

Global Security Third-Party Risk Governance Audit (16212)

Internal Audit Report

February 2017



James M. Routh, Vice President, Chief Security Officer

Control Opinion:	Issues:
	
Effective Significant Improvement Needed Ineffective	High: 1 Moderate: 2 Low: 0

Internal Audit performed an evaluation of the design and operating effectiveness of controls governing third-party data security within the Global Security Third-Party Risk Governance (GS TPRG) program. The GS TPRG program provides a core service to Aetna as it assesses the security risks and exposures posed by third-party relationships. Third-party (TP) risk governance is the intersection of two of Aetna's top Enterprise Risk Management categories, Cyber Security and Vendor Performance/Third-Party Management. Furthermore, third-party security is one of Aetna's key risk pillars, which comprise the broader third-party governance framework for the enterprise. Since its inception in November 2014, the GS TPRG program has been continuously evolving beginning with a focus on the Procurement (Supplier Management Services) tranche. During 2016, six additional business tranches were added to the GS TPRG program (Brokers, Law Firms, Affiliates, International, Delegates, and Accountable Care Organization (ACO)/ High Performance Network (HPN)/Joint Ventures (JV)).

Our audit assessed key controls used to support the GS TPRG program, which included controls for third-party inventory management, security risk assessments, ongoing monitoring, exception processes, issue escalation, and reporting. Based on testing performed, we determined that the criteria used to evaluate the risk level of third parties, oversight of the third-party initial security risk assessment process, and the use of third-party questionnaires to support the risk assignment and exception management process are designed and operating effectively. However, oversight of third-party security risk is inconsistently performed as business owners assume self-governance responsibilities and their practices vary, such as the type of evidence maintained to demonstrate security risk results, form of escalation used when third-party security control gaps are identified, and the processes performed to validate effectiveness of fourth-party relationships. In addition, we are aware that the Connecticut Department of Insurance (DOI) Statutory Financial Examination of Aetna has shared one observation with management related to high-ranked third-party annual risk assessments. The Global Security organization evidenced their response to this finding with plans for remediation. As of the date of our report, the DOI had not yet responded nor has a final report been issued.

Overall, until the Department of Insurance, management self-identified issues, and the high-priority issue noted herein, we cannot opine favorably on the effectiveness of controls associated with third-party security risk governance. We will monitor the progress of all management's action plans to remediate the GS TPRG findings as well as perform a follow-up review the later part of 2017. Although the high-priority issue noted herein is addressed to the Global Security organization, to appropriately mitigate this risk, a broader enterprise solution is required. Internal Audit will continue to work with enterprise management, including Global Security, Procurement and the Executive Committee on identifying and implementing improvements to the Company's third-party vendor management approach. Two moderate priority issues were identified by management and will be tracked by Internal Audit.

This report may not be released to others outside Aetna without the written consent of the Aetna General Auditor or the Assistant Head of Internal Audit

Technical Overview

Aetna's Global Security organization is responsible for information security, physical security, business continuity, and ensuring that Aetna's global information and physical assets are adequately protected. Within the GS organization is the Global Security Third-Party Risk Governance (GS TPRG) team, which oversees the business-driven monitoring and enforcement of third-party risk assessment activities in an effort to protect company information assets accessible by third-party organizations. This organization plays a key role in minimizing enterprise risk associated with third party security.

The GS TPRG team was established in 2014, and consists of four full-time Aetna resources, including one Director with offshore risk assessment support from Ernst and Young. Over the last two years, the GS TPRG team has developed and refined a risk-based security program to monitor third-party security risks. In addition, GS TPRG provides transparency around the communication of risk and/or potential issues associated with all business tranches across the enterprise. GS TPRG conducts a series of risk assessments, including a Security Performance report, which provides a comprehensive open source assessment of threat indicator vulnerabilities, a Standardized Information Gathering (SIG) questionnaire, which is aligned to the International Organization for Standardization, HIPAA and NIST standards and is used to perform the third-party self-assessment, agreed upon procedures, which occur upon funding by the third party and are performed at the vendor location to validate data represented in the self-assessment questionnaire, Vendor Building Security In Maturity Model, which measures software and mobile security maturity and their ability to deliver software development lifecycle securely, and Vulnerability Code Scanning, which identifies vulnerabilities within code provided by software and mobile providers.

Third-party security risk is ranked as high, medium or low. This ranking is determined through a series of phased assessments including the Security Scorecard, vBSIMM, SIG, and onsite reviews. High risk third-parties are defined as those in which critical security control gaps are identified and / or third-parties who have access to or store restricted and confidential data elements.

The GS TPRG program is responsible for establishing the inherent and residual risk awareness of Aetna third parties and for overseeing the business' compliance to GS control standards spanning all seven tranches. Cumulatively, Aetna has approximately 5,400 third parties and 191,000 brokers being managed across the enterprise. The table below provides a breakout of third-party counts by business tranche.

Tranche	Third-Party Count
ACO / JV/ HPN	256
Affiliate	1,268
Broker	190,680
Delegates	1,125
International	1,545
Law Firms	200
Procurement	1,037

We noted that the GS TPRG team inherited the oversight for the ACO tranche in October 2016 due to a self-disclosed data breach event at Banner Health, an ACO vendor and future JV partner. At the time of this report, the GS TPRG team advised that their program was also supporting International limited to “Network Management “third parties during 2016. This was due to a language barrier and an effort to identify all regulatory requirements. All remaining International third-party types and brokers will be further monitored by GS TPRG during 2017. The ACO/HPN tranche was also in the process of assessment launch scheduled to complete on or before end of first quarter of 2017 in order to avoid impact to open enrollment. While the GS TPRG team is dependent upon third-party profiles, which contain third-party information required to perform initial and as-needed security risk assessments, they do not own the data as it is owned by Aetna Supplier Manager Services (Procurement).

From November 2016 through early December 2016, a joint initiative was launched with Global Security and Procurement to formalize the supplier risk governance model and framework with the Achieving Business Excellence (ABX) organization. During the ABX preliminary meetings, the DOI and IA findings were taken into consideration as well as 74 improvement opportunities related to Global Security Third-Party Risk Governance, Business Continuity, Procurement (SMS), Sourcing and Business Area Relationship Management. The goal of the program is to ensure Aetna’s supplier risk governance model and framework will satisfy cross functional requirements. GS TPRG was identified as a critical driver during the lifecycle of this effort.

Scope of Work

The scope of our review was over the Global Security Third-Party Risk Governance program and included the following areas of focus:

- The use of a complete and accurate Inventory of third parties, for all tranches
- Establishment of criteria used to evaluate risk level of third party
- Oversight of third-party security risk assessment (initial and ongoing) process
- Third-party security issue identification, escalation and remediation
- The existence and use of third-party questionnaires to support risk assignment
- Third-party onsite security reviews and scheduling efforts

While this audit specifically ties to third-party security risk governance controls and processes owned by Global Security, it was noted that there were two additional internal audits in progress, at the time of this review, to examine the broader scope of the International and Center of Excellence Procurement (SMS) controls.

Internal Audit Findings

1. Global Security Third-Party Risk Governance (GS TPRG) Oversight	High
<p>Issue: Global Security lacks controls to ensure that all third and fourth parties, identified by the business, are promptly and appropriately assessed for security risk.</p> <p>Issue Detail:</p> <ul style="list-style-type: none"> 103 third parties lacked relationship managers; out of these: <ul style="list-style-type: none"> Eight were risk ranked: 3 High (Category A), 2 affiliates and outside the scope of the program, 2 Medium (Category B & C), 1 an “NA” category (Wells Fargo Insurance Services USA) and 2 Low. Ninety-Five had no risk categorization with risk assessments pending for at least 6 months; 69 being greater than 365 days old. Information required by GS TPRG, to effectively perform third-party security risk assessments was incomplete within the Archer system of record. Such fields included (a) risk scoring, (b) third-party contact information, and (c) Aetna business/relationship contact. There was no evidence of escalation by GS TPRG to the business owners. Though disclosure of third-party subcontractor relationships (e.g., fourth parties) may be provided on the Standardized Information Gathering (SIG) questionnaire during onboarding, there is no known validation performed to ensure this data is transposed to the third-party tracking tools correctly. Accurate subcontractor data is needed so that GS TPRG effectively manage security risk over time. This backlog is limited to Procurement-related vendors; as other tranches are in the pipeline for future assessments and will require appropriate resourcing and business/vendor support to complete in 2017. 	<p>Impact: Increased potential for Aetna restricted and confidential data to be compromised.</p> <p>Root Cause: Capability – Global Security TPRG resources are allocated based on security risk to the organization; a backlog exists in completing validation controls due to limited resource availability.</p> <p>Enterprise Risk: Cyber Security, Espionage and Information Privacy, Vendor Performance and Management</p> <p>Management Action Plan:</p> <ul style="list-style-type: none"> GS TPRG to analyze and validate the spreadsheet of 103 third parties missing content. GS TPRG to provide Internal Audit (IA) with conclusion of the analysis. GS TPRG to create a monthly policy violation report for escalation. GS TPRG will use a 3-level escalation communication through the Security Steering Committee. GS TPRG to provide IA evidence of the report existence, the process for use and evidence that the report was distributed to the key stakeholders monthly. GS TPRG to define reportable fields as required fields within Archer in support of the ABX initiative. GS TPRG to supply IA with evidence of communication to the ABX team on the defined reportable fields. GS TPRG to develop an implementation plan for an annual fourth-party completeness assurance review. A fourth-party self-assessment questionnaire will be developed requiring confirmations around the use of a third party (which would be a fourth party to Aetna) and if so, defined data elements that must be provided. In addition, GS TPRG will present Key Performance Indicators (KPI) and Key Risk Indicators (KRI) at the quarterly TPRG Steering Committee advising of Relationship Manager gaps along with a required timeline to close gaps. To close the MAP provide IA with: <ul style="list-style-type: none"> Process description/ documentation including outlined escalation procedure. Process and Prevalent questionnaire implementation plan Screen shots of Prevalent questionnaire noting required fields and evidence it operates as intended Defined requirements for the Annual completeness report Evidence of the communication to TPRG Steering Committee advising of gaps and evidence of how closure of gaps is tracked. <p>Accountable Contact: Brenda Ferraro Overall Estimated Completion Date: April 1, 2017</p>

Management Self-Identified Issues

During our audit, the GS TPRG team self-disclosed remediation efforts that are underway in response to one incident related to the ACO tranches. Although these issues were identified by management, Internal Audit will track and close the MAPs following the protocol used for traditional internal audit findings.

1. Accountable Care Organizations (ACO) and Healthcare Provider Networks (HPN)		Moderate
<p>Issue: The implementation of the GS TPRG program to monitor the Accountable Care Organizations (ACO) and Healthcare Provider Networks (HPN) tranche was halted to address open enrollment.</p> <p>Issue Detail: Third parties for Accountable Care Organizations (ACO) and Healthcare Provider Networks (HPN) were recently assessed for security risk under the GS TPRG program during our audit review in November 2016. Prior to November 2016, ACOs, JVs and HPN third parties were not being assessed for security risks by GS TPRG. Management's approach to conduct security scorecard reviews started in November for ACOs, JVs and HPNs, with a plan to perform Standardized Information Gathering (SIG) Lite assessments throughout November 2016 through February 2017.</p>	<p>Impact: Lack of an ACO/HPN assessment process may result in an increased exposure to security breaches and/or data loss events.</p> <p>Root Cause: Capability – Prior to GS acquiring governance responsibilities of the ACO and HPN tranche, third-party data and assessments were managed by business units across Aetna and governance was not centralized.</p>	<p>Management Action Plan: ACO and HPN action includes communication and launch of assessments using the Prevalent tool (TPRG Platform) with a target completion of assessment by 4/1/2017.</p> <p>Monthly status meetings are conducted with key stakeholders for progress transparency. Exception process will be used for third parties that fail to complete assessment requirements and business acceptance of risk will be identified and tracked.</p> <p>Accountable Contact: Brenda Ferraro Estimated Completion Date: April 1, 2017</p>
2. Broker Security and Encryption Requirements		Moderate
<p>Issue: A validation control needs to be implemented to ensure all third-party devices are properly configured to encrypt confidential data.</p> <p>Issue Detail: The GS TPRG program requires that broker third parties (a combination independent brokers and broker firms) download AlertSec, software to identify if a broker is meeting requirements set forth in Aetna's encryption security policy (ATCS-839 Workstation Encryption), and there is no check to ensure encryption has been</p>	<p>Impact: Lack of third-party broker ongoing data security monitoring activities may result in an increased exposure to breaches and/or data loss events.</p> <p>Root Cause: Capability - The GS TPRG team has not rolled out their</p>	<p>Management Action Plan: Broker Portal improvement to require encryption validation at time of Broker onboarding and annual contract renewal. (This is owned by the Broker Organization) GS TPRG provides requirements only.</p> <p>To assist with compliance efforts for the broker encryption notifications are scheduled throughout 2017 into September to reach out to the approximately 191,000 brokers.</p> <p>Encryption validation reporting to be used as Key Performance Indicators (KPI) inclusive of AlertSec reporting for downloaded</p>

completed. In addition, there is no notification from GS TPRG to the Brokers Organization when a broker is identified as non-compliant.	program to ensure third-party brokers are compliant with minimum-security standards due to open enrollment.	encryption where devices were not already encrypted. Accountable Contact: Brenda Ferraro Estimated Completion Date: October 31, 2017
---	---	--




Other Observations

The following observations have been provided to GS TPRG management with recommendations for increased efficiencies within the program:

- During the audit, we discovered an existing ability for business units to use a corporate card for purchases of third-party goods and services without detection by the expense management process. These instances have allowed arrangements to be established between Aetna and third parties without adequate GS third-party risk assessments and bypassing potential procurement requirements. There is opportunity to review both the accounting expense management process and supporting data for control points to alert the GS TPRM team (as well as Procurement) once such expenditures have been identified.
- During audit walkthroughs we learned that Emptoris, the Procurement and Contracting system, was able to provide reporting to GS TPRG noting third-party arrangement changes and new additions for Aetna. This information could be used to help support an interim or compensating control to help GS TPRG complete the early detection of required risk forms/risk assessments.
- During the audit, we discovered that several fields within Archer did not contain information for third parties. Specifically for those TP's categorized as "A", this information is required by GS TPRG to completely and accurately assess the third party and potentially its subcontractor(s). Since the data is being maintained by the businesses and soon to be self-managed by the third parties in the new tool Prevalent, it is important that GS TPRG continuously remind and or enforce the business owners to keep this data up to date. The information "required" for completion should minimally include assigned Relationship Manager, Third-Party Contact, the Aetna business/relationship contact to ensure adequate escalation procedures can be taken by GS TPRG during risk governance activities.

Standard Terminology




Issue Rating:

	High	The identified risk requires the immediate attention of department and senior management to prevent the process from becoming ineffective, and an agreed-upon action plan for resolution is needed.
	Moderate	The identified risk requires the near-term attention of the responsible manager. There should be an agreed-upon action plan for its resolution.
	Low	The identified risk does not warrant immediate attention; however, there should be an agreed-upon action plan for ultimate resolution.

Root Cause Category:

Awareness	Was anyone aware? Issues were unforeseen, and no processes (e.g., policy and procedures) existed to address them.
Capability	Were processes designed correctly? While processes (e.g., policy and procedures) existed, gaps prevent objectives from being met.
Diligence	Was the control executed as designed? Processes (e.g., policy and procedures) existed but were executed incorrectly or available resources, tools, policies were not used.

Overall Control Environment Opinion:

	Ineffective	Control weaknesses are pervasive or one weakness is so severe that it impacts the entire operation under review. Immediate management attention is needed to remediate the issue identified.
	Significant Improvement Needed	One or more significant control weaknesses exist that require prompt action to prevent the process from becoming ineffective.
	Effective	Overall, controls are appropriately designed and functioning as intended. Control weaknesses, if noted, do not threaten the effectiveness of the process reviewed.

Distribution

Executive Team

Bill Baskin
Cindi Bates (ERM Risk Champion)
Mark Bertolini
Margarita Blanchard
Kathy Egan
Shawn Guertin
Rick Jelinek
Judith Jones
Tom Jones
Charlie Klippel
Bill Kramer
Gary Loveman
Karen S. Lynch
Steve Mahoney
Marc Marini (ERM Risk Champion)
Adam McAnaney
Maureen McCabe
Meg McCarthy
Deb Pillinger
Colleen Rackley-Cuda
Tom Sabatino
Jonathan Swanson
Tom Weidenkopf

Client Team

Chris Catania
Brenda Ferraro
Pamela Flemming
Kurt Lieber
Chris Krueger
Maria Spano

Other Business Area Leadership

Todd Mandirola (Procurement - SMS)
Dan Tedesco (Procurement – SMS)
Tim Tompkins (GS – Encryption Control Standard Owner)

Internal Audit

Ayoola Akanni
DJ Arguello
Dave Doherty
Diane Santiago
Kevin Thomas
Sol Vazquez
Theresa Zagarino

External Auditor

Heidi Barter
Sue Jackson