ProcessUnity

GLOBAL CUSTOMER SUCCESS

THE GLOBAL RISK EXCHANGE ASSESSMENT

Assess & Validate Your Third Parties

Developing a data protection strategy is essential to ensure data confidentiality, integrity, and availability for your business and your third parties. The Global Risk Exchange is the world's largest library of automated, attested, and validated third-party risk data, with an advanced analytical methodology that provides complete coverage on your entire vendor portfolio. With a standardized, controls-based questionnaire, the Exchange takes a data-first approach to Third-Party Risk Management – so you can focus on mitigating your most critical risks.

Assess & Validate Your Third Parties

- An enterprise-level assessment that produces standardized and structured data for analysis and benchmarking
- Inside-out, attested vendor data combined with outside-in, externally validated insights for a complete risk picture
- Maps to most customer controls as well as industry standards and frameworks (NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc.)
- Incorporates easy-to-use workflow tools allowing you to action risk findings from your assessment data

What Exchange Data Do I Need?

In Third-Party Risk Management (TPRM), it's difficult to get just the right amount of data. Either you get inundated with irrelevant data or you don't get enough information; in either case, you spend more time than you can afford trying to assess risk. The Exchange allows you to request different levels of Exchange data and evaluate it through whichever framework or lens is most appropriate for your context, allowing you to focus in on only the most important data for your evaluation of a third party.

Automated Risk Profiles

What is it?

Get insight into inherent risk, residual risk, and firmographic data on more than 360,000 third parties. Automated Risk Profiles give you at-a-glance information to aid in prioritizing your third parties for mitigation planning without the time investment of reviewing an attested risk assessment. Automated Risk Profiles allow for continuous monitoring of your third parties throughout the year without needing to trigger a reassessment.

What's included

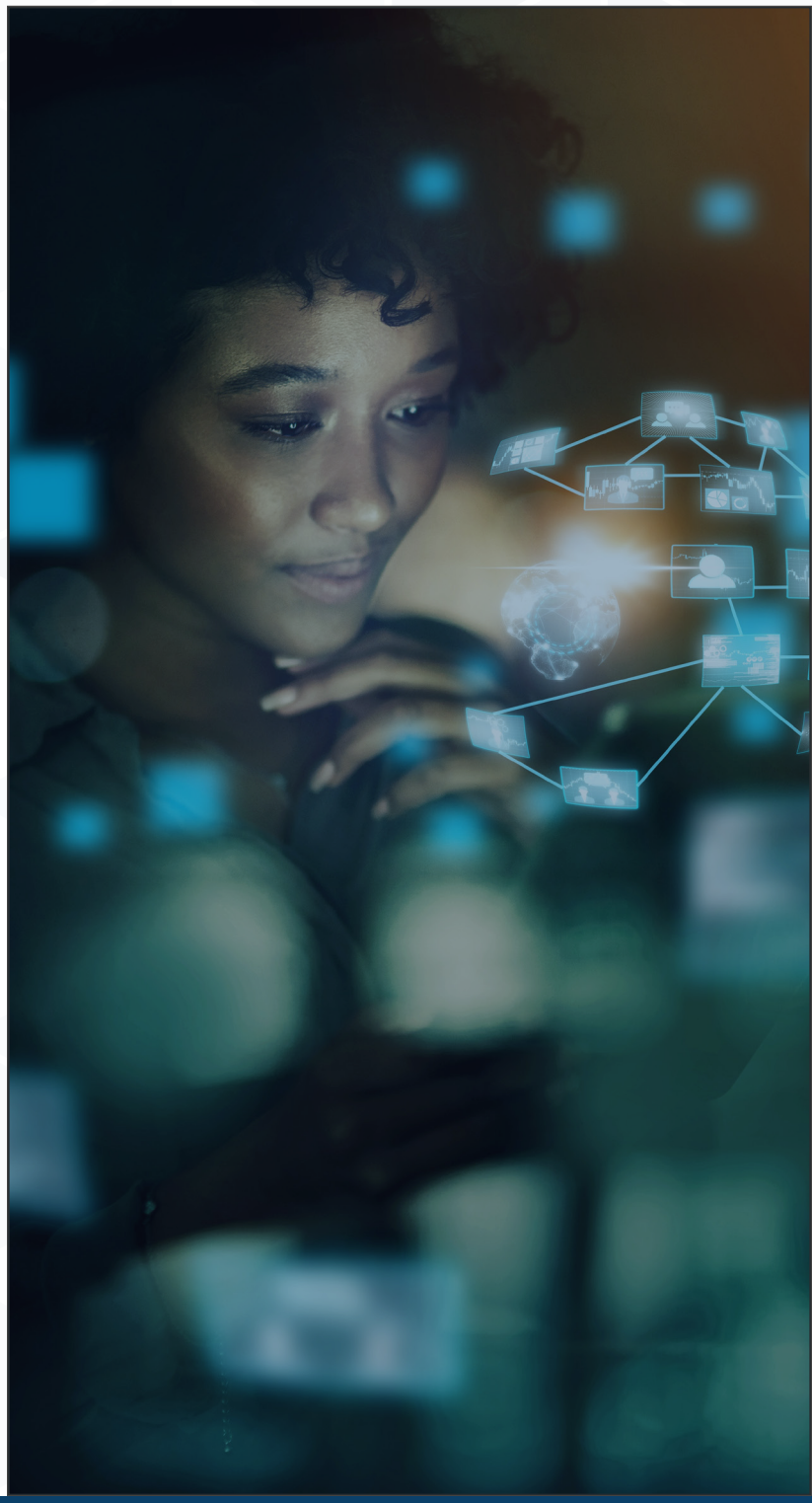
Automated inherent risk, Residual risk, Firmographic data, External scanning and threat intelligence data

When to use it

Access Automated Risk Profiles for 100% coverage of your third-party portfolio. Understand risk levels across your portfolio to prioritize the scope and frequency of due diligence for each third party.

Pre-contract: Quickly prioritize the scope of pre-contract due diligence for each third party and set them up with the appropriate ongoing monitoring cadence.

Post-contract: Continuously monitor changes in the third party's risk posture in between assessment cycles to trigger reassessment as necessary.



Attested Risk Assessments

What is it?

Order a completed risk assessment from our library of more than 18,000 third parties. The controls-based questionnaire includes 60 critical controls and 209 -controls mapped to common industry standards such as NIST and ISO.

What's included

209 Controls Questions

When to use it

Pre contract: After prioritizing due diligence scope with Auto-Inherent Risk Scores, order an attested assessment on your Critical and High Risk third parties.

Post contract: Order an attested assessment to re-assess your third parties for annual due diligence or on your preferred ongoing monitoring cadence.

Control Metrics

What is it?

Control Effectiveness Metrics provide data points on the strength, coverage, and timeliness of each control as your third parties have implemented it.

What's included

627 Metrics Questions (Control Effectiveness) plus vendor-submitted evidence documents (3 questions on the strength, coverage, and timeliness of each control)

When to use it

Order metrics on your most critical third parties that do not have effective controls in place or a satisfactory risk posture.

Validated Assessments

What is it?

Order an independent review of the 60 critical controls included in a third party's attested risk assessment.

What's included

Validation of the 60 critical controls included in a third party's attested assessment, performed by ProcessUnity's strategic audit partners.

When to use it

Pre and post contract: Order validation on any third-party assessment that requires closer scrutiny, ie, your most critical third parties.

Document Access

What is it?

Cross-validate third party responses to the questionnaire against their submitted evidence documents. Review a third party's documents, policies, and other evidence to substantiate that the implementation of third-party controls.

What's included

28 day access to a third party's submitted documents, policies, and other evidence documents.

When to use it

Request access to the documents when you need to review a vendor's policies for assurance of their control posture.

What's Included in the Exchange Questionnaire?

Exchange assessments apply a dynamic and comprehensive approach to risk assessment analysis, replacing outdated static spreadsheets and repetitive assessment requests. Our assessments integrate vendor responses with advanced analytics, threat intelligence, and sophisticated risk models, to provide an in-depth view of how a vendor's security controls will protect against potential threats.

The standardized Exchange questionnaire is designed to easily map to your requirements. The assessments include controls and sub-controls based on the following frameworks: FFIEC, ISO 27001, NIST 800-53, NIST 800- 171, NY-DFS, PCI DSS, and SOC. Since the assessment data lives on the Exchange, third parties only need to complete it once. Customers can request that the third party respond to a specific portion of the questionnaire, allowing the customer to hone in on the most necessary data points and reducing the burden on their third parties. Additionally, third parties can proactively update their information throughout the year when their security policies change.

Included Questions:

- 209 Control Questions
- 60 Critical Controls (Included in the 209 Control Questions)
- 627 Metrics Questions

Included standards:

- FFIEC
- ISO 27001
- NIST 800-53
- NIST 800-171
- NY-DFS
- PCI DSS
- DORA

Included standards:

- Threat Management
- Network Security
- Data Protection and Privacy
- Physical and Environmental Security
- Vulnerability Management
- Human Resource Security
- Incident Response and Business Continuity
- Endpoint and Device Security
- Identity and Access Management
- Application Security

How Are Global Risk Exchange Assessments Different?

The Global Risk Exchange

- An online community that facilitates data sharing, analysis, and risk prioritization
- Gain immediate visibility into inconsistencies and contradictions within a third-party assessment that highlight potential security gaps
- An inside out, independently validated view of your security posture
- Dynamic, cloud-based assessments that you can update anytime
- An assessment that adjusts to your responses and removes irrelevant questions
- Enterprise level assessment that can be shared with business departments responsible for risk

Traditional Approaches

- One-off, redundant requests that require a complete reassessment every year
- Inaccurate outside-in rating on your security posture
- Static spreadsheets that live on a desktop
- Multiple irrelevant and redundant questions
- Product level assessment tailored to only one customer
- Static spreadsheets that only capture what you add

The Exchange Assessment Workflow

ONBOARD

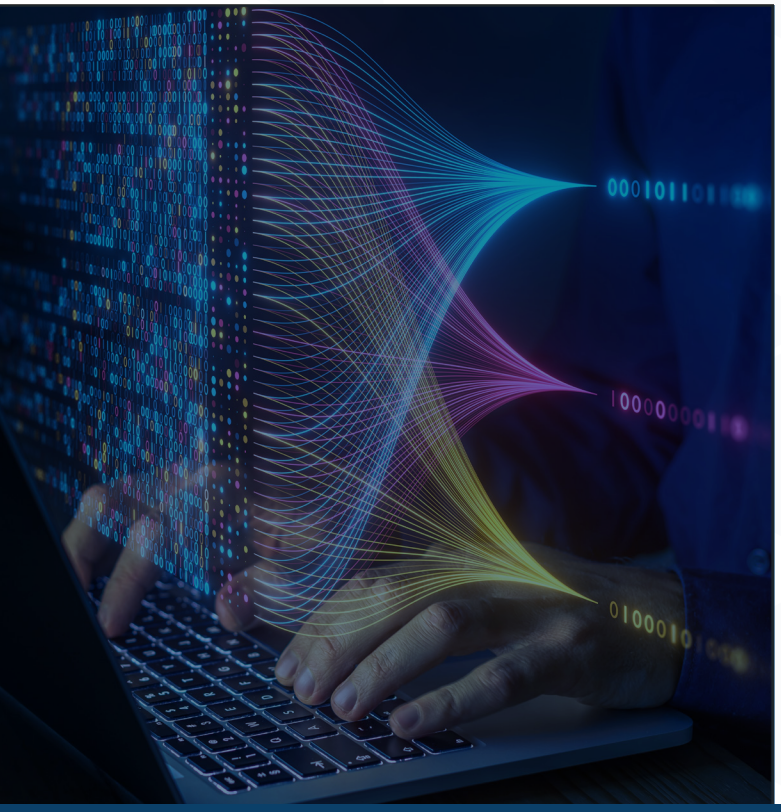
Customer adds their third parties to the Exchange platform.

If the third party already has an existing assessment on the Exchange, the third party will be prompted to authorize access. Otherwise, ProcessUnity onboards the third party to the Exchange.

PRIORITIZE

Customer receives immediate Auto Inherent Risk Scores on potential risk and business exposure specific to your relationship with the third party.

Customer requests data relevant to their relationship with each third party. They may request an attested risk assessment or automated risk profile depending on the depth of data they require.



ASSESS

Once the third party grants access, the customer receives the third party's attested assessment.

The customer immediately receives Automated Risk Profiles for all requested third parties, then determines third parties that require a full assessment based on unacceptable inherent risk levels.

If the third party does not have an attested assessment, they will be invited to complete the Exchange questionnaire.

ANALYZE

Customer reviews assessment findings in a streamlined report and identifies controls that fall outside of acceptable risk levels

RESOLVE

Customer identifies any issues within the findings report that require resolution.

Customer creates issues from non-preferred responses and collaborates with the third party on resolution.

REPORT

Customer leverages pre-built reporting to visualize third-party risk on the individual relationship level and the portfolio level..

Get Started with ProcessUnity Global Risk Exchange

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.

ProcessUnity

See how at www.processunity.com.