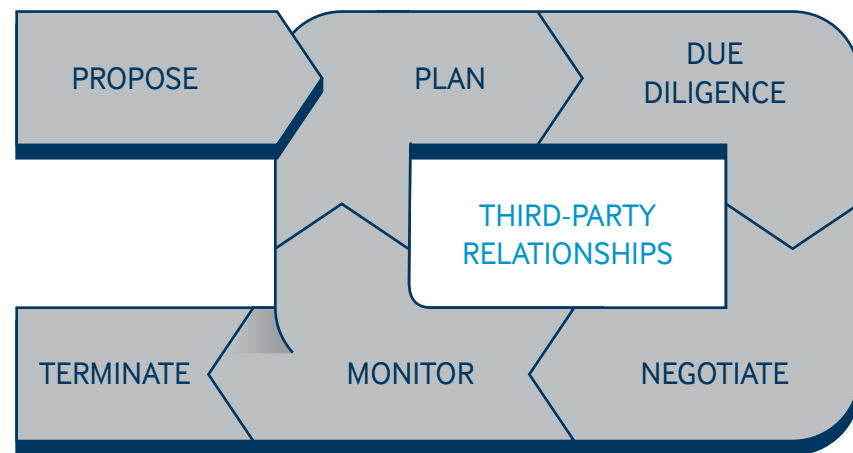
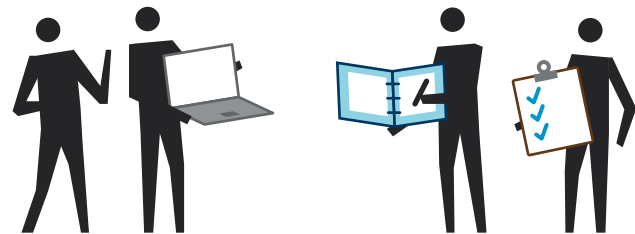


5 Tips to Reduce the Likelihood of a Third-Party Data Breach

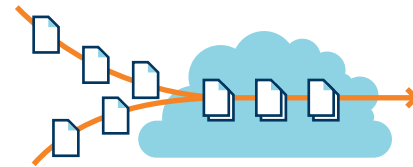
1 MANAGE ALL THIRD PARTIES BASED ON THEIR RISK



Create an inventory of all third parties, identify which ones have access to sensitive information and manage them in accordance with the risks they pose.

PONEMON STUDY: REDUCE RISK 19%

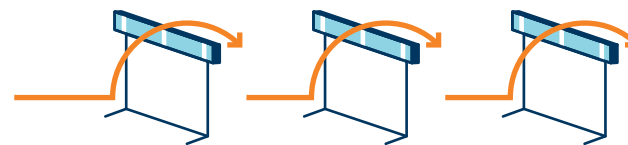
2 CENTRALIZE DOCUMENTATION AND WORKFLOWS



Use a SaaS solution to centralize third-party documentation and workflows and facilitate visibility into, and evaluation of, the security practices of all third parties.

PONEMON STUDY: REDUCE RISK 15–20%

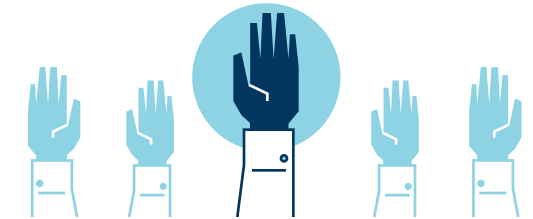
4 CREATE STANDARDS FOR SUCCESS



Standards save money and drive efficiency. Collaborate across job functions. Form a third-party risk management committee to regularly review and update standard risk management processes and controls.

PONEMON STUDY: REDUCE RISK 15%

3 DESIGNATE OWNERSHIP



Assign accountability for your company's third-party risk management program from the board of directors and senior leadership to the third party relationship manager.

PONEMON STUDY: REDUCE RISK 10–14%

5 MONITOR RISKS CONTINUOUSLY



Review and update vendor management policies regularly as well as conduct audits and assessments to ensure the security and privacy practices of third parties address new and emerging threats.

PONEMON STUDY: REDUCE RISK 18%

Trends from the Ponemon 2017 Third Party Data Risk Study you can't afford to ignore



Third-party data breaches are on the rise



Companies lack visibility into security practices of third parties, but continue to share data



The effectiveness of third-party governance programs is decreasing



Companies are beginning to take third-party data risk seriously



Third-party data risk is now a Board-level concern



Proper governance of third party data security decreases likelihood of a data breach



Read The Full Report

www.opus.com/ponemon