Managing Third Party Risk in the Extended Enterprise

February 13, 2014

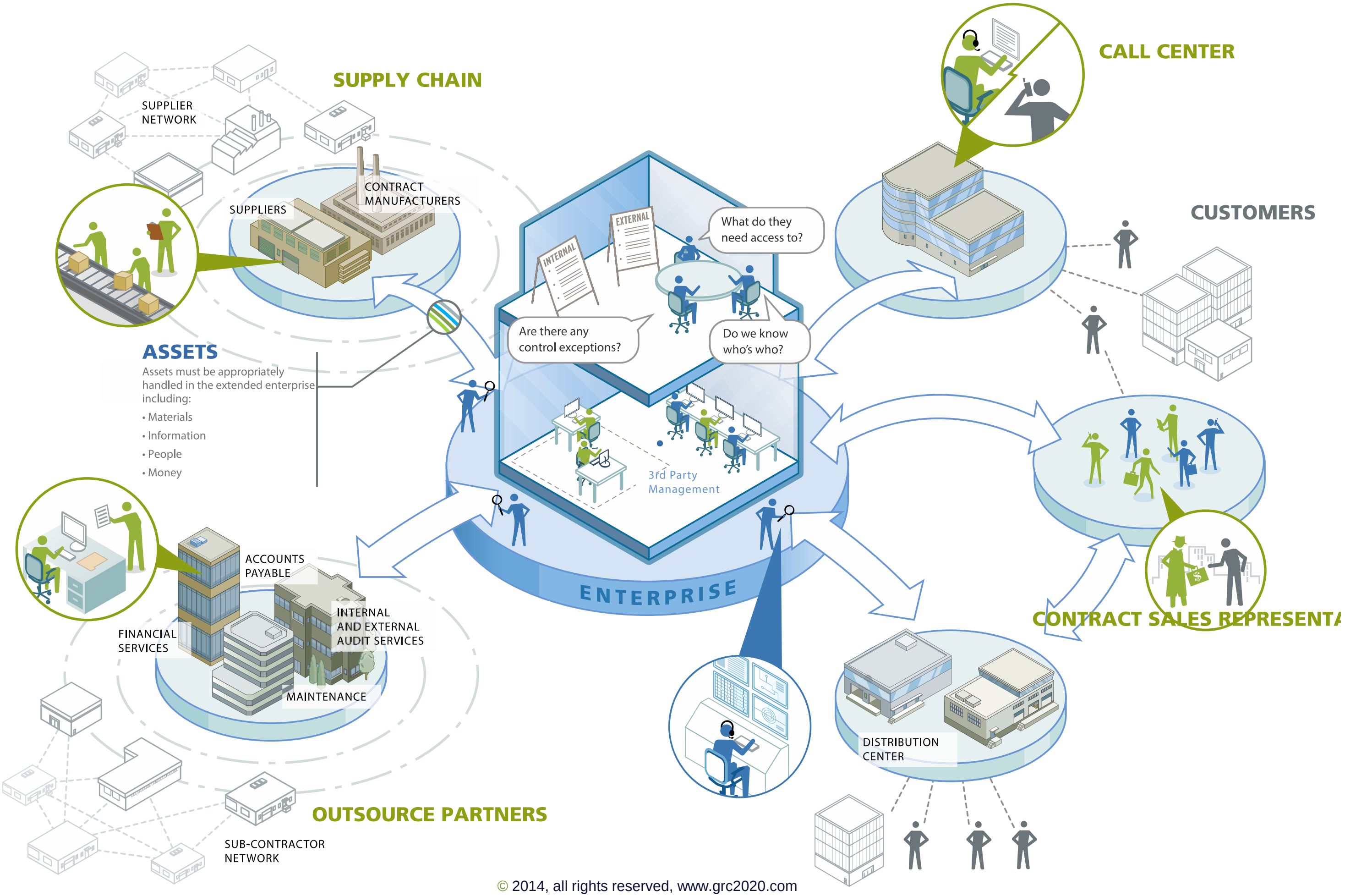
Michael Rasmussen, J.D., GRCP, CCEP

Chief GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

Marshall Toburen, GRC Strategist – Enterprise Risk Management, RSA Archer

3rd party means a wide array of relationships



3rd party risk bearing down on organizations

Integrity

Adherence to moral princi

In ethics, integrity is rega

the honesty and truthfuln

uprightness, sincerity, a

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

- □ Anti-bribery/corruption
- □ Code of conduct and ethics
- □ Conflict Minerals
- □ Corporate social responsibility
- □ Environmental
- □ Geo-political risk
- □ Health and safety
- □ 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…

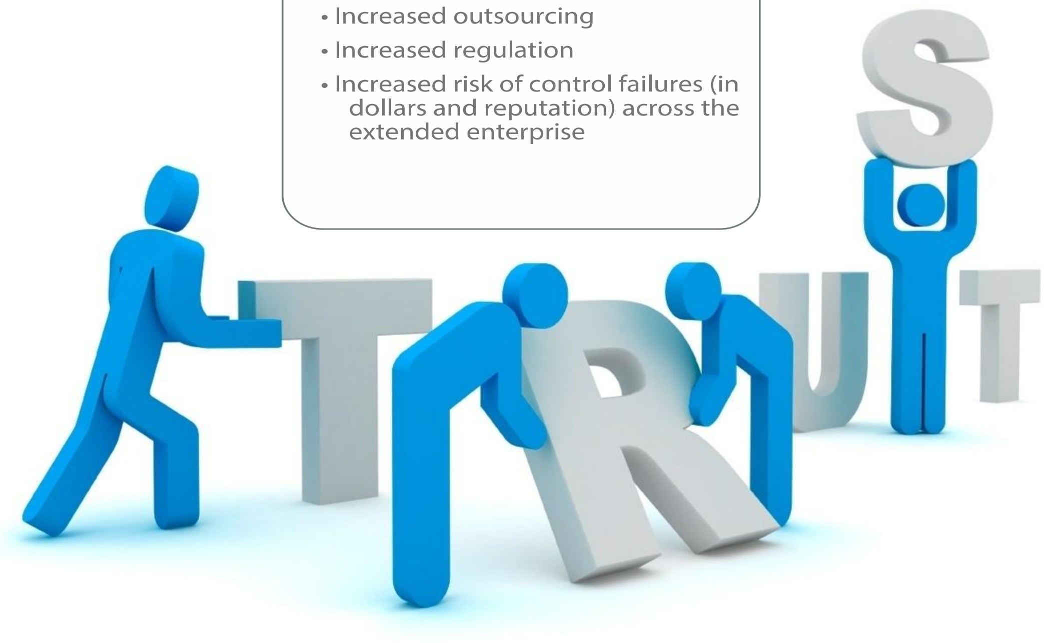
- – Most risk is incurred over the life of the relationship
- – Who owns on-going third party risk?
- – How is third party risk assessed and reported to the board?

. . . and we hope nothing fails

Challenges of 3rd Party Management

- Hundreds to thousands of 3rd party 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, & spreadsheets

Building trust & integrity across 3rd party relationships

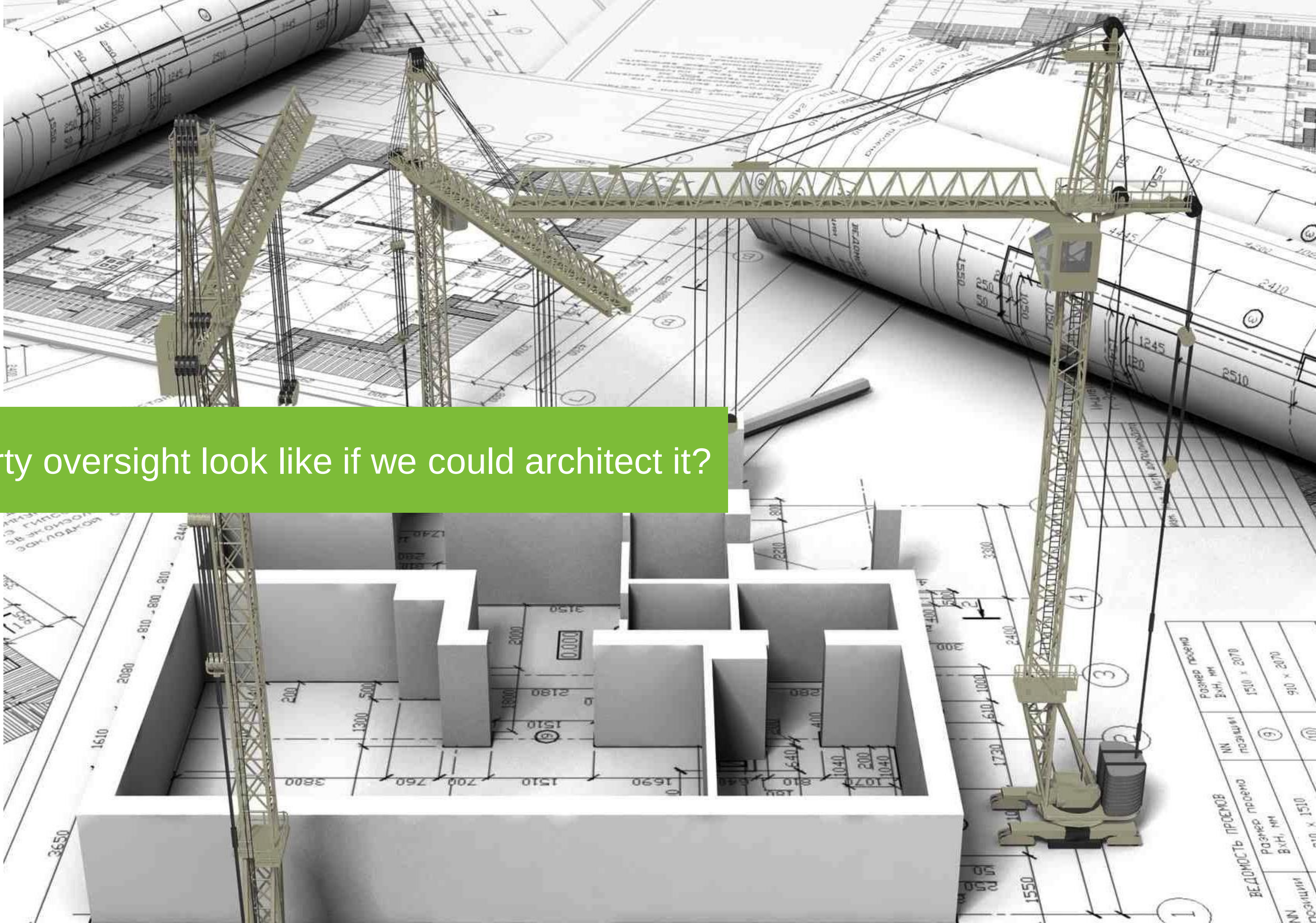


DRIVERS

- Increased global footprint
- Increased outsourcing
- Increased regulation
- Increased risk of control failures (in dollars and reputation) across the extended enterprise

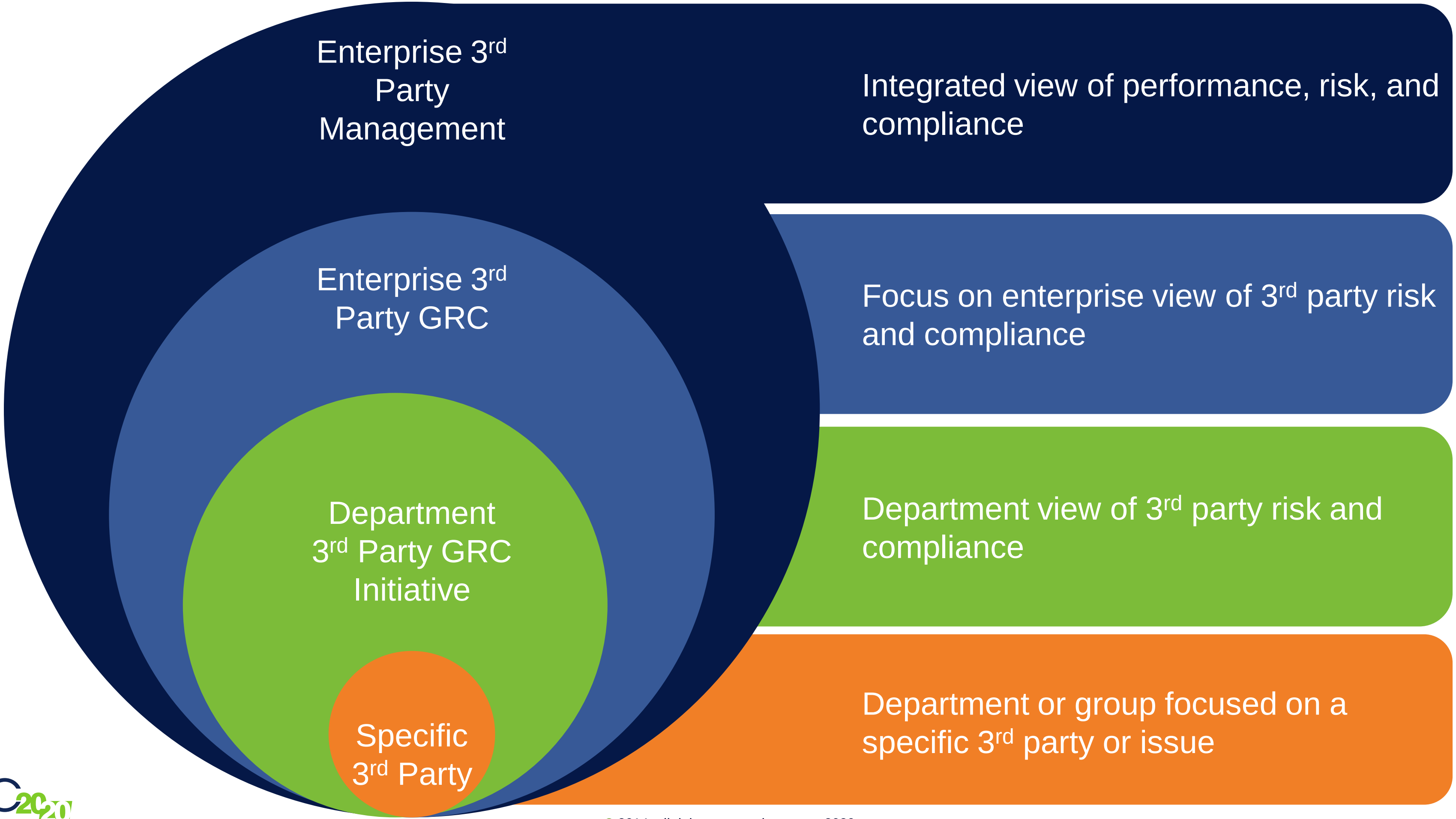
3rd Party management

- Enhances and builds trust
  - Customer trust
  - Partner trust
  - Stakeholder trust
  - Employee trust
- Enables long-term business relationships
- Enables a sustainable supply chain
- Ensures that everyone is playing out of the same playbook



What would 3rd party oversight look like if we could architect it?

Varying approaches to 3rd party management



Enterprise 3rd Party Management

Integrated view of performance, risk, and compliance

Enterprise 3rd Party GRC

Focus on enterprise view of 3rd party risk and compliance

Department 3rd Party GRC Initiative

Department view of 3rd party risk and compliance

Specific 3rd Party

Department or group focused on a specific 3rd party or issue

Getting the 3rd party team together . . .

IS YOUR PROGRAM REASONABLE?

Don't interfere with operations or be a burden on the business.

IS YOUR PROGRAM RESPONSIVE?

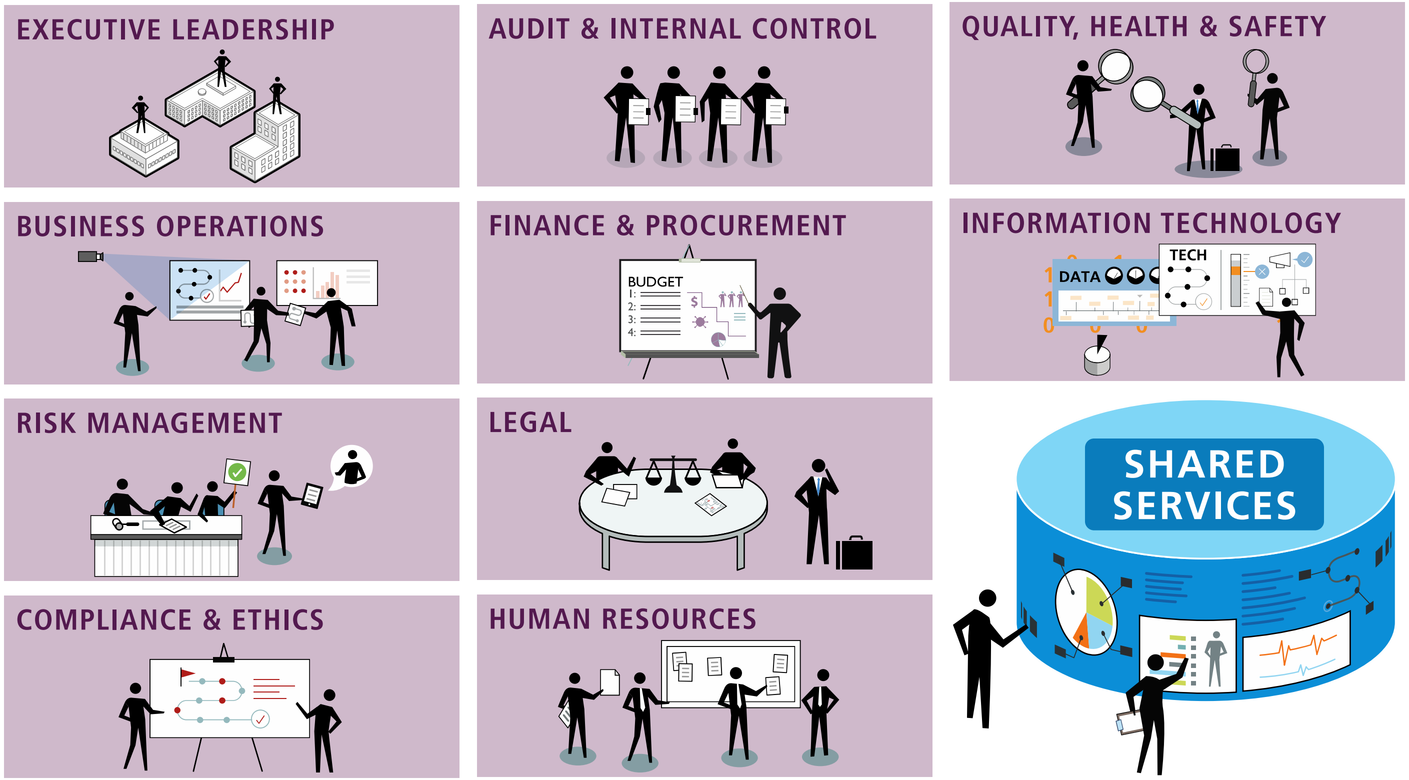
Support transparent and sound decision-making with strong management oversight and robust reporting.

IS YOUR PROGRAM CONSISTENT?

Establish standardized processes that apply to all areas of the business everywhere in the world. Incorporate standardized forms and templates to drive consistency.

IS YOUR PROGRAM INDEPENDENT?

Minimize potential conflicts of interest and ensure decisions are objective.



EXECUTIVE LEADERSHIP

AUDIT & INTERNAL CONTROL

QUALITY, HEALTH & SAFETY

BUSINESS OPERATIONS

FINANCE & PROCUREMENT

INFORMATION TECHNOLOGY

RISK MANAGEMENT

LEGAL

COMPLIANCE & ETHICS

HUMAN RESOURCES

SHARED SERVICES

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

Essential elements of a 3rd party 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 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

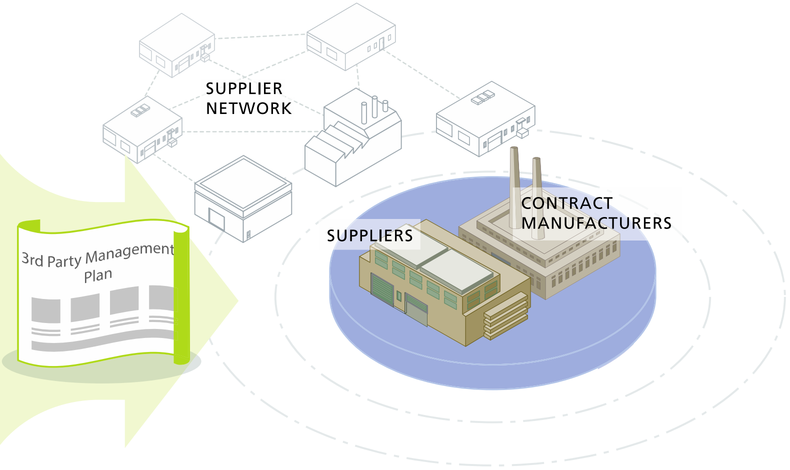
Align 3rd party management strategies with the corporate culture and Code of Conduct.

INTERNAL STAKEHOLDERS

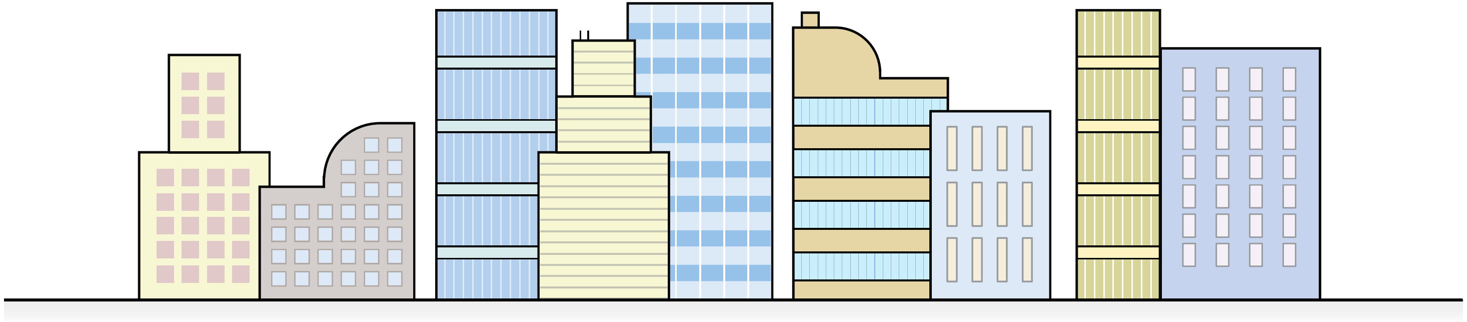
Collaborate with and enlist the support of internal stakeholders across the business.

EXECUTIVE SUPPORT

Gain executive support of the 3rd party management program



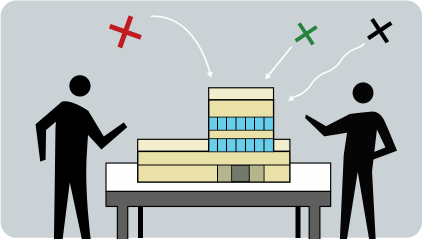
Managing risk across extended business relationships



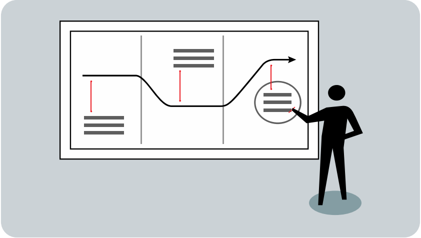
- The organization does not start and stop with traditional brick and mortar walls. The modern organization is a complex web of business relationships and activities that cross business boundaries.
- The organization should clearly define which policies, procedures and controls cross business relationships and ensure that compliance is covered in contracts.
- Periodic communication of policies, starting with a code of conduct, should be done across all business relationships. Where needed, training should also be provided.
- Business partner relationships should undergo a minimum annual self-assessment process to attest to their compliance status to governing policies, procedures, and controls.
- The organization should have defined audit processes to exercise right to audit clauses to validate compliance in extended business relationships.

Identify, assess & take action on 3rd party management risks

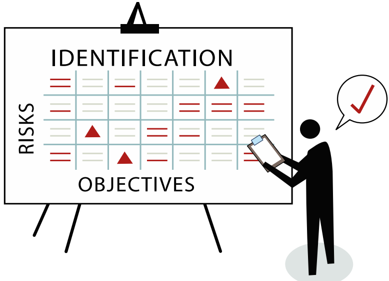
ANALYZE RISKS

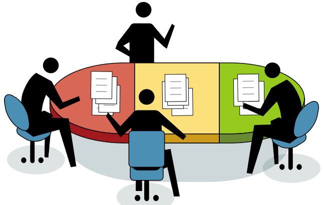


UNDERSTAND HISTORY



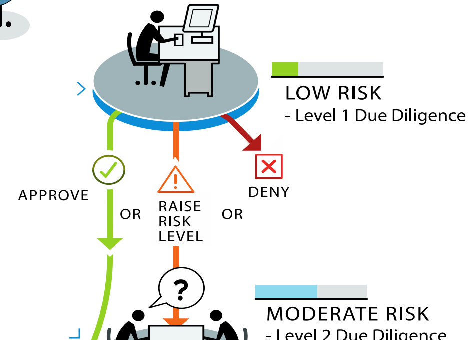
REVIEW EXISTING POLICIES

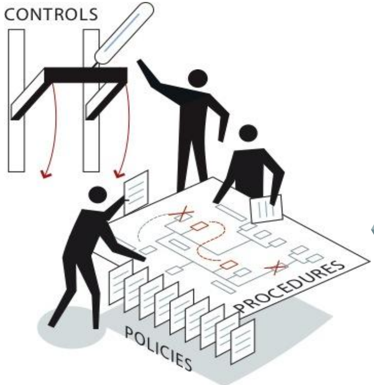


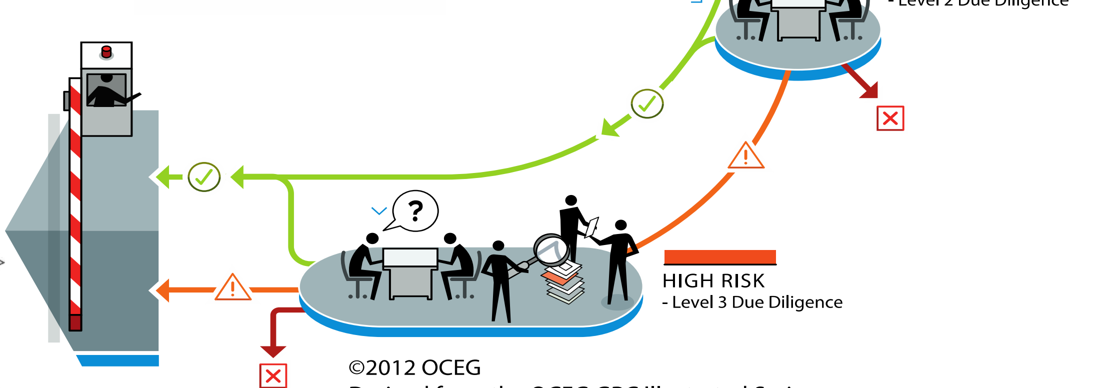


APPROVE / DENY / APPROVE WITH CONDITIONS

- Establish business rules, and automated and process triggers, to facilitate control and monitoring throughout the life of each contract
- Apply more stringent controls and more frequent monitoring to higher risk level entities, individuals and contracts







Analyze, monitor, & reassess 3rd Parties on a ongoing basis

Track and assess policies and controls for effectiveness and performance in various ways:

SCREEN
monitor internal and external information and compare vendor, partner and customer records against trusted data sources for red flags that indicate issues

IDENTIFY
establish hotline and other open channels for reporting and resolution of questions and issues

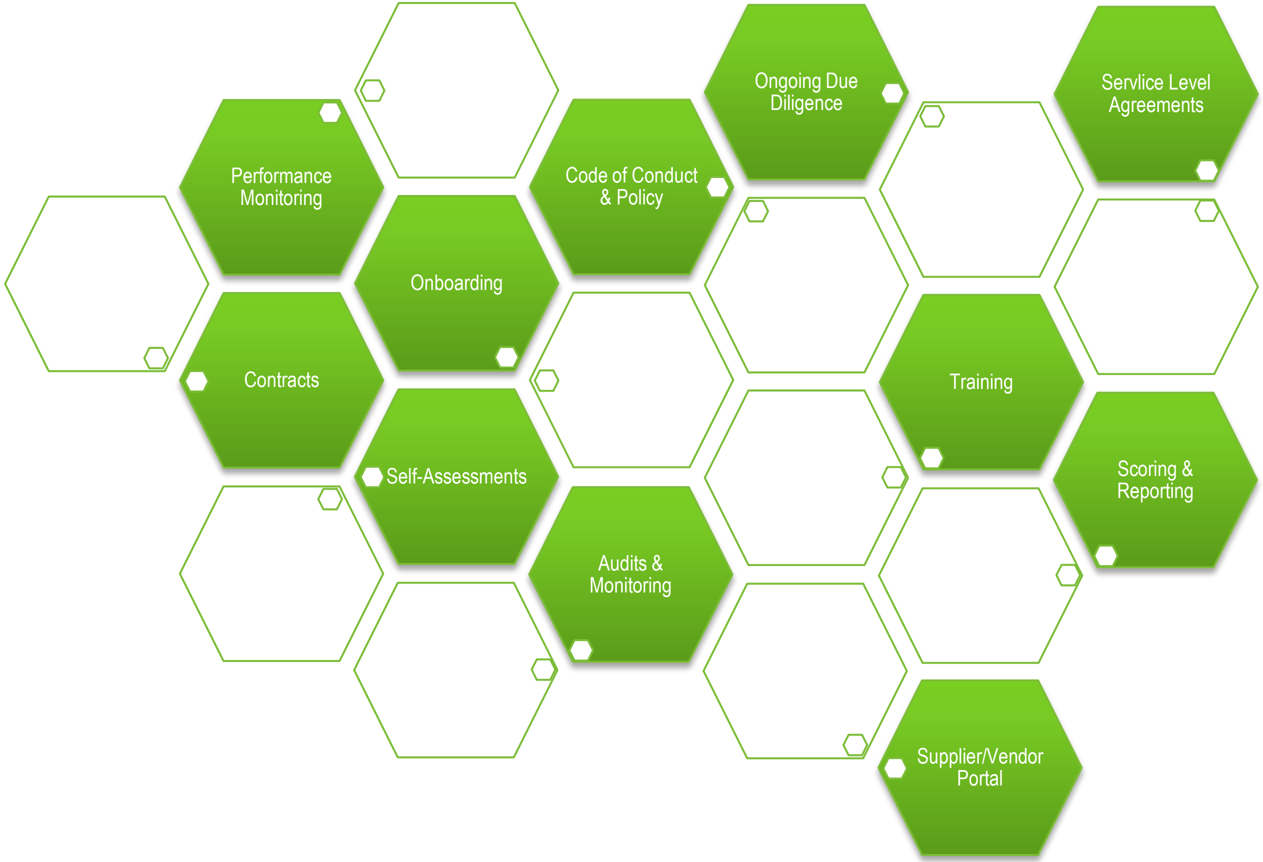
INVESTIGATE
obtain and assess information about observed or suspected misconduct, using appropriate qualified teams, and considering privilege issues

ANALYZE
evaluate data to locate concerns and potential problems by applying analytic techniques, tools and reporting capabilities

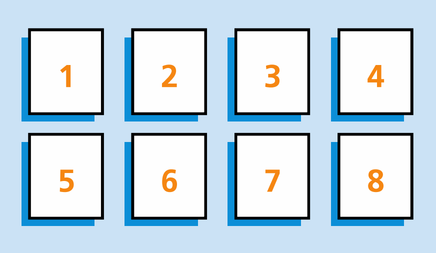
AUDIT
provide regular internal audit oversight and inspection of the anti-corruption program; test and assess controls to determine if additional or modified action is necessary

SCREENING
AUDITING/
TESTING
ANALYTICS
INVESTIGATIONS
HOTLINE
DATA
SELF-
DISCLOSED
SURVEY
DATA
MANAGEMENT

Components of 3rd party management

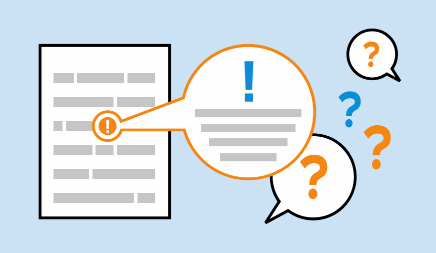


Elements of a defensible 3rd party management plan



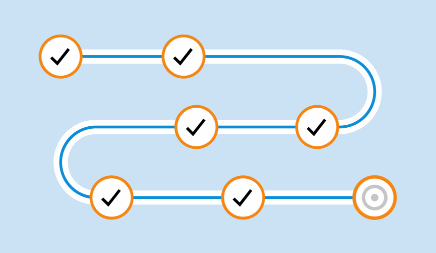
VERSION (DATE, TIME)

Effective 3rd party management-programs can pinpoint what was assessed with supporting details of activities.



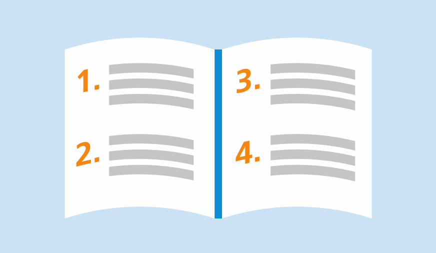
QUESTIONS & EXCEPTIONS

3rd party management requires the ability for 3rd parties to ask questions. When specific controls cannot be addressed effective programs include ways to document, approve and periodically evaluate exceptions in order to update contracts, policies, and/or identify emerging risks.



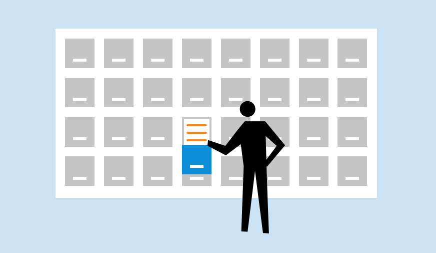
TRACKING

To defend itself and validate an effective 3rd party management program the organization should be able to have a complete historical record of communications and assessments.



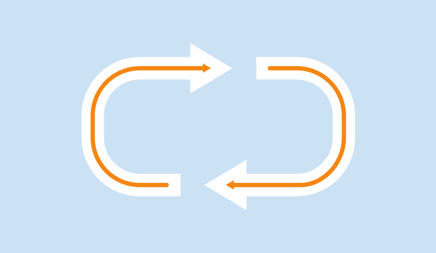
TESTING

To ensure understanding, the 3rd party should be tested to validate comprehension on critical/high-risk policies & controls to ensure that they have been properly communicated and understood.



ACCESSING PAST RECORDS

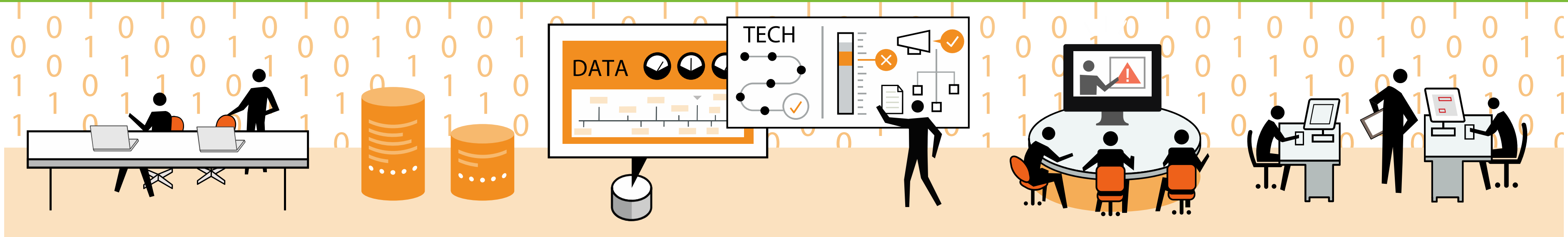
Defending the organization in legal and regulatory actions requires that a 360 degree view of the history of the assessments, contracts, policy, interactions, and communications be accessible with defensible audit trails.



REPEATABLE CYCLE

3rd party management is never complete. Repetition using different methods and tones can increase understanding and compliance.

Technology delivers the backbone of a successful 3rd party management program



Integration

Visibility

Global Reach

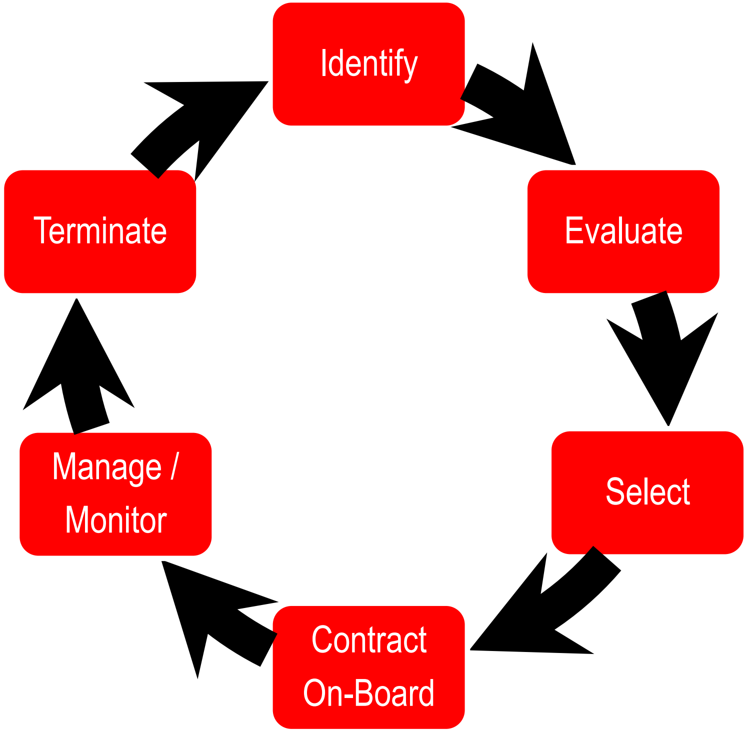
Availability

- ✓ **Ensure** ownership and accountability are clearly established and understood
- ✓ **Manage** the ongoing compliance scoring and assessment processes
- ✓ **Conduct** initial and ongoing due diligence
- ✓ **Monitor** suppliers for adherence to code-of-conduct, policies**,** and regulatory requirements
- ✓ **Adapt** to changes in risk profiles based on assessments and information collected

- ✓ **Leverage** built-in question sets to streamline surveys and questionnaires and deliver these in a consistent format and in the right languages
- ✓ **Track** status of completion of tasks such as assessments and automate escalation when needed
- ✓ **Initiate** and mange remediation follow-ups and investigations
- ✓ **Use** verifiable evidence to readily attest to “in compliance” status to provide assurance to executives and auditors whose name is on the line.

grc2020

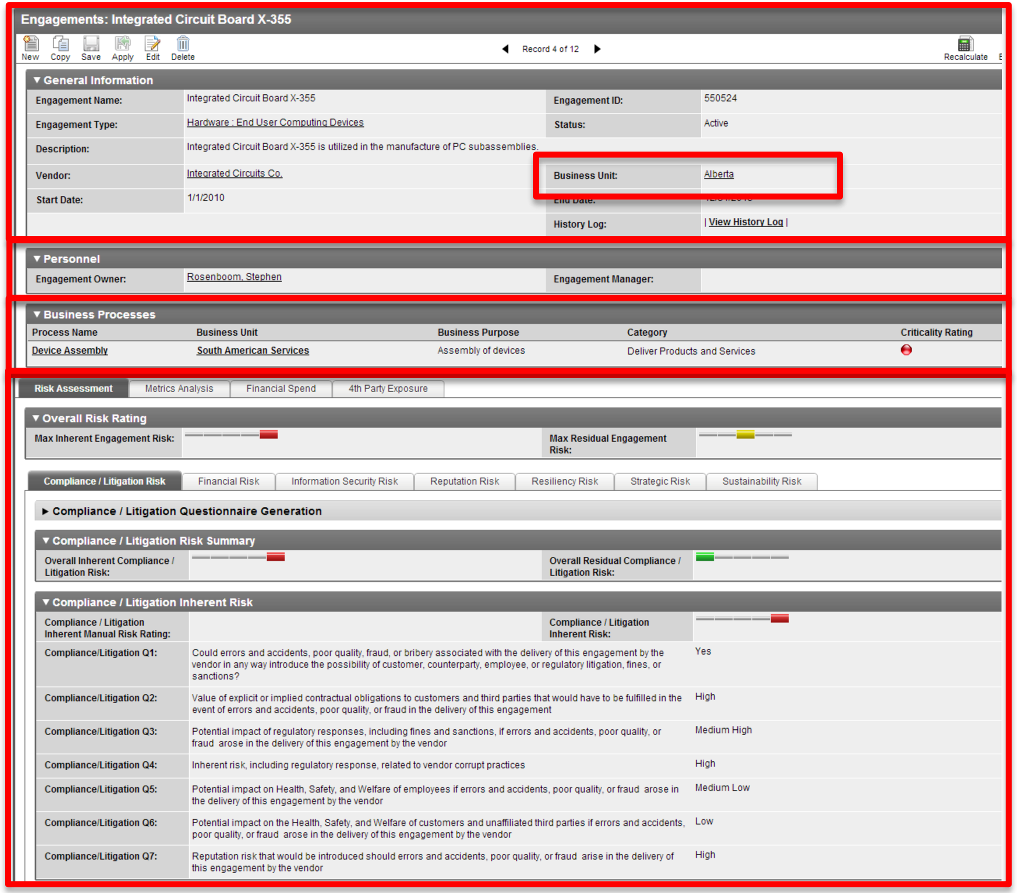
RSA Archer Supports Entire Lifecycle



Consistent & Repeatable

- Capture prospective third parties
- Evaluate based on business context and risks
- Evaluate Contracts & Financial Strength
- Enforce selection policies
- Establish monitoring and documentation requirements
- Monitor overall risk and performance
- Interact with third party
- Collaborate with stakeholders & cross-utilize information

Understand Engagements



Engagements: Integrated Circuit Board X-355

▼ General Information

Engagement Name:	Integrated Circuit Board X-355	Engagement ID:	550524
Engagement Type:	Hardware : End User Computing Devices	Status:	Active
Description:	Integrated Circuit Board X-355 is utilized in the manufacture of PC subassemblies.		
Vendor:	Integrated Circuits Co.	Business Unit:	Alberta
Start Date:	1/1/2010	End Date:	[illegible]
		History Log:	| View History Log |

▼ Personnel

Engagement Owner:	Rosenboom, Stephen	Engagement Manager:	

▼ Business Processes

Process Name	Business Unit	Business Purpose	Category	Criticality Rating
Device Assembly	South American Services	Assembly of devices	Deliver Products and Services	●

▼ Overall Risk Rating

Max Inherent Engagement Risk:	🟥	Max Residual Engagement Risk:	🟨

▶ Compliance / Litigation Questionnaire Generation

▼ Compliance / Litigation Risk Summary

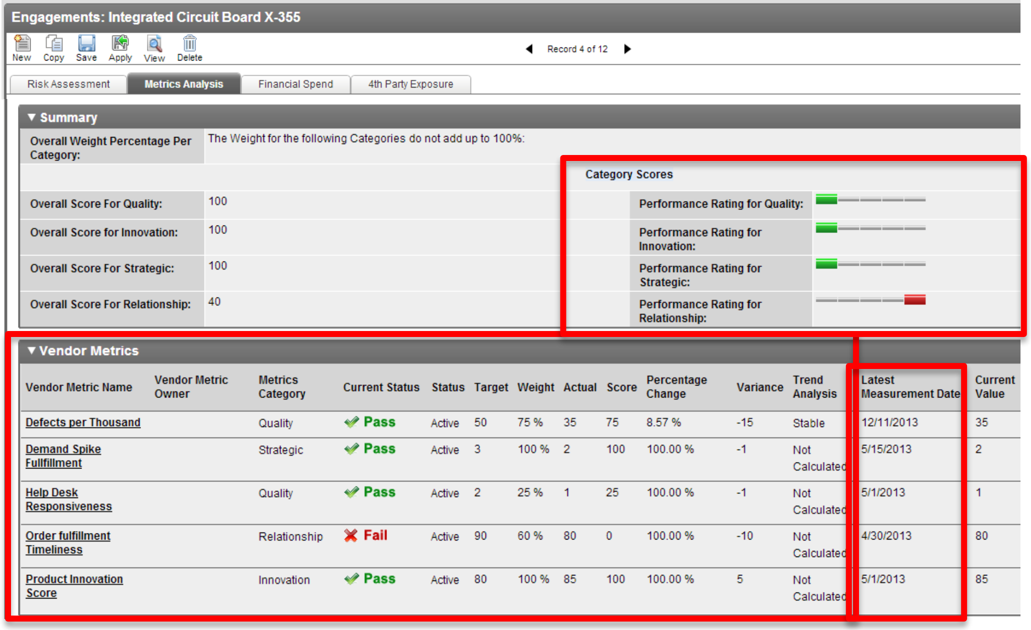
Overall Inherent Compliance / Litigation Risk:	🟥	Overall Residual Compliance / Litigation Risk:	🟩

▼ Compliance / Litigation Inherent Risk

Compliance / Litigation Inherent Manual Risk Rating:		Compliance / Litigation Inherent Risk:	🟥
Compliance/Litigation Q1:	Could errors and accidents, poor quality, fraud, or bribery associated with the delivery of this engagement by the vendor in any way introduce the possibility of customer, counterparty, employee, or regulatory litigation, fines, or sanctions?	Yes	
Compliance/Litigation Q2:	Value of explicit or implied contractual obligations to customers and third parties that would have to be fulfilled in the event of errors and accidents, poor quality, or fraud in the delivery of this engagement	High	
Compliance/Litigation Q3:	Potential impact of regulatory responses, including fines and sanctions, if errors and accidents, poor quality, or fraud arose in the delivery of this engagement by the vendor	Medium High	
Compliance/Litigation Q4:	Inherent risk, including regulatory response, related to vendor corrupt practices	High	
Compliance/Litigation Q5:	Potential impact on Health, Safety, and Welfare of employees if errors and accidents, poor quality, or fraud arose in the delivery of this engagement by the vendor	Medium Low	
Compliance/Litigation Q6:	Potential impact on the Health, Safety, and Welfare of customers and unaffiliated third parties if errors and accidents, poor quality, or fraud arose in the delivery of this engagement by the vendor	Low	
Compliance/Litigation Q7:	Reputation risk that would be introduced should errors and accidents, poor quality, or fraud arise in the delivery of this engagement by the vendor	High	

- Document Each Vendor Engagement
- Establish Accountability *(People & Business Hierarchy)*
- Connect Business Context
  - Business Processes
  - Products & Services
  - Enterprise Assets
  - Corporate Objectives
- Perform Risk Assessments
  - Inherent & Residual Risk across Multiple Risk Categories
  - 4th Party Risk & Risk Governance
  - Overall Risk by Engagement
  - Roll-Up All Engagements to Parent Co.
  - Collect, Assess, Manage Documentation

Understand Performance



Engagements: Integrated Circuit Board X-355

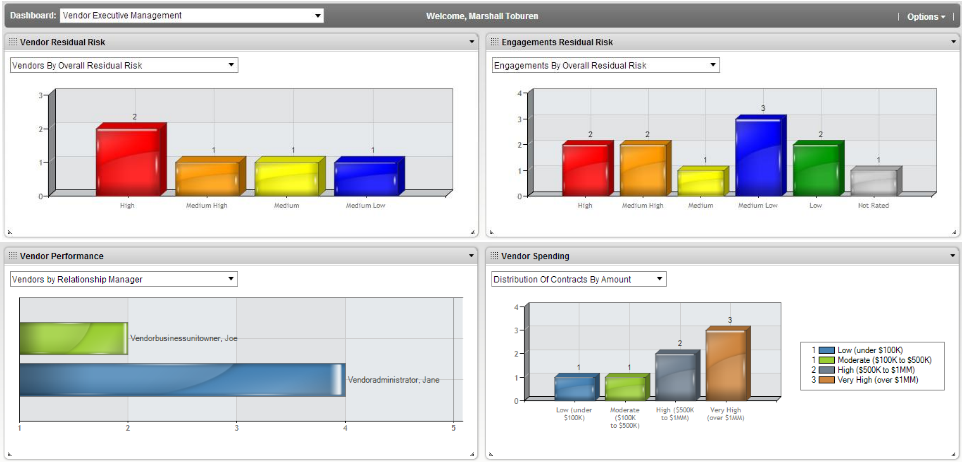
▼ Summary

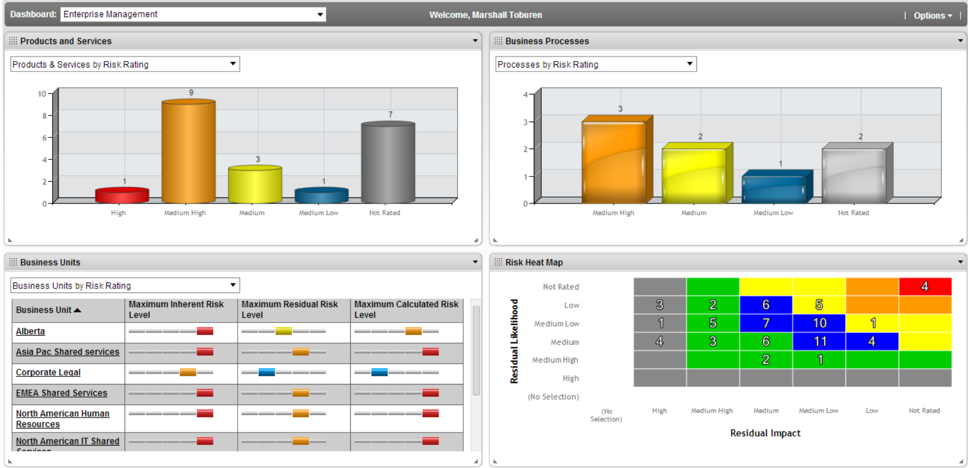
Overall Weight Percentage Per Category:	The Weight for the following Categories do not add up to 100%:		
		Category Scores	
Overall Score For Quality:	100	Performance Rating for Quality:	🟩
Overall Score for Innovation:	100	Performance Rating for Innovation:	🟩
Overall Score For Strategic:	100	Performance Rating for Strategic:	🟩
Overall Score For Relationship:	40	Performance Rating for Relationship:	🟥

▼ Vendor Metrics

Vendor Metric Name	Vendor Metric Owner	Metrics Category	Current Status	Status	Target	Weight	Actual	Score	Percentage Change	Variance	Trend Analysis	Latest Measurement Date	Current Value
Defects per Thousand		Quality	✓ Pass	Active	50	75 %	35	75	8.57 %	-15	Stable	12/11/2013	35
Demand Spike Fullfillment		Strategic	✓ Pass	Active	3	100 %	2	100	100.00 %	-1	Not Calculated	5/15/2013	2
Help Desk Responsiveness		Quality	✓ Pass	Active	2	25 %	1	25	100.00 %	-1	Not Calculated	5/1/2013	1
Order fulfillment Timeliness		Relationship	✗ Fail	Active	90	60 %	80	0	100.00 %	-10	Not Calculated	4/30/2013	80
Product Innovation Score		Innovation	✓ Pass	Active	80	100 %	85	100	100.00 %	5	Not Calculated	5/1/2013	85

- Assign Performance Metrics
  - Standardized Library
  - Multiple Categories
  - Thresholds, Expected Direction, 2 STDV
  - Separate Weights & Scores
- Performance Roll-Up
  - Each Engagement
  - Parent Vendor, across All Engagements
- Collection via Manual Input, Data Feeds, Upload
- Reports, Dashboards, Notifications of missing, stale, and deteriorating metrics


Dashboard: Vendor Executive Management
Welcome, Marshall Toburen
Options
Vendor Residual Risk
Vendors By Overall Residual Risk
3
2
1
0
2
1
1
1
High
Medium High
Medium
Medium Low
Engagements Residual Risk
Engagements By Overall Residual Risk
4
3
2
1
0
2
2
1
3
2
1
High
Medium High
Medium
Medium Low
Low
Not Rated
Vendor Performance
Vendors by Relationship Manager
Vendorbusinessunitowner, Joe
Vendoradministrator, Jane
1
2
3
4
5
Vendor Spending
Distribution Of Contracts By Amount
4
3
2
1
0
1
1
2
3
Low (under $100K)
Moderate ($100K to $500K)
High ($500K to $1MM)
Very High (over $1MM)
1 Low (under $100K)
1 Moderate ($100K to $500K)
2 High ($500K to $1MM)
3 Very High (over $1MM)



Business Unit ▲	Maximum Inherent Risk Level	Maximum Residual Risk Level	Maximum Calculated Risk Level
Alberta	🟥	🟨	🟧
Asia Pac Shared services	🟥	🟧	🟥
Corporate Legal	🟧	🟦	🟦
EMEA Shared Services	🟥	🟧	🟥
North American Human Resources	🟥	🟧	🟥
North American IT Shared Services	🟥	🟧	🟥

Residual Likelihood	High	Medium High	Medium	Medium Low	Low	Not Rated
Not Rated						4
Low	3	2	6	5		
Medium Low	1	5	7	10	1	
Medium	4	3	6	11	4	
Medium High			2	1		
High						
(No Selection)						

Management Information

- Right information for right individuals at the right time, for example:
  - Status of program activities
  - Most important 3rd party relationships
  - High risk and financially weak 3rd parties
  - 3rd parties with deteriorating performance
  - 4th party dependencies
- Robust information delivery *(dashboards, workflow, notifications)*
- Leverage information among stakeholders
- Reinforce accountability and promote culture to identify and prevent problems from turning into issues
- Rapidly investigate and respond to queries
- Demonstrate effective governance to Board, C-Suite, and Regulators

Efficient, effective & agile 3rd party management programs

higher quality information

Integrating GRC information allows management to make more intelligent decisions, more rapidly.

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.

improved effectiveness

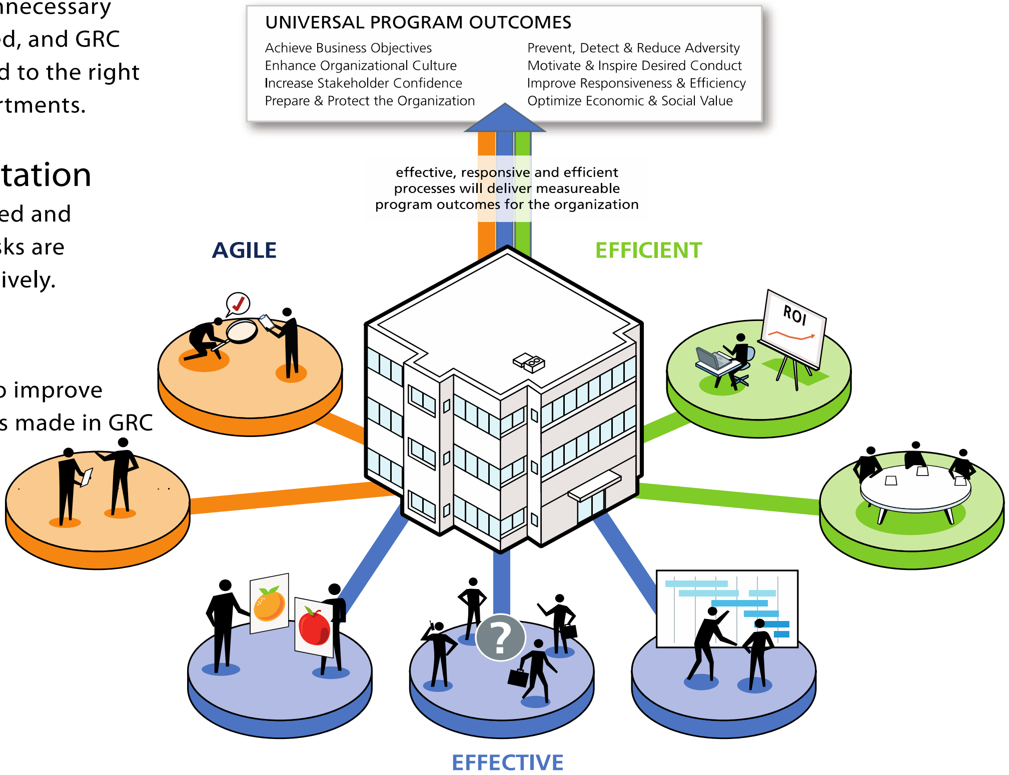
Overall effectiveness is improved as gaps are closed, unnecessary redundancy is reduced, and GRC activities are allocated to the right individuals and departments.

protected reputation

Reputation is protected and enhanced because risks are managed more effectively.

reduced costs

Reduced costs help to improve return on investments made in GRC activities.



UNIVERSAL PROGRAM OUTCOMES

Achieve Business Objectives	Prevent, Detect & Reduce Adversity
Enhance Organizational Culture	Motivate & Inspire Desired Conduct
Increase Stakeholder Confidence	Improve Responsiveness & Efficiency
Prepare & Protect the Organization	Optimize Economic & Social Value

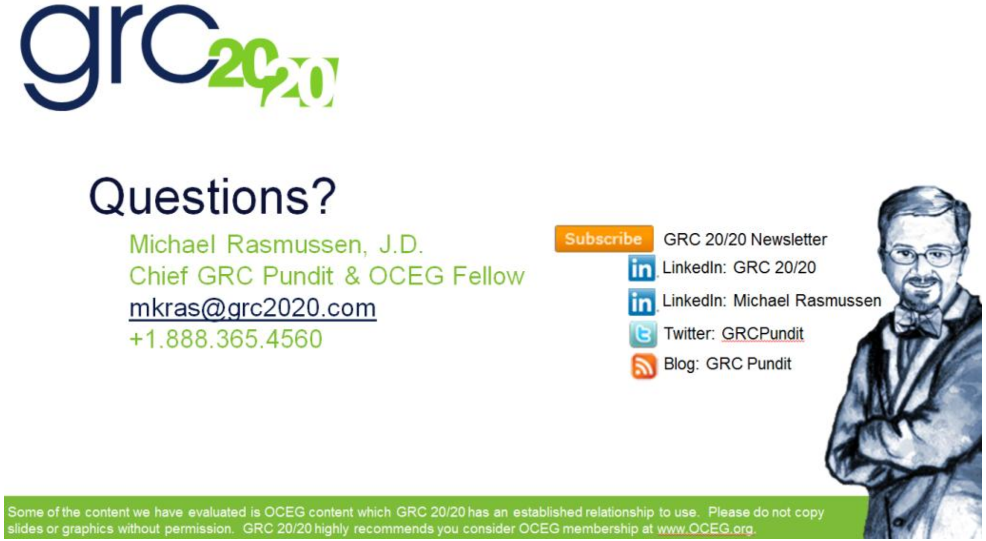
effective, responsive and efficient processes will deliver measureable program outcomes for the organization

Used by permission, contact OCEG for comments, reprints or licensing requests

Questions and Resources

RSA® Archer GRC

- Marshall Toburen, GRC Strategist, email: marshall.toburen@rsa.com
- RSA Archer private Community and Exchange
- RSA Public web site: http://www.emc.com/security/rsa-archer.htm
- Weekly complementary webcasts on various GRC leadership topics http://www.emc.com/campaign/global/rsa/rsa-webcast.htm
- GRC leadership blogs from myself and my colleagues https://community.emc.com/community/connect/grc_ecosystem
- To arrange an RSA Archer demo, contact: 1-888-539-EGRC



grc 20/20

Questions?

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

Subscribe GRC 20/20 Newsletter
in LinkedIn: GRC 20/20
in LinkedIn: Michael Rasmussen
Twitter: GRCPundit
Blog: GRC Pundit

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.