ProcessUnity

THE STEPS TO A MODERN APPROACH TO THIRD-PARTY RISK ASSESSMENTS

WHAT IS INHERENT RISK?

Inherent Risk is the natural level of risk a vendor or supplier poses to an organization throughout the relationship lifecycle.

THE STARTING POINT: WHAT ARE ORGANIZATIONS FACING TODAY?

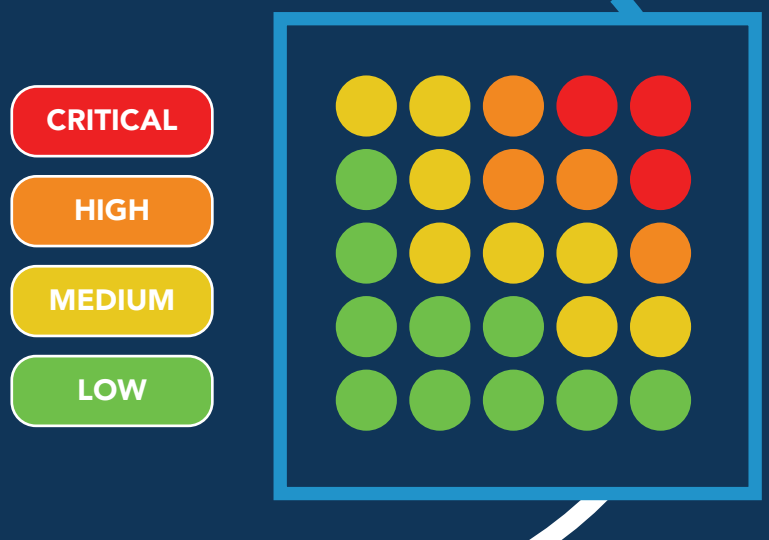
Organizations rely on hundreds, even thousands of vendors to efficiently perform many day-to-day operations. But it doesn't come without risk; Most security breaches today—54%, according to VentureBeat —occur through third-party relationships.*

1

STEP 1:

CLASSIFY YOUR VENDORS BASED ON INHERENT RISK

Whether you have a few hundred, or tens of thousands of third parties, categorizing them into tiers based on criticality-- think low-risk, medium-risk, or high-risk vendors-- will help focus resources on third-parties that pose the most significant threat to business operations if targeted.



2

STEP 2:

SCOPE AND SCHEDULE YOUR ASSESSMENTS

Now that you have a tiered and prioritized vendor population, you can efficiently determine the scope and frequency of post-contract due diligence assessments. As a general rule, more critical, higher-tired vendors should be assessed more frequently with a deeper scope of evaluation.

STEP 3:

IMPORT PREVIOUSLY COMPLETED ASSESSMENTS HELD WITHIN AN EXCHANGE

Typically, 25-40% of your vendors already have a completed assessment hosted on an exchange, and when utilized can introduce a significant cost savings for your organization. An exchange also allows you to efficiently and accurately assess third parties that normally are hard to evaluate (due to size or maturity level).

3

4

STEP 4:

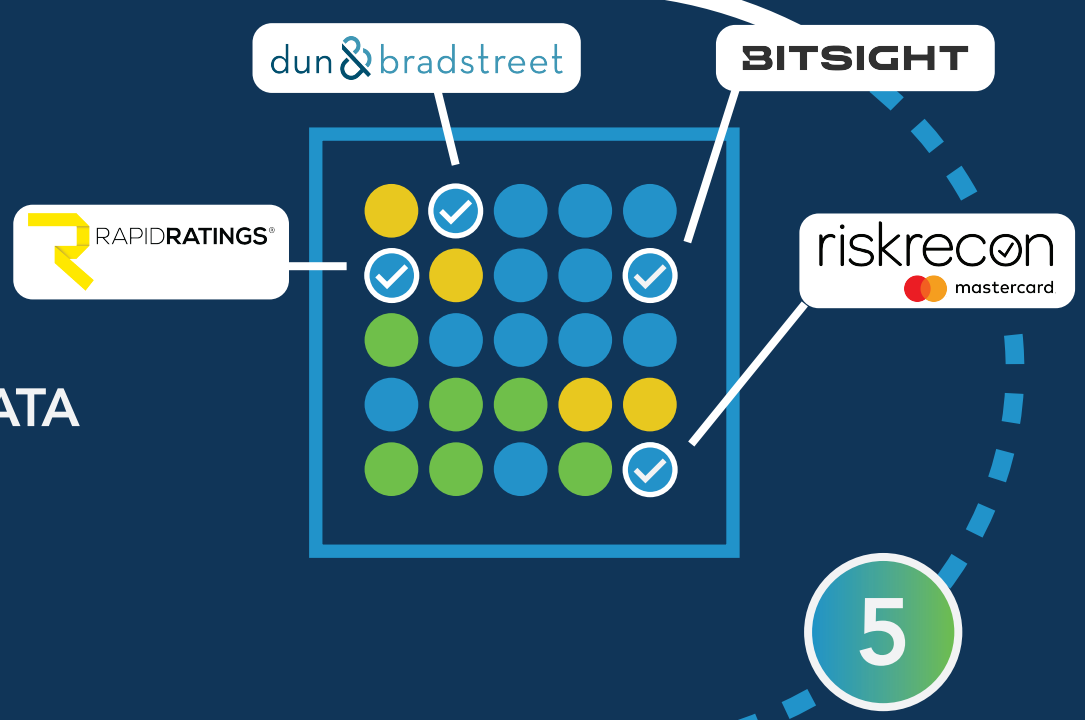
COMPLETE REMAINING ASSESSMENTS VIA YOUR ASSESSMENT ENGINE

For vendors without assessments hosted in your exchange, your TPRM team must conduct the assessment process within an online vendor portal, allowing direct collaboration with each third-party, as well as full data collection and management in one central location.

STEP 5:

CONFIRM YOUR RESPONSES WITH EXTERNAL EXPERT DATA

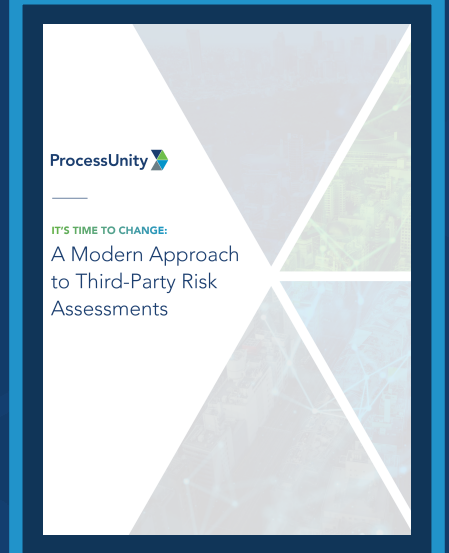
Utilize external (and unbiased) vendor intelligence providers like Risk Recon, Bitsight, Dun & Bradstreet, and RapidRatings to confirm the data you receive from your third parties.



5

DISCOVER STEPS 6-10

Steps 1-5 are only half the battle - Download our full white paper for a complete guide to modernizing your third-party risk management process, and discover the remaining steps to reach a resilient, data-driven, and proactive third-party risk management process with the ProcessUnity Third-Party Risk Management platform.



ProcessUnity is the Third-Party Risk Management (TPRM) company. Our software platforms and data services protect customers from cybersecurity threats, breaches, and outages that originate from their ever-growing ecosystem of business partners. By combining the world's largest third-party risk data exchange, the leading TPRM workflow platform, and powerful artificial intelligence, ProcessUnity extends third-party risk, procurement, and cybersecurity teams so they can cover their entire vendor portfolio. With ProcessUnity, organizations of all sizes reduce assessment work while improving quality, securing intellectual property and customer data so business operations continue to operate uninterrupted.

To learn more or request a demo, visit www.processunity.com.

SOURCES

*https://venturebeat.com/security/report-54-of-organizations-breached-through-3rd-parties-in-last-12-months/