Definitions

Key Roles and Responsibilities in Third Party Risk Management

- TPRM = Third Party Risk Management. This team is responsible for identifying, assessing, and mitigating risks associated with external vendors and partners to ensure compliance and protect organizational interests.
- Risk Assessor / Risk Manager = Evaluates questionnaire responses and suggests mitigation strategies to uphold organizational interests and compliance for the Third Party Risk Management team.
- Requestor = Any individual in the organization who initiates a request for Third Party Risk Management to review a vendor by submitting the intake form.
- Business Owner = This individual is primarily responsible for managing the day-to-day relationship with a vendor, ensuring operational needs are met and maintaining communication.
- Accountable Risk Owner = This is the individual holds ultimate responsibility for ensuring that the vendor relationship adheres to organizational policies, fulfills risk management requirements, and is answerable for the overall outcomes of the vendor engagement.
- TPRM Contact = This refers to the TPRM representative designated to a finding, who supports the vendor with remediation activities.

Product & Service Types:

- On-Premises (On-Prem) Product = This product is installed and runs directly on the organization's own local infrastructure, instead of being hosted outside or in the cloud.
- Cloud/SaaS = This product is hosted and managed by an external vendor and accessed over the internet, rather than being installed on the organization's own local infrastructure.
- Service Provider = This is a vendor that delivers specific services to the organization, such as IT support, application support, consulting, or maintenance, rather than supplying goods or products.
- Networked = This describes a product that either connects to or communicates with the organization's internal network, regardless of whether it uses wireless or wired technology.
- Integrated (Integration) = A product that connects with other systems or infrastructure to exchange data or communicate.
- Significant Change = A major modification to a vendor's product, service, or scope that affects data sharing, system integration, or access, potentially impacting risk and requiring a new review.

Third Party Risk Process Components:

- Self-Search = In OnSpring, this search feature allows you to check whether a vendor already has an engagement profile and view its status. You can also review the current scope of work to see if there have been major changes, which may mean a new intake is necessary.
- Intake = This is the form that any person within Penn Medicine can use to request that the Third Party Risk Management team review an external vendor.
- Engagement Profile = The OnSpring record that tracks all important details about a vendor's product or service, including responsible parties and their connection to our data, network, and products.
- Questionnaire = This survey is sent to third parties to collect information on their security, compliance, operations, and risks.

- Evaluation = The process where the Third Party Risk Management team assesses a cloud vendor's responses, determines their suitability, and identifies areas that require additional review or mitigation.