



Sponsored by:



How to Design a Vendor Risk Management Information & Technology Architecture

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

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

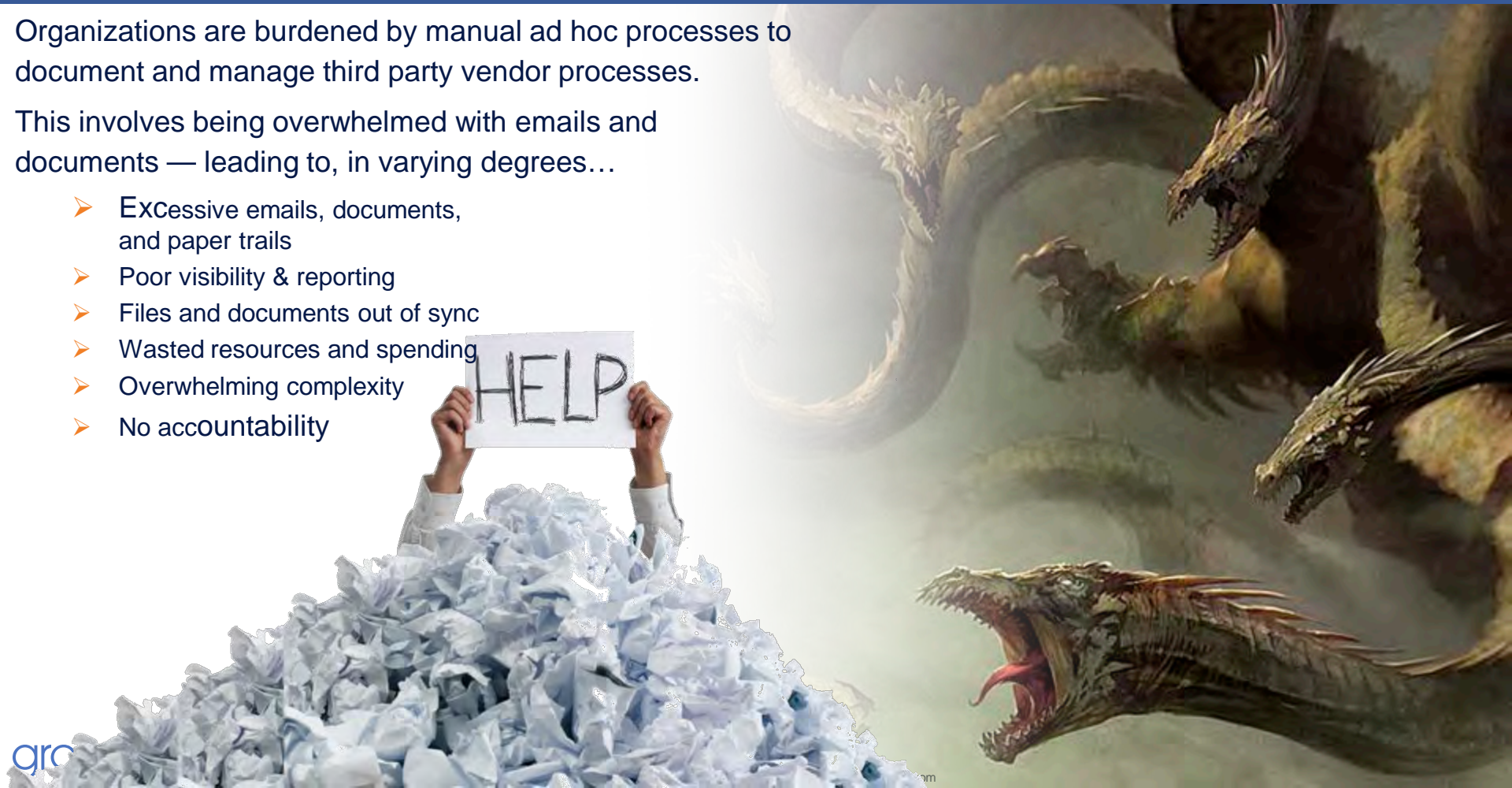
in and across it's 3rd party relationships.

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...

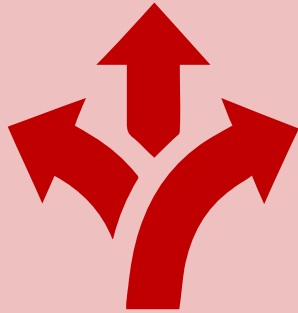
- Excessive emails, documents, and paper trails
- Poor visibility & reporting
- Files and documents out of sync
- Wasted resources and spending
- Overwhelming complexity
- No accountability



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 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.



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.



AUDIENCE

Define 3rd parties 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.



INTERNAL STAFF

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



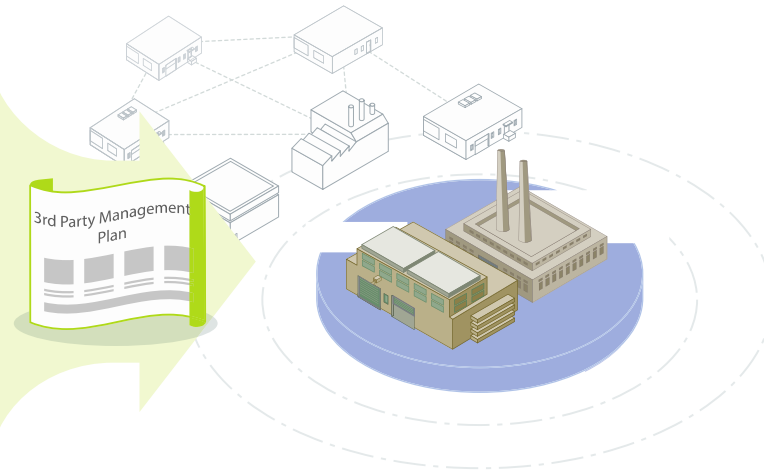
EXECUTIVE SUPPORT

Gain executive support of the 3rd party management program

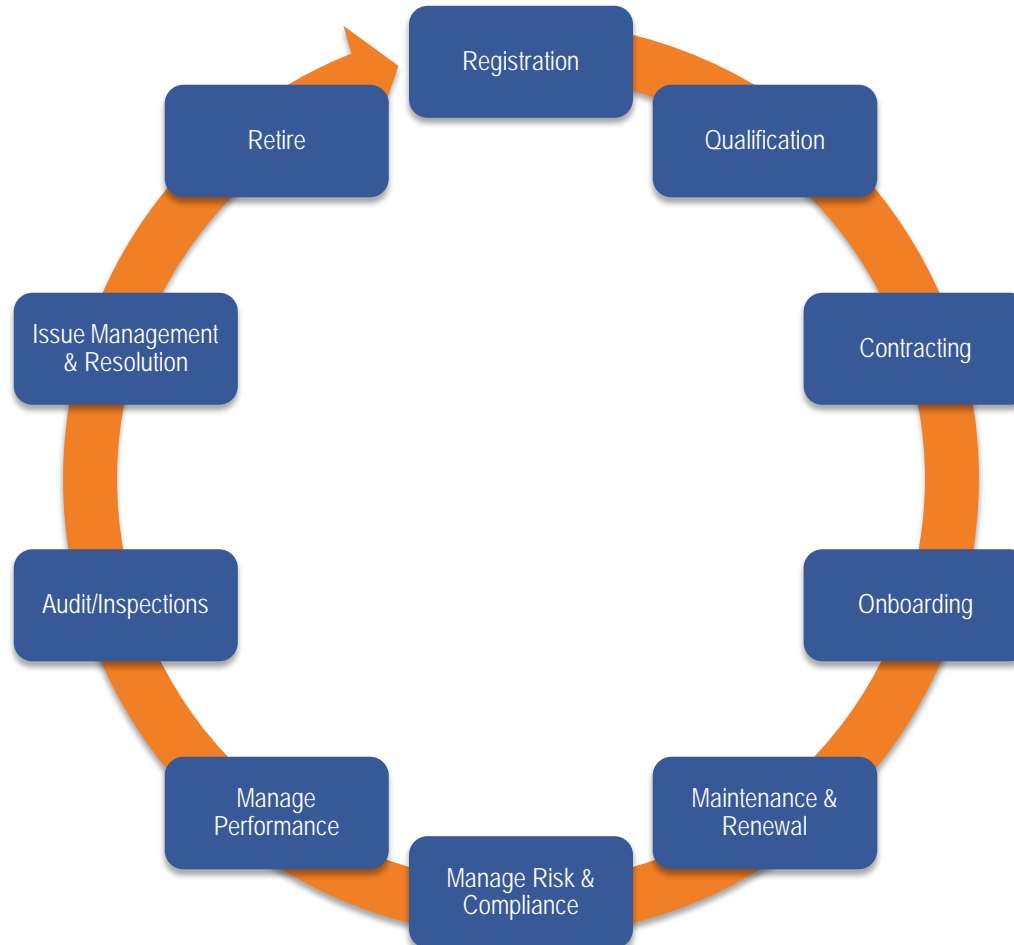


ACCESSIBILITY

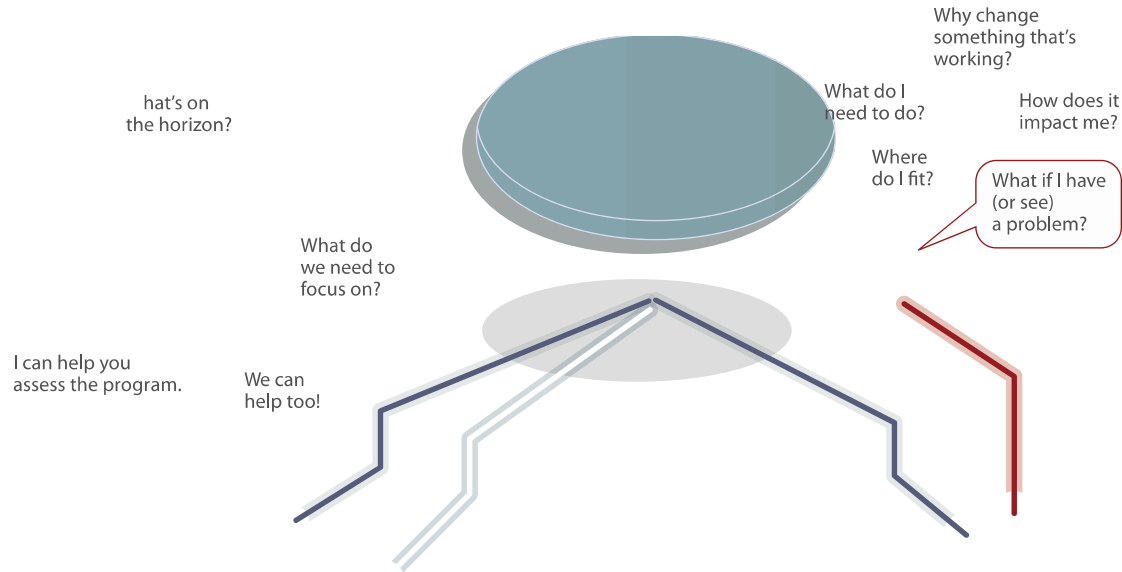
Ensure that 3rd party communications are be accessible, understandable and actionable by all groups regardless of education level, geography, culture, language, ethnic group or disability status.



Overview of a Vendor Risk Management Process



Central Hub of Vendor Risk Information

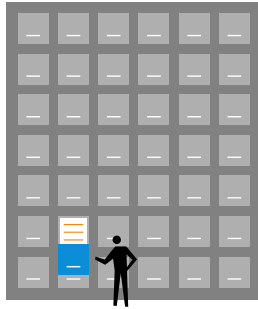


Vendor Risk Management Technology Provides Automation and Tracking

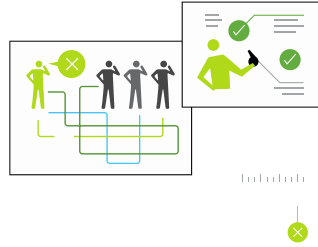
MANAGEMENT REPORTING



AUDIT TRAIL



WORKFLOW & TASKS



COLLABORATION



ENFORCEMENT



Accountability

Automation

Repository

Consistency

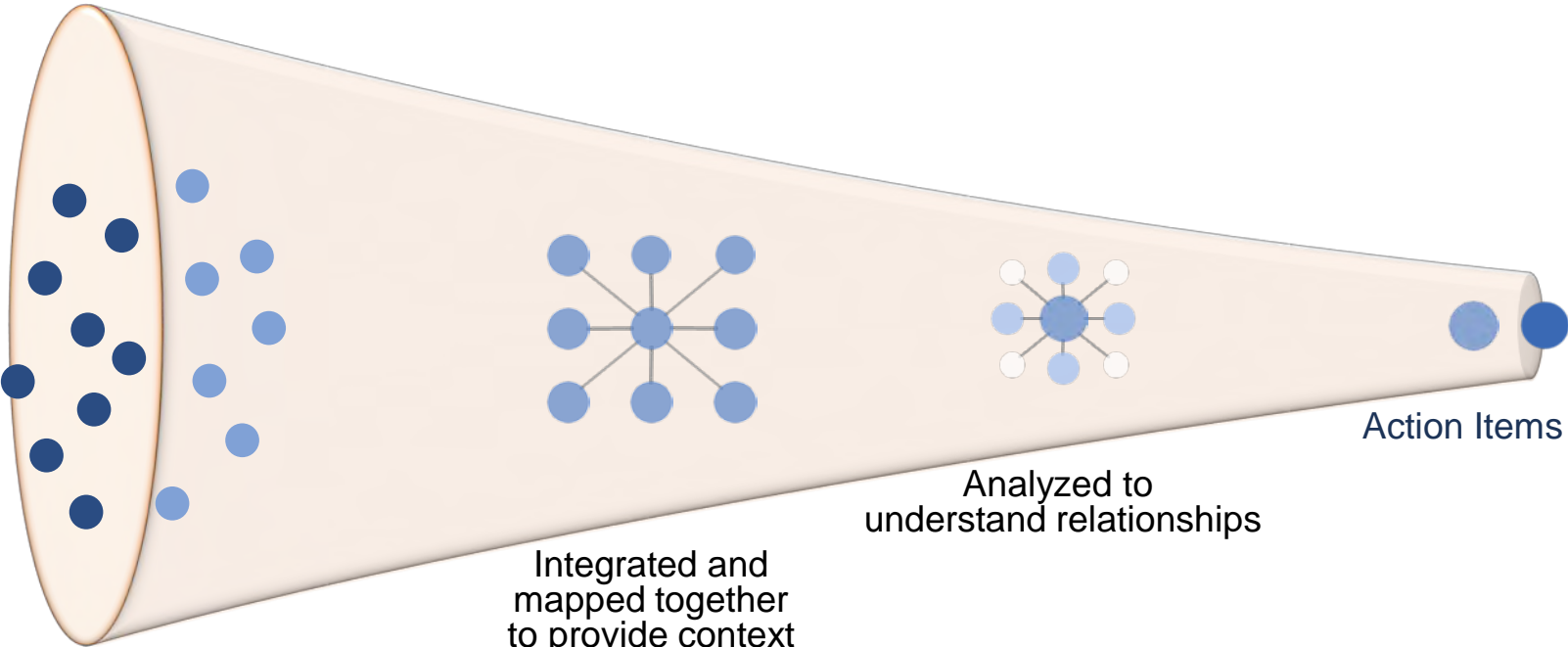


360° Vendor Risk Management Contextual Intelligence

- Contracts
- Transactions
- Due Diligence
- Geo-Political Events
- Assessments
- Attestations
- Capabilities
- Training
- Disclosures
- Performance
- Quality
- Audits
- Inspections
- SLAs
- Negative News
- Sanctions



Distributed & Disconnected
3rd Party Data Points

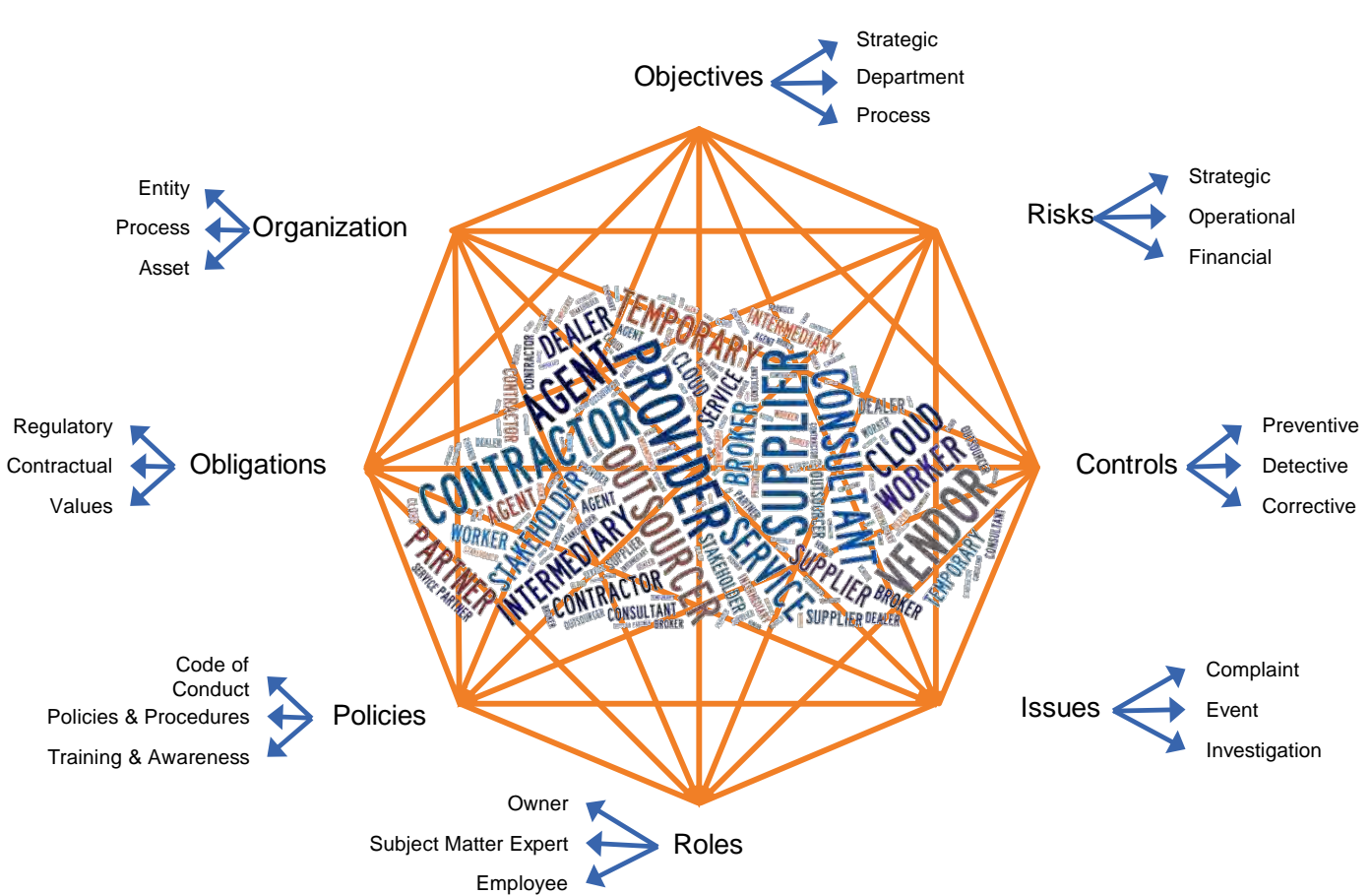


Integrated and mapped together to provide context

Analyzed to understand relationships

Action Items

Vendor Risk Information Architecture Provides 360° Contextual Intelligence



process optimization
All non-value-added activities are eliminated and value-added activities are streamlined to reduce lag time and undesirable variation.

better capital allocation
Identifying areas where there are redundancies or inefficiencies allows financial and human capital to be allocated more effectively.

reduced costs help to improve return on investments made in GRC activities

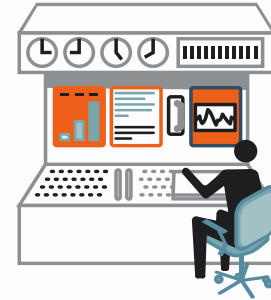


GRC Capability Area Definitions

GRC Capability Area	Description
Enterprise GRC	Capability to manage an integrated architecture across multiple GRC areas in a structured strategy, process, information and technology architecture.
Audit Management	Capability to manage audit planning, staff, documentation, execution/field work, findings, reporting, and analytics..
Automated Control	Capability to automate the detection and enforcement of internal controls in business processes, systems, records, transactions, documents, and information.
Business Continuity Management	Capability to manage, maintain, and test continuity and disaster plans, and implement these plans expected and unexpected disruptions to all areas of operation.
Compliance Management	Capability to manage an overall compliance program, document and manage change to obligations, assess compliance, remediate non-compliance, and report.
Environmental Management	Capability to document, monitor, assess, analyze, record, and report on environmental activities and compliance.
Health & Safety Management	Capability to manage, document, monitor, assess, report, and address incidents related to the health and safety of the workforce and workplace,
Internal Control Management	Capability to manage, define, document, map, monitor, test, assess, and report on internal controls of the organization.
IT GRC Management	Capability to govern IT in context of business objectives and manage IT process, technology, and information risk and compliance.
Issue Reporting & Management	Capability to notify on issues and incidents and manage, document, resolve, and report on the range of complaints, issues, incidents, events, investigations, and cases.
Legal Management	Capability to manage, monitor, and report on the organization's legal operations, processes, matters, risks, and activities.
Physical Security Management	Capability to manage risk and losses to individuals and physical assets, facilities, inventory, and other property..
Policy & Training Management	Capability to manage the development, approval, distribution, communication, forms, maintenance, and records of policies, procedures and related awareness activities.
Quality Management	Capability to manage, assess, record, benchmark, and track activity, issues, failures, recalls, and improvement related to product and service quality.
Risk Management	Capability to identify, assess, measure, treat, manage, monitor, and report on risks to objectives, divisions, departments, processes, assets, and projects.
Strategy & Performance Management	Capability to govern, define, and manage strategic, financial, and operational objectives and related performance and risk activities.
	Capability to govern, manage, and monitor the array of 3 rd party relationships in the enterprise, particularly risk and compliance challenges these relationships

3rd Party Management Technology Architecture

We need to consolidate information in a unified technology system to effectively manage, document and report on each third-party relationship.



Third Party Management Technology

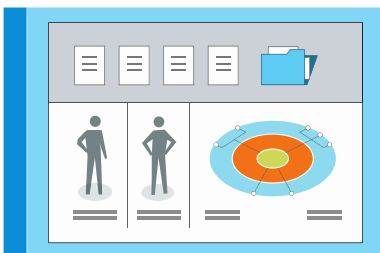
Third Party Management Platforms

Third Party Risk Management Solutions

Procurement & ERP Third Party Solutions

Screening & Due Diligence Solutions

Miscellaneous Third Party Management Tools



AUTOMATION AND TRACKING

Technology enables the change tracking and monitoring process by integrating information and content sources with software that automates and tracks workflow, accountability, and analysis of changes or additions

Third Party Intelligence & Content

Third Party Forms & Templates

PEP/Sanction/Watch Lists

Negative News

Organization/Corporate Ratings

Geo-Political Risk

Reputation & Brand Lists & Monitoring

Sourcing Information

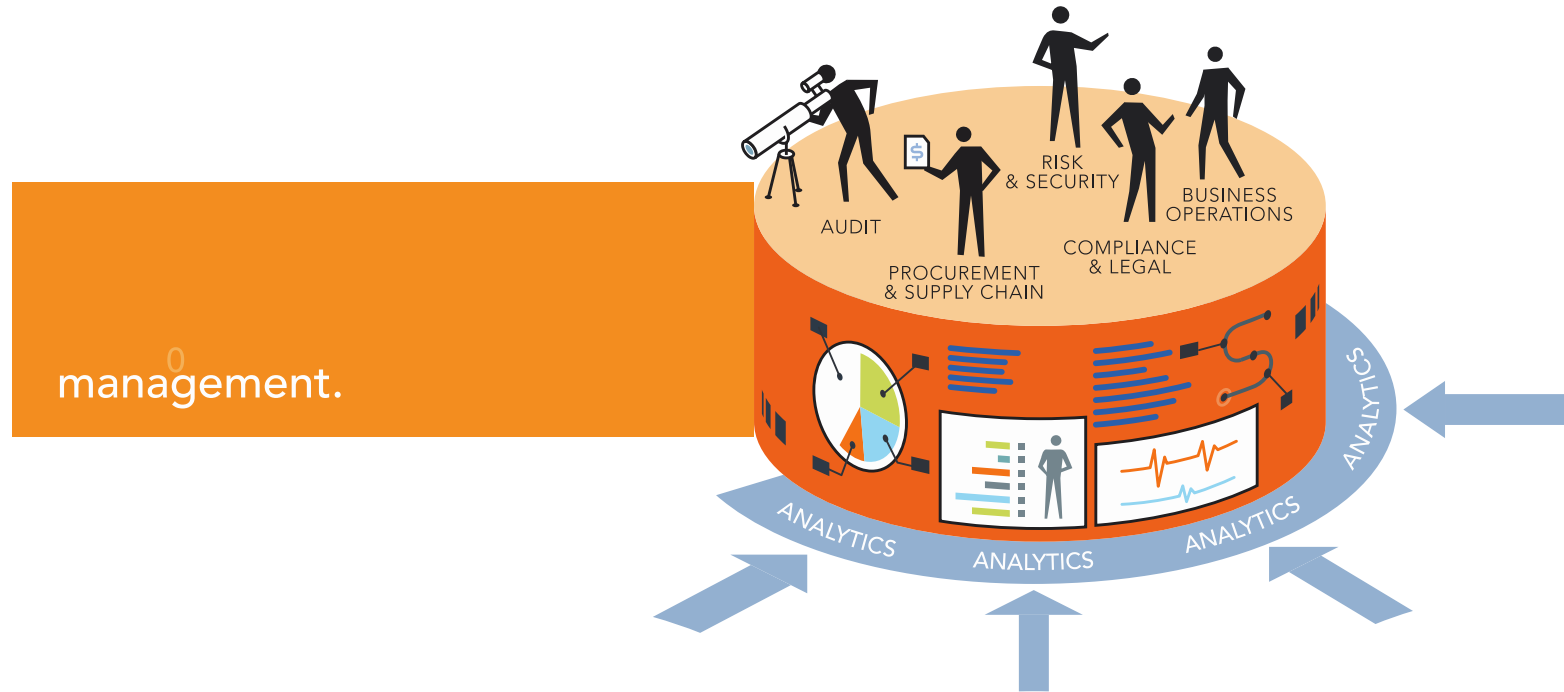
Vessels Data

Controlled Goods & Substances

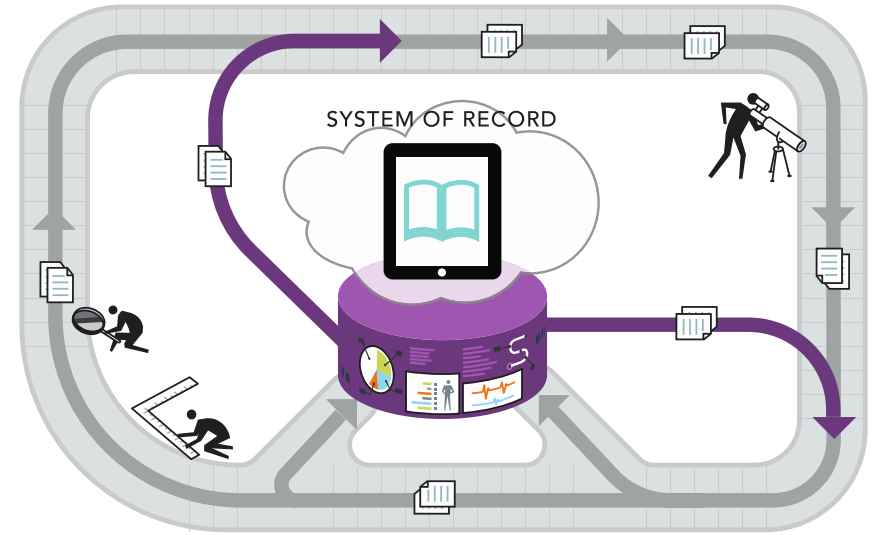
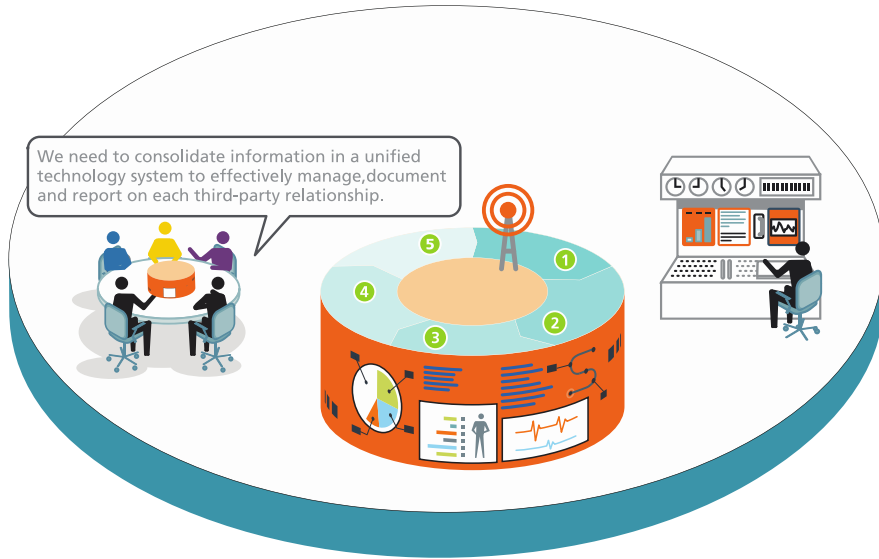
IT Security Ratings

Integrated 3rd Party Management

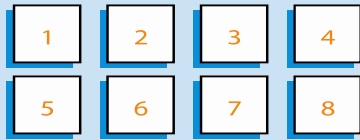
In today's complex economy, your suppliers, distributors, sub-contractors, agents and other 3rd parties play critical roles in your business success. Its too complex to manage without an integrated strategy that includes people, process and technology . The goal is to protect and grow value by establishing 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.



Vendor Risk Management Solutions Provide Defensibility & Accountability



VERSION (DATE/TIME)



ASK & RESOLVE QUESTIONS



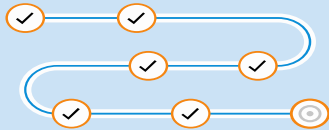
MEET REQUIREMENTS



MANAGE EXCEPTIONS



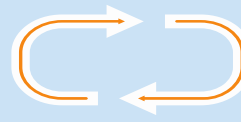
UNDERSTAND CONTEXT



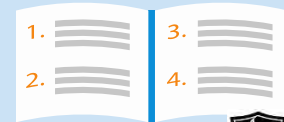
PROVIDE AUDITABLE RECORDS



REPEATABLE CYCLE



DEMONSTRATE SEQUENCE



Critical Elements of a Vendor Risk Information & Technology Architecture

Vendor EMPOWERMENT

- The need to collaborate and provide full visibility into 3rd party relationships while balancing 3rd party confidentiality.

USER EXPERIENCE

- The need to provide an intuitive and easy to use experience that is usable by an international audience

MULTI-USE INFORMATION

- Integration of internal and external data that has multiple functions and purposes to turn data into intelligence

DELIVERY MODEL

- The need to have a solution that is easy to access globally and provides a platform for collaboration and sharing in a network while providing confidentiality of sensitive information.

CONFIGURATION

- The need to have a solution that is agile in its ability to be extended and modified to meet specific organization requirements.

LIFECYCLE

- The need to manage the lifecycle of 3rd party relationships from onboarding to offboarding

Solution Area Definition

Vendor Risk Management solutions provide capabilities to govern, manage, and monitor the array of 3rd party relationships in the enterprise, particularly risk and compliance challenges these relationships bring.

This enables organizations to manage:

- 3rd party management process of onboarding, approval, due diligence, communications, assessment, evaluation, issue management, and off-boarding. This includes workflow, task management, and content management capabilities.
- 3rd party portal for 3rd parties to be able to submit and share information, take assessments, provide attestations, and other related requests and forms, to complete tasks.
- Provide evidence to provide a system of record and audit trail of all interactions, assessments, audits/inspections, and interactions with
- 3rd parties.



Critical Capabilities

- ❑ Onboarding process to register suppliers and have them submit necessary documentation
- ❑ Due diligence process during onboarding and periodically or continually thereafter
- ❑ Risk assessment and analysis of 3rd party relationships
- ❑ Policy communication & attestation to 3rd parties
- ❑ Training & awareness of 3rd parties
- ❑ Compliance assessment and analysis of 3rd party relationships
- ❑ Issue management through issue reporting/identification, response/investigation, and resolution.
- ❑ Forms & disclosure management for 3rd parties to fill out forms and submit information
- ❑ Audit & inspection management of 3rd parties in context of right to audit clauses
- ❑ Management of the off-boarding process





Characteristics: Basic 3rd Party Management Solutions

Basic 3rd party management platforms focus on the workflow, forms, and tasks of 3rd party management. The value focus is on task automation by removing inefficiencies of manual approaches of documents, spreadsheets, and emails and replacing this with a solution that can collect information, manage workflow and tasks, and simplify reporting. Content, if provided, is typically in context of a single 3rd party management area (e.g., anti-bribery & corruption, information security).

Capabilities

- ✓ Supports back-end process of 3rd party management
- ✓ Workflow & task management
- ✓ Compliance & risk self-assessments & reporting
- ✓ Basic due diligence in context of workflow and tasks
- ✓ Notification
- ✓ Tracking attestations
- ✓ Reporting and tracking issues
- ✓ Survey capabilities to deliver self-assessments
- ✓ Audit trail/system of record of 3rd party related activities

Limitations

- Limited content integration, typically in context of one area and not across the organization
- Focus is rather narrow in addressing specific issues of 3rd party management and not a platform for managing a range of 3rd party governance, risk, and compliance



Characteristics: Common 3rd Party Management Platforms

Common 3rd party management platforms have the range of features commonly found in enterprise 3rd Party Management RFPs that span the organization's 3rd party needs. They build upon the foundation of workflow, tasks, assessments, and forms with features to provide greater integration with other systems, and have better content integration.

Capabilities

- ✓ Has workflow, task, assessment, and content capabilities of Basic solutions
- ✓ Ability to manage the entire 3rd party management process from onboarding through offboarding
- ✓ Integration with ERP and other business systems to collect and monitor 3rd party information and transactions
- ✓ Basic contract management capabilities with ability to define and monitor SLAs, KPIs, and KRIs in 3rd party relationships
- ✓ Basic portal capability to collect and communication information with 3rd parties
- ✓ Audit & inspection management of 3rd parties

Limitations

- 3rd party content and intelligence sources is still often limited in scope
- Portal for 3rd parties is more utilitarian in focus and lacks advanced collaborative features
- Typically does not offer self-registration capabilities

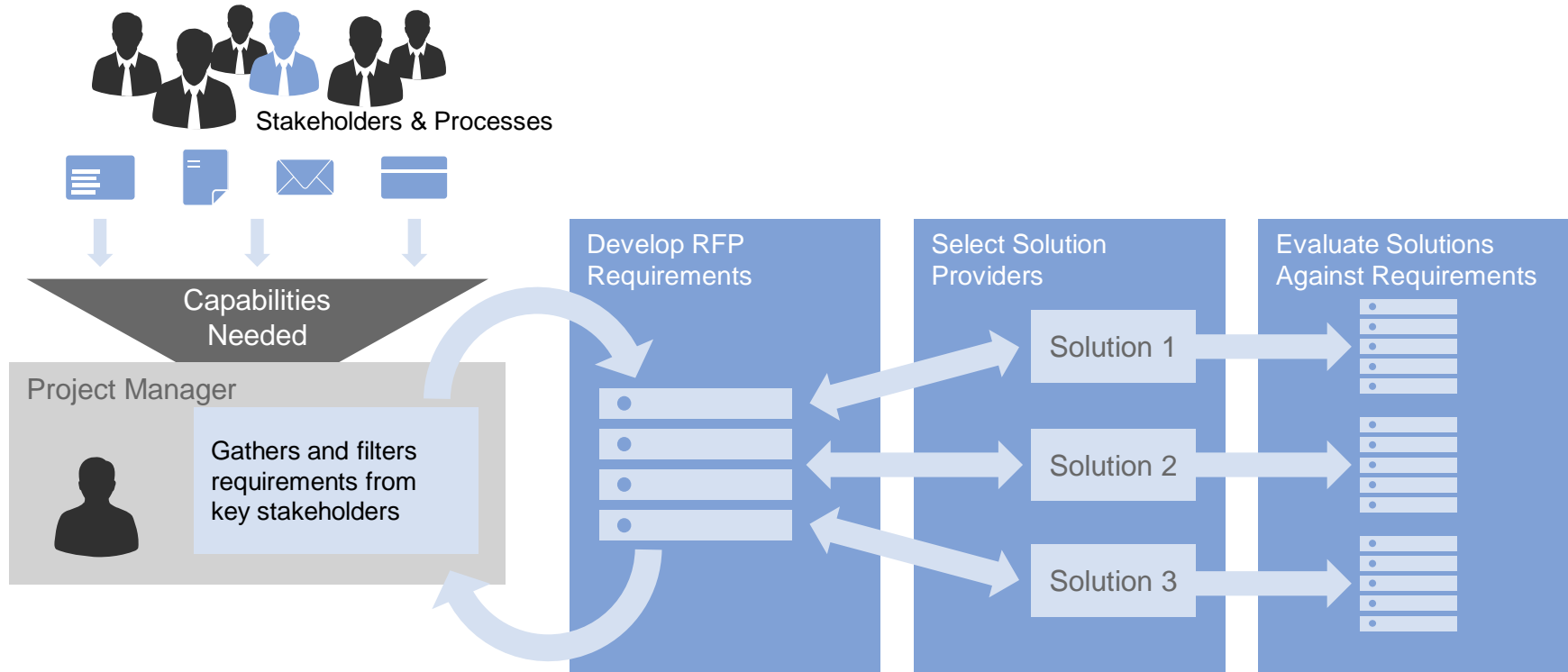


Characteristics: Advanced 3rd Party Management Platforms

Advanced 3rd party management platforms are Common Platforms that have distinguished themselves from competitors by offering advanced capabilities in different areas. Areas of Advanced Capabilities (note, a solution might have one or more of these) include:

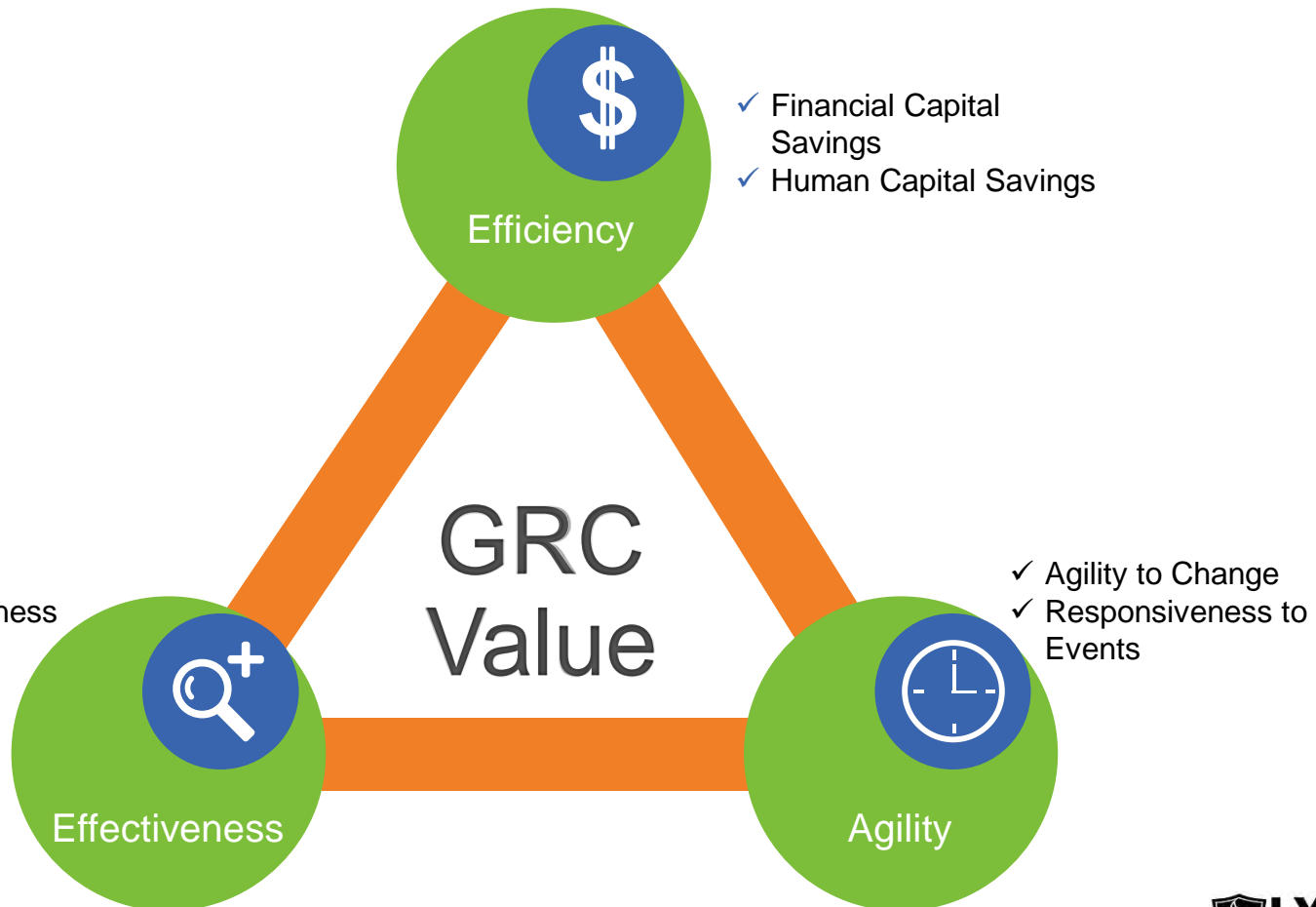
- ✓ 3rd party portal. The solution has a strong, intuitive, engaging portal for 3rd parties to access and interact with policies.
- ✓ Self-registration. The solution and portal supports a 3rd party self-registration process during onboarding with a wizard interface to scope relationship, level of due diligence and acceptance and collect information.
- ✓ Master data records & 3rd party information management. The solution can integrate with a variety of ERP and other business systems to collect information and be the primary source of master data records on 3rd parties.
- ✓ Ongoing/continuous due diligence. The solution provides the capability to monitor 3rd parties on a continuous basis against a range of screening, sanction, negative news databases to proactively alert the organization on changes.
- ✓ Contract lifecycle management. The solution has full contract lifecycle management capabilities.
- ✓ 3rd party networks. The solution provides a collaborative platform for organizations to participate in that allows many to many interactions and the ability to assess once and the assessment to be good for multiple relationships.
- ✓ Spend analysis. The solution allows for overall spend analysis and performance management of 3rd party relationships.
- ✓ 3rd party planning. The solution enables the organization to strategically plan 3rd party relationships.

3rd Party Management Platform Selection Process

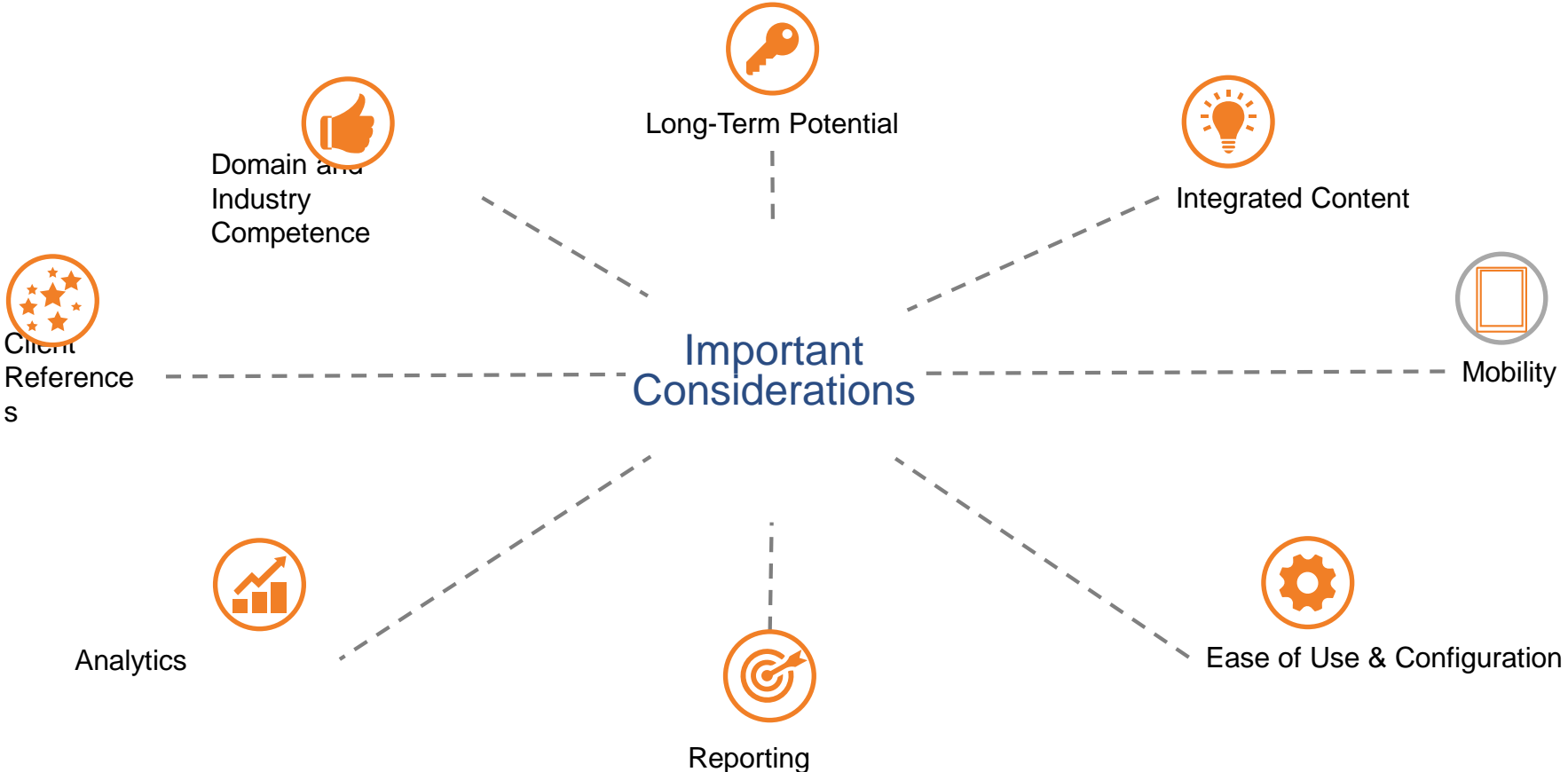


NOTE: these are just a selection of some common elements from GRC 20/20's RFP template containing over 250 requirements for 3rd Party Management Platforms

GRC 20/20 Value Perspective: 3 Angles of GRC Value



Important Considerations



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 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

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 1 – Recording



<http://bit.ly/2IJP6yu>

Part 2 – Recording



<http://bit.ly/2m4ilKk>



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