OCEG
DRIVING PRINCIPLED PERFORMANCE®

THIRD PARTY RISK AND PERFORMANCE MANAGEMENT

SPEAKER:
MARSHALL TOBUREN, RSA ARCHER GRC STRATEGIST
marshall.toburen@rsa.com

January 16, 2014

OCEG WEBINAR SERIES

RSA Archer GRC

Housekeeping

- Download slides at http://www.oceg.org/event/moving-enterprise-risk-management-complexity-simplicity/
- Answer all 4 poll questions
- Certificates of completion (only for OCEG Premium/Enterprise members and All-Access Pass holders)
- Evaluation survey at the close of the webinar
- Archive at Recorded Events on OCEG site
- Thank you to our webinar sponsor, RSA

POLL #1

What industry do you primarily represent?

A. Energy
B. Financial Services
C. Healthcare, Biotechnology, or Pharmaceuticals
D. Information Technology
E. Manufacturing or Construction
F. Retail
G. Telecommunications
H. Other

Learning Objectives

- Identify key drivers of third party risk & performance management programs (TPRPM)
- Distinguish key elements of a TPRPM & where to apply them within the life cycle of a third party
- Discern the benefits of an integrated approach to TPRPM
- Understand maturity paths to help organizations begin this journey

Presentation Terminology

- Third-Party, Vendor, Counterparty, Agent – Largely synonymous. Directly provides product/services, typically by contract
- Fourth Party – provides product/services through supply chain but no direct relationship
- Engagement – a product / service delivered by a TP
- Risk – Effect of uncertainty on objectives (bad & good)
- Risk Category – a division of risk having particular shared characteristics (financial, reputation, info sec., strategic, etc.)
- Inherent Risk vs. Residual Risk – Risk in the absence of controls vs. risk considering risk treatments in place and operating
- Performance – how well product / service engagement delivered per objective. May or may not be formal SLA

Examples of Third Parties

Credit Bureaus

Utility & Telecom Companies

Partners/Ventures Integrators

Financial Counterparties

Law Firms

Consultants

Marketing Companies

SaaS Providers

Employment Agencies

Parts Suppliers

Insurers

Public Accounting Firms

Property Managers

Raw Material Suppliers

Hardware Providers

Maintenance Companies

Security Guards

ISPs

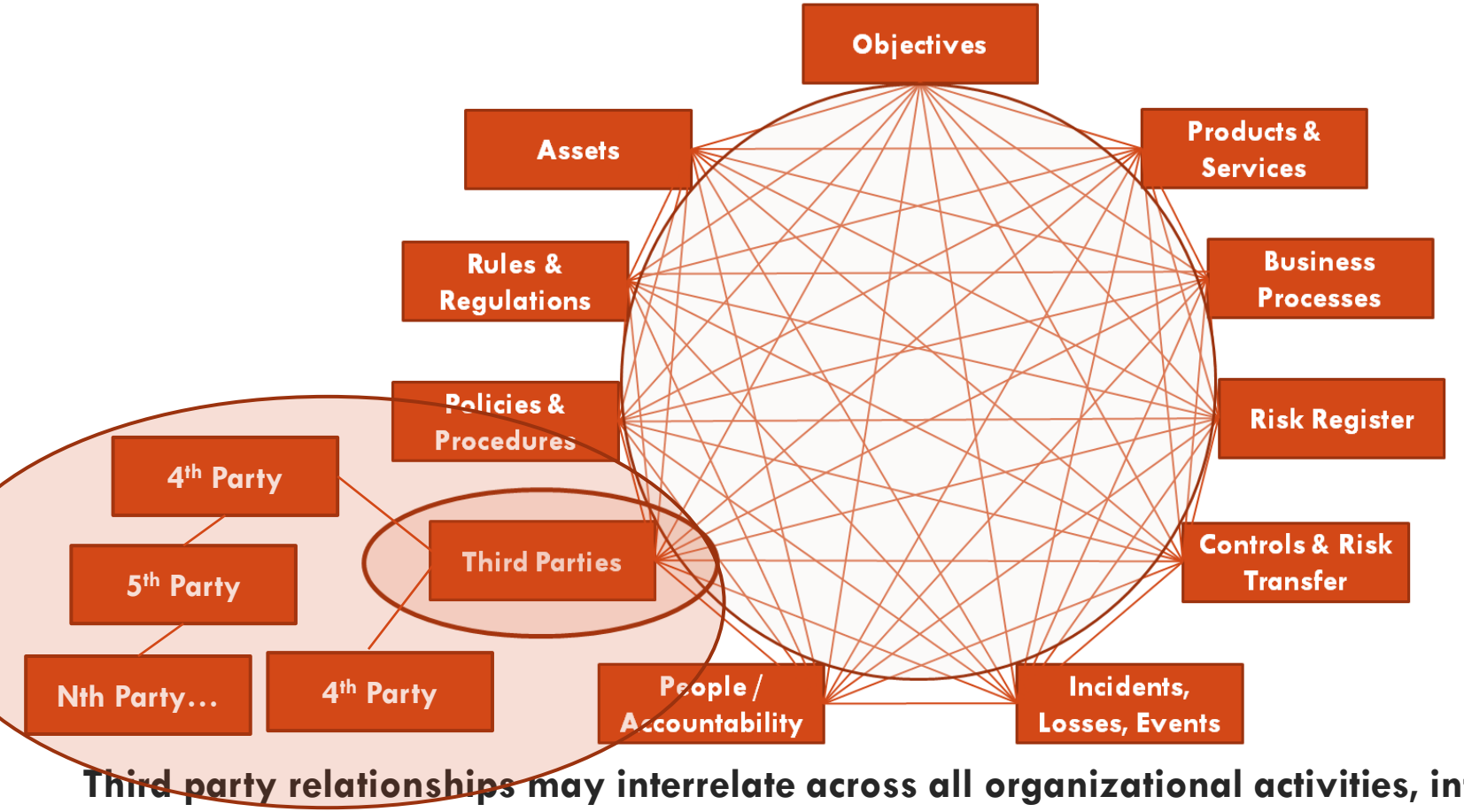
Landlords / Lessors

Couriers

Medical Counterparties

Software Providers

Third Party Interrelationships



Third party relationships may interrelate across all organizational activities, introducing the same risk to the organization as if the organization internalized the activities

RSA Archer GRC

Risk vs. Benefit

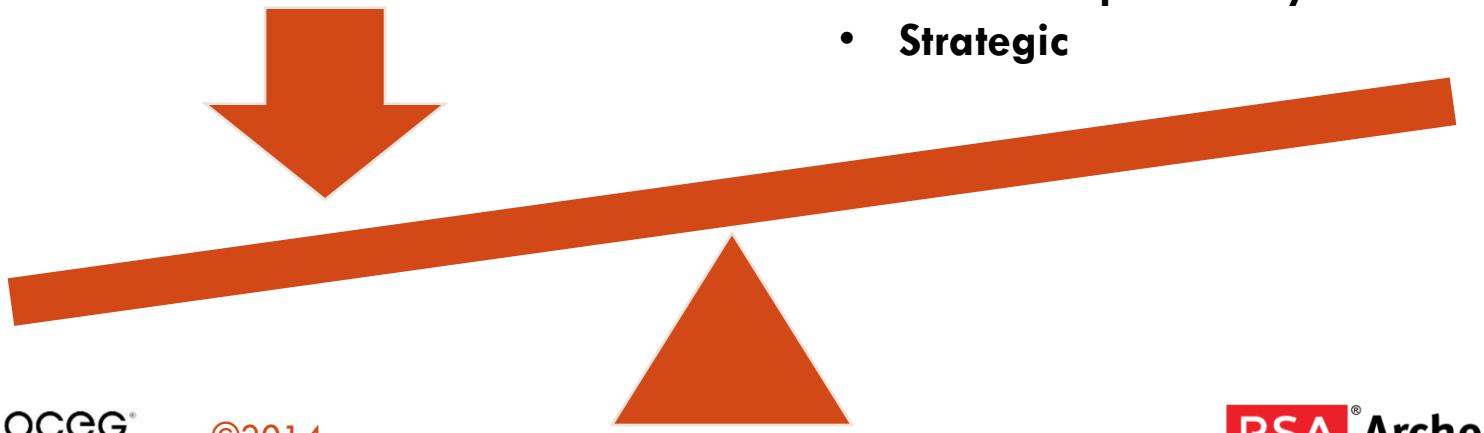
BENEFITS SHOULD OUTWEIGH THE RISKS

BENEFITS

- Competitive Edge
- Leverage TP's Expertise
- Resource Optimization
- Cheaper / More Profitable
- Risk Transfer
- Expand Market Share

RISKS

- Poor performance
- Financial
- Compliance / Litigation
- Information Security
- Resiliency
- Reputation
- Social Responsibility
- Strategic



Bad Third Party Experiences

- NSA Leaks by Edward Snowden, subcontractor of Booz Allen Hamilton
- Iowa Public Retirement System led class action seeking $351B in damages from Countrywide's involvement with mortgage-backed securities
- Hyatt walkway collapse kills 114 due to gross negligence of engineering co.
- Nike child labor violations from foreign third party manufacturing facilities
- Heartland Payment Systems – $6B in damages to credit card issuing banks as a result of 134 million credit cards being breached
- BP Deepwater Horizon 87 day oil spill killed 11, $47B in fines, litigation, and settlements. Partially faulting Transocean and Halliburton
- London 2012 G4S Olympics event security problems leads to UK government review of outsourcing services to private firms
- Burger King accused of animal rights abuse through relationship with Bettencourt Dairies
- Thousands of companies impacted by Amazon Web Services cloud outages
- Lululemon, $45M lost revenue from product recall and supply interruption of women's yoga pants due to poor quality fabric from manufacturing partner

POLL #2

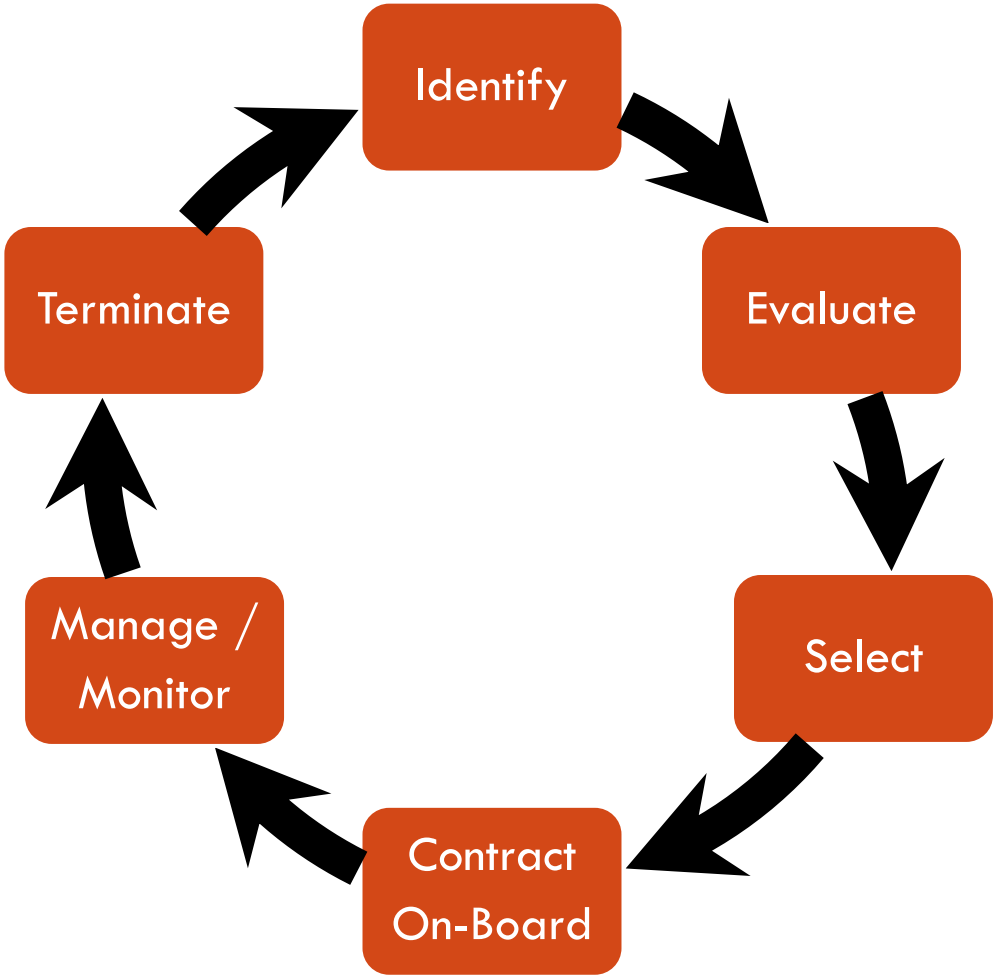
What is the primary driver for your organization's interest in integrated third party risk and performance management?

A. Avoid / minimize negative risk events
B. Regulatory pressure
C. Performance / strategic optimization
D. It's the latest management craze

Foundational Governance Considerations

- Policies and Procedures
  - Scope & Authority (organizationally, by type, by materiality)
  - Agreed upon terminology
  - Roles, Functions, Accountabilities
  - Risk & Performance Assessment Methodology
  - Risk Decisions / Escalation
  - Monitoring, Communication, and Reporting
  - Tools and system(s) of record
- Education and training
- Tone at the Top
- Alignment with ERM policies and practices
- On-going Refinement

Third Party Management Lifecycle

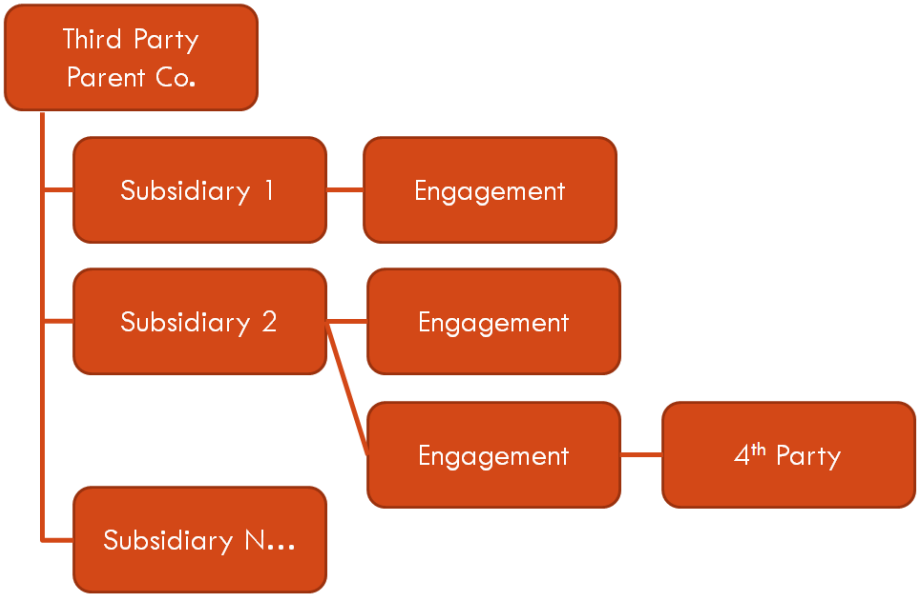


RSA Archer GRC

Identification

- Embedded in Workflow (Ex Ante)
  - Purchasing / Legal Department
  - New Products / Services
  - Business Process Change
  - Accounts Payable
  - Credit
- Validation (Ex Post)
  - General Ledger – Expense Account Review
  - General Ledger – Asset Analysis
  - Business Unit Manager Affirmation / Reaffirmation
  - Business Continuity Plans / Product Services Analysis

Evaluation



STEPS

- Establish Business Context
- Determine if ROI Acceptable
- Assess Engagement Inherent Risk
- If Engagement IR level warrants, evaluate:
  - Parent Co
  - Risk treatments
- Determine if Residual Risk exceeds tolerance
- Decision whether to move to contract stage

Risk Assessment Process

Risk Category / Assessment Target	
Inherent Risk Considerations	**Residual Risk Considerations**
Compliance & Litigation Risk / Engagement	
• Product liability • Health & Welfare • Fines & sanctions for non-compliance with laws & regulations	• TP internal controls • TP assertions of compliance with regulations • Reported incidents • Risk Transfer (proof of insurance)
Financial Risk / Engagement	
• Value of assets under control of/processed by TP that could be lost or stolen • Impact from interruption of liquidity • Amount of credit, market, and Fx risk that could be introduced by volume and process due to error or fraud	• TP internal controls • Financial viability • TP assertion of compliance • Risk transfer (proof of insurance)

Risk Assessment Process *(continued)*

Risk Category / Assessment Target	
Inherent Risk Considerations	**Residual Risk Considerations**
Information Security Risk / Engagement	
Type and amount of information being handled	• TP internal controls • Quality of TP's info sec staff • Reported incidents
Resiliency Risk / Engagement	
Business Impact Analysis of interruption	• TP internal controls • TP critical continuity dependencies • Organization's own contingency plans • Un-remediated issues from continuity tests / reviews

Risk Assessment Process *(continued)*

Risk Category / Assessment Target	
Inherent Risk Considerations	**Residual Risk Considerations**
Sustainability Risk / Engagement	
• Degree of natural resource consumption • Impact of uncontrolled pollution	• TP internal controls • TP assertions about adherence to sustainability practices • Vendor reported supply chain sustainability issues • Sustainability Incidents, fines, sanctions
Strategic Risk / Engagement	
• Importance of engagement to company objectives • Uniqueness of engagement	• Innovation • Quality • Effectiveness • Capacity

Risk Assessment Process *(continued)*

Risk Category / Assessment Target	
Inherent Risk Considerations	**Residual Risk Considerations**
4th Party Risk / Engagement & the 4th Party	
Risk concentration across portfolio of vendors and engagements	• TP's internal controls over their supply chain oversight & governance • 4th Party due diligence
Reputation Risk / Engagement	
Subjective – based on all other risk categories	Subjective – based on all other risk categories
Viability Risk / Parent Company	
Risk if vendor goes out of business unexpectedly or performance significantly deteriorates	Financial statements

Selection

- Residual risk accepted by policy or by persons with authority to accept risk outside policy, within their delegated authority
- Selection conditional based on:
  - Receipt, review, and acceptance of all required documentation (proof of insurance, licenses, certificates of good standing, SSAE16s, assessment questionnaires, assertions, etc.)
  - Mutually acceptable Contract negotiation

Contracts

- Contract spells out rights & obligations of both parties:
  - Scope, term of services & associated fees
  - Liability, penalties & remuneration if something goes wrong
  - Performance standards & expectations / SLAs
  - Information security expectations and agreed upon procedures
  - Business Continuity expectations & testing frequency & scope
  - Subcontractor relationships
  - Ownership & licenses
  - Internal controls, assessments, right to audit
  - Indemnification & limits of liability
  - Procedures for dispute resolution & winding down relationship
- Methodically evaluate contracts. The risk associated with exceptions to preapproved contract language should be escalated for approval by authorized individuals

On-Boarding

- Finish up loose ends
- Gather remaining documentation
- Complete third-party management system inputs (if applicable):
  - Create metrics (quality, innovation, strategic, performance)
  - Establish accountabilities
  - Set-up ticklers

Management & Monitoring

- Objective: Identify material changes in TP risk & performance soon enough to prevent negative outcomes
- Risk & Performance activities:
  - New vendor and engagement evaluation
  - Periodic reaffirmation of existing risk
  - Actions to be taken on Engagements & Parent risk profiles exceeding risk tolerance (contingency & remediation plans)
  - Periodic reaffirmation of policy exceptions and risk that exceeds tolerance
  - Actions on vendors with deteriorating performance
  - Incident root-cause-remediation & loss recovery

Management & Monitoring *(continued)*

- Administrative activities to monitor:
  - Status of prospective third parties in pipe-line
  - Status of on-going metric collection
  - Status of risk & performance reassessment cycle
  - Aging and collection of key required documents & associated reviews (expiring contracts, financial statements, certificates of insurance, SSAE16s, social & environmental assertions, etc.)
  - Changes in ownership & workflow as organization changes
  - Periodic Management Reporting (Most significant, Highest Risk, Significant outstanding issues)

Termination

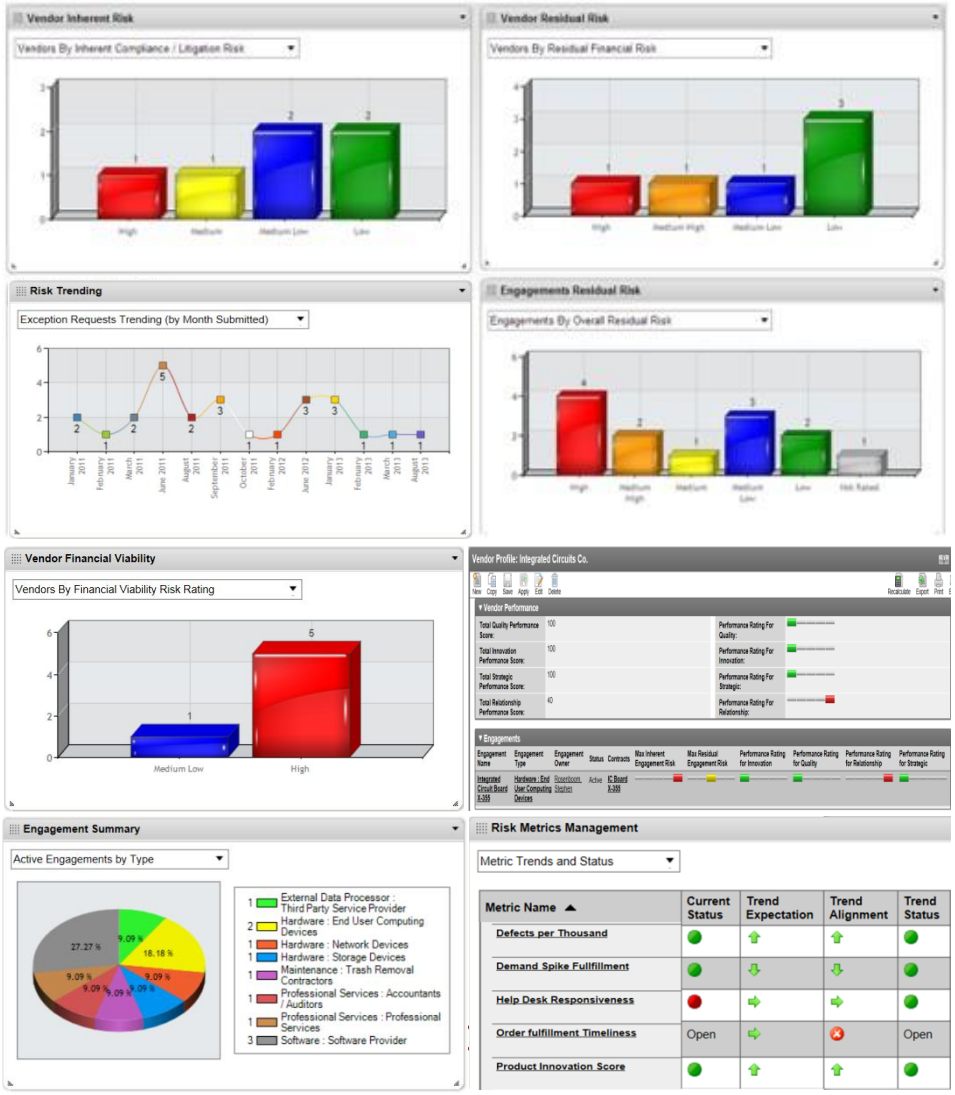
- Termination due to risk
- Contingency plans
- Termination
  - Facilitate timely migration
  - Return and/or destruction of sensitive information

POLL #3

What is the status of your third party risk and performance management program?

A. TPRPM is generally fragmented, managed in silos, and coordinated manually
B. We have a core TPRPM system and are in the process of implementation
C. We have a fully implemented & integrated TPRPM system
D. I don't know

Integration & Technology



Positive Business Outcomes

- Obtain enterprise-wide transparency
- Leverage information across-domains
- Add business context & reduce complexity
- Enforce consistency in approach
- Capture changes in risk and performance profile more quickly
- Exceptions don't fall through the crack
- Identify & respond to critical dependencies further down supply chain
- Inform risk transfer requirements
- Reinforce risk management culture
- Reduce surprises
- Demonstrate Effective Governance to Board, C-Suite, and Regulators
- Reduce cost through efficiency

RSA Archer GRC

Additional Resources from RSA Archer

- Marshall Toburen, GRC Strategist
  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

POLL #4

Are you a PAID member of OCEG who is interested in receiving CPE credit for this event?

A. Yes, I am a PAID OCEG member and would like to receive a Certificate of Completion for this event

B. No, I am not a PAID OCEG member

Questions?