**Internal Audit Memorandum**

**Subject: Introduction of Systemic Aggregate Third-Party Data Exposure Risk**

**To: Chief Audit Executive**

**From: Internal Audit**

**Executive Summary**

Our firm is subject to an unrecognized information technology risk that derives from our relationships with the third parties which drive or support a number of our business operations. This systemic risk stems from data breaches occurring or which have yet to occur at our business partners. While it is true that we have processes and controls in place through our Computer Security and Third Party Risk Management teams, they address the risk from an individual partner company standpoint. The problem is not with individual companies, but rather from the aggregate residual risk from these partner firms as a whole. This residual risk is added to by each partner company which holds or has access to sensitive information.

It is possible to determine the likelihood of a significant, reportable data breach across our population of third parties by using a simple equation derived from probability theory which shows that the risk of a third-party data breach is proportional to the number of third parties with access to sensitive data. But beyond this, knowing the value of this likelihood will then allow our company to manage this systemic risk by strategically limiting unnecessary access to sensitive data (i.e., Data Minimization Principle) while still being able to add third parties when appropriate.

**1. Description of the Systemic Risk**

**1.2 Nature of the Risk**

Our organization maintains a large and growing number of third-party relationships that store, process, or transmit sensitive data. Each of these third parties introduces a non-zero probability of breach, even after due diligence and mitigation. When aggregated across all of our third parties, the cumulative probability becomes material and orders of magnitude higher than the risk posed by any single vendor. Analysis of the frequency of data breach sources shows the number third-party breaches relative to internal data breaches[[1]](#footnote-1) is more than two times higher, making this risk likely the biggest data breach risk for our organization. Probability theory allows us to calculate the Expected Value[[2]](#footnote-2) (likelihood) of such a breach as simply the product of the number of third parties that could expose data and the average probability across all third parties[[3]](#footnote-3).

**1.2 Why the Risk Is Systemic**

Third‑party data breach risk is systemic because it arises not from any single vendor, but from the aggregate structure of the entire third‑party ecosystem. Each vendor contributes its own probability of causing a breach, and **probability theory** tells us that the expected loss is the sum of all those independent probabilities. As the number of third parties grows, the cumulative probability grows with it — even if each individual vendor is well‑managed.

**2. Risk Assessment**

**2.1 Likelihood**

Organizations typically fall into one of three conditions:

|  |  |
| --- | --- |
| **Employees** | **Mean Vendors** |
| 50 | 18 |
| 100 | 33 |
| 200 | 49 |
| 400 | 65 |
| 800 | 80 |
| 1,600 | 96 |
| 3,200 | 111 |
| 6,400 | 127 |
| 12,800 | 143 |
| 25,600 | 158 |
| 51,200 | 174 |
| 102,400 | 190 |
| 204,800 | 205 |
| 409,600 | 221 |

Table 1, Average number third parties that could expose data, by company size. Data from VivoSecurity, 2025.

1. The number of third parties holding large volumes of sensitive data is unknown.
2. The number of third parties with access to sensitive data is known, but the volume of data each holds is not.
3. Both the number of third parties and the volume of data they hold are known.

The sections that follow should be tailored to your specific condition. Remove any blue instructional text as you customize the memo.

* **If you are in Situation 1:** Estimate the number of third parties (N) using your organization’s employee count and the reference table provided. Complete Section 1 and remove Sections 2 and 3.
* **If you are in Situation 2:** Set N equal to the total number of third parties that could expose any amount of sensitive data. Complete Section 2 and remove Sections 1 and 3.
* **If you are in Situation 3:** Select a breach size threshold that would constitute a material breach for your organization, and set N to the number of third parties whose data holdings meet or exceed that threshold. For example, if a material breach is defined as affecting 100,000 or more individuals, count the number of third parties capable of exposing data for 100,000+ individuals. Complete Section 3 and remove Sections 1 and 2.

In Sections 1, 2, and 3, complete the calculations and populate the table using the following method:

* **Mean Years Between Breaches** (MYB): Compute MYB as 1 ÷ (N×0.066%), where N is the number of third parties.
* **50% Probability Interval:** Calculate this as MYB ÷ 2.
* **30% Probability Interval:** Calculate this as MYB ÷ 3.

|  |  |  |
| --- | --- | --- |
| Mean years between breaches | 50% chance | 30% chance (one in three) |
| MYB = 1 / (N x 0.066%) | MYB / 2 | MYB / 3 |

**Example:** an organization has 1000 employees and the number of third parties that could expose data is unknown. Using table 1, we estimate that we might have about 84 third parties that could expose our data. We therefore forecast an expected value of 84 × 0.066% = 5.5% and a MYB as 1 ÷ 0.055 = 18 years with a 50% chance in 18 ÷ 2 = 9 years and a 30% chance in 18 ÷ 3 = 6 years.

Section 1

Using probability theory, it is possible to forecast **Expected Value** (likelihood) in real world units, based upon the number of third parties that could expose data. Unfortunately our organization was not able to independently generate a list of third parties that could expose sensitive data, but it is possible to estimate the number of third parties based upon the average number of employees for a company of our size. The average for a company with 1000(replace with your value) employees is 100(replace with your value) third parties. We estimate an Expected Value of 6.6% which equates to a third-party breach every (15 years)(replace with your value)on average, based upon 100(replace with your value) third parties.

| Mean years between breaches | 50% chance | 30% chance (one in three) |
| --- | --- | --- |
| 15(replace with your value) | 7.5(replace with your value) | 5 years(replace with your value) |

Section 2

Using probability theory, it is possible to forecast **Expected Value** (likelihood) in real world units, based upon the number of third parties that could expose data. Our organization does not accurately track the amount of data, so we have calculated Expected Value for a third party breach of any size. I estimate an Expected Value of 6.6% which equates to a third-party breach every (15 years) (replace with your value) on average, based upon 100(replace with your value) third parties that have been identified as having sensitive data that could be exposed in the event of a third-party breach.

|  |  |  |
| --- | --- | --- |
| Mean years between breaches | 50% chance | 30% chance (one in three) |
| 15(replace with your value) | 7.5(replace with your value) | 5 years(replace with your value) |

Section 3

Using probability theory, it is possible to forecast **Expected Value** (likelihood) in real world units, based upon the number of third parties that could expose data. I estimate an Expected Value of 6.6% which equates to a third-party data breach every (15 years)(replace with your value) on average, based upon 100(replace with your value) third parties that have been identified as having sensitive data for 100,000 thousand (replace with your value) or more people and whose information could be exposed in the event of a third-party breach.

|  |  |  |
| --- | --- | --- |
| Mean years between breaches | 50% chance | 30% chance (one in three) |
| 15(replace with your value) | 7.5(replace with your value) | 5 years(replace with your value) |

**2.2 Impact and Significance**

The risk of a third‑party data breach presents multi‑category significance under the IIA framework, affecting Compliance, Financial Reporting, Operations, and Strategic Objectives. The impacts arise not only from a breach event itself but also from misunderstanding the underlying cause of such breaches and from organizational decisions made under that misunderstanding.

**2.2.1 Impact of a Third‑Party Breach**

A reportable third‑party breach can result in substantial direct and indirect costs, including investigation and forensic analysis, customer and regulatory notification, privacy‑liability insurance claims, litigation and regulatory penalties, and reputational damage that may impair customer trust and long‑term strategic positioning. In addition, such a breach would likely materially affect financial reporting through breach‑related expenses, reserves, and disclosures.

**2.2.2 Impact of Misunderstanding the Cause of Breaches**

A significant portion of the risk arises from **misattributing the root cause of third‑party breaches**. Current TPRM practices typically assume that breaches occur because a “weak link” vendor failed due diligence. In reality, probability theory shows that the dominant driver of breach likelihood is the **number of third parties with access to sensitive data**, not the individual strength of any single vendor.

When the systemic nature of the risk is understood, organizations can **intentionally structure data exposure**, ensuring that only a very small number of third parties have access to very large amounts of data, while a large number of third parties may have access to small amounts of sensitive data. Under these conditions, an occasional small breach is **expected**, mathematically predictable, and aligned with management‑approved risk levels. No preventive escalation is required; only routine corrective action is needed.

However, when the cause is misunderstood, organizations may misinterpret this expected small breach as a narrowly avoided catastrophic event. This leads to **ineffective responses**, such as doubling down on vendor‑by‑vendor due diligence, rather than recognizing that the small breach reflects the predictable behavior of a well‑managed system. As a result, resources are diverted away from the controls that actually matter—those that **limit total data exposure**—toward activities that do not meaningfully reduce systemic risk.

**2.2.3 Impact of Limiting Third‑Party Use Due to Misperceived Risk**

Misunderstanding the systemic nature of the risk can also lead to an overly restrictive use of third parties, limiting operational flexibility and strategic innovation. Organizations may avoid beneficial third‑party solutions out of fear of a large‑scale breach, resulting in higher internal costs, slower adoption of modern capabilities, and reduced competitiveness. When the systemic risk is properly understood, organizations can safely expand third‑party usage by limiting shared data, obfuscating or encrypting sensitive information, and consolidating vendors where appropriate. For example, using encrypted platform configurations (such as enhanced versions of major SaaS systems) allows broader third‑party engagement while materially reducing exposure.

**2.3 Current Controls**

A fundamental insight in cybersecurity is that **probability—and therefore risk—increases with the number of opportunities for failure**. This logic underpins both the **Principle of Least Privilege (PoLP)** and the **Data Minimization Principle**, both of which seek to reduce opportunities for high impact events.

However, this same logic has been overlooked when it comes to exposure of sensitive data shared with third parties. All frameworks and most regulators[[4]](#footnote-4) overlook the **aggregate risk** created by the *number* of external entities holding sensitive data. Even the IIA’s **Third‑Party Topical Requirement (2025)** does not address this systemic exposure.

As a result, existing TPRM programs concentrate on controls such as:

* vendor due diligence
* SOC 2 reviews
* security questionnaires
* contractual requirements

While important, these controls do **not** address the **aggregate risk** created by the sheer number of third parties with access to sensitive data.

**3. Gap Analysis**

Probability theory shows that the likelihood of a third‑party data breach can be forecast solely from the **number of third parties capable of exposing sensitive data[[5]](#footnote-5)**. Accordingly, managing third‑party breach risk becomes a function of **controlling the number of external entities** relative to the **amount of data each could expose**.

Current TPRM practices do not include controls designed to manage this aggregate, probability‑driven exposure. To address this gap, our organization should consider:

* an executive‑level committee to establish probability thresholds based on breach magnitude (measured by number of individuals affected)
* processes to govern the allowable number of third parties as a function of potential breach size, to remain within these thresholds.

**4. Recommendation**

We recommend that the Chief Audit Executive:

* Read and understand *Mathematical Basis of Third-Party Data Breach Risk*, Pages 22 through 28, in *How to Calculate Probability of a Third-Party Data Breach*, Lee and Smith Sept 19, 2025
* Devise and execute a plan for Internal Audit to forecast and report this risk independent of the first or second line
* Communicate this emerging risk to executive management and the Audit Committee
* Consider adding an audit or advisory engagement focused on:
  + Quantifying cumulative breach probability
  + Identifying data concentration across third parties
  + Assessing governance ownership for systemic third-party risk
* Request that management develop a risk metric and assign ownership for aggregate exposure

**5. Conclusion**

The number of third parties with access to sensitive data creates a systemic, mathematically compounding risk that is not currently recognized or owned within the organization. In accordance with IIA Standards and the Internal Audit Charter, we recommend that you Internal formally elevate this risk for consideration by company management and the Board of Directors / Audit Committee.

The original draft of this memorandum was written by Tim Smith. Tim retired after 20 years with KPMG US and KPMG International, where he specialized in data and analytics for IT and financial audit. In the last part of his career, he focused on the design, testing, implementation, documentation and training for the data analytics modules of KPMG’s proprietary audit software, CLARA. He previously led the IT audit practice in the KPMG San Diego office, providing IT audit, Sarbanes-Oxley compliance assistance, computer-assisted audit to clients in multiple industries. He also spent four years as IT Audit Manager at LPL Financial, the nation’s largest independent Broker-Dealer, leading a team of IT auditors, managing work on a variety of IT, financial and regulatory compliance audits and special projects. Tim is a CPA (California) and a Certified Information Systems Auditor. He is a member of AICPA, California Society of CPAs, ISACA San Diego and IIA. Tim is a coauthor on the white paper: Thomas Lee and Timothy Smith (2025). *How to Calculate the Probability of a Third-Party Data Breach*. Tim can be reached at Tim@CPA4it.com.

1. Data was compiled by Patricia Drooff from <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>, posted by the U.S. Department of Health and Human Services Office for Civil Rights as required by section 13402(e)(4) of the HITECH Act [↑](#footnote-ref-1)
2. See How to Calculate Probability of a Third-Party Data Breach, Lee and Smith Sept 19, 2025, Page 23 & 26. [↑](#footnote-ref-2)
3. See How to Calculate Probability of a Third-Party Data Breach, Lee and Smith Sept 19, 2025, Page 28, Figure 3 [↑](#footnote-ref-3)
4. The Canadian Government’s OSFI, however, explicitly requires financial institutions to manage the aggregate risk arising from their third‑party relationships, as set out in Guideline B‑10: Third‑Party Risk Management (2023). [↑](#footnote-ref-4)
5. See How to Calculate Probability of a Third-Party Data Breach, Lee and Smith Sept 19, 2025, Page 24 [↑](#footnote-ref-5)