



Onboarding Guide for Third- Party Members



Table of Contents

Introduction	2
Why Is The ProcessUnity GRX Assessment Best In Class?	3
GRX Assessment Methodology	3
Why Join The Exchange?	4
How Do Customers Gain Access To An Assessment?	5
Obtaining Assistance During The Assessment Process	5
Quick Start: New Assessment	6
Quick Start: Assessment Refresh	7
Sharing Your Assessment To Reduce Due Diligence	8
The ProcessUnity Platform	9



Introduction

The ProcessUnity GRX is an exchange platform for Third-Party Cybersecurity Risk Management that allows both Third-Parties and Customers to more efficiently and effectively manage the risk associated with their Third-Party ecosystem.

We are the the recipient of several awards, including:

[2023 Cybersecurity World Awards](#)

[2023 Cybersecurity Excellence Awards](#)

[2023 Cyber Defence Magazine Global Infosec Awards](#)

[2022 Frost & Sullivan Market Leadership](#)

These awards recognize the GRX's commitment to delivering best-in-class risk management capabilities and fostering a community for like-minded professionals to collaborate and reduce shared risk.

Why Is The ProcessUnity GRX Assessment Best In Class?

The ProcessUnity GRX Assessment is based on the NIST 800-53 standard. The assessment content [maps back to multiple industry standards](#), such as ISO 27002, and industry-specific regulations, such as PCI.

Because of the GRX Assessment's depth, it can be mapped very closely to any internally developed assessment and thus allows Third-Parties and Customers alike to gain quicker access to insights into a Third-Party's enterprise security program, resulting in more confidence in its accuracy and independence.

Third-Parties will answer and provide evidence for anywhere between 430 to 1090 security questions – and, when relevant, we will validate and report on the assessment.

Once an assessment becomes available, Third-Parties can grant Customers access to their most up-to-date risk assessment so they can measure the Third-Party's enterprise security program's overall maturity and effectiveness.

Customers leverage GRX to obtain more information about their Third-Party's information security programs. A partnership with the ProcessUnity GRX allows Customers to access Third-Party security data faster, easier, and from a trusted source.

GRX Assessment Methodology

The GRX's cloud-based assessments feature five control groups (Strategic, Operations, Core, Management, and Privacy) that include controls and sub-controls to help measure both maturity (how advanced an organization is performing across process, people, and technology as it relates to cyber risk controls) and control effectiveness (how well the organization implements their controls in terms of strength, coverage, and timeliness) by the GRX's integrated cyber security controls framework.

Additionally, the GRX methodology identifies inherent and residual risks to provide a holistic view of a Third-Party's cyber risk posture.

LEARN MORE: [Assessment Methodology](#)



71% of Due Diligence Requests Can Be Satisfied in Minutes, Not Months.



Why Join The Exchange?

One-To-Many Convenience

Complete one security profile (assessment + desired artifacts) and share it for free to unlimited Customers or Prospects on and off the Exchange to satisfy due diligence requests. Free up your team to focus on matters more important to you instead of responding to bespoke assessment requests.

Control Your Data & Reputation

All attested assessment data requests require an authorization release from you first. Take control of how your organization is represented to the biggest brands in the world's largest global exchange.

Provide Your Entire "Trust Package"

We allow you to store and share artifacts in addition to your assessment (certifications, policies, etc.) that make up your complete "trust package", helping increase your share acceptance rate.

Active Third-Party Members can apply for a complimentary landing page. A landing page allows anyone to request access to your GRX Assessment and profile that you can link to from a web page like [AWS](#) and [Google](#) have, or even from a default email your team sends.

Flex To Many Standards

The ProcessUnity GRX Assessment has been mapped to 30+ different shared framework standards such as NIST 800-53, NIST Cybersecurity Framework (CSF), ISO 27001, PCI DSS, HIPAA, and more. By mapping responses to frameworks you can satisfy more requests with just one assessment.

Benchmark Against Your Industry

Compare your program maturity to companies in your industry across 13 MITRE tactics to gain insights on areas you excel, or where you lack measures, to systematically begin improving your risk posture.

Prepare & Respond To Major Threats

Leverage the MITRE ATT&CK® framework and taxonomy to uncover possible gaps against today's biggest threats. Utilize the sharing functionality to efficiently communicate your status to Customers and Prospects at scale after the next attack (e.g. Log4J) hits the news.

How Do Customers Gain Access To An Assessment?

Customers who are already partnered with the GRX to facilitate their Third-Party risk program can simply [submit their request](#) via the GRX platform. That request will then appear on the Third-Party's authorization tab for the Third-Party to approve the release of their report.

If the request is coming from a Customer who is not partnered with the GRX, the Third-Party can go into the GRX platform and use the [proactive share dashboard](#) to send a share invitation to their Customer. The Customer will receive the invite to log in and accept the Third-Party's report share.

Obtaining Assistance During The Assessment Process

The GRX supports their Third-Parties by offering an [Onboarding Webinar](#) to introduce the assessment process and [Out-brief Webinar](#) to walk through the results. On average, Third Parties that attend complete the assessment in HALF the time and are twice as likely to get value from additional offerings. Additionally, each Third-Party is assigned an Assessment Coordinator to help them through the process once they begin their assessment.

If it is outside of business hours and the Third-Party needs assistance immediately, the GRX offers a [knowledge base site](#) with a plethora of helpful "how to" and informational articles to guide the Third-Party through the assessment.

LEARN MORE: [GRX Knowledge Base](#)

Making Life Easier For Third-Parties



"[ProcessUnity's Global Risk Exchange] platform provides an effective and flexible solution for helping organizations meet their due diligence, risk management, and regulatory compliance needs."

Rani Urbas - Global Head of Enterprise Trust



"Having a third-party, award-winning, and credentialed assessment of our security posture drastically reduces the noise from uncredentialed opinions of our security posture by scoring agencies in the marketplace. [ProcessUnity's Global Risk Exchange] is best in class at being this third-party for us."

Jacob Luna - Director, Client Security Advocacy

Quick Start: New Assessment

1. Register For The Assessment Using The Link

If this is your first time on the GRX, you will receive a link to claim your company. Please complete this step before registering.

A registration link will be sent via email. The link expires after 48 hours. Subsequent logins can be made with your established credentials at <https://portal.cybergrx.com>.

2. Accept The Terms And Conditions

Upon logging in to the portal for the first time, you will be met with our Terms and Conditions in a click-through format. The agreement includes confidentiality and non-disclosure provisions that protect your data within the framework of our exchange model vs a one-to-one relationship.

3. Attend Third-Party Onboarding

[Register for a live onboarding session](#) to learn more about the assessment process and free benefits available to Third-Parties who join our Exchange.

4. Answer The Questionnaire

You must complete your GRX Assessment at the enterprise level - it cannot be scoped to the requesting Customer or any individual business unit, product line, system or division.

5. Submit The Assessment

Submit through the 'Review and Submit' button at the bottom of the page.

6. Submit Relevant Evidence

If completing a [validated assessment](#), upload artifacts directly to our secure portal (**video conference also an option**) where our team will review and verify them. Validated controls are shown on the Validation tab of your Assessment Dashboard.

7. Review The Report

Once your assessment has been fully attested and validated (if relevant), you may access the findings via the Assessment Dashboard within the platform.

8. Share your results with your Customer

As a Third-Party, you have sole ownership over your assessment data. Click on Authorizations at the top of the portal to either Approve or Deny your Customer access for free.

9. Share your results with other Customers

Use the 'Share Assessment' section of the portal for free to [share your assessment results with other Customers](#) outside the Exchange who may be requesting risk assessment information from you.

10. Update your assessment

Be sure to update your assessment as your environment changes. We will be in touch annually to coordinate an update for your Customers.

LEARN MORE: [Watch Our "Getting Started" Video](#)

Quick Start: Assessment Refresh

1. Respond To The Refresh Notice To Reopen Your Assessment For Updates

At 11 months post-completion of the Assessment, we will send a Refresh kickoff email requesting participation in the annual assessment refresh process. Respond to the email to have your assessment opened for updates. Logins can be made with your established credentials at <https://portal.cybergix.com>.

2. Add New Users

If you need to add additional members of your team to help update your assessment, you can [Add and Manage Users](#) by clicking on your initials in the top right corner and navigating to 'manage your company's user accounts' in the drop-down menu.

3. Finding Unanswered and New Questions

The new questionnaire will be uploaded with your previous answers and opened for you to make the necessary revisions. The sections in the questionnaire showing 'continue' indicate there are unanswered questions in the section. You can also click into the 'review and submit' at the bottom of the assessment page to [sort out unanswered questions in the answer breakdown](#).

Remember as you update your annual refresh to complete it at the enterprise level - it cannot be scoped to the requesting Customer or any individual business unit, product line, system or division.

4. Re-Submitting The Assessment

Attest your answers by clicking '[Review and Submit](#)' at the bottom of the Assessment page and clicking the blue 'submit assessment' on the following page. If this button is grayed out, then there is still an unanswered question.

5. Submit Relevant Evidence

If completing a [validated assessment](#), upload artifacts directly to our secure portal where our team will review and verify them.

6. Review The Report

Once your assessment has been fully attested and validated (if applicable), you may access findings, analysis, and the framework mapper via the Risk Navigator under the Risk Profile tab. You can access this by clicking on your initials in the top right corner and navigating to 'manage my company profile' in the drop-down menu. via the Risk Navigator in the Risk Profile tab.

7. Refresh Results Are Automatically Available To Authorized Customers

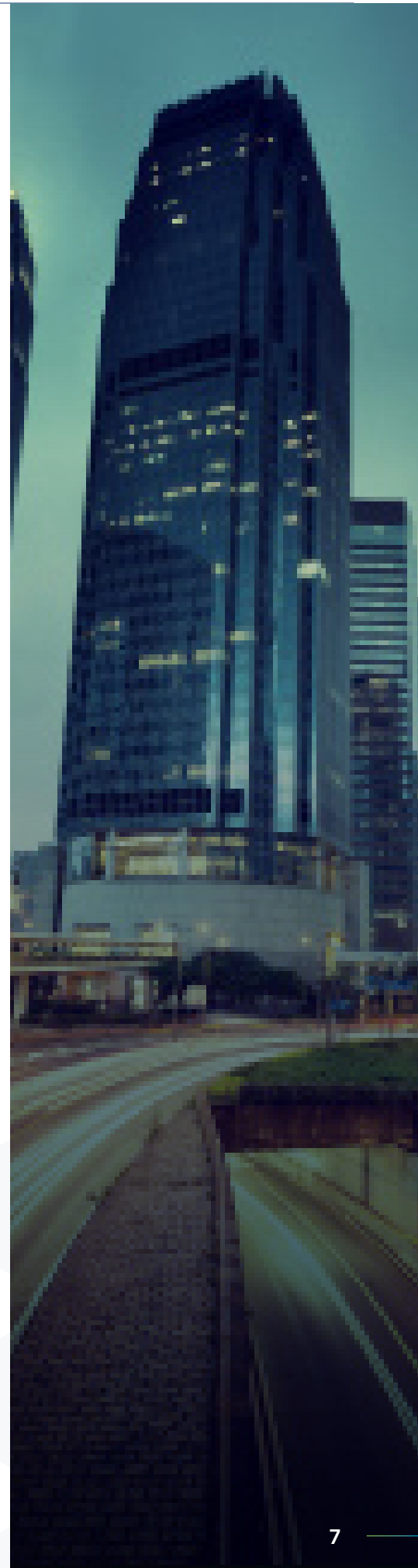
As a Third-Party, you have sole ownership over your assessment data. Once the new report is ready, it automatically becomes available to Customers who are subscribed and who you have given prior authorization. You can approve new and existing authorization requests by clicking on Authorizations at the top of the portal.

8. Share Your Results With Other Customers

Use the 'Share Assessment' section of the portal to [share your assessment results with other Customers](#) outside the Exchange who may be requesting risk assessment information from you.

9. Keep Your Assessment Updated

Be sure to update your assessment as your environment changes. You can update your questionnaire before your annual update. However, we will be in touch again in 11 months to coordinate an update for your Customers.



Sharing Your Assessment To Reduce Due Diligence

Third-Parties (those receiving requests) are seeing huge increases in due diligence-related asks from a quick question to a 1,000+ question assessment from their Partners and Prospects.

With the lack of industry standardization around especially framework formats, requests are often redundant leading to wasted time answering the same question worded different ways to satisfy the request.

As the world continues to see breach after breach, there is an intensifying pressure to protect our shared ecosystems. Because of these pressures, security is becoming a key part of the procurement process where the security team now has an even bigger role to play on the revenue side of the business.

Sharing a default assessment and/or artifacts (certifications, policies, etc.) to satisfy multiple due diligence requests can significantly alleviate these pain points. Sharing reduces sales cycle time improves the satisfaction of your teams by removing redundant work, and reduce sales cycle time.

The Benefits of Sharing Your Assessment

- Organizations may share with Customers or Prospects within the ProcessUnity Global Risk Exchange AND outside of the Exchange **at no cost to either party**. We do not charge for this functionality because it simply helps grow the Exchange.
- The current average acceptance rate of a GRX Assessment share is 71%. Meaning, you can **remove all but a third of your requests in MINUTES not months**.
- ProcessUnity's GRX Assessment takes a structured, standardized approach to our assessment. As a benefit to that, we are able to provide a tool called [Risk Navigator](#) that allows both parties (the sharer and the share recipient) to view the GRX Assessment in the framework of their choosing. **We offer 30+ industry frameworks** to view within such as NIST 800/CSF, HIPAA, GDPR, and more.
- We offer the **ability to upload and share complementary policies, certifications, etc.** in addition to your GRX Assessment should you choose to.
- Additionally, the ProcessUnity **GRX Assessment questions are mapped to the MITRE ATT&CK framework and taxonomy**. This enables Customers to discover the controls that can mitigate the threats applicable for their industry, and the supporting controls that indirectly affect the efficacy of the attack techniques.
- We have found Third-Parties are increasingly eager to provide an efficient, quality experience to Customer and Prospects to self-serve what they need from their Trust Package. Active Third-Party Members can apply for a complimentary landing page. A landing page allows anyone to request access to your GRX Assessment and profile that you can link to from a web page like [AWS](#) and [Google](#) have, or even from a default email your team sends.
- If you care to join one of our weekly webinars on how to leverage your GRX profile and assessment and/or schedule a call with our team directly, [register here](#).

LEARN MORE: [How To Share Your Assessment](#)

The ProcessUnity Platform

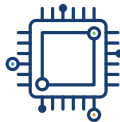
ProcessUnity offers the only all-in-one risk platform for modernizing Third-Party Risk Management.



TPRM Automation:

The ProcessUnity platform automates time-consuming tasks like assessment scoping, distribution and response gathering so your TPRM team can direct their attention to the most critical actions. With the workflow automation capability ProcessUnity provides, your team can onboard Third-Parties faster and generate configurable reports in real

[LEARN MORE: TPRM Automation](#)



Universal Data Core:

By gathering risk data from automated assessments and the Global Risk Exchange, as well as predictive insights and scores from trusted data partners, into a single repository, ProcessUnity allows TPRM teams complete visibility into the state of their Third-Party ecosystem.

[LEARN MORE: Universal Data Core](#)



Global Risk Exchange:

With a repository of over 15,000 attested risk assessments, validated by our strategic audit partners, the Global Risk Exchange accelerates the TPRM process while enhancing its efficacy. By providing detailed insights into Third-Party risks, it eliminates the time-consuming task of assessing every Third-Party individually.

[LEARN MORE: Global Risk Exchange](#)



AI-Powered Teams:

AI technology makes it easier to review policies at scale and make decisions based on accurate, real-time predictive insights into the broader Third-Party ecosystem. TPRM teams can multiply their efforts by partnering with ProcessUnity's AI capabilities, achieving a more consistent TPRM process while reducing cycle times.

[LEARN MORE: AI Powered Teams](#)



Further Reading

- [Closing Your Third-Party Risk Vulnerability Gap](#)
- [The Ultimate Guide to Third-Party Risk Management Workflow](#)
- [Third-Party Risk is a Data Problem: Solve it with a Universal Data Core](#)
- [Third-Party Risk Management: How the Exchange Model will Revolutionize Third-Party Due Diligence](#)
- [Third-Party Risk Management: AI-Powered Teams Elevate Human Performance](#)



ABOUT PROCESSUNITY

ProcessUnity provides leading enterprises with comprehensive end-to-end cybersecurity and Third-Party risk management solutions. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest cyber risk exchange database, and powerful artificial intelligence capabilities, ProcessUnity enables organizations to quickly identify security gaps, reduce Third-Party onboarding and offboarding time, and proactively mitigate first- and Third-Party risks. As a result, organizations can more effectively safeguard their critical assets while lowering program costs. ProcessUnity is trusted by major brands around the globe and is backed by Marlin Equity Partners. To learn more or request a demo, visit www.processunity.com.

ADDRESS

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

SOCIALS

Twitter: [@processunity](https://twitter.com/processunity)
LinkedIn: [processunity](https://www.linkedin.com/company/processunity)

WEBSITE

www.processunity.com

EMAIL

info@processunity.com