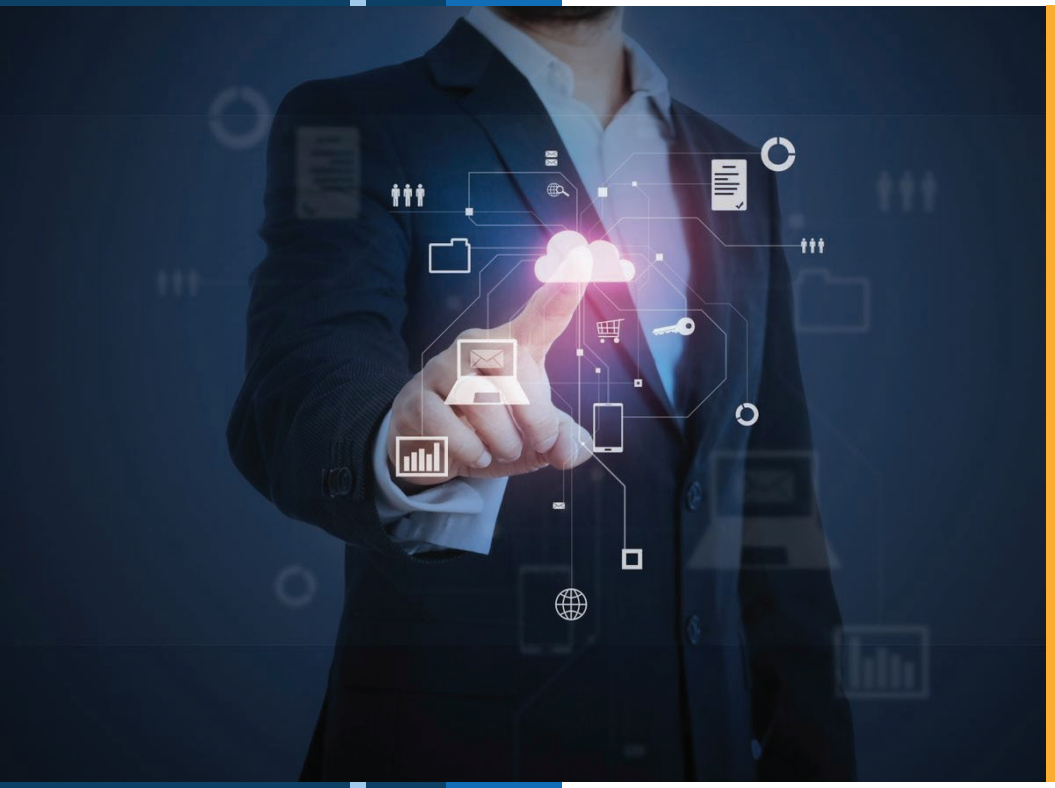
CORPORATER

THIRD-PARTY
RISK MANAGEMENT

ARTICLE

AUTHOR: **DAVID VINCENT**



What Is Third-Party Risk Management?

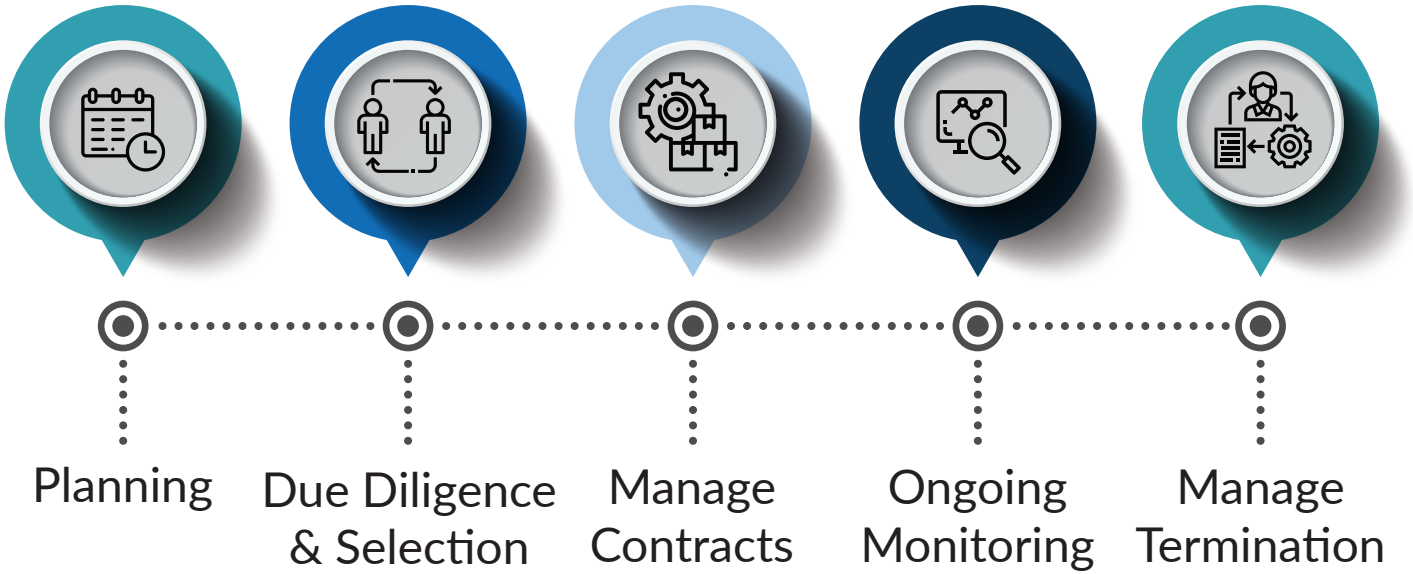
Third-Party Risk Management (TPRM) is the process of analyzing and controlling risks presented to your organization by outsourcing to third-party service providers (TPSP). On average organizations spend $10M+ responding to third-party security breaches each year. However, information security is not the only area impacted. TPSP relationships can introduce strategic, financial, operational, regulatory, and reputational risks.

For example, some TPSPs are involved in the storage, processing, and/or transmission of cardholder data (CHD), while others are involved in securing cardholder data, or securing the cardholder data environment (CDE).

Point-of-sale companies (or integrators/resellers) are involved with the installation, maintenance, monitoring, or otherwise, support of their systems.

Digital relationships with third-party providers increase opportunities for growth, but they also increase opportunities for cyberattacks — a recent study found that 61% of U.S. companies said they had experienced a data breach caused by one of their third-party providers (up 12% since 2016) [(i)].

Traditionally, the TPSP lifecycle incorporates these five phases, which required effective integration of governance, performance, and risk management in each step.



What Is Due Diligence?

Due Diligence is the investigative process by which TPSPs are reviewed to determine suitability for a given task before establishing a relationship for the engagement with an organization. Organizations can improve the effectiveness of their due diligence process by utilizing external intelligence services such as: BitSight for cybersecurity, Dun & Bradstreet for financial performance, Refinitiv for financial crime, Polecat for reputation, and riskmethods for supply chain resilience information.

Additionally, it is very important to understand that due diligence MUST be an ongoing activity, including reviewing, monitoring, and management communication over the entire TPSP lifecycle.

Monitoring of the TPSP compliance status helps to provide the organization with assurance and awareness about whether the provider is complying with the applicable requirements for the services provided.

Therefore, the effectiveness of your due diligence process will directly impact the success of your TPSP Risk Management program.

Five Key TPSP Risk Assessment Objectives For Your Due Diligence Process

Identify – Understand the specific products and/or services your TPSP provides, determine if TPSPs will require access to critical business processes and data within your environment, and review relevant data from external intelligence service providers (e.g., BitSight, Dun & Bradstreet, LexisNexis, etc.).

Analyze – Quantify the risk to your organization of engaging with the TPSP and assign a security risk ranking to prioritize the risk exposure of each TPSP relationship.

Respond – Based on your risk analysis, decide if you are willing to engage with the TPSP or not, and define your risk response plan for each approved TPSP necessary to effectively monitor and manage the TPSP residual risk exposure against your organization's acceptable risk tolerance level.

Monitor – Perform TPSP engagement management monitoring through ongoing due diligence assessments of TPSPs to identify any changes in the initial risk exposure. The creating of effective risk assessment survey questionnaires is an important step in maintaining an effective due diligence monitoring process.

Test – Conduct quarterly self-assessments of your end-to-end TPSP Risk Management process to validate the effectiveness of the controls and identify opportunities to make improvements. Also, have your Internal Audit department conduct their own independent assessments to validate the effectiveness of your TPSP Risk Management process.

15 Examples of Third-Party Risk Management Leading Practices

1. The organization has established a Tone at the Top with Board-level oversight to enable effective Governance over the TPRM Program.
2. The TPRM Program has been established following a Third-Party Management Lifecycle, and effective policies, processes, procedures, guidelines, tools, and templates exist, which have been communicated to all relevant TPRM members via periodic TPRM training.
3. The TPRM Program roles and responsibilities have been clearly defined, communicated, and understood by all members.
4. An accurate and complete inventory of all providers exists and is updated frequently.
5. The organization is effectively identifying, analyzing, evaluating, and responding to all engagement risks and performing appropriate due diligence.
6. The organization is effectively incorporating risk, compliance, and performance requirements in the contracts/agreements as KPIs to proactively monitor and measure variances.
7. The organization is effectively performing periodic risk management actives and continuous control monitoring to proactively identify and resolve exceptions.

8. The organization performs continuous monitoring to identify changes and performance variances with providers.
9. The organization is effectively determining the need to terminate and off-board or renew.
10. The effectiveness of the TPRM Program is independently evaluated to identify opportunities to correct problems and make improvements.
11. The organization has an effective business contingency plan for interruptions and disasters caused by vendors, which is periodically tested for operating effectiveness.
12. A formal self-assessment is performed periodically to evaluate the capability and effectiveness of the TPRM team's performance and the effectiveness of the mentoring and training program.
13. The capability and effectiveness of the TPRM Program are independently evaluated to identify opportunities to correct problems and make improvements.
14. The organization consolidated all of its TPRM data and functions into one centralized solution to increase the efficiency, effectiveness, productivity, and transparency across the organization for managing TPRM.
15. The organization has established Continuous Controls Monitoring (CCM) to enables organizations to transition from performing periodic assessments of randomly selected samples from a larger population to conducting control assessments 24/7/365 for the full populations.

How to Build an Effective Risk Assessment Questionnaire?

Regarding the risk assessment questionnaire, organizations should decide whether they will be using a standard assessment questionnaire from popular sources like PCI-DSS, HIPAA, GDPR, ISO, NIST, or a custom questionnaire.

Standard assessment questionnaires are created to fit regulations or specific industry trends to assess different areas of privacy or security risk more effectively, so they are a better starting point.

However, the need for specific answers and more control often results in custom questionnaires.

Custom questionnaires are tricky because they force providers to answer both standard and custom questions, which causes more work for TPSPs that prevent them from leverage existing answers from past risk assessments they have completed.

According to a 2018 E&Y study, 72% of companies use industry-standard questionnaires or have built their own by using a standard as a baseline. There are best practices to use as a starting point for the high-level items in the questionnaires.

Below are several industry-standard security assessment methodologies you can start with to gather and build your questionnaires:

1. The SANS (System Administration, Networking, and Security Institute) Top 20 Critical Security Controls — a shortlist of controls developed by security experts based on practices that are known to be effective in reducing cyber risks.
2. The NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity — combines a variety of cybersecurity standards and best practices together in one understandable document [ii].
3. Shared Assessments — An organization that develops assessment questionnaires for use by its members. The members of this organization work together to create and share third-party risk management assessment guides their organizations are utilizing.
4. ISO/IEC 27000 – The International Organization for Standardization is an international standard-setting body composed of representatives from various national standards organizations. The ISO/IEC 27000 family of standards helps organizations keep information assets secure.

5 PCI-DSS – The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store, or transmit credit card information maintain a secure environment. Within their document library, you can access numerous sources of information to build your questionnaire, such as the Third Party Security Assurance document.

6 HIPAA – The Health Insurance Portability and Accountability Act of 1996 was enacted by the 104th United States Congress and signed by President Bill Clinton in 1996 and requires the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.

7 GDPR – The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

8 HITRUST – The Health Information Trust Alliance, is a privately held company located in Frisco, Texas, United States that, in collaboration with healthcare, technology, and information security leaders, has established the HITRUST CSF, a comprehensive, prescriptive, and certifiable framework, that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data.

9 OWASP – The Open Web Application Security Project is a global organization that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security best practices such as their OWASP Top 10 most critical web app security list.

How to Build Effective Risk Assessment Survey Questionnaires?

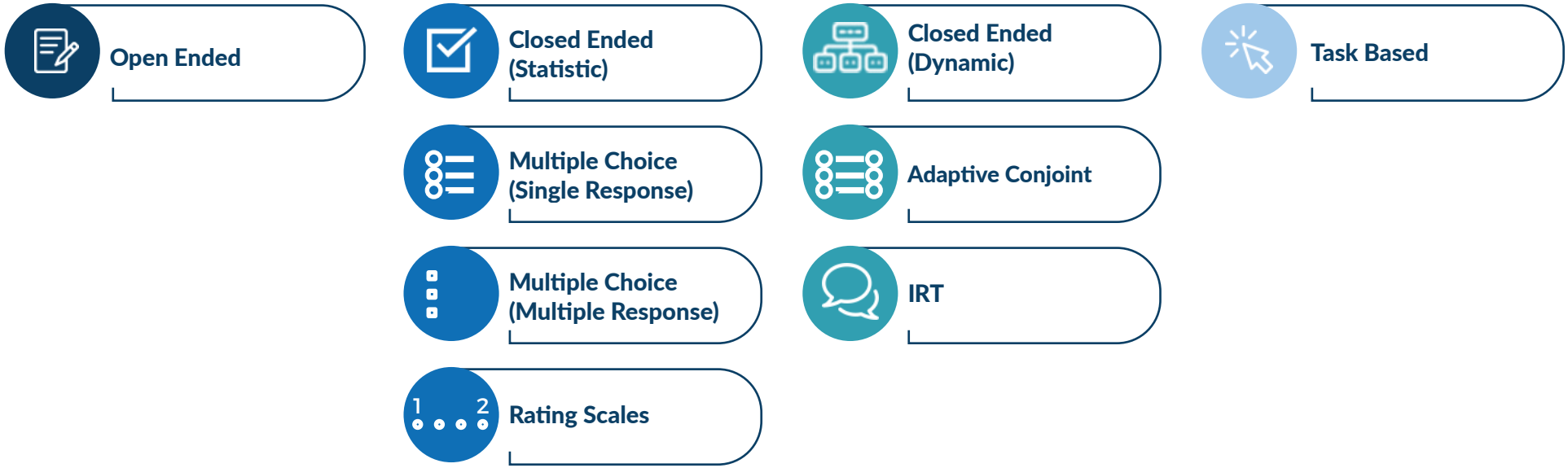
Depending upon the Third-Party Risk Management software you are using, you may or may not have a robust survey capability within that solution. If you have hundreds or thousands of TPSPs, you will need to build effective risk assessment surveys to support your due diligence process. It will be important for your organization to understand how to build effective survey questions.

Survey Questions

In the article Four Classes of Survey Questions, the author mentions that survey questions can be broadly classified into four classes:

1. Open-ended (free responses),
2. Closed-ended (static),
3. Closed-ended (dynamic), and
4. Task-based [iii].

As illustrated below, you can see that closed-ended questions themselves can be classified into different types.



When properly written, closed-ended questions are usually straightforward to the respondents as they typically involve concrete selections.

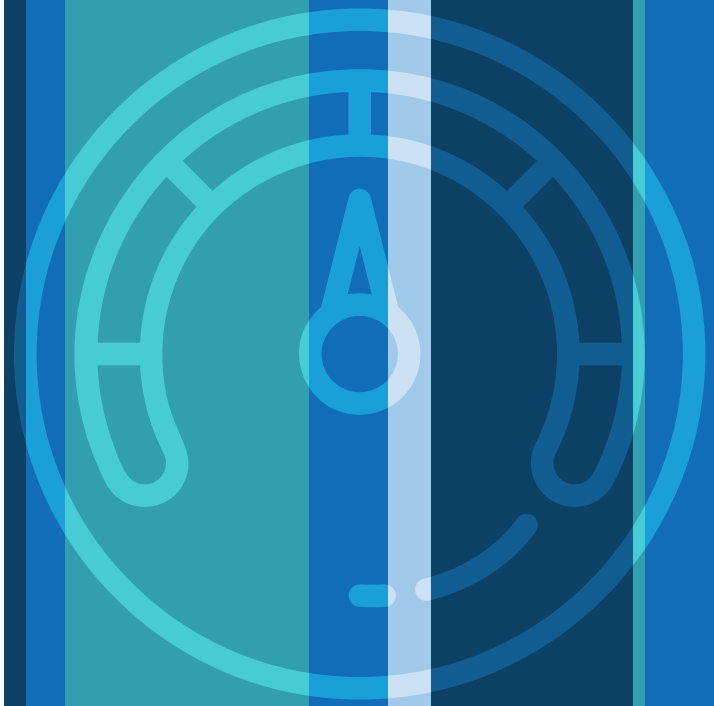
Rating Scales

After selecting your survey question type, you will need to determine which rating scale to utilize. A rating scale is a method designed to elicit information about a quantitative or a qualitative attribute.

Rating scales usually involve asking participants to rate abstract concepts, such as satisfaction, ease, or likelihood to recommend. The proper selection of a rating scale can have a big impact on both responses and interpretation.

Dynamic questions are utilized to build smarter surveys because they enable the response of one question to change the remaining questions that will be presented.

For example, the first question in a survey could be a qualifying question – have you completed the annual bring your own device training? The remaining questions could change based on the response to the first question, and prevent respondents from having to answer unnecessary questions.



There are at least 15 different rating scale options to choose from (e.g., Linear Numeric Scale, Likert Scale, Multiple Rating Matrix, Frequency Scales, Forced Ranking Scale, Paired Comparison Scale, etc.).

The point is there are many rating scales available, and slight variations can result in different looking results, even though they are variations on the same scale.*

However, the goal is to help you understand the importance of conducting your own research and carefully plan the survey question and rating scale method you wish to utilize. Then have an independent quality control review performed before they are utilized. Seek the help of a professional service provider if necessary.

* It is not the intention of this article to discuss all of the variations of the potential survey questions and rating scales; that could take an entire chapter.

Time spent getting quality TPSP risk assessment survey questions developed for your due diligence process should be seen as an investment in your TPSP Risk Management program; not an expense!

AUTHOR

David Vincent
Director of Partnerships, North America,
Corporater
vincent@corporater.com

References:

(i) Friel, Sean. “Third-Party Risk Management: Keeping Your Healthcare Organization’s Information Safe”. Security Magazine. September 2019.

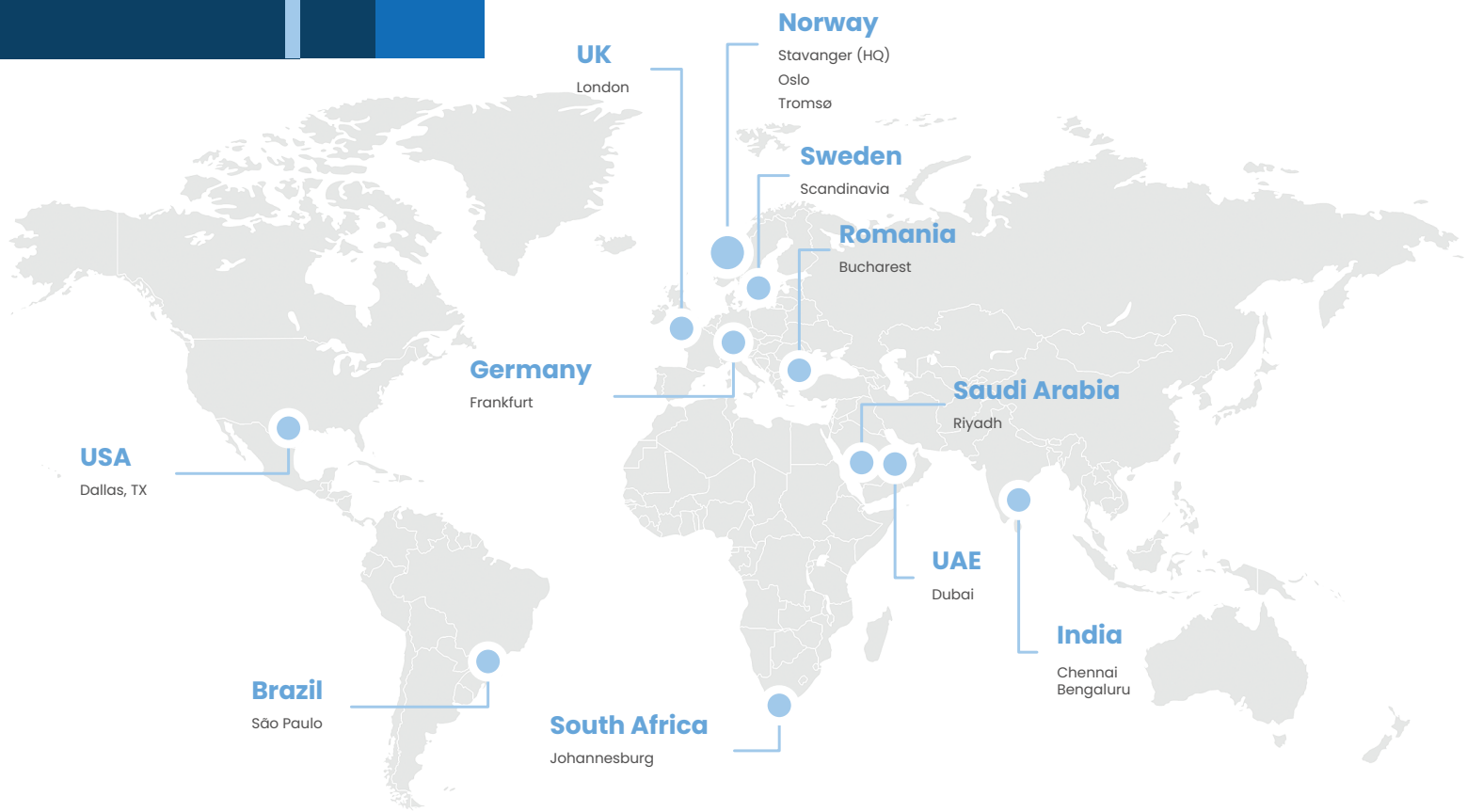
(ii) Thomas, Brian. “A Vendor Risk Management Questionnaire Template”. BitSight, September 2019.

(iii) Sauro, Jeff. “4 Classes of Survey Questions”. MeasuringU, September 2018.

Corporater offers a fully integrated risk management solution to handle all aspects of your organization (e.g., financial, operational, technology, performance, compliance, digital, third-party, etc.), which provides accurate visualizations of your risk exposure within your business context, and enables proactive identification and management of risk events before they negatively impact the success of your organization.

Allow your organization not only to increase the efficiency of your risk management program but realize significant cost savings each year to pay for your investment in the Corporater risk management solution.

Learn More **Request Demo**



CORPORATER

Corporater empowers medium and large organizations to manage Governance, Performance, Risk, and Compliance by providing them with a business management platform that is highly configurable and adaptable to their unique business model. We use our gains to make a social impact.

Contact us for demo at
www.corporater.com/requestdemo
info@corporater.com