



Sponsored by:



How to Develop a Vendor Risk Management Strategy

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

February 2017

Michael Rasmussen, J.D., GRCP, CCEP

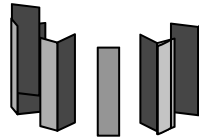
The GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

Who is a 3rd party?

“No [organization] is an island, entire of itself; Every [organization] is a piece of the continent, a part of the main.”

- John Donne





” Realize that everything connects to everything else.
Leonardo da Vinci

3rd Party Vendor Risk Bearing Down on Organizations

The issues organizations face in managing risk and compliance across extended business relationships include:

- ❑ Bribery & corruption
- ❑ Business continuity
- ❑ Code of conduct and ethics
- ❑ Conflict minerals
- ❑ Corporate social responsibility
- ❑ Environmental
- ❑ Geo-political risk
- ❑ Health and safety
- ❑ Human rights, trafficking & slavery
- ❑ Import and export compliance
- ❑ **Information security**
- ❑ Labor standards
- ❑ Operational risk
- ❑ **Privacy**
- ❑ Quality
- ❑ Regulatory compliance
- ❑ Physical security
- ❑ Supply-chain risks



You cannot outsource liability

- You “stand in the shoes” of your business relationships
- Their problems are your problems
- Their problems directly impact your brand and reputation

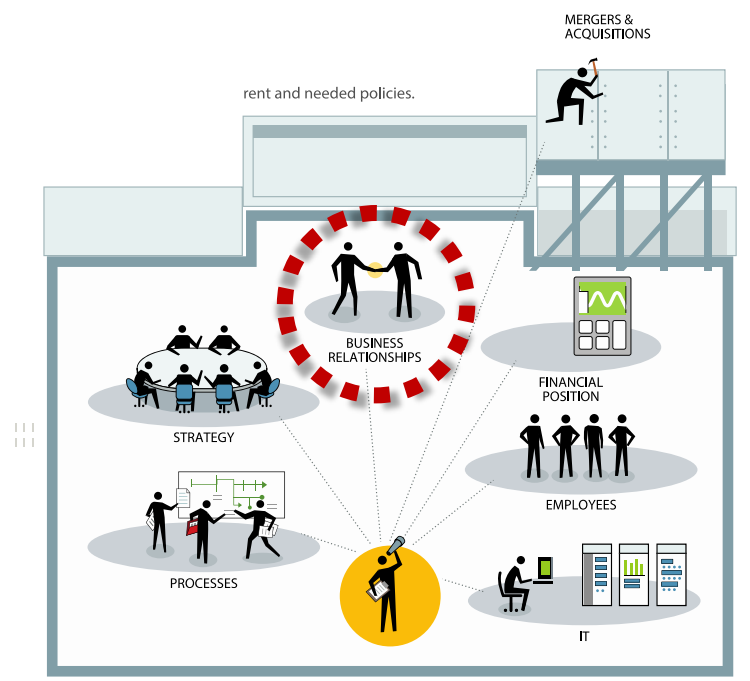
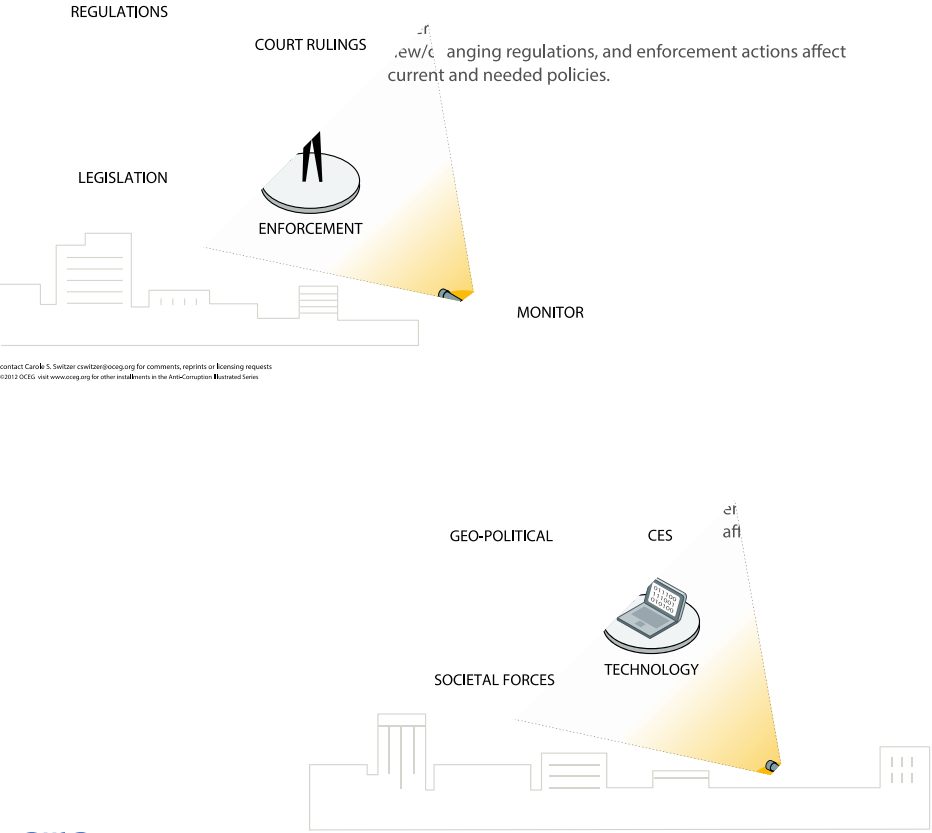
Increasing regulatory focus

- Can you attest to an “in-compliance” status?

Many companies focus on the on-boarding process...

- Most risk is incurred over the life of the relationship
- Who owns on-going third party risk?
- How is third party risk assessed and reported to the board?

Change is the Greatest Challenge Impacting Third Party Vendor Management



contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
 ©2012 OCEG visit www.oceg.org for other installations in the Anti-Corruption Illustrated Series

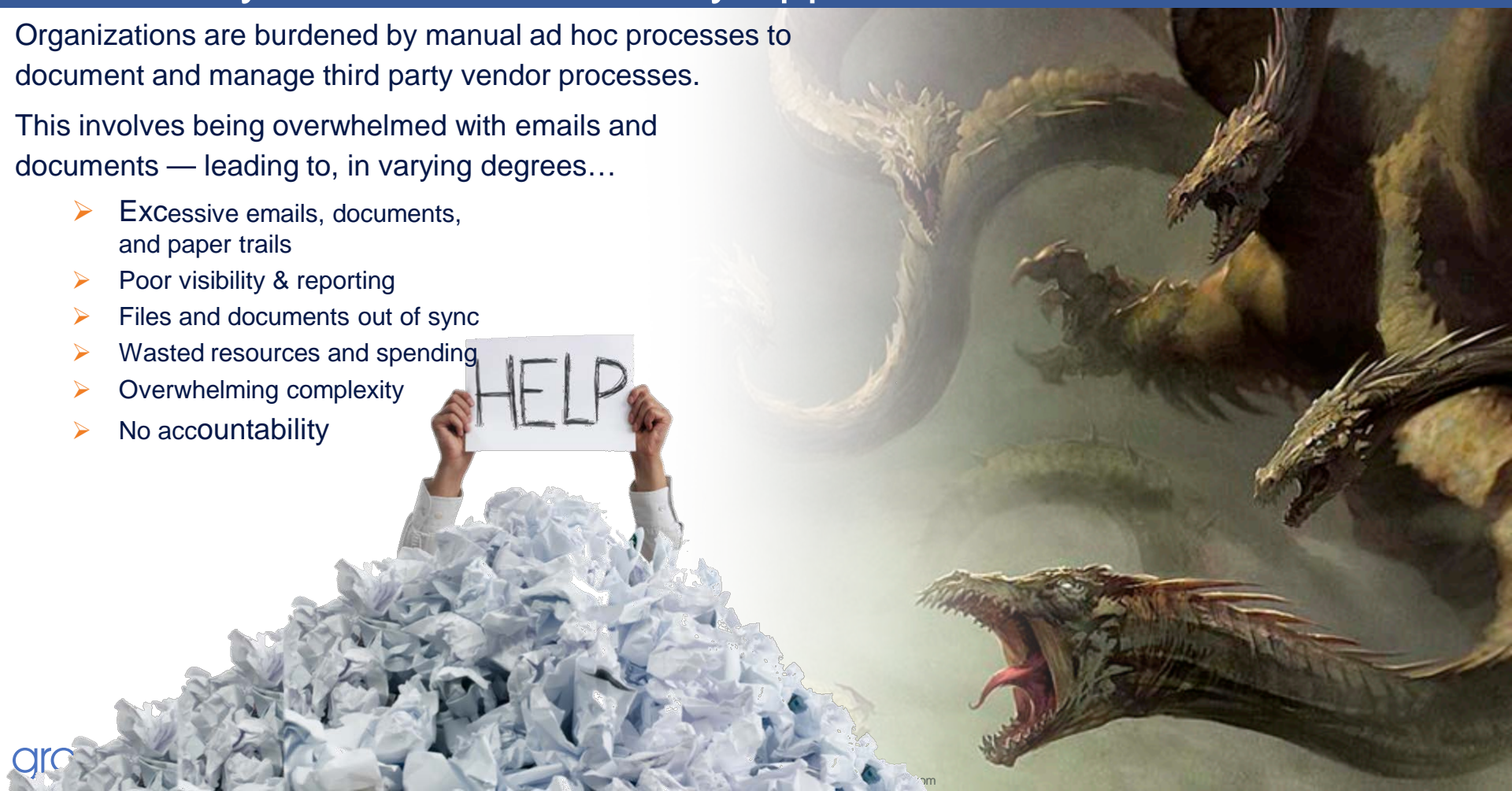
contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
 ©2012 OCEG visit www.oceg.org for other installations in the Anti-Corruption Illustrated Series

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



. . . And We Hope Nothing Fails

- Hundreds to thousands of 3rd party vendor relationships
- Different departments doing different things
- Growing regulatory and legal concern
- Reputation and brand on the line
- Lack of agility to respond timely to changing environments
- Manual processes encumbered by documents, emails, and spreadsheets

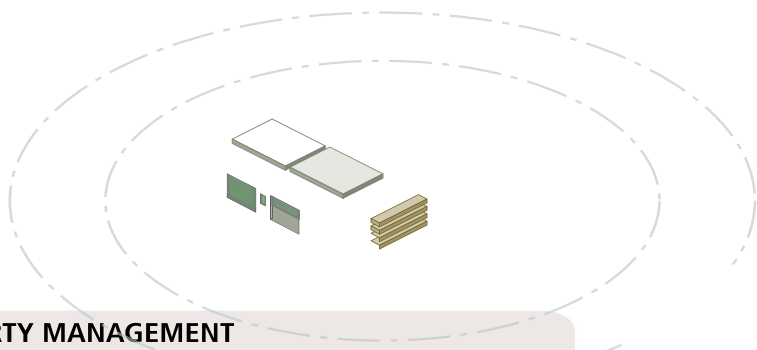


The challenge:

Can you attest to the governance, risk management, and compliance (GRC) of the organization's extended business relationships?

Typical response:

Organizations tend to look at the formation of a third party relationship and fail to foresee issues that cascade and cause damage to reputation and exposure to legal and operational risk throughout the ongoing relationship.

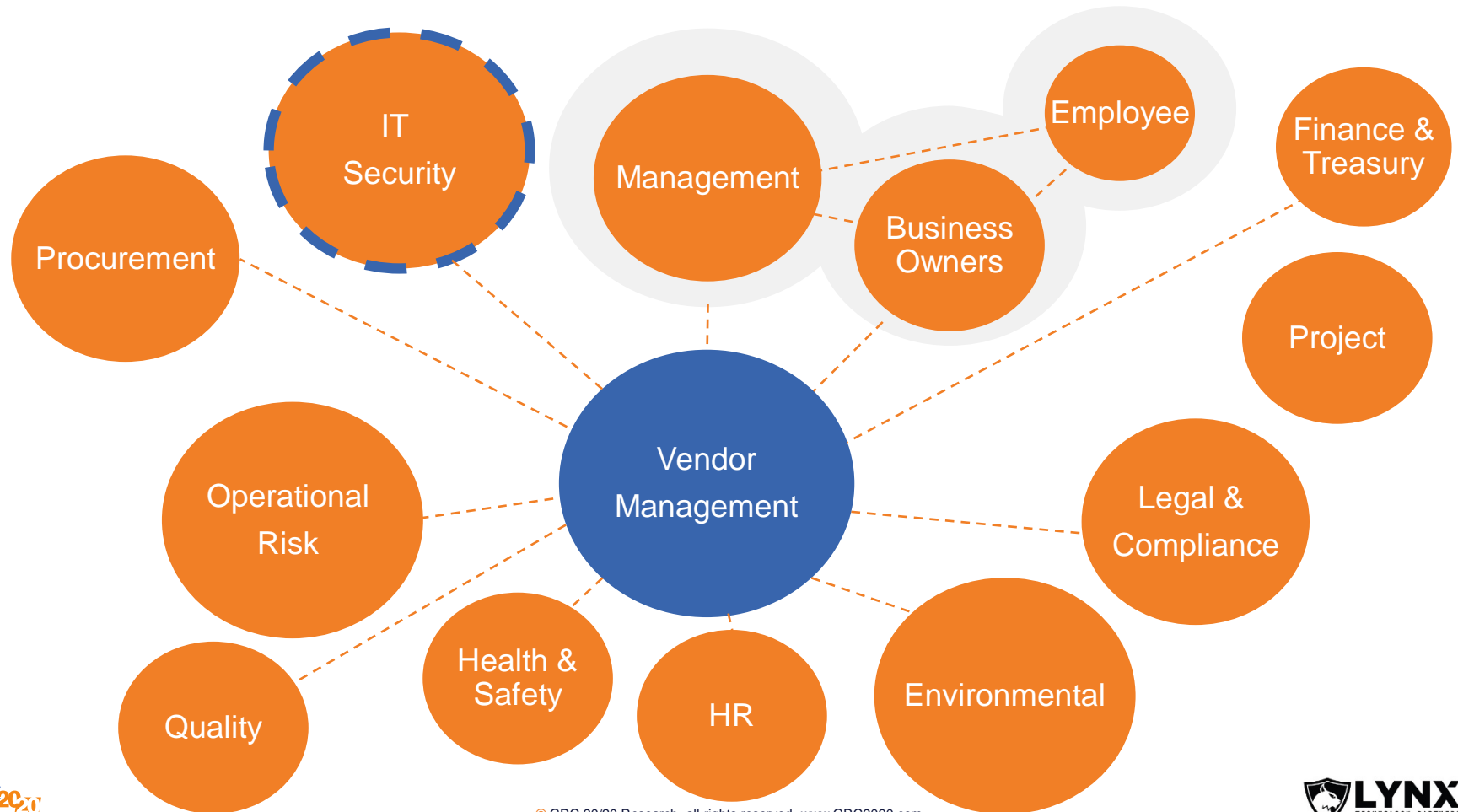


3rd PARTY MANAGEMENT

Organizations' operations are distributed across a maze of business relationships: suppliers, vendors, outsourcers, contractors and agents. Federated GRC includes the integration and oversight of performance, risk, and compliance across the organization's third party relationships and transactions.

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests
©2013 OCEG visit www.oceg.org for other installments in the GRC Illustrated Series

Vendor Management is Often a Distributed & Disconnected Function





The Organization Has to be Able to See . . .

- ❑ The Tree. The individual vendor relationship
- ❑ The Forest. The interconnectedness of relationships (e.g., risk) on the organization

GRC Definition Adapted to 3rd Party Management . . .



3rd party management is a capability that enables an organization to:

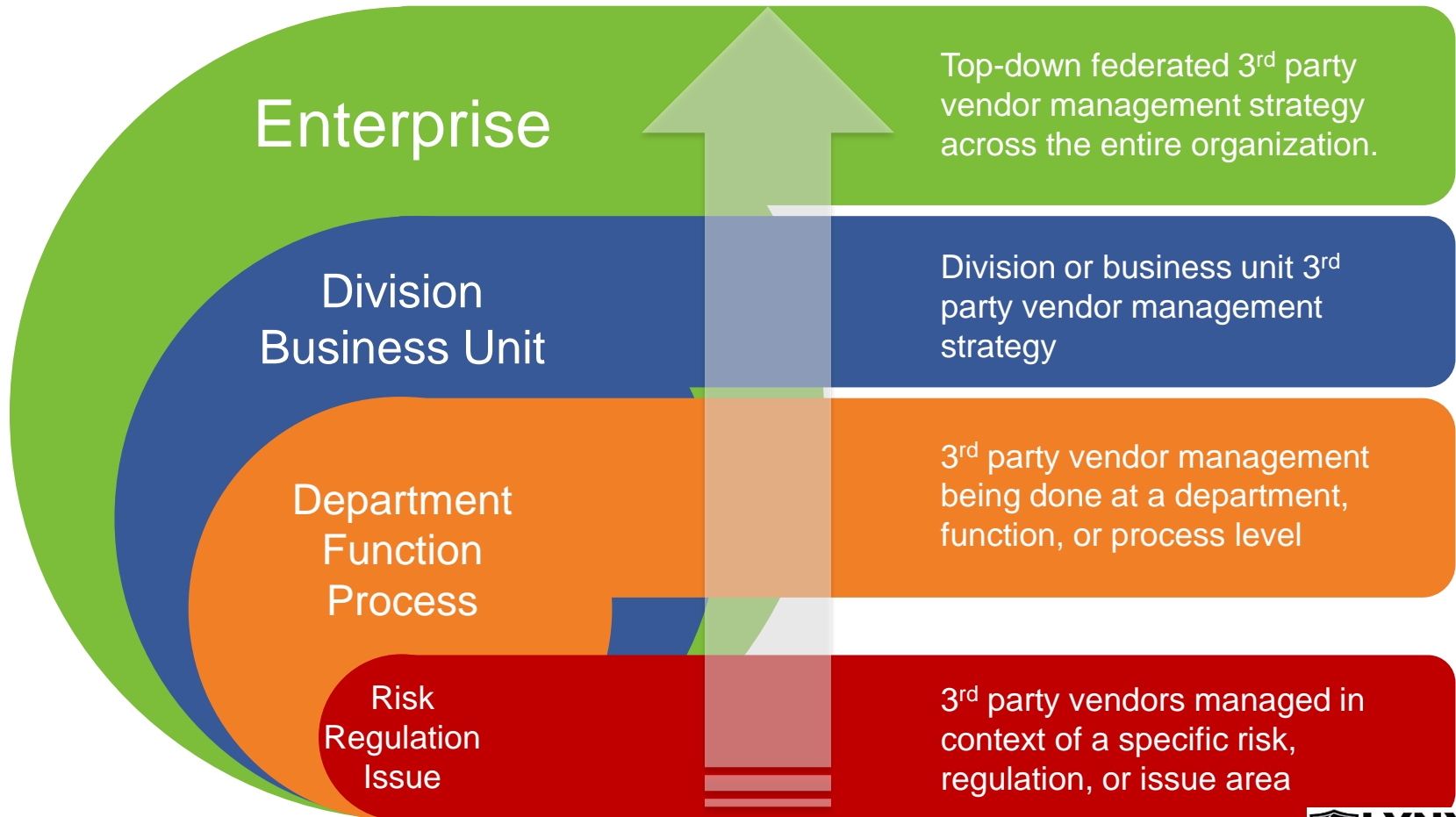
G) reliably achieve objectives

R) while addressing uncertainty and

C) act with integrity

in and across it's 3rd party relationships.

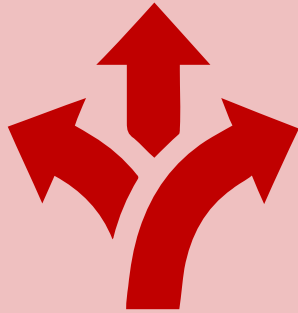
Varying Levels of Vendor Management



What is Your Approach to Vendor Management?

Distributed Vendor Party Management

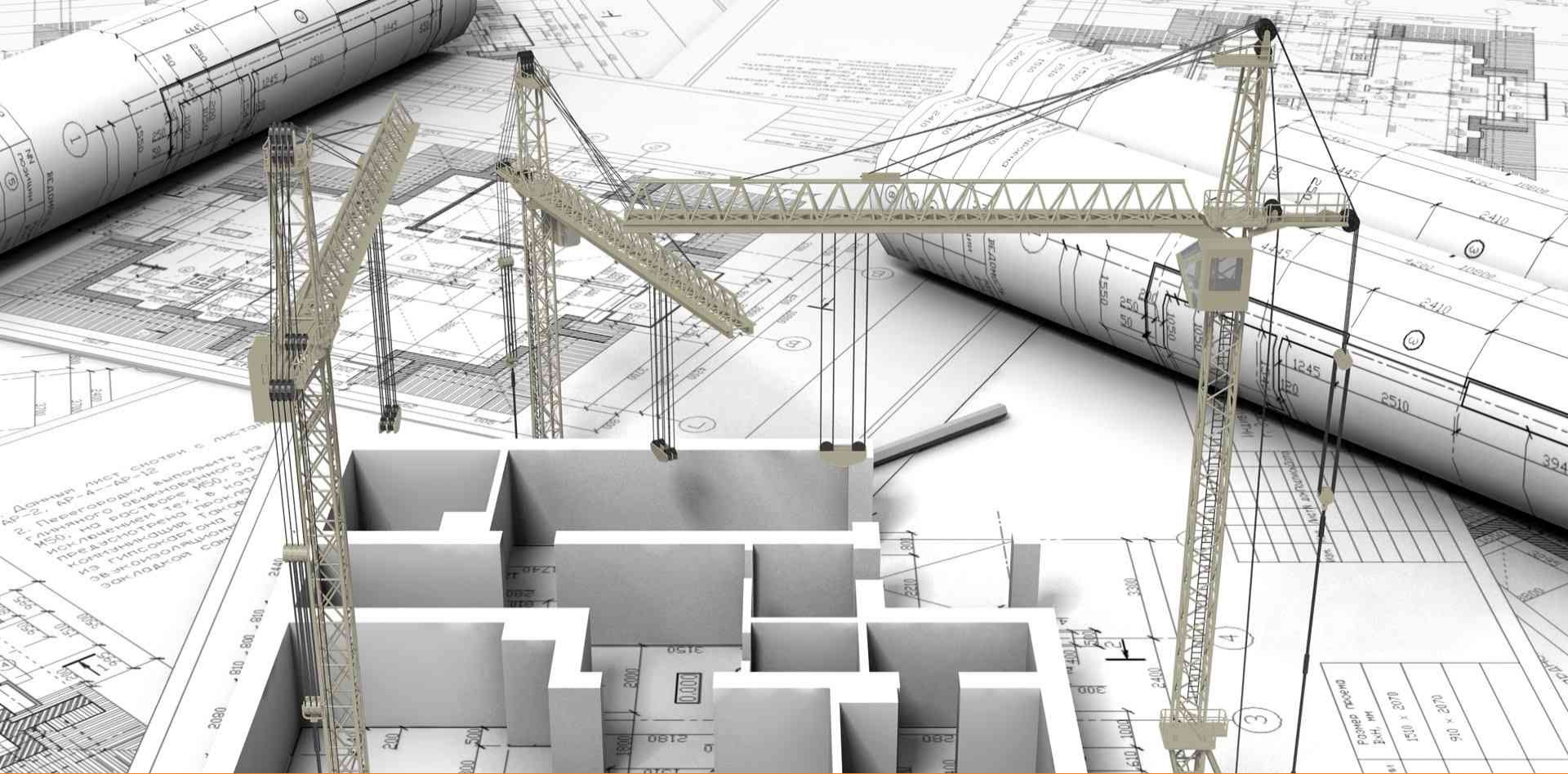
- Disconnected departments managing vendor relationships in different ways with little or no collaboration with other departments



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 Party Management Collaboration: Providing Collaboration on Vendor Management Across the Organization





Vendor Management Strategy



Vendor Management Process



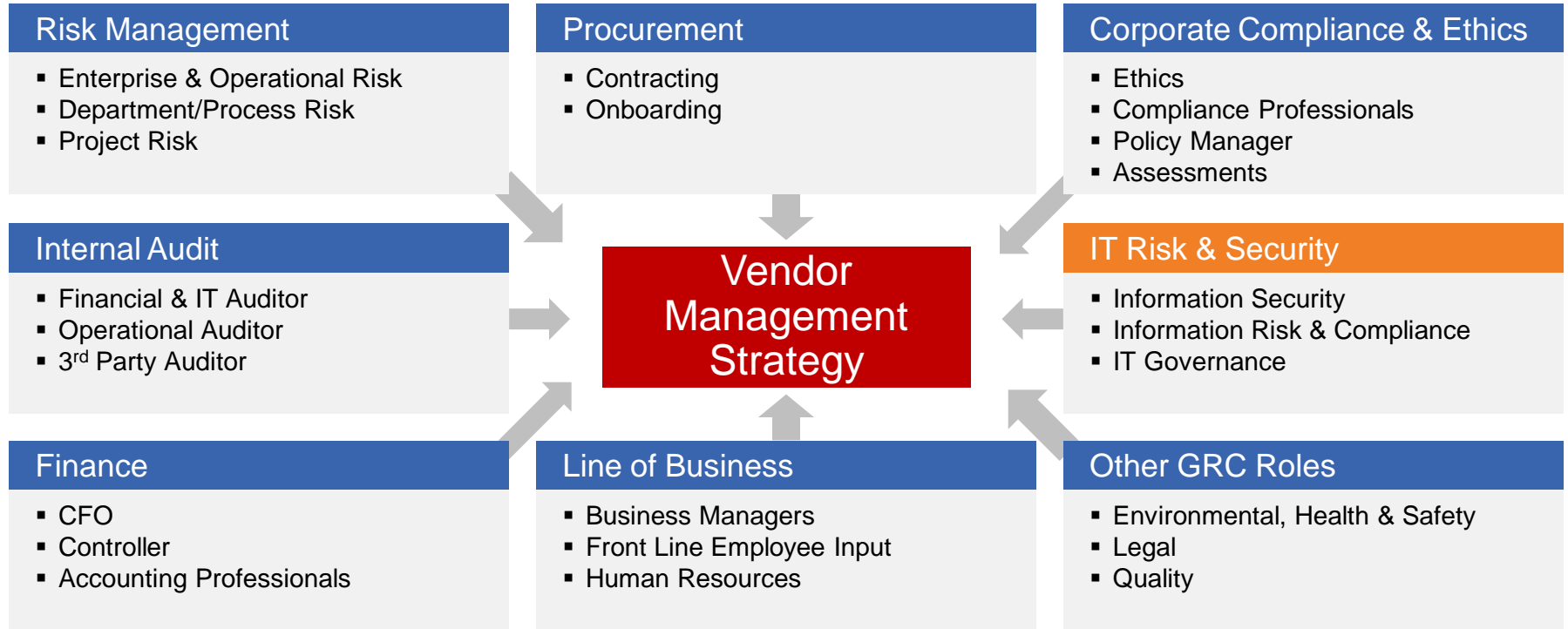
Vendor Management Information



Vendor Management Technology

Critical Roles in Vendor Management

Board of Directors & Executive Management Oversight



Vendor Party Management Charter

Mission Statement



STATEMENT

Accountability



REPORTING

Roles Groups Involved



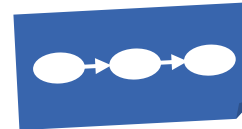
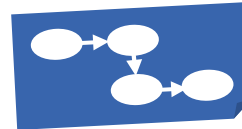
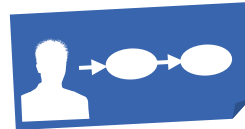
PERSONAS



Vendor Management Lifecycle & Responsibilities



PROJECTS



Resources



PORTAL

GRC/ERM

PROCUREMENT

FORMS

Understanding Vendor Management Strategy Drivers

Drivers

- What are the strategic business and regulatory drivers for vendor management in the organization?
- What are the top risks and emerging risk facing the organization in context of vendor management?
- What risks could derail business strategy?

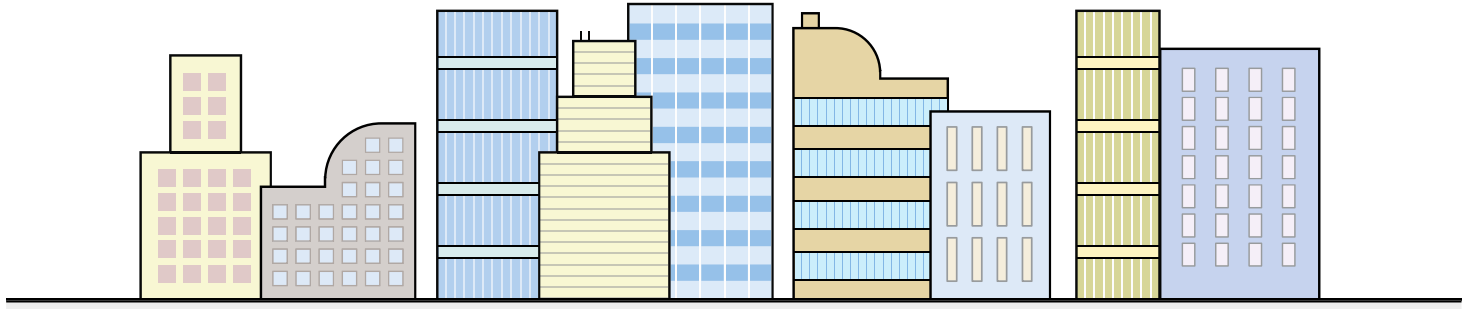
Process, Improvements and Visibility

- What is the process to manage vendors today?
- What kinds of improvements are required and being contemplated?
- What 'distinctive competence' can be gained by optimizing vendor management in the organization?
- How will a vendor management program help the organization improve business performance?
- How will a vendor management program gain visibility into risks across business units?

Governance, Team and Collaboration

- Who are the current executive sponsors for vendor management?
- How are they engaged to work collaboratively on a vendor management program?
- What culturally, and organizationally will need to change to meet the vision?
- What kinds of skill sets are required to meet the vision?
- What other stakeholders could or should be driving the program?
- What do you expect to get out of this program?

Basic Components of a Vendor Management Program



se right to audit clauses
to validate compliance in extended business
relationships.

KEYS TO SUCCESS



KNOW WHO, WHERE & WHAT

Maintain a database on each 3rd party and 3rd party relationship, internal relationship owners, locations of operations, contract terms, risk and value assessments, required controls and measurements, and issues that arise.

CONTINUALLY EVALUATE RISK & VALUE

Use a 3rd party management platform to rank each party for risk in areas of concern and value added by the relationship; establish appropriate requirements and controls and revisit as factors

ENSURE NOTIFICATION & ACTION

Automate triggers for notifications to all necessary internal and external parties when new information arises or review is needed; automate revised risk assessments, new training or other actions where possible and appropriate.

COMMON MISTAKES



MANAGING MANUALLY

Allowing siloed oversight of 3rd party contracts in spreadsheets and documents that do not provide a unified approach or view of information; failing to keep information updated in context of change in internal or external events.



NOT STANDARDIZING POLICIES & PROCEDURES

Allowing different parts of the organization to use different procedures and systems for onboarding 3rd parties, conducting risk assessments and managing relationships.



FAILING TO CONSIDER INTERNAL PARTIES

Failing to map responsibilities for aspects of 3rd party relationships; applying the same controls to all internal relationship managers, regardless of the level of risk or value presented by their 3rd party contracts.

Maturing Vendor 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

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.

Part 2 – February 14, 2:00 EST



<http://bit.ly/2jWw21E>

Part 3 – February 21, 2:00 EST



<http://bit.ly/2kfcldv>



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