Thank you for your interest in working with Cencora!

Our vendor relationships are essential to delivering innovative products and services to our customers, and we view every vendor engagement as a partnership built on trust, transparency, and shared accountability.

As a regulated global pharmaceutical solutions organization, we are committed to maintaining a comprehensive Third-Party Risk Management (TPRM) program that protects our customers, our organization, and our partners.

As part of these efforts, we include a formal, standardized Due Diligence process facilitated by our TPRM Technology solution, Aravo, to ensure we can evaluate your company's control frameworks across multiple risk domains.

While we understand that TPRM – risk assessments processes often differ in requirements and expectations, we have included an outline below provide transparency into what our vendors can expect when being engaged.

Cencora's TPRM Program Expectations and Requirements for Your Company:

Initial Engagement and Screening: Our team may ask your company to provide basic company information to initiate the vendor request.

Risk Identification and Classification: We assess the inherent risk of your product(s) / service(s) to Cencora and conduct an upfront sanctions screening.

Due Diligence Assessment: Your company completes required questionnaires and submits supporting documentation to identify the strength of your control framework across identified in-scope risk domains (listed below) relevant to the product(s) / service(s) your company is providing

- Artificial Intelligence (AI) Governance
- Business Continuity
- Compliance
- Information Security
- Corporate Security
- Environmental Health and Safety
- Financial Viability
- Internal Controls
- Privacy
- Quality

Additional Examples of Key TPRM Assessment Areas
Assessments are tailored based on risk classification; however, common evaluation themes include:

- **Breach / Incident History & Preparedness**
  Has the organization experienced a security breach, and does it maintain a formal program to detect, respond to, and remediate such incidents?
- **Privacy Impact Assessment (PIA)**
  Does the organization have an established process to identify and mitigate privacy risks

associated with collecting, using, sharing, and storing personal information (including sensitive data such as PHI)?

- **Business Continuity / Disaster Recovery**
  What protocols, plans, and testing mechanisms are in place to ensure operational continuity in the event of a disruption?

Findings and Remediation: Any gaps or deficiencies related to your company's control framework, may be subject to findings identification and remediation requirements to ensure compliance with Cencora expectations.

Code of Conduct: Acknowledgement to Cencora's Code of Conduct.

Thank you for your consideration and for any questions or concerns regarding the outlined requirements, please contact tprm@cencora.com.