Meeting Agenda

30-minute meeting:

- Cybersecurity Third Party Risk Management (TPRM): Outline the identified risks
- TPRM / Business Owner: Confirm the following:
    - Is the third-party vendor product new or existing? New / Existing
    - Are you aware of use by another business unit? Y / N
    - Is there, or will there be, a contract established with this third party (i.e., not a fourth party)? Y / N
    - Does the contract grant the third-party vendor access to our data or network? Y / N
    - Is the data involved classified as non-public information? Y / N
    - Is this a state or government mandated third party? Y / N
    - Can the confidential/sensitive information that is being shared, be de-identified or eliminated?
- TPRM : Outline the required next steps
- TPRM / Business Owner / EIO: Identify the appropriate Accountable Risk Owner
- TPRM / Business Owner / EIO: Q&A

FAQS

What is an Unsatisfactory TPRM Engagement Opinion?

- This is the outcome of a security risk assessment carried out on a new *or* existing third party vendor with a cloud component (SaaS) that stores, processes, or transmits any non-public Penn Medicine data. The TPRM evaluation found that the third party vendor lacks an independent audit (such as SOC 2 Type II, FedRamp, TXRamp, HiTrust i1 or r2, ISO27001 or has a considerable number of identified issues.

Why does not having an independent audit report lead to an Unsatisfactory rating?

- Our master services agreement requires vendors with a cloud component to maintain this annually. Even if your older contract does not specify this, Penn Medicine has required it since 2021, and TPRM must mark third parties as Unsatisfactory until an independent audit report is provided (see excerpt from Master Services Agreement below).

What actions are required if I intend to engage, or am currently working with, an Unsatisfactory third party vendor?

- A finding and exception must be requested and approved.

How does a Finding/Exception get created?

- **Following the Unsatisfactory review meeting, TPRM will generate a Finding with Exception and assign it to the designated Accountable Risk Owner identified during the meeting.**
- The Accountable Risk Owner will receive an email with a link to Approve the Exception.
    - This individual's required authority level is based on the risk rating and is specified in the table below.
    - The Accountable Risk Owner is typically a senior leader within the business unit that intends to engage or is currently working with the third party vendor. This individual is responsible for evaluating and accepting the risks associated with the vendor and must have the authority to approve exceptions as specified in organizational policies. The exact required level of approver is outlined in the corresponding table, ensuring that the person has sufficient oversight and decision-making capacity to manage vendor-related risks effectively.
    - 

What should I expect after the Exception is Approved?

- Once the exception is approved, you may move forward with your process.
- A TPRM representative will be assigned to the exception to ensure the vendor delivers the required reports or evidence in a timely manner.
- Exceptions cannot extend for more than 1 year.

What if we are not the only entity that uses this vendor, who should be listed as the Accountable Risk Owner?

- When several entities in Penn Medicine use the same vendor, the primary Accountable Risk Owner should be the senior leader of the business unit that initiated the Third Party Risk Assessment. If you identify other Accountable Risk Owners, we can inform them about the risk, and if they are more directly involved with the vendor or their data is greatly impacted by the vendor's services, we can discuss having them approve the risk as well.

How should questions or new information from an Unsatisfactory Third Party vendor that may affect the exception be addressed?

- All vendor inquiries should be directed to the designated TPRM representative identified in the record. Please contact this individual for further guidance.

How and when will the exception be closed?

- When a third party submits evidence to resolve an exception to the Business Owner or Accountable Risk Owner, consult the TPRM representative indicated in the record. If the evidence meets requirements, you will be notified to initiate closure and the TPRM Engagement Status will be updated accordingly.
- When a third party submits evidence to resolve an exception to the TPRM Representative and the evidence is determined to be acceptable, you will be notified to initiate closure and the TPRM Engagement Status will be updated accordingly.

What are the Circumstances under which an exception may not be required?

- The current contract does not involve any confidential/sensitive data sharing.
- It's an existing vendor that has provided evidence that the audit report will be provided within 60 days.
- It's a covered entity, with a BAA in place
- It's a 4th Party
- It's a government or state mandated third party
- Penn Medicine did not pursue relationship
- Confidential or sensitive information will be removed or de-identified before sharing with third parties.

Appendix 1

- 5.8.1. Each calendar year, Vendor shall engage independent third-party auditors to conduct a "SOC 2" service auditor's examination related to operations at the Vendor facilities in accordance with the American Institute of Certified Public Accountants' Statements on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, or its successor standard, as applicable ("SSAE 16"). Vendor shall deliver to UPHS, within a reasonable time (but in no event later than one (1) month) after the issuance by such third-party auditors, a copy (or, if and as requested by UPHS from time to time, a specific number of copies) of the independent service auditor's report produced in connection with such examination (the "Independent Service Auditor's Report"). UPHS shall be permitted to provide input to Vendor regarding specific needs of UPHS regarding SSAE 16 and the examinations described in this Section, and Vendor shall reasonably consider any such input for the purposes of maintaining Top Tier Standards with regard to such examinations and the relevant operational controls, processes, and safeguards and their effectiveness.
- 5.8.2. Without limitation to Vendor's other duties under this Agreement, Vendor shall at all times use reasonable efforts to maintain operational controls, processes, and safeguards of sufficient effectiveness to provide reasonable assurance that management's control objectives are achieved. Vendor, at its sole expense, shall, as promptly after each SSAE 16 SOC 2 examination as is reasonable under the given circumstances and through measures determined by Vendor, correct any control deficiencies noted by Vendor's own independent third-party auditors in such examination that prevent the achievement of management's control objectives.