Enhancing Third Party Risk Management in Cybersecurity and Privacy Programs

Darren Hulem,
CISA, Security+, PCIP
Moderator

Ricardo Trujillo,
CPA, CITP, CISA
Partner

Melissa Musser,
CPA, CITP, CISA
Principal

Gelman, Rosenberg & Freedman CPAs is now GRF CPAs & Advisors

Please note our new address:

4550 Montgomery Avenue, Suite 800N, Bethesda, MD 20814

grf CPAs & ADVISORS

Housekeeping

CPE Credit/Technical Support

- **Important:** Three (3) CPE words will be provided during the presentation. Please write them down – **we will not provide them again via Zom or email (no exceptions)**.
- Please complete the electronic survey that will appear automatically at the **end of the webinar**.
- Attendees seeking CPE for this presentation must complete the survey and **enter all three CPE words**. You cannot claim CPE unless we receive a completed evaluation with the correct words.
- This presentation will be recorded and made available to download at www.grfcpa.com/webinars.
- Technical questions about the survey can be addressed to Nathan McElveen at nmcelveen@grfcpa.com.

Housekeeping

Additional Information

Learning Objective To provide attendees with an overview of the cybersecurity & fraud landscape and best practices for protecting their organizations from threats	**Instructional Delivery Methods** Group Internet-based
Recommended CPE 1.0 CPE Credit	**Recommended Fields of Study** Information Technology
Prerequisites None required	**Advance Preparation** None
Program Level Basic	**Course Registration Requirements** None
Refund Policy No fee is required to participate in this session.	**Cancellation Policy** In the event that the presentation is cancelled or rescheduled, participants will be contacted immediately with details.
Complaint Resolution Policy GRF CPAs & Advisors is committed to our participants' 100% satisfaction and will make every reasonable effort to resolve complaints as quickly as possible. Please contact *kdavis@grfcpa.com* with any concerns.	
Disclaimer This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.	

Presenters

Meet the Instructors

Melissa Musser,

CPA, CITP, CISA

Principal

Ricardo Trujillo,

CPA, CITP, CISA

Partner

Darren Hulem,

CISA, Security+, PCIP

Moderator

Presenters

Meet the Instructors

Ricardo Trujillo,

CPA, CITP, CISA

Partner | *rtujillo@grfcpa.com*

Mr. Trujillo has worked in auditing and accounting since 2000. He has proven expertise in assurance and advisory services, and his nonprofit experience spans across a variety of organizations, including foundations, trade and membership associations, charitable institutions and US-based non-governmental organizations.

Mr. Trujillo leads the firm's information technology initiative and helps for-profit and nonprofit organizations bridge the gap between business and technology by carefully analyzing IT infrastructures. He presents to the nonprofit community on cybersecurity and enterprise risk management topics.

Melissa Musser,

CPA, CITP, CISA

Principal | *mmusser@grfcpa.com*

Mrs. Musser is a principal at GRF with over 15 years of professional experience. She and her team deliver comprehensive risk-based assessments to help organizations respond to strategic, financial, compliance, operational and IT risks. Her expertise includes establishing, maintaining and optimizing internal controls, compliance, Enterprise Risk Management (ERM), and cybersecurity programs. Mrs. Musser is the proud recipient of the 2018 AICPA Information Management and Technology Assurance (IMTA) Standing Ovation award.

Agenda

Topics and Questions

- The value of third-party risk management (TPRM) in your organization
- TPRM's role in cybersecurity and privacy
- Is your current third-party oversight adequate? Does your organization's risk management of third parties occur throughout the lifespan of the relationship, or primarily just during the onboarding process?
- How to develop your organization's TPRM framework in an efficient and cost effective manner while also maintaining baseline security and privacy expectations

Polling Question #1

To your knowledge, does your organization have a TPRM Program in place?

A. *Yes*

B. *No*

C. *Unsure*

The value of third-party risk management (TPRM) in your organization

grf CPAs & ADVISORS

Negative Media Attention

Pentagon Staff Hit by Major Data Breach

30,000 civilian and military personnel PII Compromised

"The department is continuing to gather additional information about the incident, which involves the potential compromise of personally identifiable information (PII) of DoD personnel maintained by a single commercial vendor that provided travel management services to the department," the statement noted. "This vendor was performing a small percentage of the overall travel management services of DoD."

https://www.infosecurity-magazine.com/news/pentagon-staff-hit-by-major-data/

grf CPAs & ADVISORS

Third Party Risk Management (TPRM)

Third-party risk management is now a critical component of any enterprise risk management framework as **Third Parties are more involved in all aspects of business.**

TPRM's role in cybersecurity and privacy

Third Party Risk Management (TPRM)

- The process of analyzing and mitigating risks to your organization by parties OTHER than your own organization.
- Due Diligence is the process by which the vendor is reviewed to determine its suitability for a given task.
    - Due diligence is an ongoing activity, including review, monitoring, and management communication over the entire vendor lifecycle!

TPRM's role in cybersecurity and privacy

- Reduce likelihood of:
  - data breach costs
  - operational failures
  - vendor bankruptcy
  - reputation damage

Polling Question #2

Do you consider third parties when conducting your IT risk Assessments?

A. Yes

B. No

C. Unsure

grf CPAs & ADVISORS

Risk Assessment

IT Risk Assessment

- Are you doing it correctly?
- Are you thinking about the right risks?
- Who is doing it?
- Are you benchmarking your process against well know frameworks: i.e. ISO 27001
- Do you have an up to date network and third party diagram?

ISO 27001 Controls

- Information Security Policies
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

ISO 27001 Controls

A.15 Supplier relationships

Information security in supplier relationships

- Is information security included in contracts established with suppliers and service providers?
- Is there an organization-wide risk management approach to supplier relationships?

Addressing security within supplier agreements

- Are suppliers provided with documented security requirements?
- Is supplier access to information assets & infrastructure controlled and monitored?

Information and communication technology supply chain

- Do supplier agreements include requirements to address information security within the service & product supply chain?

Monitoring and review of supplier services

- Are suppliers subject to regular review and audit?

Managing changes to supplier services

- Are changes to the provision of services subject to a management process which includes security & risk assessment?

Annual Process

How to develop your organization's TPRM framework

Pinpointing Third Party Risks

- Assess your current environment
- Develop a 3rd party framework based on your organizations context
- Develop a risk stratification guidelines to highlight risks by vendor
- Implement and conduct vendor assessments
- Establish a reporting process

Example Stratification

Vendor stratification - Example

- Tier 1 – Critical vendors (10%) – PII + critical systems
- Tier 2 – Major vendors (40%) – PII OR critical systems
- Tier 3 – Vendors (50%) – commodities/low risk purchases

Design

Third Party Due Diligence

Risk Assessment (Documentation, Categories of Risk,

Financial projections & review

Insurance Review

Legal Review

Vendor Audits and/or SOC reports

Background check

grf CPAs & ADVISORS

Polling Question #3

Do you request or perform audit / assessments of your third parties?

A. *Yes*

B. *No*

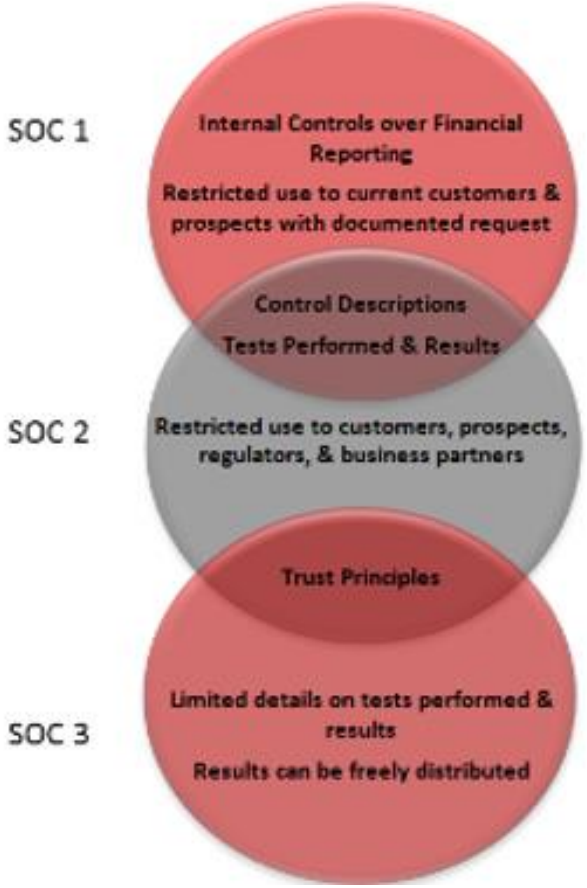
C. *Unsure*

Is your current third-party oversight adequate?

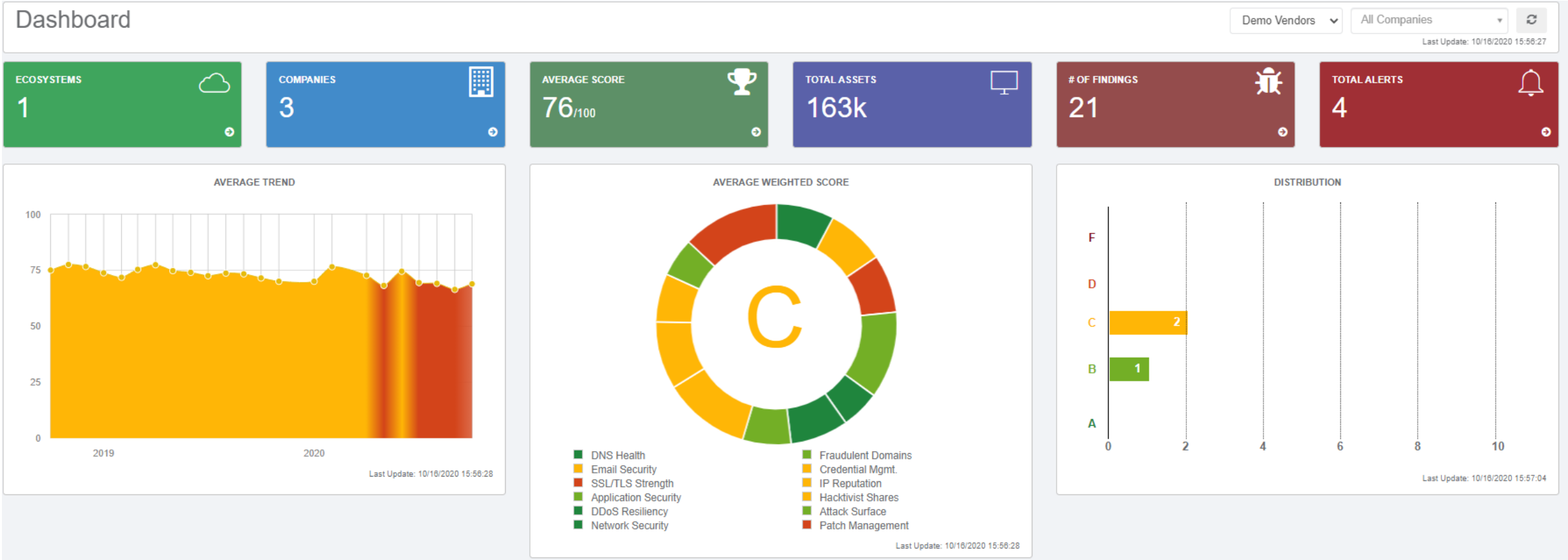
Audits

- Request Audit your own TPRM process (internal audit)
- Request audits of Vendors (i.e. SOC Audits)

Not just a one time deal…must audit again, and again!



Cyber Risk Scorecard



CPAs & ADVISORS

Service Level Agreements (SLA)

The Service Level Agreement contains the contractually relevant data for an outsourced Service:

- Contact persons
- Contract duration
- Service description
- Procedures for requesting service
- Responsibilities
- Quality assurance and Service Level Reporting

Service Level Agreement (SLA) Considerations

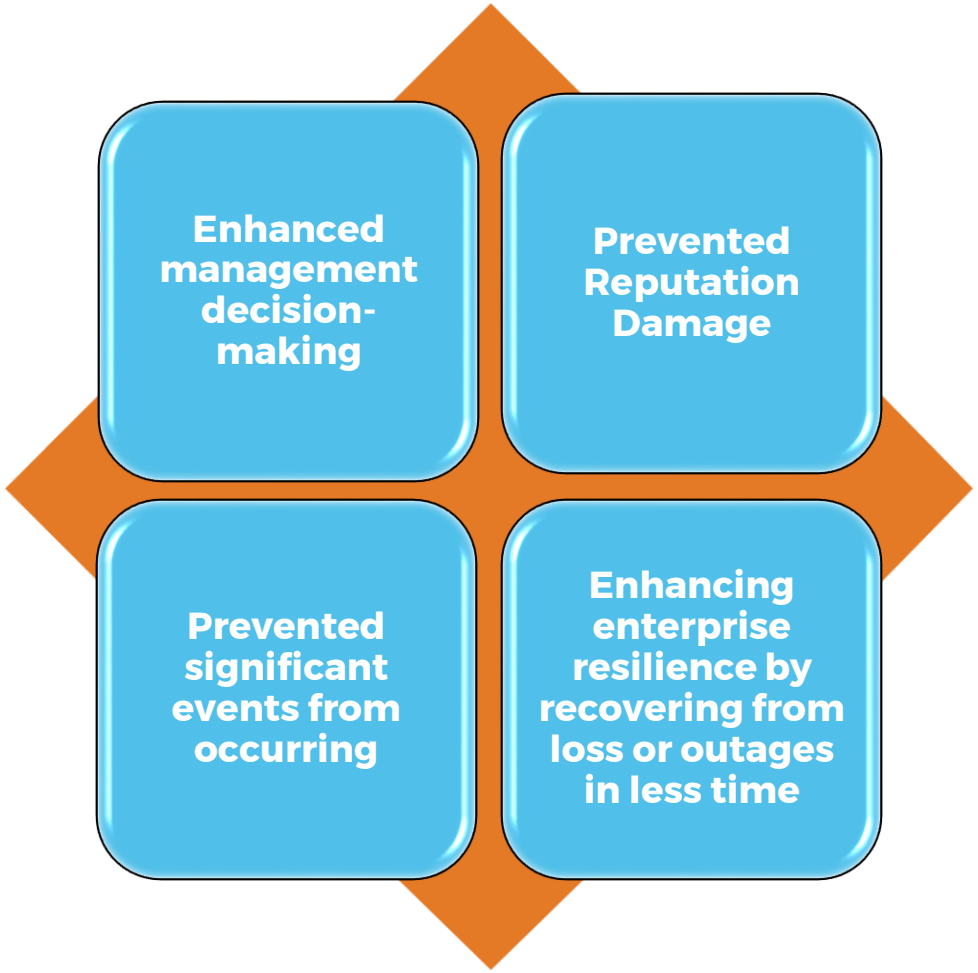
- How are service levels and availability measured, monitored & reported?
- How are SLA issues resolved?
- Incident reporting systems, access and usage reports
- Notifications of scheduled downtime

Procurement Process

- Competition is good. Don't decide on a vendor too early in the process.
- Best price does not equal best vendor, focus on meeting your requirements

Developing Next Steps

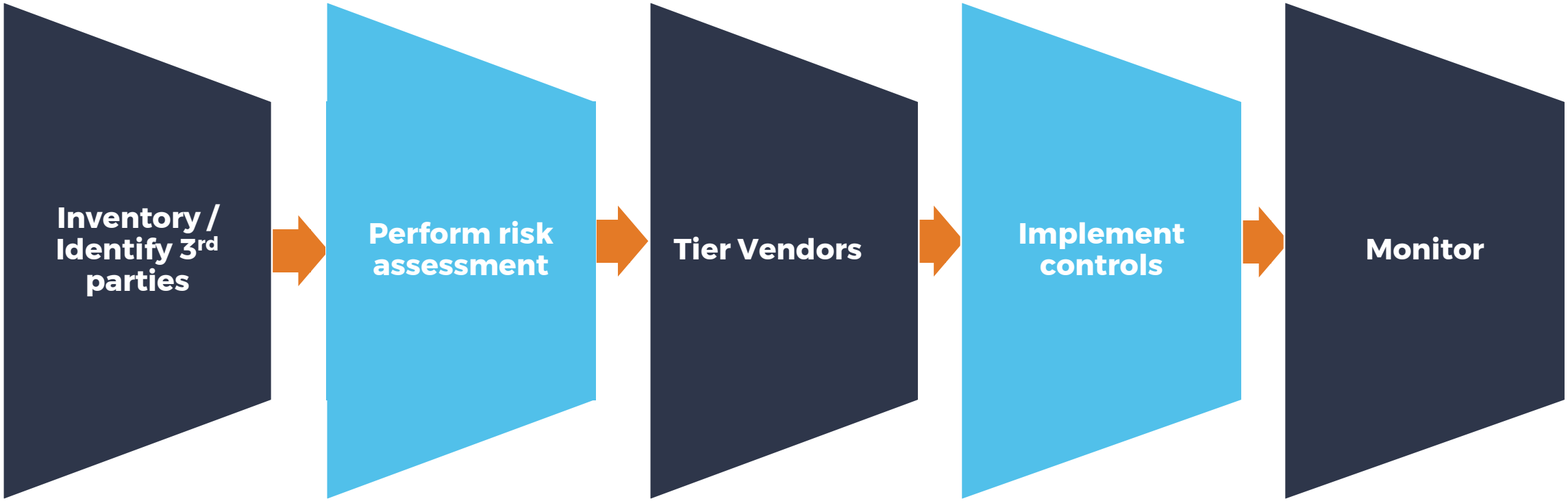
Benefits of TPRM



CPAs & ADVISORS

Developing Next Steps

Critical Success Factors



CPAs & ADVISORS

Developing Next Steps

Developing Procedures

- Develop and document procedures for conducting risk assessments and develop templates and tools to facilitate and standardize the process
- The procedures generally contain the following information:

Who is responsible for initiating and conducting risk assessments

Who will participate

What steps will be followed

How disagreements will be handled and resolved

What approvals will be needed

How assessments will be documented

How documentation will be maintained

To whom reports will to be provided

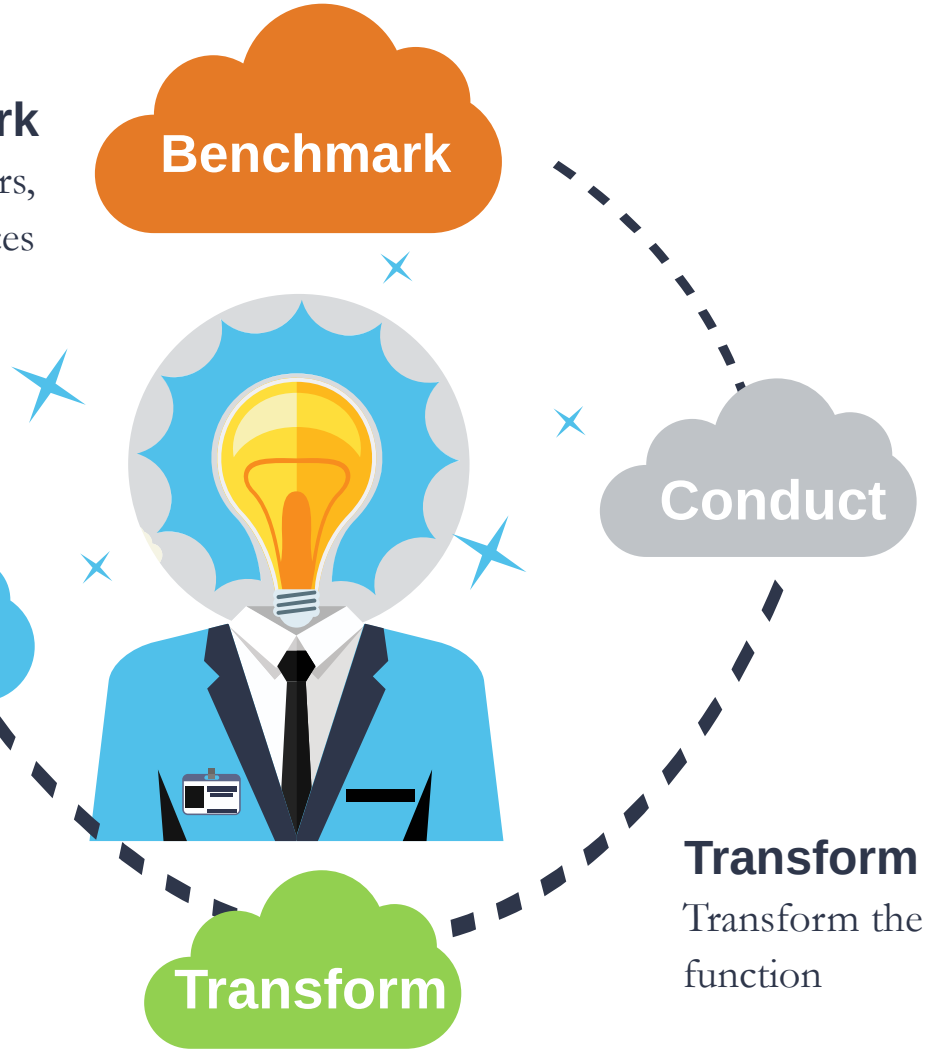
grf CPAs & ADVISORS

Developing Next Steps

TPRM

Benchmark

Benchmarking against peers, frameworks and leading best practices



Conduct

Conduct risk assessments

Simplify

If needed, simplify the process

Transform

Transform the procurement function

CPAs & ADVISORS

GRF Resources

Third Party Risk in a Post-Pandemic World:
https://www.grfcpa.com/resource/third-party-risk-in-a-post-pandemic-world/

Third Party Risk Management Checklist
https://www.grfcpa.com/wp-content/uploads/2020/06/Third-Party-Risk-Management-Checklist.pdf

Sign Up for Industry Alerts:
https://www.grfcpa.com/resources/newsletters/

Cybersecurity Scorecard:
https://www.youtube.com/watch?v=S0YuaYaPOjE

Upcoming Events

3-Part Virtual Workshop Series: Navigating the World of Uncertainties Impacting Nonprofit Organizations

Workshop in Partnership with NC State University's Poole College of Management | 12:00 pm – 2:00 pm

Pandemic Survival for Associations – Diversifying Revenue in Challenging Economic Times

Virtual Roundtable | 9:00 am – 11:00 am

Internal Audit & ERM Priorities for 2021

Webinar | 1:00 pm – 2:00 pm

grf CPAs & ADVISORS

Questions?

Contact Us

CPAs & ADVISORS

Maryland | DC | New York

877-437-4771 | www.grfcpa.com

Melissa Musser,
CPA, CITP, CISA

mmusser@grfcpa.com
301-951-9090

Ricardo Trujillo,
CPA, CITP, CISA

rtrujillo@grfcpa.com
301-951-9090

Darren Hulem,
CISA, Security+, PCIP

dhulem@grfcpa.com
301-951-9090

Disclaimer

This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. While we use reasonable efforts to furnish accurate and up-to-date information, we do not warrant that any information contained in or made available in this webinar is accurate, complete, reliable, current or error-free. We assume no liability or responsibility for any errors or omissions in the content of this webinar.

The use of the information provided in this webinar does not establish any contractual or other form of client engagement between GRF CPAs & Advisors and the reader or user. Any U.S. federal tax advice contained in this webinar is not intended to be used for the purpose of avoiding penalties under U.S. federal tax law. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.