Lessons Learned in Streamlining the Third-party Risk Assessment Process
Agenda

• Welcome & Introductions
• Overview of the Third Party Risk Management Lifecycle
• Three Unique Perspectives on:
  • Third Party Inventories
  • Due Diligence & Ongoing Monitoring
  • How the HITRUST Assurance Program Helps
• Third Parties’ (Service Provider Perspective
• Q&A & Wrap-up
Introductions

Aaron Shapiro
PwC Director
Cybersecurity & Privacy

Debbie Hutchinson
Availity Senior Manager
Audit and Third Party Assurance

Jeff Martin
Senior Manager
Information Security
Anthem
Overview of the Third Party Risk Management Lifecycle

A robust Third Party Risk Management (TPRM) program is based on adoption of key building blocks, and successfully linking the program strategy, policies and processes together. TPRM is focused on understanding and managing risks associated with vendors and other third parties with which the company does business and/or shares data.

The PwC Third Party Risk Management Program Framework

- **Third parties**
  - Vendors
  - Suppliers
  - Joint Ventures
  - Business Channels
  - Marketing Partners
  - Affiliates
  - Subsidiaries
  - Regulated Entities

- **Risk Considerations**
  - Reputational
  - Operational
  - Credit/Financial
  - Business Continuity and Resiliency
  - Strategic/Country
  - Subcontractor
  - Technology
  - Info Security & Privacy
  - Compliance

- **TPRM Program Components**
  - Governance Framework
  - Policy & Procedures
  - Inventory
  - Stratification
  - Issues Management

- **Lifecycle Activities**
  - Pre-contract
  - Post contract

© PwC. Not for further distribution without the prior written permission of PwC. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.
THREE UNIQUE PERSPECTIVES
The inventory, risk rating and on-going testing model enables a focus on efforts to establish the third party inventory and oversee services with higher levels of inherent risk.
Three Unique Perspectives - PwC

Third party inventory

This framework will assist the TPRM Program in focusing in on the inventory list by analyzing multiple sources in rapid manner and identifying the third parties that need to be included as part of the program, and rated by inherent risk.

Common Third Party Inventory Data Attributes

- Third Party Name
- Third Party Parent Name/Associated Third Parties
- Product/Service
- Third Party Type (Business Process Outsourcing, Partnership, Technology etc.)
- Spend
- Business Lines/Processes Supported by the Third Party
- Country/Region where Third Party is Based
- Contract Date (Engagement Date)
- Results of Third Party Risk Classification
- Results of Third Party Risk Assessments (e.g., Third Party Information Security Assessments)

We then clean and enhance the existing third party data to be put into the inventory repository.
Results of the inherent risk should drive the nature, timing and extent of activities used to monitor, oversee, and re-assess third party relationships. Due to the higher costs associated with more in-depth assessment activities, a risk based approach should be leveraged so that higher risk relationships receive more active risk management than lower risk relationships.

Depth of Due Diligence Activities

- None
- Request and review third party report (e.g., HITRUST certification, SOC 1/2/3, ISO 27001 certification, etc.)
- Require the completion and evaluation of a due diligence questionnaire
- Request and review third party report (e.g., HITRUST certification, SOC 1/2/3, ISO 27001 certification, etc.)
- Perform on-site assessments (1-5 days)
- Require the completion and evaluation of a due diligence questionnaire
- Request and review third party report (e.g., HITRUST certification, SOC 1/2/3, ISO 27001 certification, etc.)

Inherent Risk Rating

- Very Low 40-50%
- Low 20-30%
- Moderate 10-15%
- High 3-5%

© PwC. Not for further distribution without the prior written permission of PwC. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.
Third Party Inventories - Anthem

• Follow the data; not the spend.
  • Requires strong internal partnerships.

• Risk tiering can be more difficult in a highly regulated space.
  • In-scope inventories can tend to balloon.
Due Diligence and Ongoing Monitoring- Anthem

- Inefficient pre-contract due diligence processes can impede timely procurement processes.
  - Again, strong internal partnerships are necessary.
  - Especially for larger organizations.

- Change is constant.
  - Assessments are a point-in-time measurement.

- Additional pressures for enhancing ongoing monitoring.
  - New regulations, new technologies, global marketplace, maturing client base.
How HITRUST Assurance Program Helps - Anthem

- Risk assurance activity can create exponential volumes of work.
  - Leveraging the HITRUST Assurance Program helps to ensure a consistent and efficient approach.

- Anthem Information Security is requiring vendor Business Associates to achieve HITRUST certification on the environment that supports Anthem.

- Anthem Business Associates can leverage their HITRUST certification across the HITRUST Alliance partners.
Availity

THREE UNIQUE PERSPECTIVES
Third Party Inventories - Availity

• Conduct a complete inventory of all third parties activities ranked by risk factors.

• Include all types of third party relationships that can include business associates, trading partners, service partners, subcontractors etc.

• Evaluate the relationships to have a comprehensive understanding of who are your third parties, what services/functions they provide and what level of access they have to your organization’s data/systems.
Due Diligence and Ongoing Monitoring- Availity

• Conduct due diligence assessments to identify any potential gaps that could create risks or compliance issues prior to contract. Third parties who have completed a HITRUST validated assessment may submit certification letter as part of their due diligence.

• Continue to monitor relationships to proactively account for any changes that can occur throughout the relationship cycle.

• Organizations need to move beyond the initial due diligence and annual reviews to proactively address the bigger challenge of monitoring and assessing third-party risks on an ongoing basis.
How HITRUST Assurance Program Helps – Availity

- HITRUST assessment can help to evaluate your third party assurance program.
- Accepting the HITRUST certification can help due diligence by reducing time and efforts.
- Leveraging the CSF enables a single assessment to be accepted by many organizations across the industry.
- Focusing on third party risk management and consistent requirements of our third parties can help drive industry efficiencies.
Third Parties’ (Service Provider) Perspective

• Ability to effectively respond varies drastically
• Customer assessments come in all shapes and sizes and it can be very frustrating and difficult for third parties to respond timely
• Alignment to a recognized security/privacy framework (e.g., HITRUST CSF) helps organizations respond quickly, with less effort, and with positive results
• HITRUST certification and SOC 2s can relieve much of the headache associated with responding to customer requests