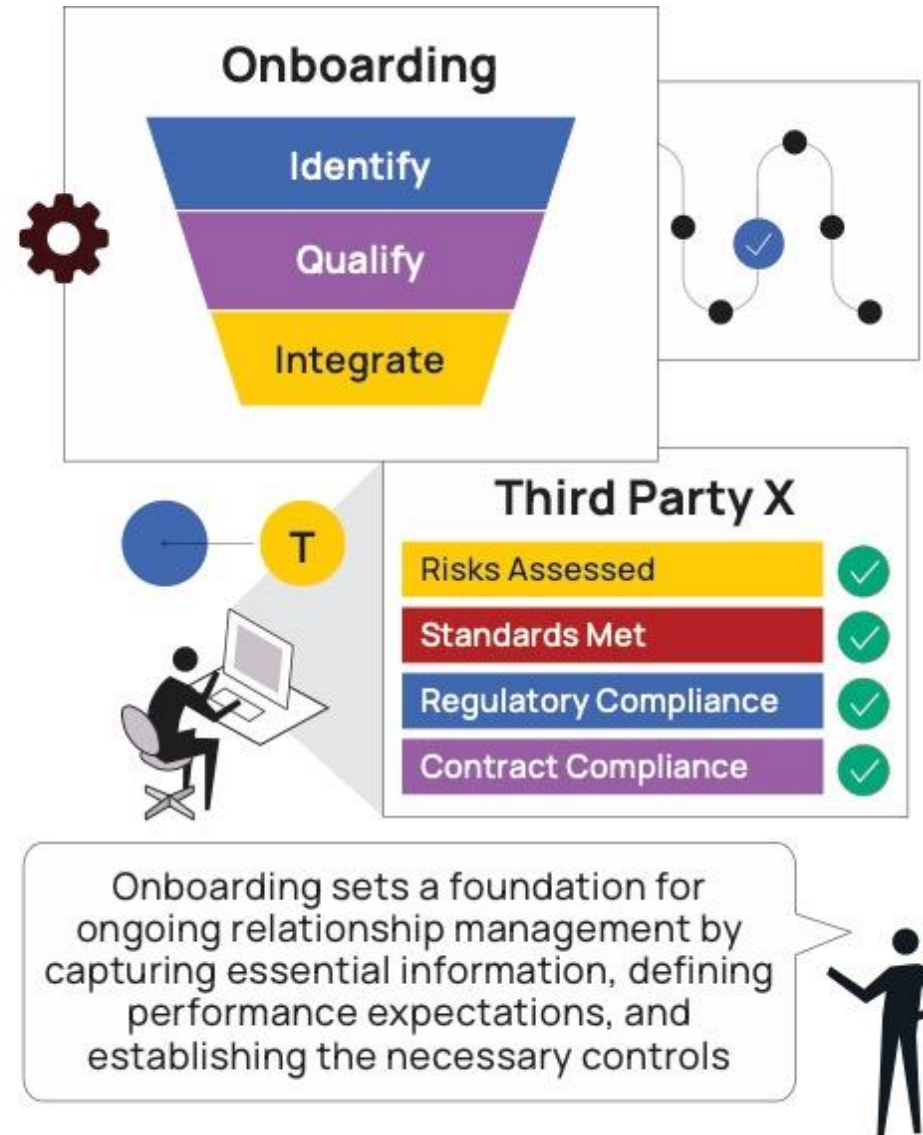
Gain executive support of the 3rd party management program





# 1 Onboarding

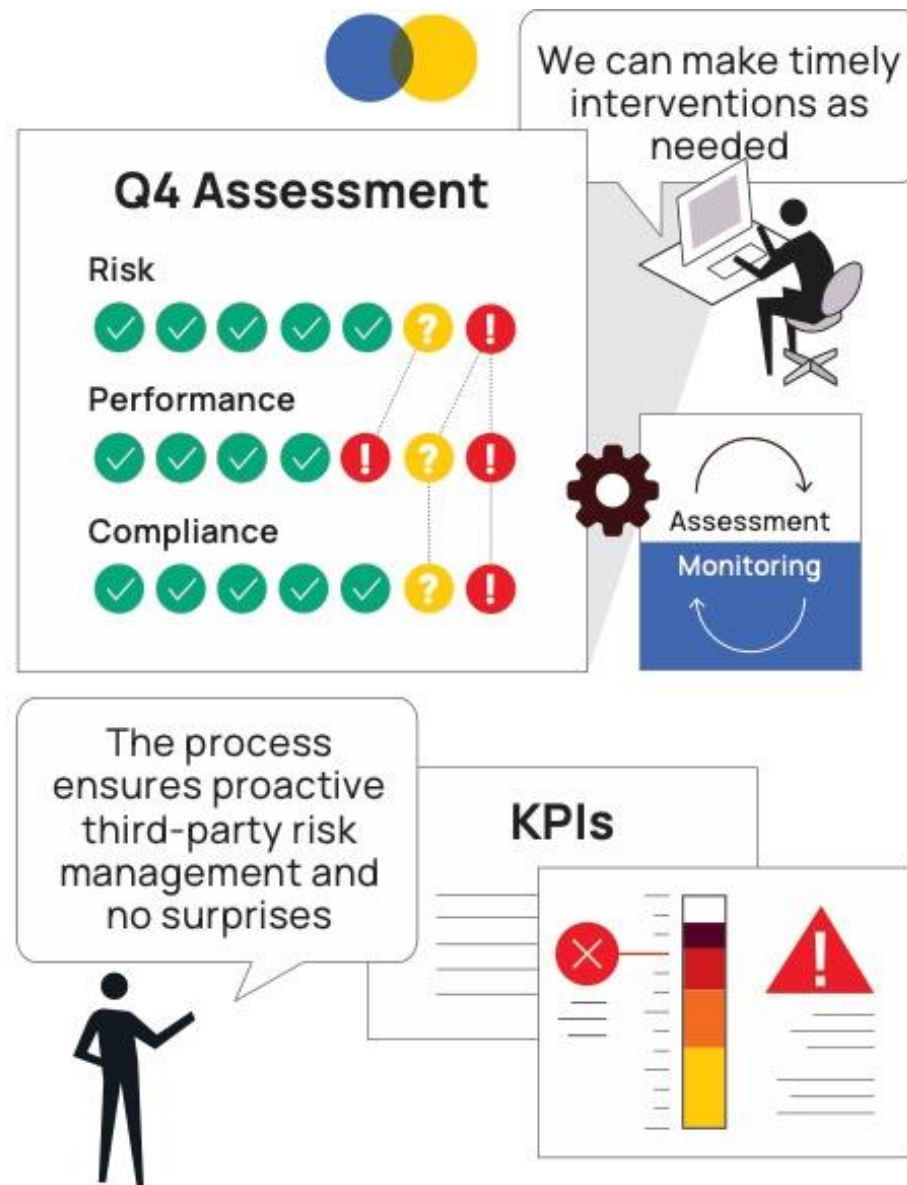
The onboarding process for third-party GRC involves the systematic identification, qualification, and integration of third parties into the organization's operations. This includes conducting thorough due diligence to assess potential risks, verifying that the third party meets the required standards, and ensuring compliance with regulatory and contractual obligations.



Contact [info@oceg.org](mailto:info@oceg.org) for comments, reprints or licensing requests ©2024 OCEG for additional GRC illustrations and resources visit [www.oceg.org/resources](http://www.oceg.org/resources)

## 2 Ongoing Monitoring & Assessment

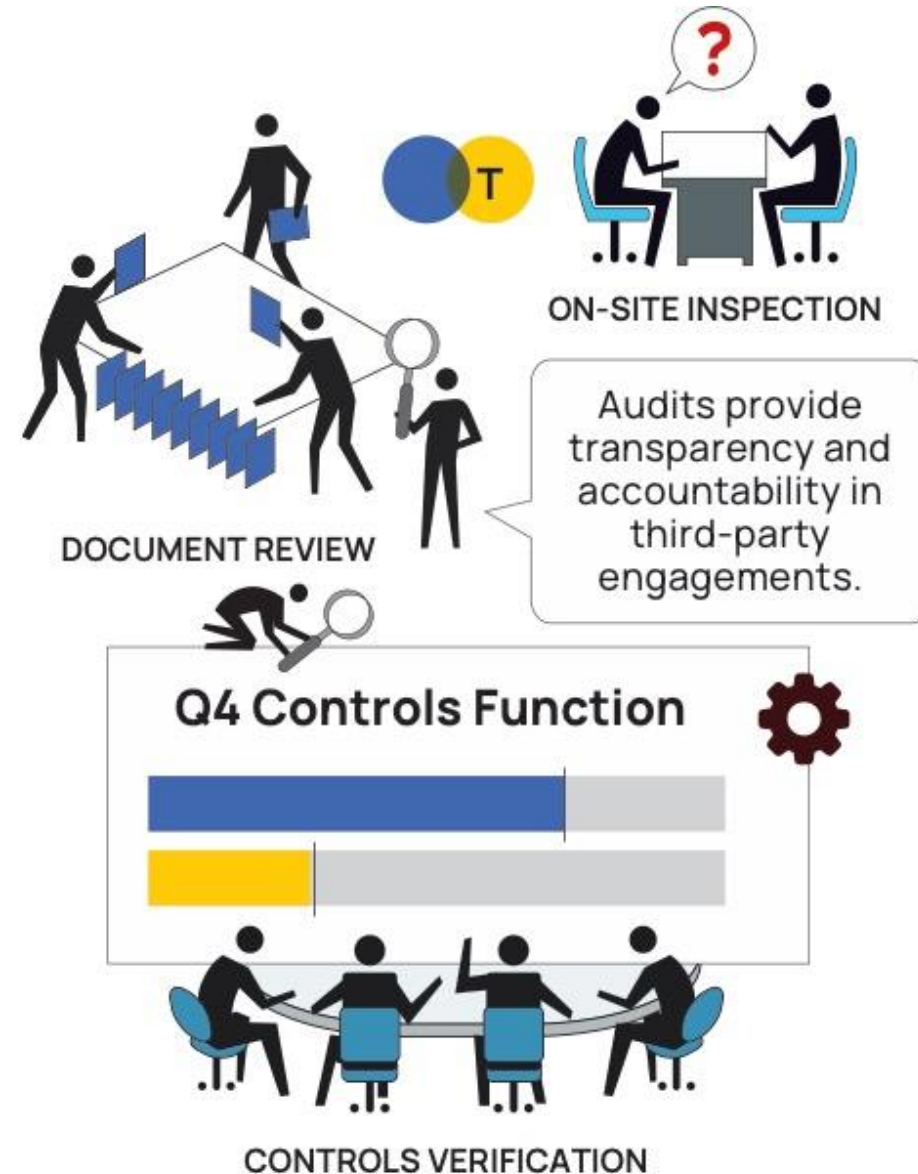
Ongoing Monitoring & Assessment is the continuous process of evaluating third-party relationships to ensure they meet the organization's performance, risk, and compliance standards. This includes regular tracking of third-party activities, monitoring key performance indicators (KPIs), and conducting periodic risk assessments to detect any emerging issues.





### 3 Audits & Inspections

Audits & Inspections involve systematically reviewing and evaluating third-party compliance with contractual obligations, regulatory requirements, and organizational policies. Audits and inspections help identify any discrepancies or non-compliance issues, ensuring that third-party relationships are managed with integrity and that risks are mitigated effectively.



#### 4 Offboarding

Offboarding is the process of systematically disengaging from a third-party relationship when it is no longer needed or viable. This includes ensuring that all contractual obligations are fulfilled, securely transferring or terminating data access, and resolving any outstanding issues.



Offboarding aims to minimize risks associated with ending the relationship, such as data breaches or compliance violations, and ensures that the organization can transition smoothly, preserving operational continuity and security.





---

GRC Technology Illustrated Series

# Third-Party GRC Management Solutions

Third-Party GRC management solutions facilitate and automate the governance, risk management, and compliance of an organization's third-party relationships. These solutions enhance transparency by providing real-time insights into the performance, risk, and compliance of third-party entities, ensuring that risks are managed and compliance requirements are met throughout the lifecycle of third-party engagements. They enable organizations to proactively achieve objectives in third-party relationships, manage uncertainty, and ensure integrity and compliance, while improving overall efficiency and ensuring alignment with organizational objectives and performance.

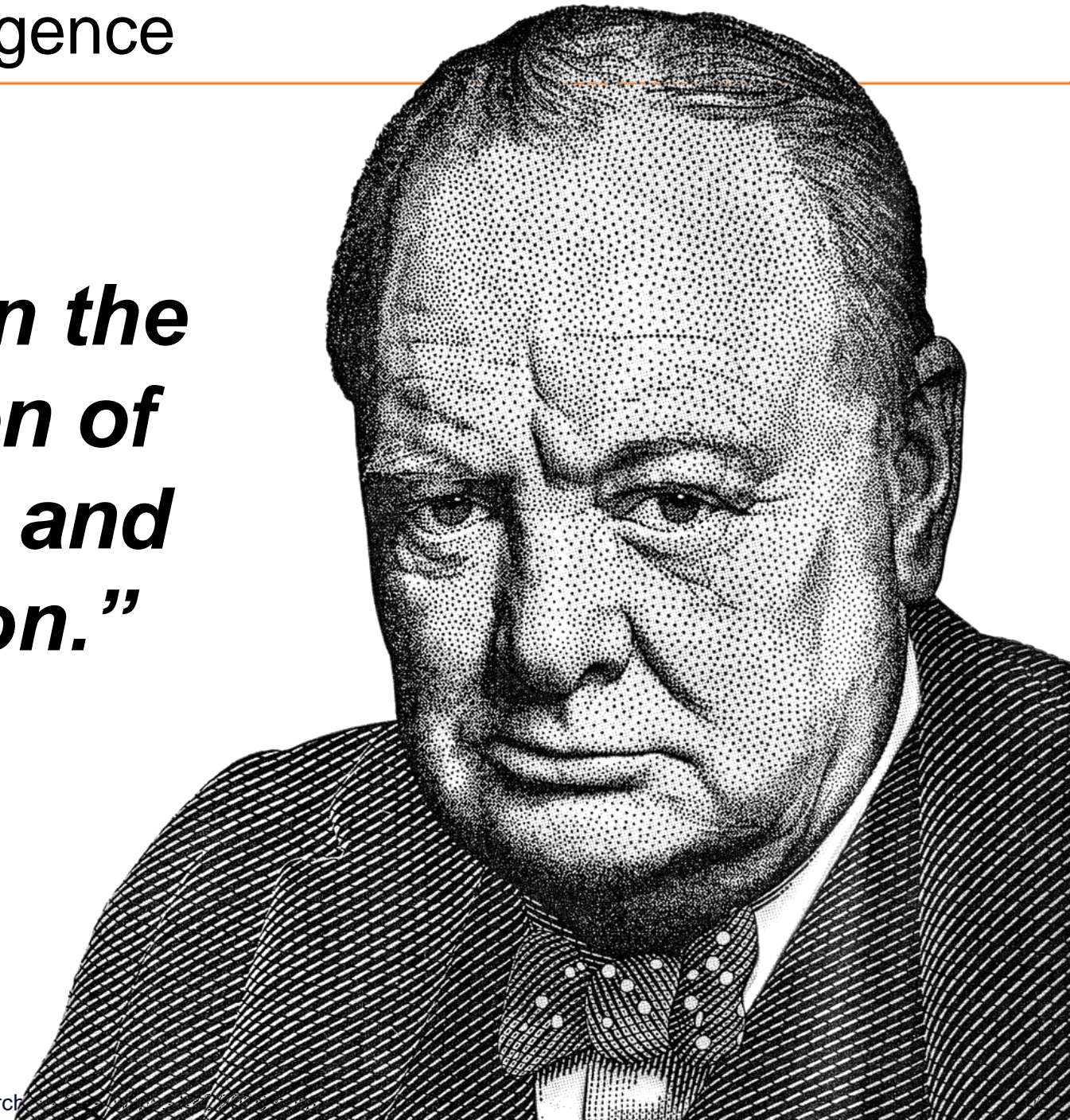
Contact [info@oceg.org](mailto:info@oceg.org) for comments, reprints or licensing requests ©2024 OCEG for additional GRC illustrations and resources visit [www.oceg.org/resources](http://www.oceg.org/resources)

# TREND: Third-Party Risk Intelligence

---

***“True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information.”***

**Winston Churchill**





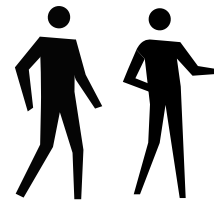


**Third-Party GRC management platforms  
are empowered with integration into third-party  
risk intelligence that delivers content for:**

- Watch Lists
- Sanctions
- Negative News
- Adverse Media
- Security Ratings
- Financial Viability Ratings
- ESG Ratings & Information
- Politically Exposed Persons

## Critical Capabilities

- ✓ Integrated Third-Party Risk Assessment
- ✓ Real-Time Monitoring
- ✓ Automated Due Diligence
- ✓ Onboarding
- ✓ Offboarding
- ✓ Issue Management
- ✓ Compliance Tracking
- ✓ Audit Trails
- ✓ Performance Metrics
- ✓ Data Integration
- ✓ Third-Party Portal
- ✓ Dynamic Reporting
- ✓ Contract Management
- ✓ Risk Alerts
- ✓ Scalability





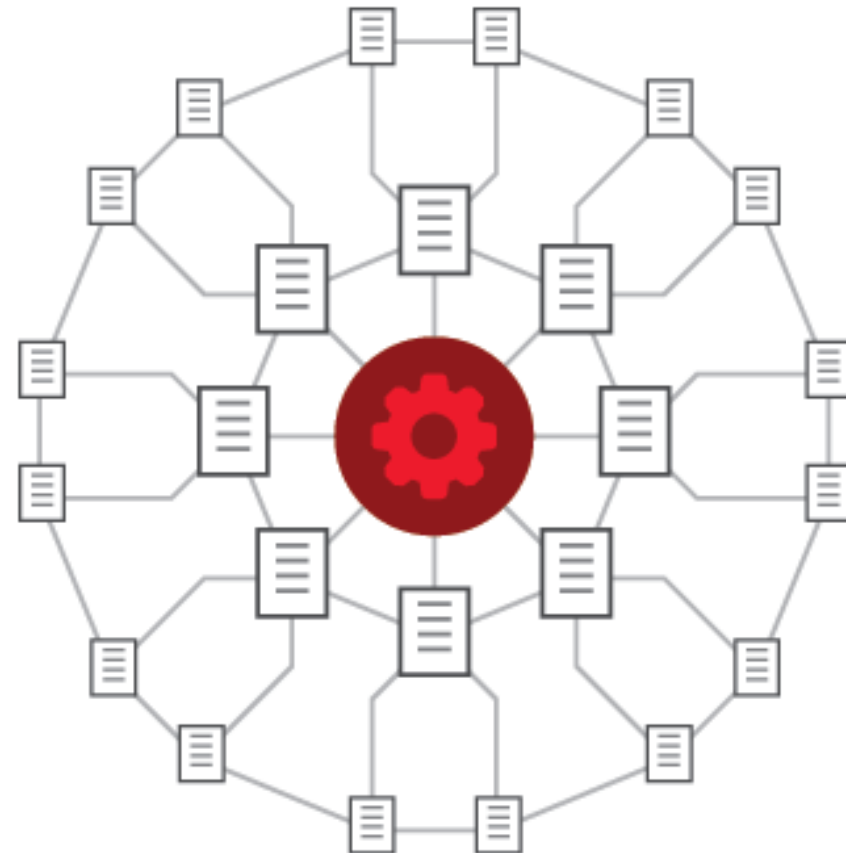
## CURRENT STATE

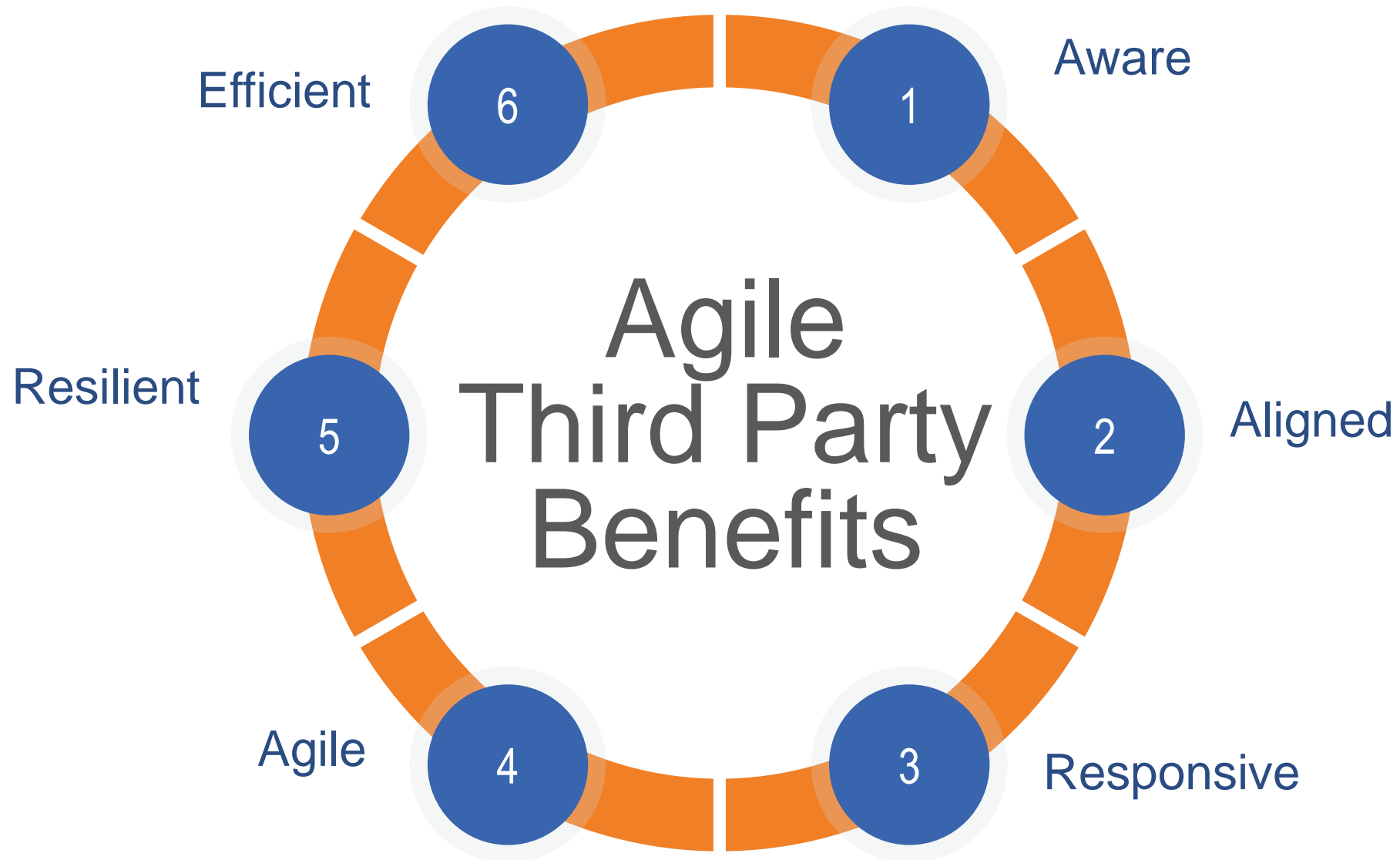
### Manual Processes, Disparate Systems



## FUTURE STATE

### Automated Processes, Integrated Systems







# Step 1: Develop a 3<sup>rd</sup> Party GRC Strategic Plan

**It is critical to plan  
your journey by  
laying out the route  
ahead of time**





## Step 2: Conditioning is Critical, Make Sure Your Team and Systems are Ready

Is your organization prepared for the 3<sup>rd</sup> Party GRC journey?





## Step 3: Select the Right Equipment for the 3<sup>rd</sup> Party GRC Journey

You don't just throw everything in a bag, you carefully select your equipment for the task





## Step 4: Tackle 3<sup>rd</sup> Party GRC in Stages



A good journey is not done with one effort but is broken down into stages



## Step 5: Preparing for the Next Journey



Once complete it is not over, you begin preparing for the next project



# Questions?

*GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis.*

grc20/20

**Michael Rasmussen, J.D.**



GRC 20/20 Research, LLC

*The GRC Analyst, Pundit, & OCEG Fellow*

[mkras@grc2020.com](mailto:mkras@grc2020.com)

[www.grc2020.com](http://www.grc2020.com)

+1.262.3329188



*The GRC Report is the first word in governance, risk, and compliance news – providing leading analysis, insights, and updates for GRC professionals.*

*We are dedicated to delivering transparency and providing relevant news to help individuals and organizations stay informed in this ever-evolving field.*

grcreport

[hello@grcreport.com](mailto:hello@grcreport.com)

[www.grcreport.com](http://www.grcreport.com)

