**Board Strategy:** Audit the governance processes and key controls used to assess and mitigate third-party IT security risk including (1) third-party security risk assessment, (2) security issue identification and remediation, (3) third-party onsite security reviews.

**Audit Objective/Scope:** Review the processes and controls to assess and mitigate third-party security risks including:

* Inventory of third parties; all tranches
* Criteria used to evaluate risk level of third party
* Third-party security risk assessment (initial and on-going) process
* Third-party security issue identification and remediation
* Third-party questionnaire
* Third-party onsite security reviews

**ERM:** (1) Cyber Security, Espionage & Information Security

(2) Vendor Performance Management

**Preliminary Risks:**

1. Data in motion and at rest at third party location is not appropriately protected
2. Unavailability and instability of systems

**Key Process Areas:**

* 1. **Risk Criteria & Categorization/Prioritization**:
     + Third parties are appropriately risk categorized; which drives the frequency and level of security requirements and oversight
     + Review of control inventory/documentation, criteria and governance expectations
     + Understanding established risk appetite (inherent & residual risk planning)
     + Exit Strategy and governance process (*when initiated through disengagement*) to ensure controls for Data and Operation Protection such as ensuring data removal from Third Party (“TP”).
  2. **Governance & Oversight Standards**:
     + Completeness of Third Party Risk Management (“TPRM”) inventory of all third parties (All tranches) contracted with Aetna
     + Review standards (onsite & questionnaire) – The documentation and process controls in place that facilitates oversight, accountability, monitoring, and on-going risk management;
     + Frequency of reviews – Scheduling, tracking, and approach (Based on risk tier of the third party). Questionnaires vs on sites
     + Reporting and communications, including escalation
  3. **On-Going Risk Monitoring**:
     + Understanding the assessment of new/evolving risks and/or vendor changes (including how Aetna’s relationship changing) that impact Aetna;
     + How results of ongoing monitoring activities ensure risks are re-prioritized, re-assignment, and re-classified; and
     + Reporting and communications, including escalation.

**Auditee/EC+1:** Jim Routh

**Key Auditee Contact:** Brenda Ferraro

**Fieldwork Start/End:** October 17, 2016 / Nov 18, 2016

**Report Date Target:** December 09, 2016

**Audit Portfolio Leader:** Diane Santiago (PL)

**Audit Team:** Nirav Shah (M2), Theresa Zagarino (IC), Sol Vazquez, David Ronca, Kevin Thomas & Ayoola Akanni

**Initial Data/Information requests\*, please place this information in the Box repository by 10/19/16**

|  |  |
| --- | --- |
| **ID#** | **Data Requests** |
| **01TSM** | Third Party Security Risk Governance Charter |
| **02TSM** | Third Party Security Risk Governance Policy |
| **03TSM** | Third Party Security Risk Governance Standards |
| **04TSM** | List of Third Party Security Risk Governance key controls |
| **05TSM** | Self-testing results related to the key controls, or access to the system that houses the data |
| **06TSM** | Criteria used to risk rank third parties |
| **07TSM** | Automation (i.e. system used to perform the automation, logic used within this sytem) used to risk assess third parties |
| **08TSM** | Copy of the training provided to third parties regarding the security control techniques that are required |
| **09TSM** | 9/23/16: An inventory of all third parties.   * Please provide us with a “confirmed” list of the sources and access to systems that house this data. The individuals that need access are the audit team noted above. IA will need to be able to ascertain of this list the type of provider, the tier rating (risk rating) and the start/end date of the relationship. |
| **10TSM** | 9/23/16: Population of Third-Party Risk governance exceptions and acceptance criteria |
| **11TSM** | 9/23/16: Link to Risk Category Grid |
| **12TSM** | 9/23/16: Link to Security Category Grid |
| **13TSM** | 9/23/16: A List of any "known issues".  *To ensure our audit adds maximum value, discussing issues that are “known” to management during our audit planning is important as this may reduce the time audit staff spends in your area, avoids having auditors duplicate efforts already undertaken by management, and may eliminate the need for unnecessary discussions at the end of fieldwork*. |
| **14TSM** | 10/7/16: Dept. of Insurance audit results/audit reports as related to governance of third-parties |
| **15TSM** | 10/12/16: Copy of the ACO schedule for third & fourth party providers for 2016 and planned for 2017 |
| **16TSM** | 10/12/16: The results and or grading for all completed ACOs for 2016 |
| **17TSM** | 10/12/16: A list of businesses that chose not to perform on-site reviews of third-parties in the last 12 months, including reason provided to your governance team. |

*\*This is an initial data request list to enable the Internal Audit Department to obtain a current understanding of the business function being audited, prior to the start of fieldwork. Additional data will be requested after completion of the walk-throughs with the auditees.*

**Preliminary Questions for Auditee (*Meeting 10/17/16 to close these*)**

|  |
| --- |
| 1. How the TP governance team is made aware of new arrangement and or edited arrangements with third/fourth parties? What is the intake process? |
| 1. What role does Procurement and Legal have as part of the governance oversight of TP? What are other required and critical Aetna business organizations that support the process? |
| 1. How is the TP Governance & Monitoring team advised of changes with or to third/fourth parties? Changes can be changes to established arrangements and or issues that could pose legal risk to Aetna. |
| 1. Please provide location to the Security category list referenced in acs-4751, Third Party Categorization standard. |
| 1. Where we maintain third party business partners (TPBP), are relationship managers identified? What about identified contacts for TPBPs? |
| 1. How often is the risk criteria reviewed to identify needs for update? And by whom? (factors include: emerging/new risks, industry risks, changes to regulatory landscape etc) |
| 1. With regard to the assessments completed, who is responsible for executing the assessments and to whom do they report results? |
| 1. Please confirm that assessments on-site are optional for businesses due to expenses on business cost centers. Also for those TPBPs that fall into Tier 1, are those on-sites optional? |
| 1. How do you identify non-compliance behaviors? And where is this documented/tracked? What is Aetna’s action to non-compliance on behalf of the TPBPs? |
| 1. How does your team manage and track “extended service” arrangements made between a business and a TPBP? Are there any assessments or approvals in place to ensure that extended arrangement or use of services/products doesn’t impact current risk rating? |
| 1. How does your team monitor expenditure related to TPBPs? Is it possible that a business area can charge services/products using a corporate card and expense them without that expense falling into the proper expense classification for TPBPs? |
| 1. What requirements do you place on the business groups that own the relationships with TPBPs? For example, if a business group manages relationship and governs that TPBP, if the TP falls into a specific tier is it mandatory that your team be involved in certain discussions related to the arrangement? How is that managed? |
| 1. Understanding that the risk assessment criteria can be around 500 questions, can you explain how you intake evidence supporting the replies by the TPBPs? Does your team conduct initial on-site evaluations as part of the assessment process for TPBPs? |
| 1. Is it possible that a TPBP that was determined to be lower tier could have shifted into higher rating before the ACO is completed? How would your team identify those instances? |