Sponsored by:

How to Define a Process Lifecycle for Vendor Risk Management

Blueprint for an Effective, Efficient & Agile Third Party Management Program

February 2017

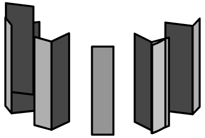
Michael Rasmussen, J.D., GRCP, CCEP

The GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

Who is a 3rd party?

PROVIDER
CONTRACTOR
SUPPLIER
CONSULTANT
VENDOR
OUTSOURCER
AGENT
TEMPORARY
INTERMEDIARY
DEALER
CLOUD
WORKER
SERVICE
BROKER
STAKEHOLDER
PARTNER



GRC Definition Adapted to 3rd Party/Vendor Management . . .

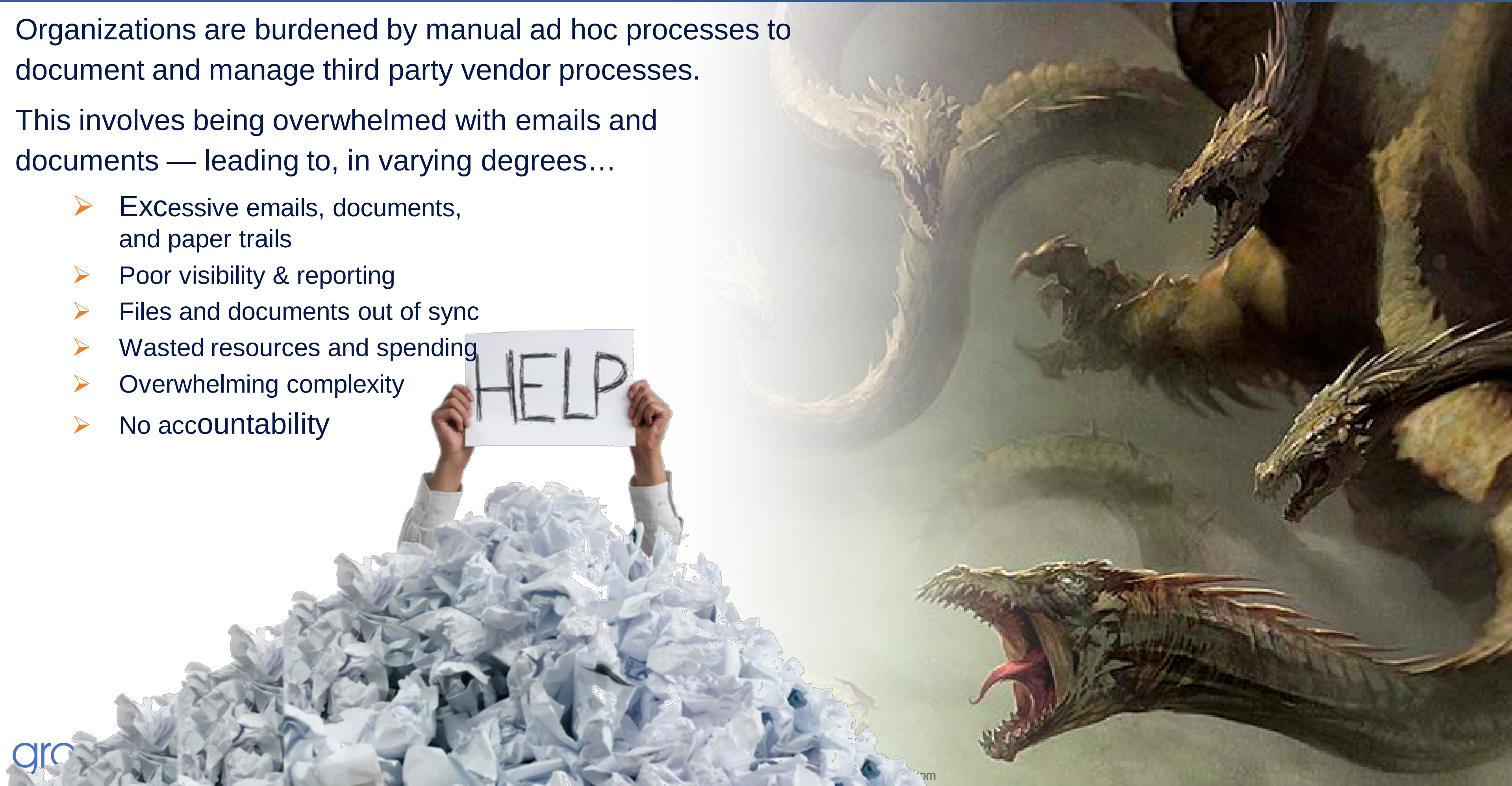
> 3rd party/vendor management is a capability that enables an organization to:
>
> G) reliably achieve objectives
>
> R) while addressing uncertainty and
>
> C) act with integrity
>
> in and across it's 3rd party relationships.

Inevitability of Failure: Too Many Approaches

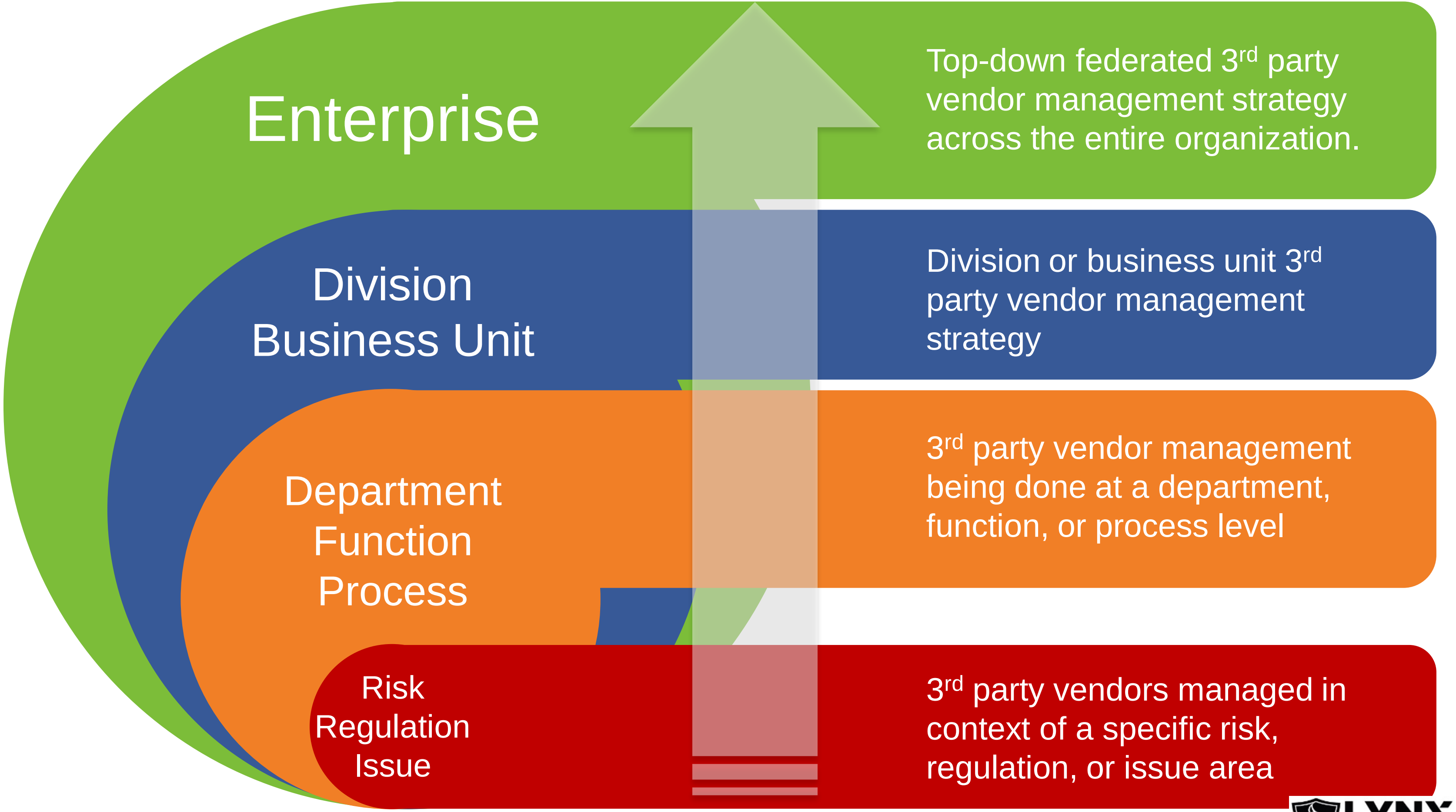
Organizations are burdened by manual ad hoc processes to document and manage third party vendor processes.

This involves being overwhelmed with emails and documents — leading to, in varying degrees…

- Excessive emails, documents, and paper trails
- Poor visibility & reporting
- Files and documents out of sync
- Wasted resources and spending
- Overwhelming complexity
- No accountability



Varying Levels of Vendor Management



Top-down federated 3rd party vendor management strategy across the entire organization.

Division or business unit 3rd party vendor management strategy

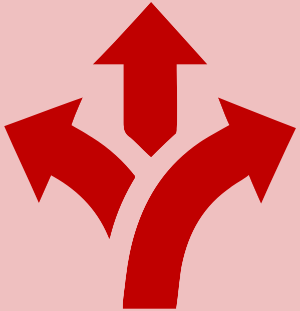
3rd party vendor management being done at a department, function, or process level

3rd party vendors managed in context of a specific risk, regulation, or issue area

What is Your Approach to Vendor Management?

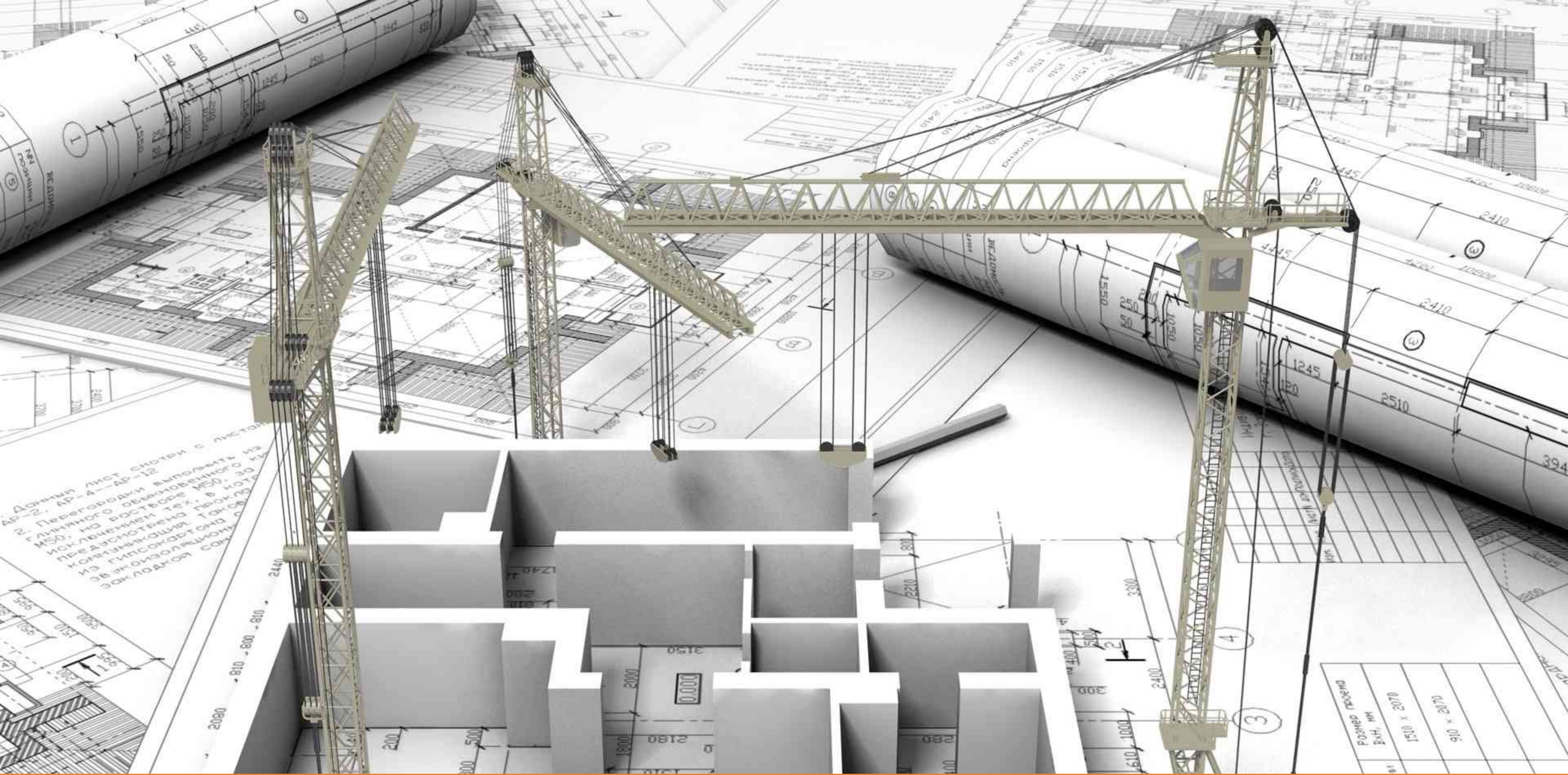
Distributed Vendor Party Management

- Disconnected departments managing vendor relationships in different ways with little or no collaboration with other departments



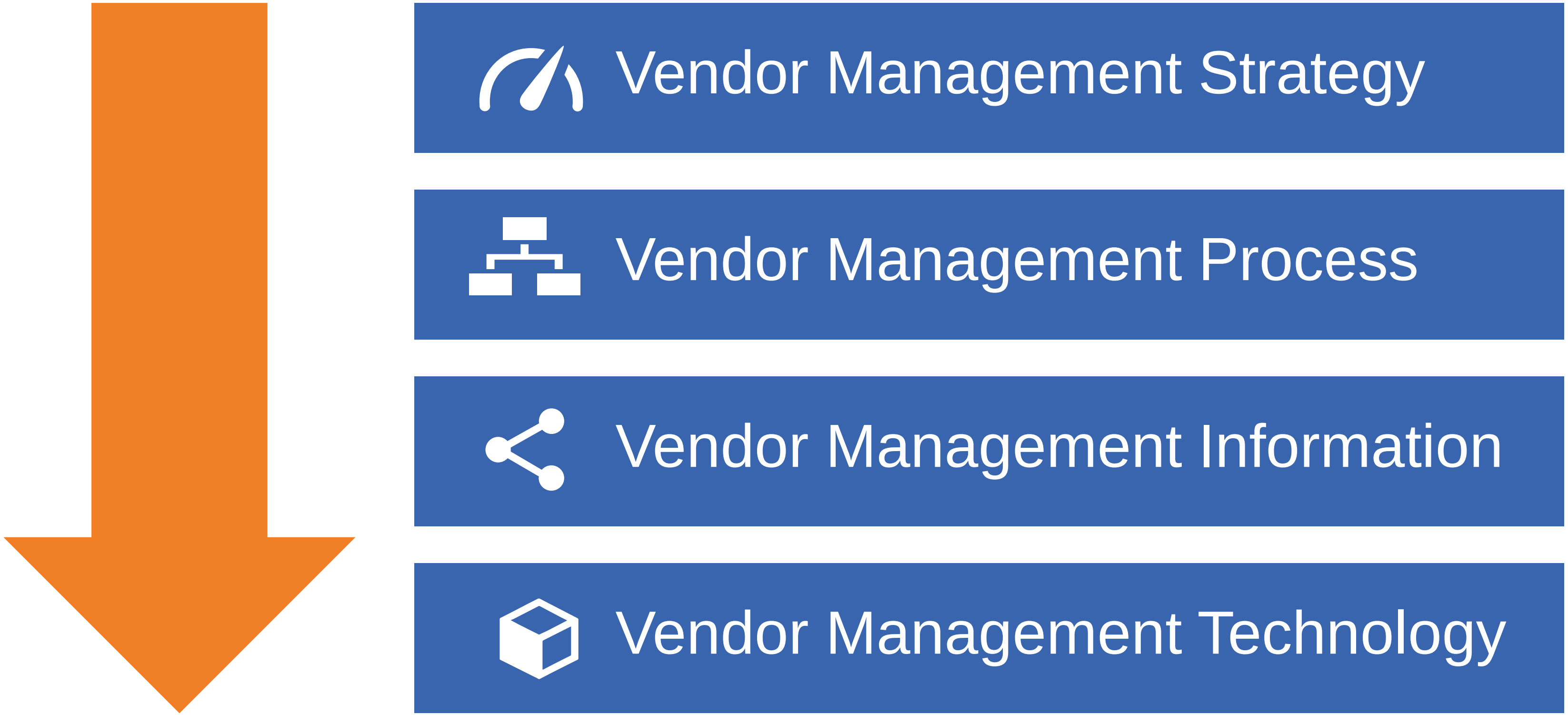
Federated Vendor Party Management

- An integrated approach that balances vendor management centralization with distributed participation and collaboration



What if we could design vendor management?

Vendor Management: a Top Down Approach



Vendor Management Strategy

Vendor Management Process

Vendor Management Information

Vendor Management Technology

Core Components: Vendor Risk Management Plan

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

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

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

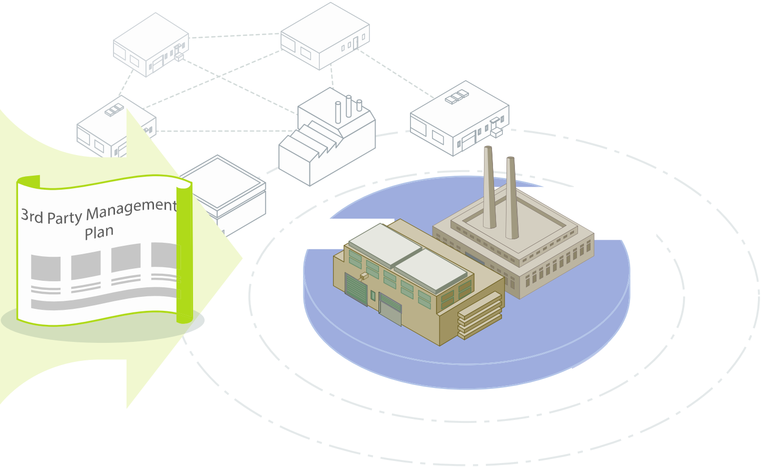
ACCESSIBILITY
Ensure that 3rd party communications are be accessible, understandable and actionable by all groups regardless of education level, geography, culture, language, ethnic group or disability status.

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

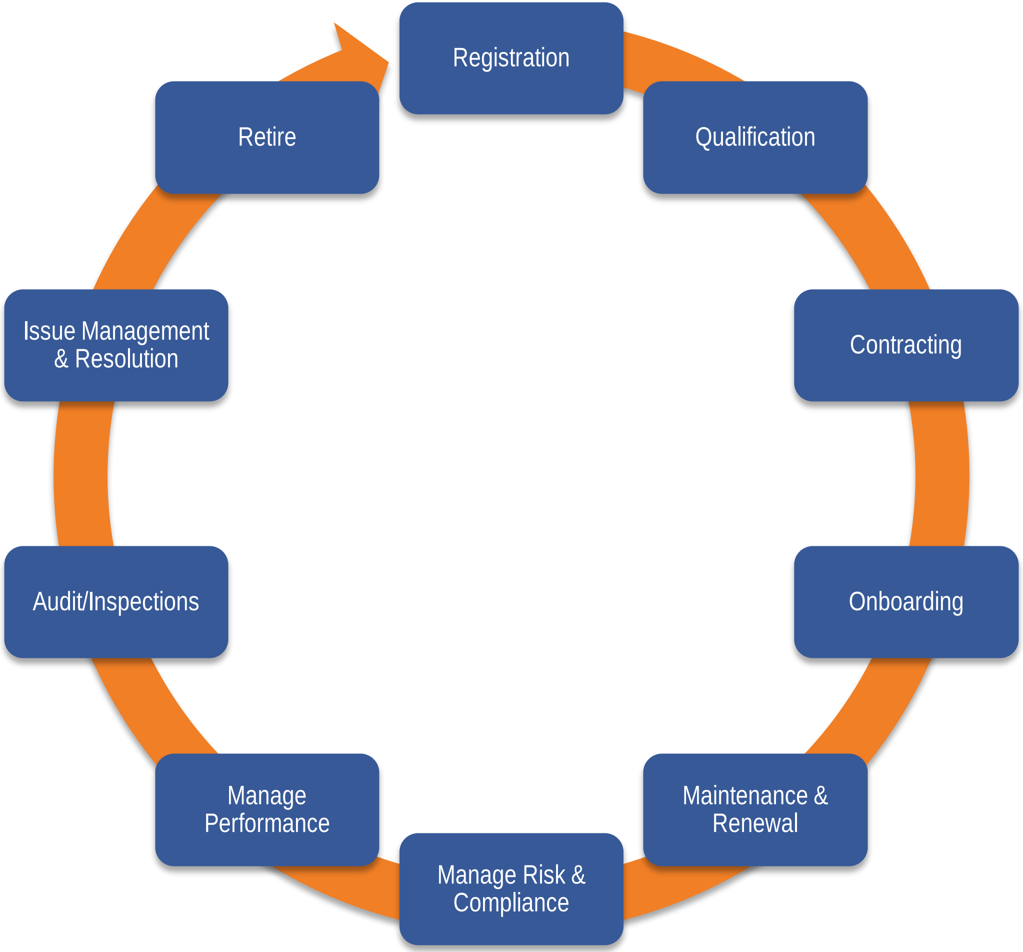
ALIGNMENT
Align 3rd party management strategies with the corporate culture and Code of Conduct.

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

EXECUTIVE SUPPORT
Gain executive support of the 3rd party management program



Overview of a Vendor Risk Management Process



Registration

Qualification

Contracting

Onboarding

Maintenance & Renewal

Manage Risk & Compliance

Manage Performance

Audit/Inspections

Issue Management & Resolution

Retire

Foundational Components: Vendor Risk Management Program

In today's complex economy, your suppliers, distributors, sub-contractors, agents and other 3rd parties play critical roles in your business success. Its too complex to manage without an integrated strategy that includes people, process and technology . The goal is to protect and grow value by establishing a capability to see your entire 3rd party landscape with real time information about external and internal events that may change risk profiles and impact performance.

RISKS

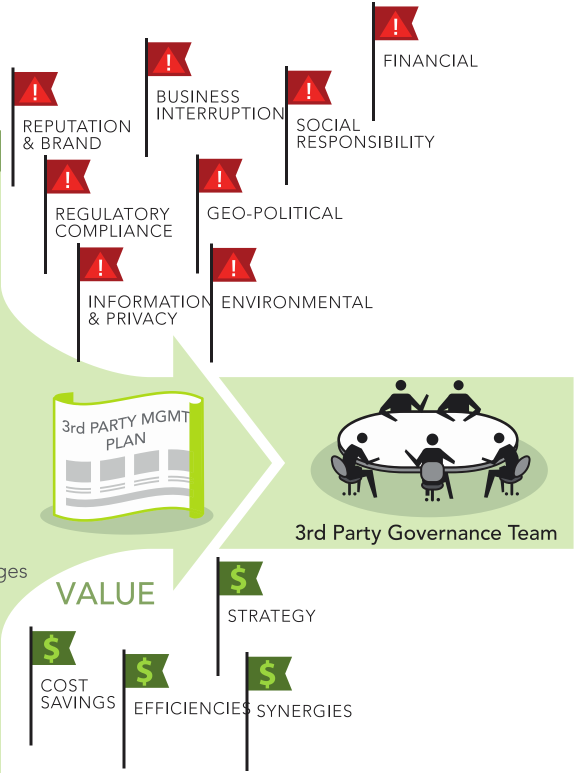
CORE COMPONENTS

1 IDENTIFY
- Contracts and contact info for all 3rd parties
- Mapping of internal relationships
- Relevant triggers for alerts or changes
- Risk exposure and level of control

2 MONITOR
- Contracts and contact info for all 3rd parties
- Mapping of internal relationships
- Compliance with contract requirements
- Changes to risk, obligations and business

3 ASSESS
- Risk and compliance
- Performance against SLAs and KPIs
- Identified internal and external events and changes
- Effectiveness of 3rd party program

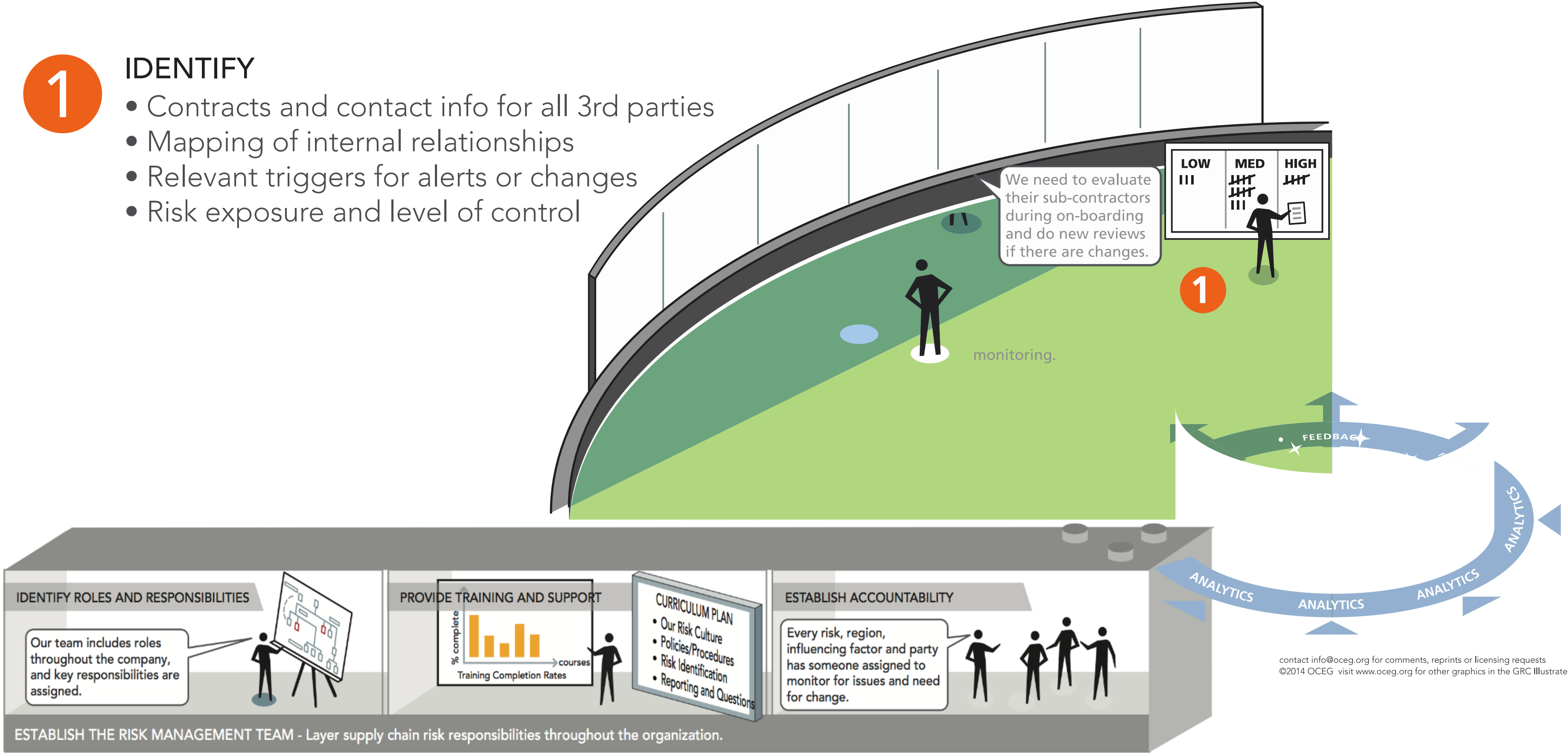
4 RE-EVALUATE
- Contract provisions and controls
- Use of each 3rd party and internal relationships
- Program design and operation
- Issue investigations and resolutions



Foundational Components: Vendor Risk Management Program

1 IDENTIFY

- Contracts and contact info for all 3rd parties
- Mapping of internal relationships
- Relevant triggers for alerts or changes
- Risk exposure and level of control



We need to evaluate their sub-contractors during on-boarding and do new reviews if there are changes.

monitoring.

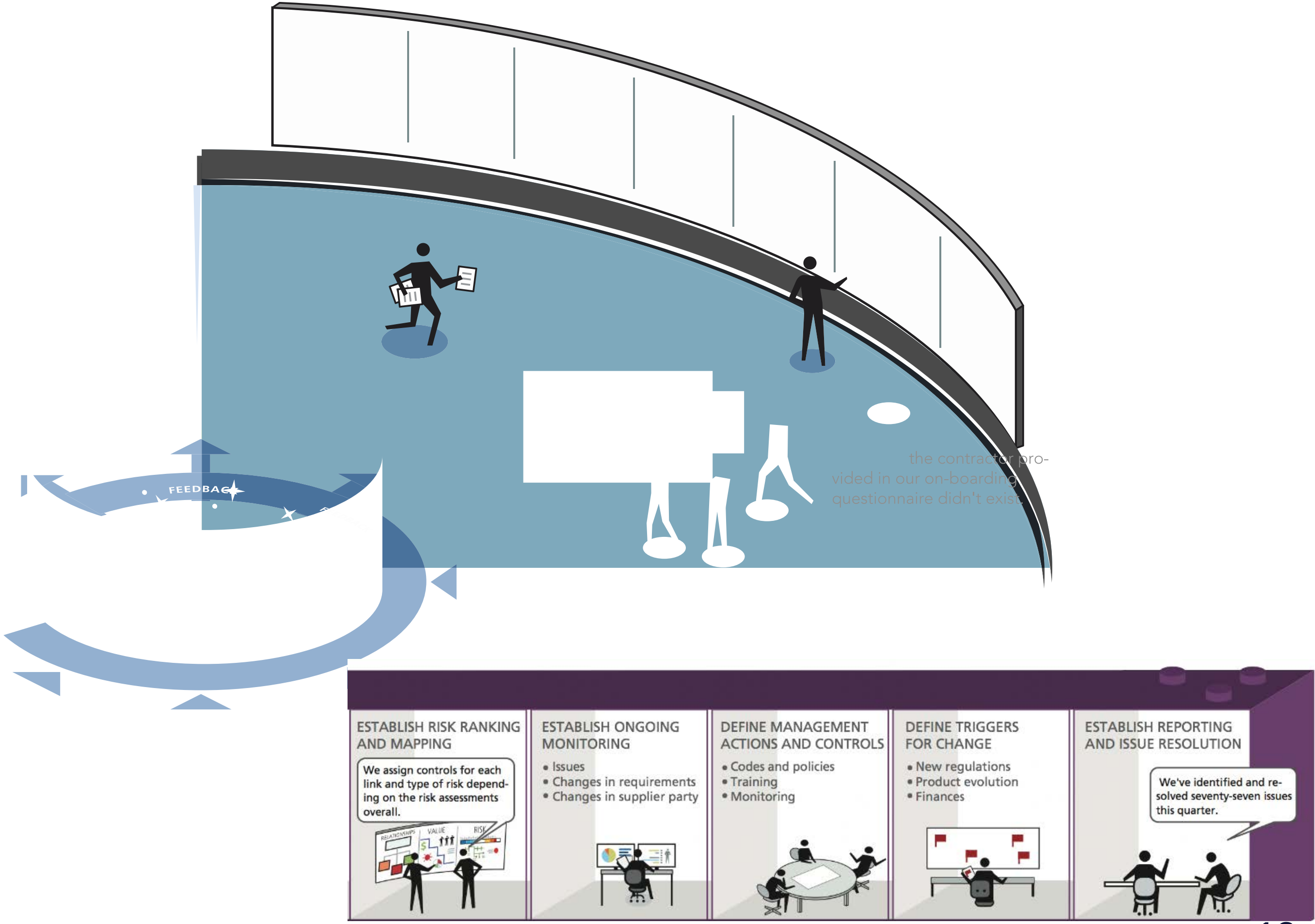
Our team includes roles throughout the company, and key responsibilities are assigned.

CURRICULUM PLAN
- Our Risk Culture
- Policies/Procedures
- Risk Identification
- Reporting and Questions

Every risk, region, influencing factor and party has someone assigned to monitor for issues and need for change.

ESTABLISH THE RISK MANAGEMENT TEAM - Layer supply chain risk responsibilities throughout the organization.

Foundational Components: Vendor Risk Management Program



ESTABLISH RISK RANKING AND MAPPING

We assign controls for each link and type of risk depending on the risk assessments overall.

ESTABLISH ONGOING MONITORING

- Issues
- Changes in requirements
- Changes in supplier party

DEFINE MANAGEMENT ACTIONS AND CONTROLS

- Codes and policies
- Training
- Monitoring

DEFINE TRIGGERS FOR CHANGE

- New regulations
- Product evolution
- Finances

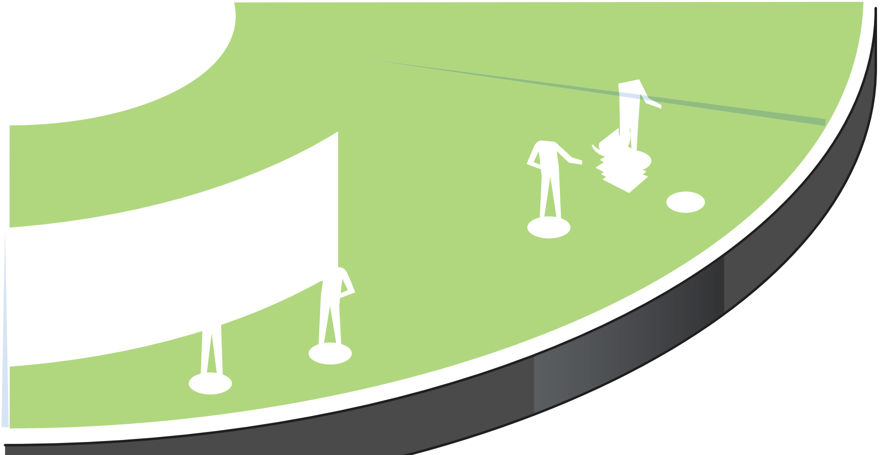
ESTABLISH REPORTING AND ISSUE RESOLUTION

We've identified and resolved seventy-seven issues this quarter.

Foundational Components: Vendor Risk Management Program

3

ness of 3rd party program

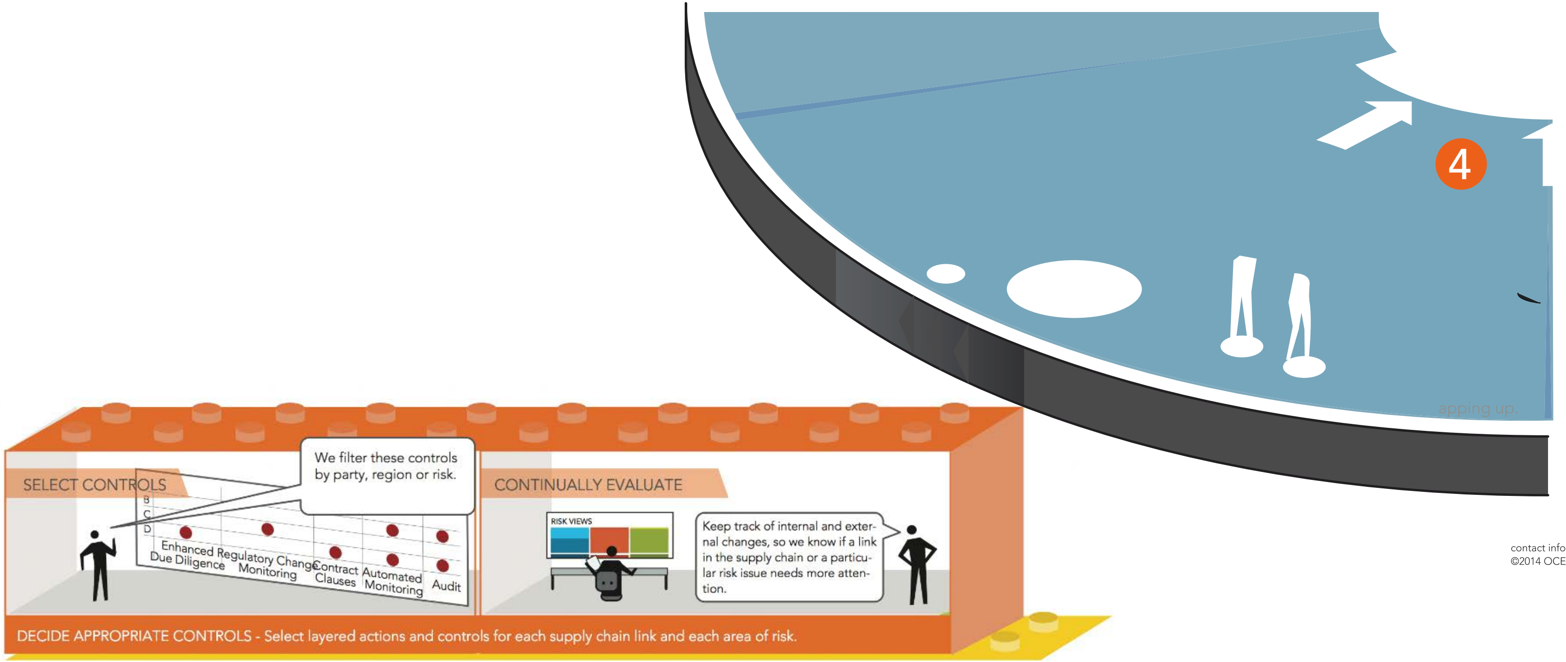


PROFILE RISKS
"Looking at each type of risk across supply chains I see too much cumulative risk in some areas.
RISK
Environmental
Labor
Disruption
PROFILE LINKS
Here we can look at each party involved across all of our supply chains to assess the real risk from each.
PRIORITIZE RISKS / PARTIES
We've set priorities and assigned management responsibilities.
We' can prove strong oversight through our system's audit trail.
DETERMINE RISK PROFILES - Analyze links and risk factors in every supply chain to identify hot spots and cumulative effects.

contact info@oceg.org for comments, reprints or licensing requests
©2014 OCEG visit www.oceg.org for other graphics in the GRC Illustrated Series

Foundational Components: Vendor Risk Management Program

4



We filter these controls by party, region or risk.

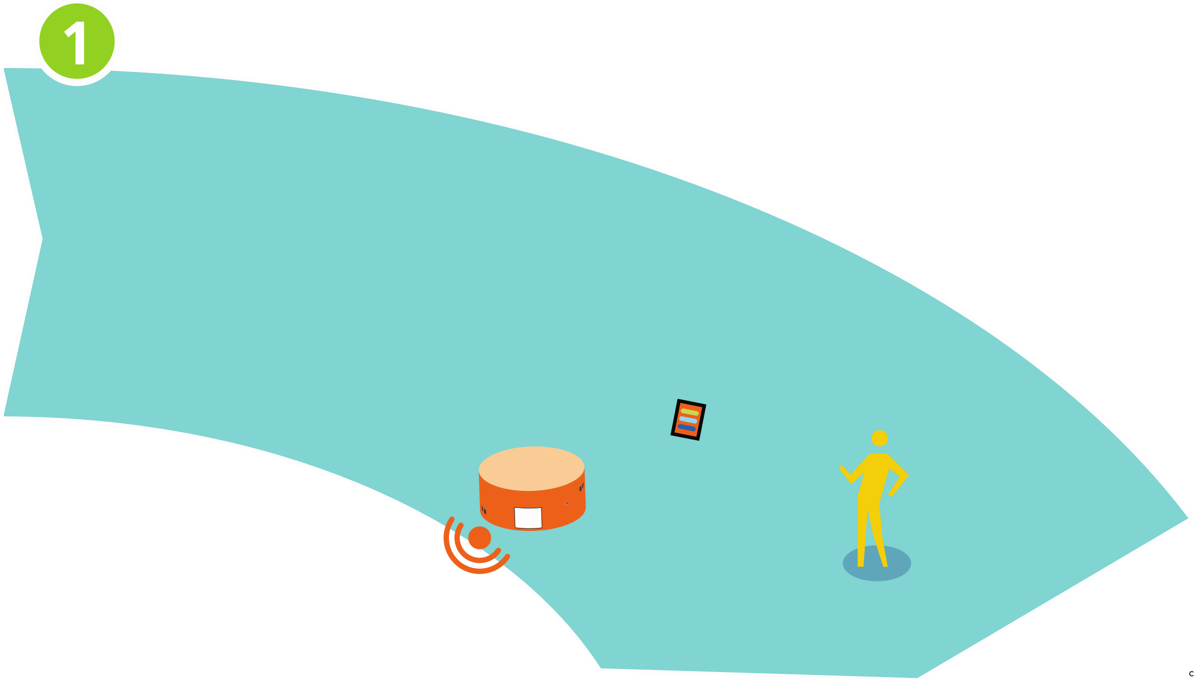
Keep track of internal and external changes, so we know if a link in the supply chain or a particular risk issue needs more attention.

DECIDE APPROPRIATE CONTROLS - Select layered actions and controls for each supply chain link and each area of risk.

contact info@oceg.org for comments, reprints or licensing requests

1 - Plan & Organize

ess supported by unified technology ensures consistency, effective communication and documentation in each step throughout the relationship lifecycle.



contact info@oceg.org for comments, reprints or licensing requests
©2014 OCEG visit www.oceg.org for other graphics in the GRC Illustrated Series

2 - Perform Due Diligence

PERFORM DUE DILIGENCE
Evaluate each third-party's controls relative to the level of defined inherent risk; determine mitigating controls to implement and document in the

ation Security and Systems
· Incident Management and Reporting
· Human Resource Management
· Conflicts of Interest

We put the self-disclosure surveys, interview reports and documentation of other credible information into the system.

3 - Manage Contracts

CONTRACT TERMS

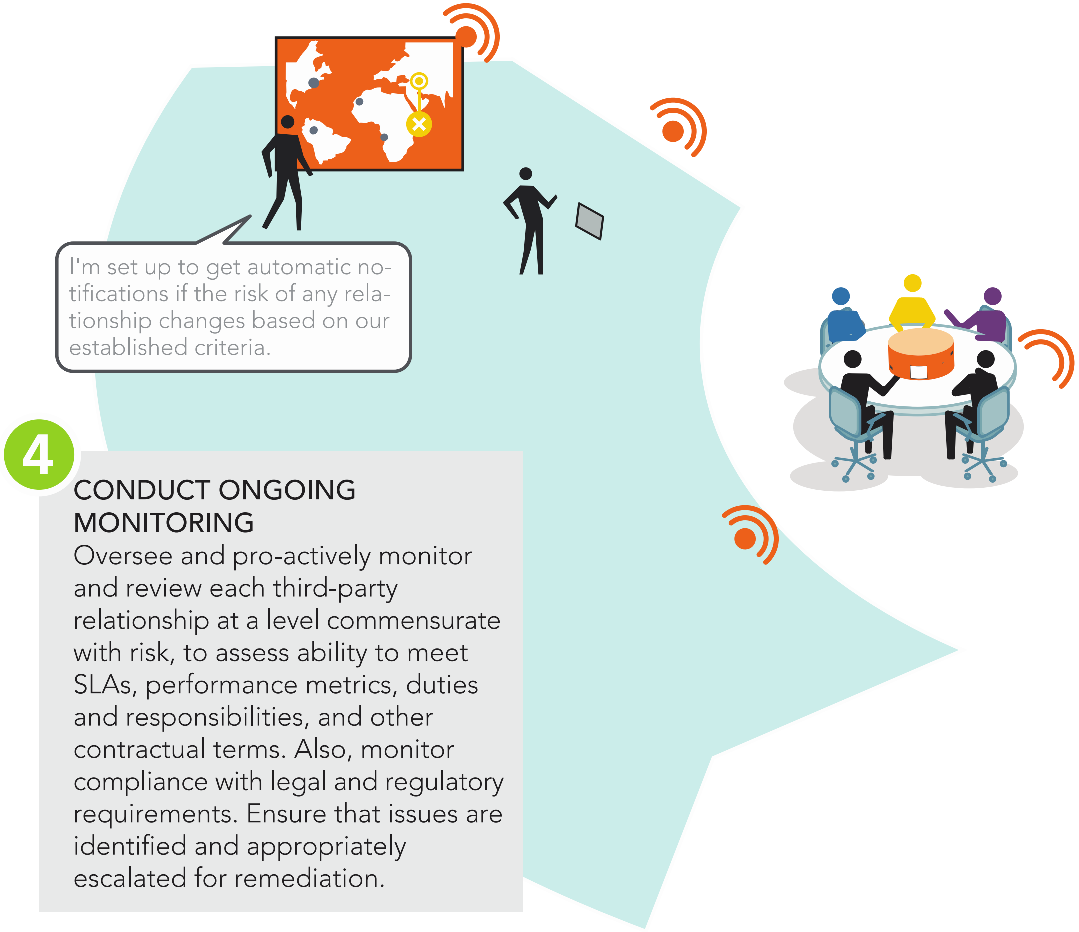
Key Performance Indicators (KPI)
Information Management/Reporting
Audit and Oversight Rights
Compliance Requirements
Use of Information, IP and Technology
Confidentiality and Integrity
Conflicts of Interest
Subcontractor Requirements
Termination Terms
Covenants

MANAGE CONTRACTS

Establish contract terms based on due diligence conclusions; through ongoing review of the relationship, re-negotiate terms addressing required and prohibited actions, SLAs and KPIs; gain oversight approval for critical contracts or those with exceptional risk.

contact info@oceg.org for comments, reprints or licensing requests

4 - Conduct Ongoing Monitoring



I'm set up to get automatic notifications if the risk of any relationship changes based on our established criteria.
4

CONDUCT ONGOING MONITORING

Oversee and pro-actively monitor and review each third-party relationship at a level commensurate with risk, to assess ability to meet SLAs, performance metrics, duties and responsibilities, and other contractual terms. Also, monitor compliance with legal and regulatory requirements. Ensure that issues are identified and appropriately escalated for remediation.

contact info@oceg.org for comments, reprints or licensing requests

5 - Manage Terminations

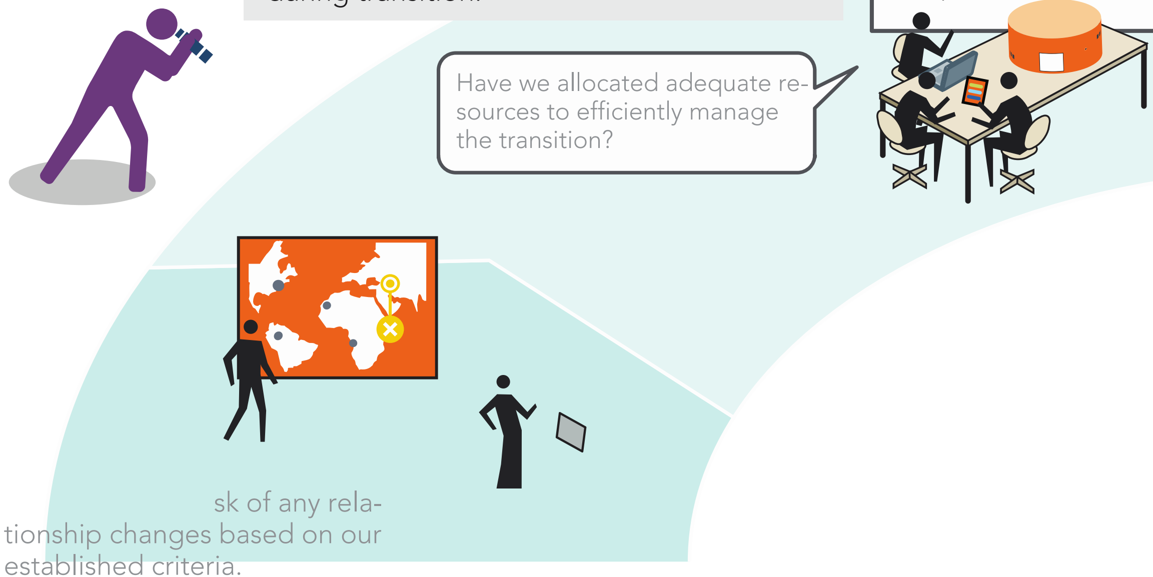
5

MANAGE TERMINATIONS

Whatever the reason for termination, follow an established plan for transitioning to another third-party, bringing activities in-house, or ending activities. Consider need to protect information, maintain smooth operations and protect reputation during transition.

STEPS TO TERMINATION

1. Implement established transition plan
2. Manage disposition of data, IP and assets
3. Discontinue and monitor all access points
4. Evaluate need to address reputation risk


Have we allocated adequate resources to efficiently manage the transition?

sk of any relationship changes based on our established criteria.

Independent Assessment

INDEPENDENT ASSESSMENT

Conduct independent review of the risk management system design and operation to ensure alignment with organizational strategy and effective third-party risk management. The level of assurance desired will determine the scope and frequency of internal and external audit. Assessment also enables preparation for supervisory review.

INTERNAL AUDIT
We are here for the annual audit of the risk system
EXTERNAL AUDIT
This integrated technology system lets us really see what is being done and how well it is working
SUPERVISORY REVIEW

DEFINING THE THIRD-PARTY RELATIONSHIP

- Outsourced products and services
- Independent consultants
- Networking and joint ventures
- Merchant payment processing
- Affiliates and subsidiaries
- Other business arrangements

Maturing Vendor Risk Management Delivers Contextual Intelligence . . .

1. Aware

- ✓ Have a finger on the pulse of business
- ✓ Watch for change in internal & external environment
- ✓ Turn data into information that can be, and is, analyzed
- ✓ Share information in every relevant direction

2. Aligned

- ✓ Support and inform business objectives
- ✓ Continuously align objectives and operations to risk of the entity
- ✓ Give strategic consideration to information from risk management enabling appropriate change

3. Responsive

- ✓ You can't react to something you don't sense
- ✓ Gain greater awareness and understanding of information that drives decisions and actions
- ✓ Improve transparency, but also quickly cut through the morass of data to what you need to know to make the right decisions

4. Agile

- ✓ More than fast, nimble
- ✓ Being fast isn't helpful if you are headed in the wrong direction.
- ✓ Risk management enables decisions and actions that are quick, coordinated and well thought out.
- ✓ Agility allows an entity to use risk to its advantage, grasp strategic opportunities and be confident in its ability to stay on course.

5. Resilient

- ✓ Be able to bounce back quickly from changes in context and threats with limited business impact
- ✓ Have sufficient tolerances to allow for some missteps
- ✓ Have confidence necessary to rapidly adapt and respond to opportunities

6. Lean

- ✓ Build the muscle, trim the fat
- ✓ Get rid of expense from unnecessary duplication, redundancy and misallocation of resources within the risk management
- ✓ Lean the organization overall with enhanced capability and related decisions about application of resources

Two Things to Note . . .

Complimentary Inquiry

- Organizations evaluating or considering GRC solutions are free to ask GRC 20/20 on our understanding and comparison of solutions in the market to meet your GRC requirements.
- Inquiries are single focused questions that can be answered in under 30 minutes.
- Complimentary inquiry is only available to organizations evaluating or considering GRC solutions for their internal use.

RFP Development & Support

- GRC 20/20 has an extensive library of RFP requirements across a range of GRC capability areas presented in this presentation.
- GRC 20/20 can be engaged in RFP development and support projects to streamline your process, gain perspectives learned from other organizations, and to keep solution providers honest in their responses.

Two More Things to Note . . .

Part 1 – Recording

http://bit.ly/2lJP6yu

Part 3 – February 21, 2:00 EST

http://bit.ly/2kfcIdv

grc 20/20

LYNX TECHNOLOGY PARTNERS

Michael Rasmussen, J.D.
The GRC Pundit & OCEG Fellow
mkras@grc2020.com
+1.888.365.4560

Subscribe GRC 20/20 Newsletter

LinkedIn: GRC 20/20

LinkedIn: Michael Rasmussen

Twitter: GRCPundit

Blog: GRC Pundit

+ 1.800.314.0455
info@lynxtp.com

GLOBAL HEADQUARTERS

1501 Broadway
12th Floor
New York, NY 10036

Pittsburgh, PA

309 Smithfield Street
3rd Floor
Pittsburgh, PA 15222

lynxgrc.com

Some of the content we have evaluated is OCEG content which GRC 20/20 has an established relationship to use. Please do not copy slides or graphics without permission. GRC 20/20 highly recommends you consider OCEG membership at www.OCEG.org.