ASMGi | Prevalent

Third-Party Risk:

Critical Requirements for Benchmarking Your Business & Supply Chain Resilience

Your Presenters

Brenda Ferraro
VP, Third-Party Risk
Prevalent

The Top 25 Women Leaders in Cybersecurity 2020
TSR The Software Report

Steve Roesing
President, CEO
ASMGi

Discussion Topics

- *Introduction / Background*
- *Understanding how to adjust business continuity plans according to the possibility of degraded product/service due to regional quarantines*
- *Knowing your third-party ecosystem and identify your weakest third-party link for providing your products and services*
- *Identifying where it is best to cut cost to minimize damage to the supply chain*
- *Addressing questionnaire fatigue*
- *Proactively preparing for the regulatory heyday after the dust settles from COVID-19*

IBM Security

2019 Cost of a Data Breach Report

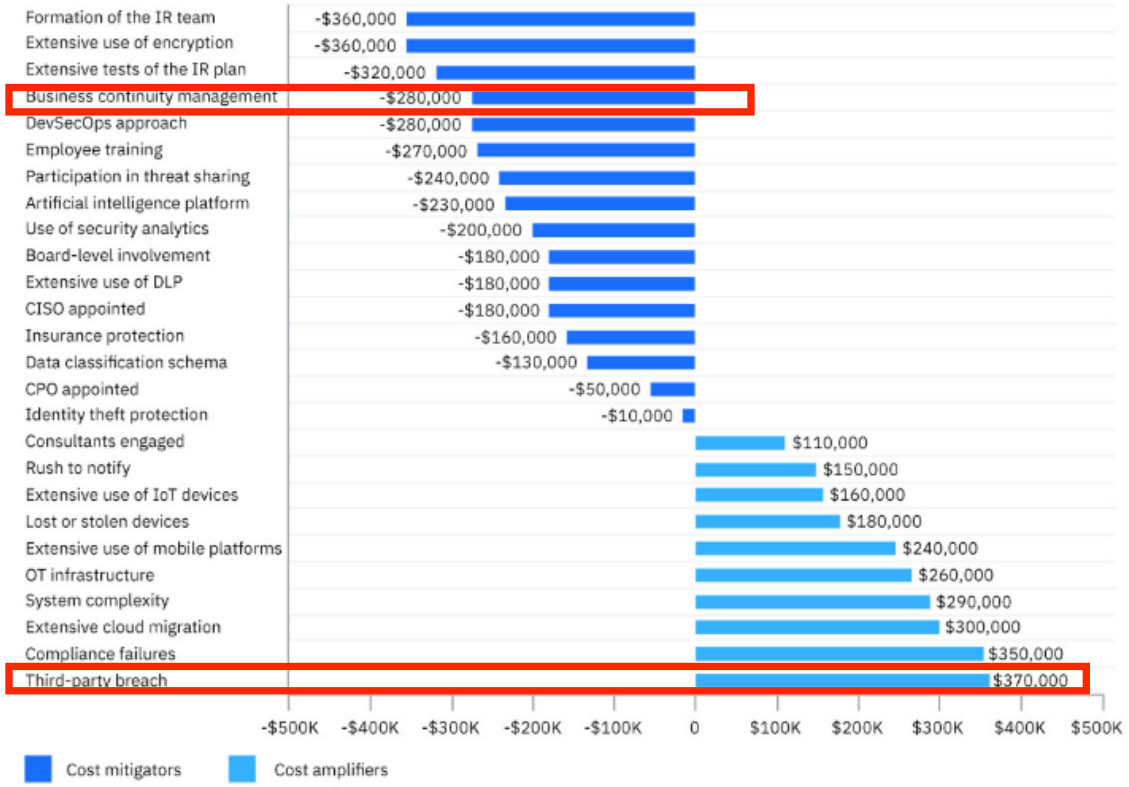
ASMGi

How factors increase or decrease the total cost of a data breach

Difference from average total cost of US $3.92 million

- $280,000 (7%)

+ $370,000 (9%)



Prevalent

IBM

Ponemon Institute

Source: KPMG International

A Holistic Approach to Cyber Security

ASMGi

ONEteam = TOTAL SOLUTION

Program + Technology + Operations

Prevalent™

Poll #1 – Which area presents the biggest challenge for you?

a. Program	a. 0%
b. Technology	b. 26.67%
c. Operations	c. 40%
d. All of the above	d. 33%
e. None of the above	e. 0%

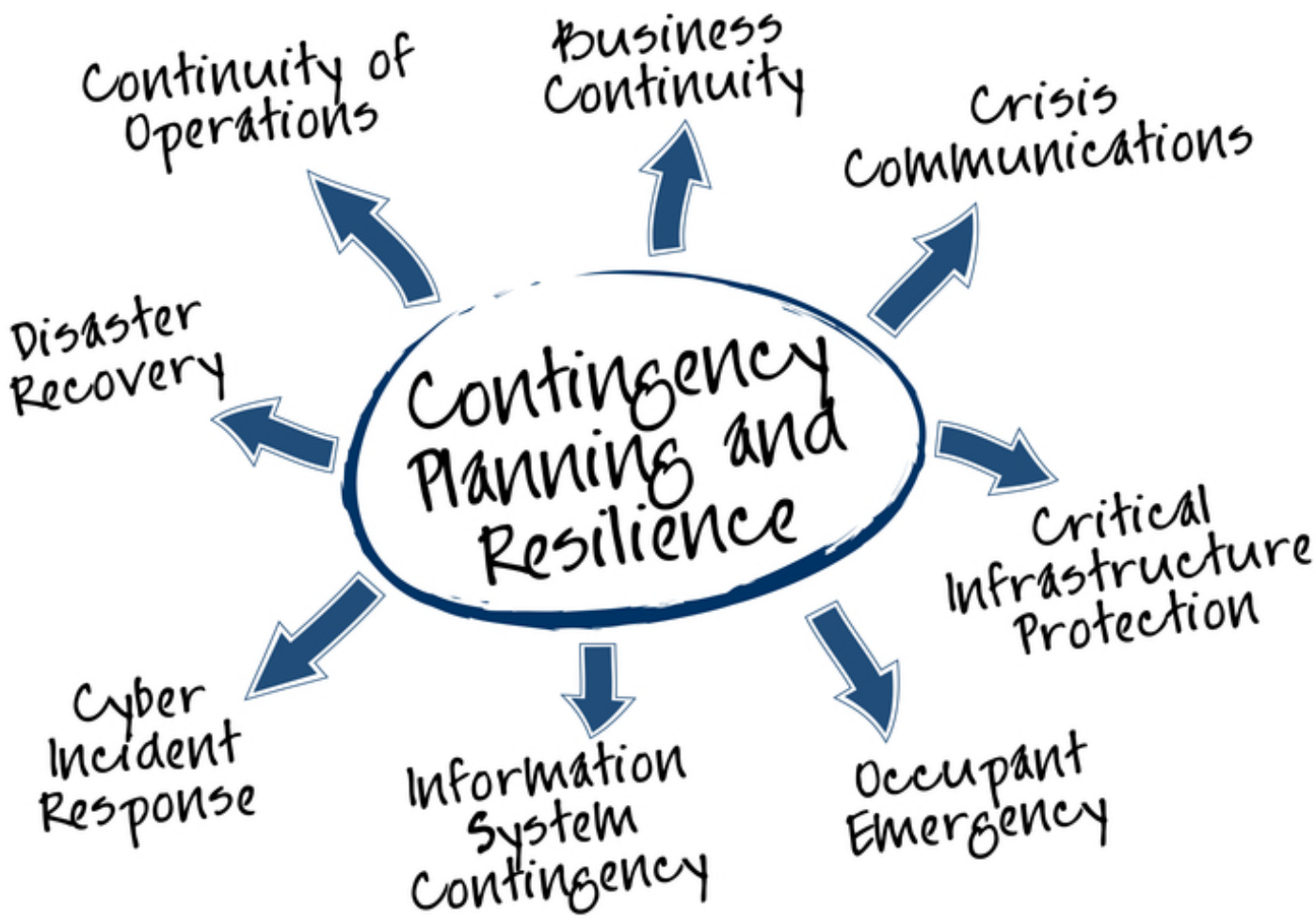
Business Resilience

The ability of an organization to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.

What Business Resilience Involves

Prevalent

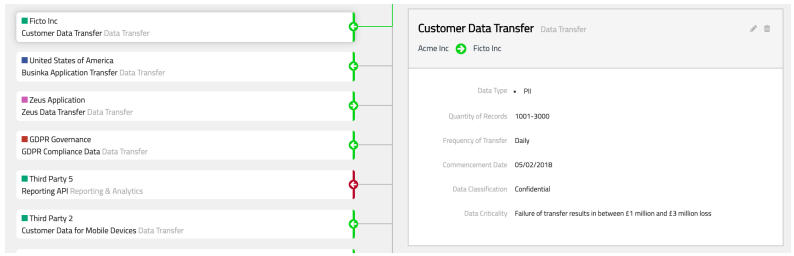
Assessments (both internal and external for third-parties) play a **vital role** in gauging an organization's resilience



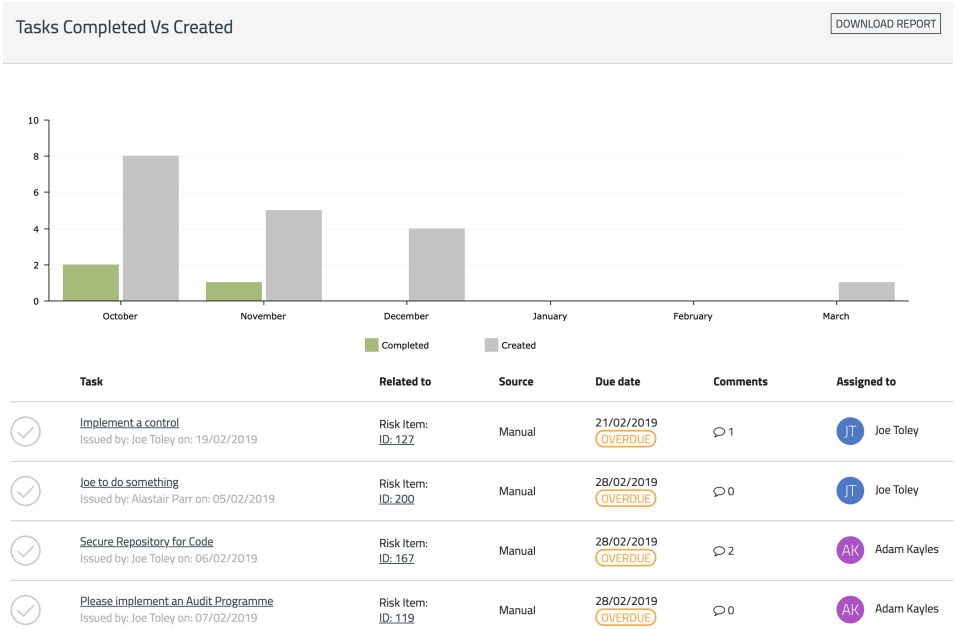
Key Risk Indicators (KRIs)

Prevalent

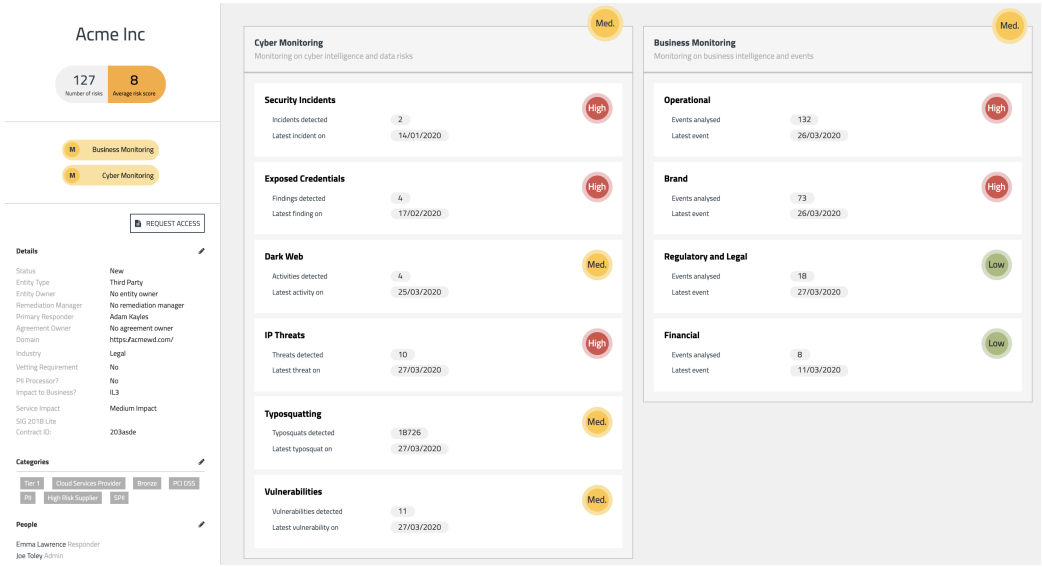
Nth Party Span of Risk



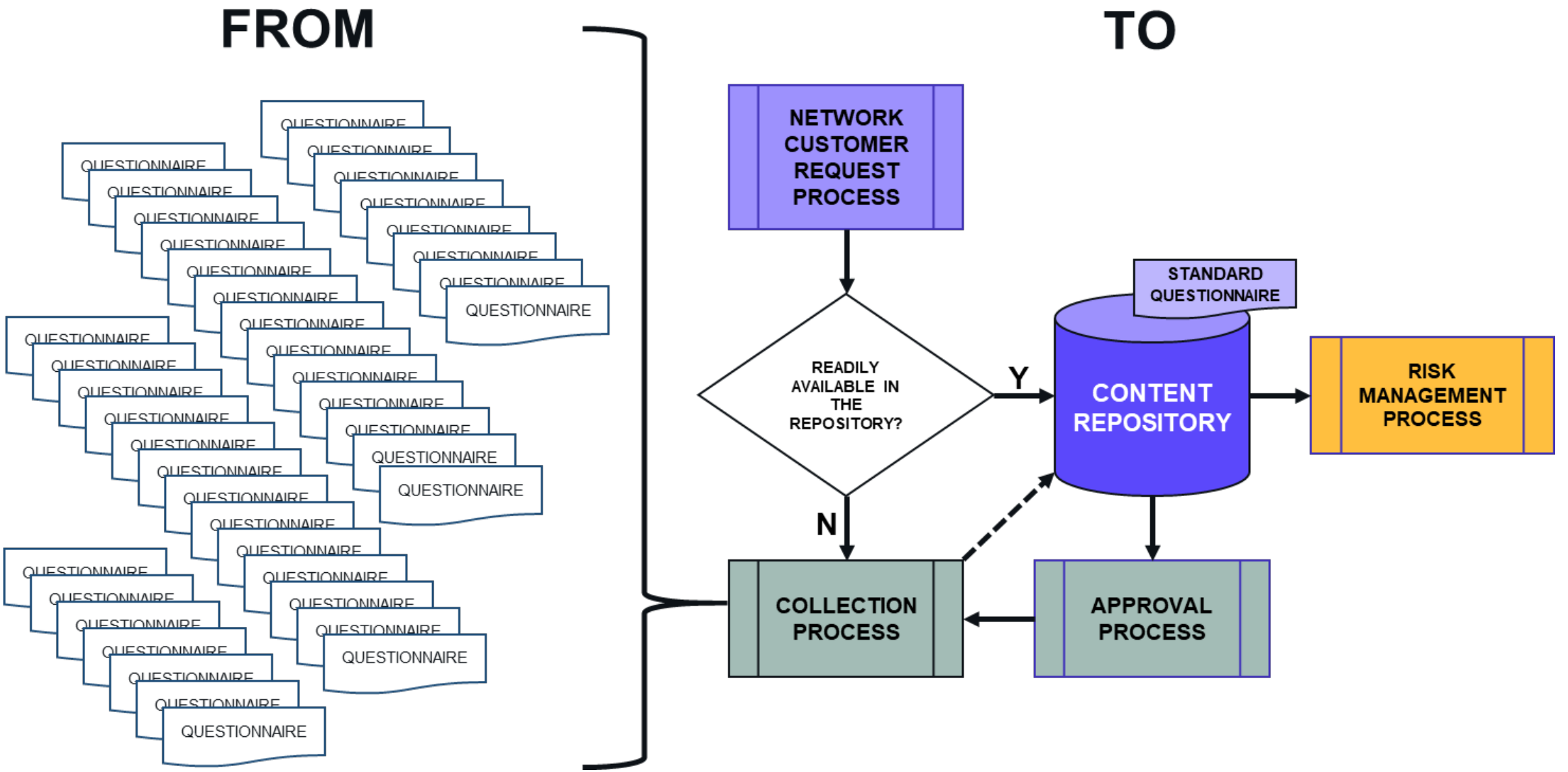
Overdue Risk Remediations



Threat Score Monitoring



Questionnaire Fatigue



Proactively Prepare for the Regulators

Prevalent

- ✓ Know your third-party and Nth parties
- ✓ Ensure compliance readiness:
  - ✓ GDPR
  - ✓ PCI
  - ✓ NYDFS
  - ✓ HIPAA / BAA
  - ✓ CCPA
- ✓ Measure third-party risk program maturity and governance
  - ✓ KRI / KPI
- ✓ Assess internal and external risk for business continuity and resilience preparedness

Key Takeaways

ASMGi

- *Business & Supply Chain Resilience is critical*
- *TPRM is a vital component of Business & Supply Chain Resilience*
- *Assessing Third-Party Risk is complex and should follow a process and leverage automation*
- *A Total Solution includes Program + Technology + Operations*

Prevalent™

ASMGi ONEteam TPRM Services

ASMGi

1 Program

- Business Objectives
- What framework will you use to assess your vendors?
- How many vendors do you have and how are they tiered?
- What is your SLA for vendors in each tier?
- How many vendors will you assess per year?

2 Technology / Platform

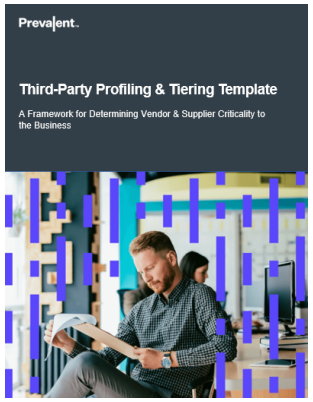
- Technology is critical to keep up with ever-changing landscape
- Discover, Tier, Store & Risk Rate all vendors here
- Automate Assessment process
- Continuous Vendor Risk Management and Monitoring

3 Operations

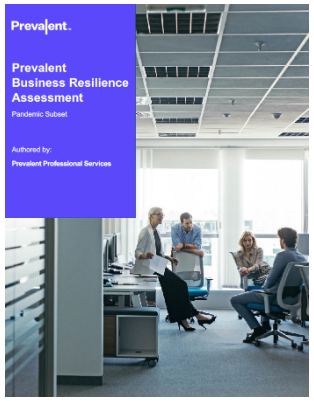
- Complete vendor assessments per Program requirements
- How will you get the assessments done?
- You can do the work, or we can – it's up to you!

Prevalent™

Special offers for attendees…



Third-Party Profiling & Tiering Template



Business Resiliency Assessment - Pandemic

To download these templates
Visit www.asmgi.com/prevalentwebinar

Zero to TPRM in 30 Days

Prevalent.

TPRM Jump Start

Quickly onboard and assess your vendors for business resilience

Prevalent TPRM Jump Start provides an easy, affordable way for any size organization to build a structured third-party risk management program and see actionable results in 30 days or less.

Vendor Discovery
Discover vendors with an automated onboarding process

Inherent Risk Scoring
Quantify the inherent risk vendors pose to your business

Vendor Tiering
Tier and categorize vendors based on the criticality of their service

Automated Vendor Assessment
Assess against best-practice industry frameworks to benchmark vendor risk

Clear Risk Scoring
Report on risks through a clear risk score

Remediation Recommendations
Mitigate vendor residual risk with built-in remediation recommendations

Jump Start your TPRM by contacting ASMGi: sales@asmgi.com

***Poll #2** – In the next 12 months, do you plan to evaluate TPRM vendors in an effort to establish or enhance your TPRM program?*

a. Yes	**a. 53.85%**
b. No	**b. 23.08%**
c. I don't know	**c. 23.08%**

QUESTIONS / DISCUSSION

Question – *What are the options that we as team can connect during this pandemic when there is only option to connect virtually and exchanging data which is of higher risk?*

Become part of a network that meets for your industry such as the ISACs or ISAO or Associations. Peer to Peer practitioner support is not only education but important during virtual wfh situations.

With regards to data exchange at higher risk confirm you have DLP in place to assist with streamlining the data that is handled/hosted/processed/stored.

You may even want to look into securing the data control with homomorphic encryption to contain the data within your four walls and/or cloud environment (however this means the data can't leave your watch or premises and that sometimes is not doable for the engagement).

Question – *We usually go through 60 on site audits annually, and this year all our clients are performing virtual audits. So far we have concluded 6 of them, and have 3 others are scheduled. I think our clients are finding that they can perform the same audit without the travel cost.*

Virtual validation is becoming more popular. Keep in mind the effectiveness of controls need to be tested to make sure they are enforced. Incident Response Scenario based tests or table top exercises can also help in lieu of onsite visits. Also, Threat Intelligence is bridging a portion of the gap as well.

Question – *Is it critical to have a Steering Committee to disposition third parties?*

Steering Committee(s) are used when third parties either do not comply with contractual obligations, are unresponsive, require risk acceptance based on compensating controls, and can provide final risk based decisions in cases where risk mitigation items are not completed on time.

Disposition of third parties is critical to make sure the business takes ownership of the risk, identifies the risk appetite and balances the risk tolerance of the company.

Question *– How do you hold third parties accountable for fulfilling your TPRM program requirements, is it with contracts, or do you have a relationship with Procurement?*

Begin with partnering with your procurement department to use threat intelligence and key control and/or a inherent profile risk questionnaire as part of the risk stratification scoring technique for selection process during RFx.

Contracts need to reflect an un-red-line-able security expectation addendum that informs all third parties the Key Controls that must be in place to partner in business with them.

Also the Contract should stipulate the TPRM due diligence process completion requirement that is separate from the annual audit clause. TPRM Assessments are continuous and are not bound by an annual timeline. Audits should be limited to once per year due to the amount of time and effort an audit consumes.

Question *– With automation techniques implemented, what is the average time to collect content, average time to assess for risk, and average time to negotiate with the third party?*

When automation is in place for onboarding a third party with automated chaser reminder emails the collection of due diligence response should only take an average of 7 days for a questionnaire that is around 175 questions. In cases where the point of contact is on vacation you may experience a 14 day turnaround.

When automation is in place for assess review to identify risk with pre-configured risk scoring and risk recommendations the risk assessment should be instantaneous. As soon as the responses are submitted the platform will reflect the risk and the risk recommendations with the appropriate role based access review capabilities, risk register, and compliance mapping.

When automation is in place for negotiations with third parties on compensating controls and/or risk mitigation action item timelines with automation the negotiation timeline is reduced based on the platform communication portal. Meetings with the third party is not required only if the third party requires a discussion with the TPRM team due to misunderstanding of the recommendation requirement and/or a fiscal challenge impedes the ability to complete the risk remediation action within the required timeline.

Question – *Is there a standard questionnaire we could use for vendors?*

Within the Prevalent Platform there are standard questionnaire(s) available from the Shared Assessments Standard Information Gathering (SIG) Questionnaire, the H-ISAC Questionnaire, and the Prevalent Control Framework Questionnaire just to name a few. The platform has over 50 questionnaire(s) within the library to use.

Question - *What does continuous monitoring entail? Could we do it through your platform?*

ASMGi

Continuous Monitoring is in all essence Threat Intelligence that comes from threat feeds to provide transparency of what can be scanned in the wild. The Prevalent Platform has a capability known as Vendor Threat Monitoring (VTM) and it includes Cyber and Business Threat Intelligence for risk based decisions and triggers.

Prevalent™

***Question** - It can be challenging to get vendors to respond, any thoughts on how to make that part work better?*

Using the Prevalent Platform there are automated email notifications that will assist in helping the vendors respond.

Also you can apply an unresponsive risk. The main goal is to help the company improve their risk posture while creating a strong relationship. Utilizing a platform that is easy to use will help.

Also if you adopt a standard questionnaire or become part of a network the ease of repurposing readily available content will speed up the process to focus on identifying and reducing risk.

Remember to make sure your contracts include stipulations on the requirements to complete the TPRM due diligence requirements.

Question - *What the difference between a platform for enterprise risk versus a platform for third-party risk?*

Platform for Enterprise Risk can include a multitude of departments that share the content that is submitted for review and the Platform will provide different views for the role based access rights for the viewer. Content can be sliced and diced for things such as PCI, HIPAA, NIST, ISO, etc.

Platform for Third-Party Risk assists in TPRM and Third Party communication as the engine to support the collect/assess/mitigate management whereas APIs are used to feed GRC or IRM solutions to speak to the Internal Business Executives and Committees.

Question - *Are there any standards or frameworks for insurance companies?*

Depending on what type of insurance company you are, you may need to include the financial regulatory requirements.

It is recommended that you implement an information classification model and then apply the regulatory requirements for compliance.

As far as a standard, Prevalent sees majority of the financial insurances using the SIG questionnaire and for the healthcare insurance the H-ISAC Lite questionnaire is used.

Question - *We don't have a program. How do we get started?*

Contact ASMGi (sales@asmgi.com) to help you better understand where to start. There are several packages that will fit the needs of your company to create an evolutionary approach to build a mature TPRM program.

From jump start, to essential inherent risk profiling, to automation and scalability realization. If you are a company that already has a program in place, look to conduct a Prevalent Maturity Assessment to recognize the great work you have in place and opportunities for growth.

Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com