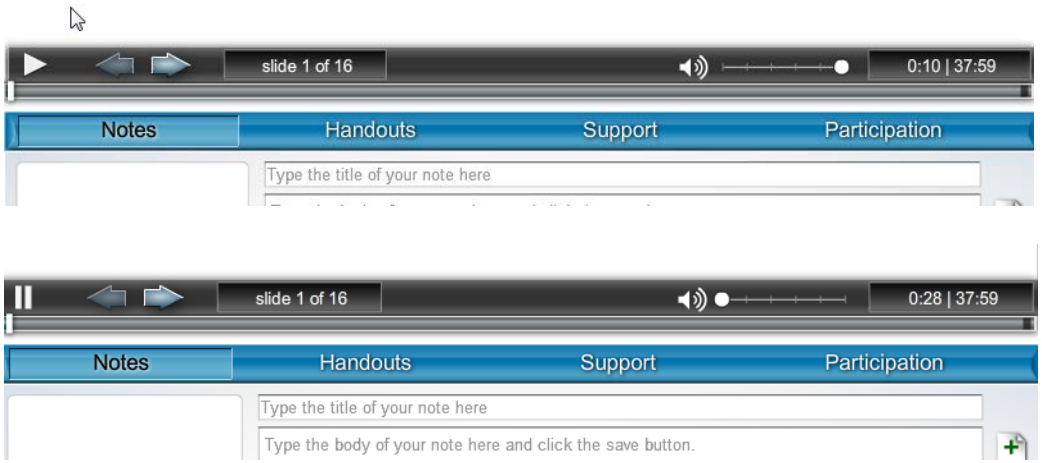
AIG Operational Risk Management
Audit Lunch and Learn

October, 10, 2019
New York

Corporate ORM
Richard.O'Brien@aig.com
Kimberly.Fix@aig.com
Damian.Matthews@aig.com
Victor.miller@aig.com
Jacqueline.Wing@aig.com
Christopher.Lebano@aig.com

Key Navigational Features

- To move forward or back in the course from the classic view, mouse over anywhere on the slide and use the “ ▶ ”next and “ ◀ ”previous buttons. To pause, click on the “ ⏸ ” button and to return playing click on the “ ▶ ”button.
- This course has a glossary of key terms that you can access at any time from the “Handouts” tab. Once you access this document, you can search it quickly using “CTRL + F”.



Housekeeping

- **Turn off all electronic devices**
- **During Q&A sessions, wait for the microphone**
- **CPE credits are offered for this course. To ensure you receive credit:**

- Perfect attendance is mandatory
- If attending in person
  - Sign in and out on the sign in sheet at the door
  - You will receive your CPE certificate and evaluation form within a week from Confirmation@learnlive.com
- For webcast participants
  - Log-in using your own computer to receive CPE credit.
  - You must answer 75% of the participation pop-ups in order to receive CPE credit.
  - Your CPE certificate and evaluation form will be available immediately
- For on-demand participants
  - Webcasts will be made available for on-demand viewing shortly after the Learning Day.
    - On-demand courses are available for participation through the LearnLive University (log onto LearnLive and select “On Demand Courses” under the “My Catalog” menu dropdown).
  - You must answer 100% of the polling questions and pass 75% of the final exam questions. You will be allowed a maximum of 10 attempts before you will be required to take the course again.
  - Your CPE certificate and evaluation form will be available immediately

    - *Please complete the evaluation form so we can tailor future training sessions*

AIG

AIG Operational Risk Management - ORM Policy and RCSA Process Changes

Instructors Bio

- **Jacqueline Wing**

Jackie Wing is a Director of Operational Risk Management. Jackie joined AIG's Enterprise Risk Management team in 2015, leading the Archer eGRC initiative, for ORM, to develop the RCSA and Risk Event modules. In addition to the ORM eGRC program, Jackie is responsible for the Risk Event Framework and Issues Management Standards for AIG. Prior to joining AIG, Jackie spent 26 years in Banking, 13 at PNC Bank and 13 at JPMorgan. At PNC, she was a Commercial Lending Credit Officer and the Secretary of the Credit Risk Committee. At JPMorgan, she was a Risk Officer for Exchange Trade Funds and managed the RCSA program for the Investment Management Business. She also developed the Process, Risk and Control Taxonomy for Investment Management and Worldwide Security Services and was on the working group responsible for developing the aggregated PRC taxonomy for JPMorgan. Jackie attended Fairleigh Dickinson University.

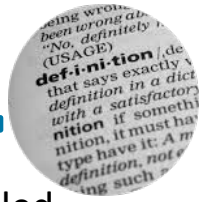
- **Christopher Lebano**

Christopher Lebano is an Operational Risk Manager in the Global Enterprise Risk Management Team. Christopher joined AIG in September 2019 is focused on corporate governance related to Risk Assessments/RCSA, Reputational Risk, Incentive Compensation Governance and Risk Management for the Corporate Functions (Human Resources, Corporate Communications and Legal). Prior to joining AIG, Christopher worked at Citigroup for 19 years. His most recent role at Citi was in Operational Risk Management for the Treasury & Trade Solutions division supporting Operations and Control. In prior roles at Citigroup, Christopher worked in Client Services and Technology Project Management for Payment monitoring applications and Encryption Key Management. Christopher holds a master's degree in Business Management from Stony Brook University.

Agenda

- What is Operational Risk
- ORM Policy Overview
- ORM Policy Revisions
- RCSA Process Overview
- RCSA Process Changes
- Inherent Risk Assessment
- Controls Assessment
- Residual Risk Assessment
- Issues and Action Plans

What is Operational Risk



Operational Risk at AIG is defined as the risk of loss resulting from inadequate or failed internal **processes**, **people** or **systems**, or from **external events**. These **four sources** are key to understanding where operational risk emanates and how to manage it.

Operational Risk includes legal, regulatory, technology, compliance, third party and business continuity risks, but excludes business and strategy risks.

ORM Policy Overview

- Operational Risk Management Policy was first published in 2011. It is presented at the Group Risk Committee and requires Board approval.

- The Policy outlines the following:
  - AIG's definition of Operational Risk
  - Roles and Responsibilities of the three Lines of Defense
  - Policy ownership is delegated to the Head of Governance and Operational Controls
  - All employees are responsible with reading, understanding and complying with this policy

  - Minimum requirements of the Operational Risk Framework including:
    - Escalation Requirements
    - Risk Identification – Identify and describe Operational Risk impacting their business
    - Assessment – Determine Top Risk Impacting the Organization and perform Risk and Controls Self Assessment (RCSA) in accordance with AIG Standards
    - Treatment – Determine the appropriate Risk Treatment options consider including Risk Appetite, Materiality, Cost-Benefit analysis and Legal/Regulatory/Compliance Requirements
      - Risk Mitigation
      - Risk Avoidance
      - Risk Transfer
      - Risk Acceptance
    - Monitoring and Reporting – Key Risk Indicators (KRI), Risk Event Reporting
    - Training and Awareness

ORM Policy Revisions

- Operational Risk Management Policy has been revised and is pending publication.
- The following updates are included in the revised policy:
  - **Major Change** – Reputational Risk has been incorporated into the policy
    - Added requirement for BU/CF protocols to be established for Reputational Risk
    - Added Reputational Risk escalation requirements related to the ELT and AIG CRO
  - **Minor Changes**
    - Removed reference to the Technology, Operations, Risk & Controls Committee and replaced with Group Risk Committee as relates to the senior management committee responsible for assessing all significant risk issues
    - Removed references to practices no longer performed or required
    - Clarified Roles and Responsibilities
    - Standardized several glossary definitions

RCSA Process Overview

The RCSA is an integral component of the firm's overall operational risk framework that provides the means of identifying, assessing, and monitoring risk exposures and control weaknesses. An RCSA:

- Identifies the risks that exist in their critical processes and prioritize risks for assessment
- Evaluates the effectiveness of control mechanisms in mitigating these risks
- Determines the level of risk that exists based on the existing control environment
- Defines and executes actions to remediate control deficiencies identified

The key phases of the RCSA process include:

Business Self-Assessment of Operational Risks, Facilitated by 2nd Line (where applicable)

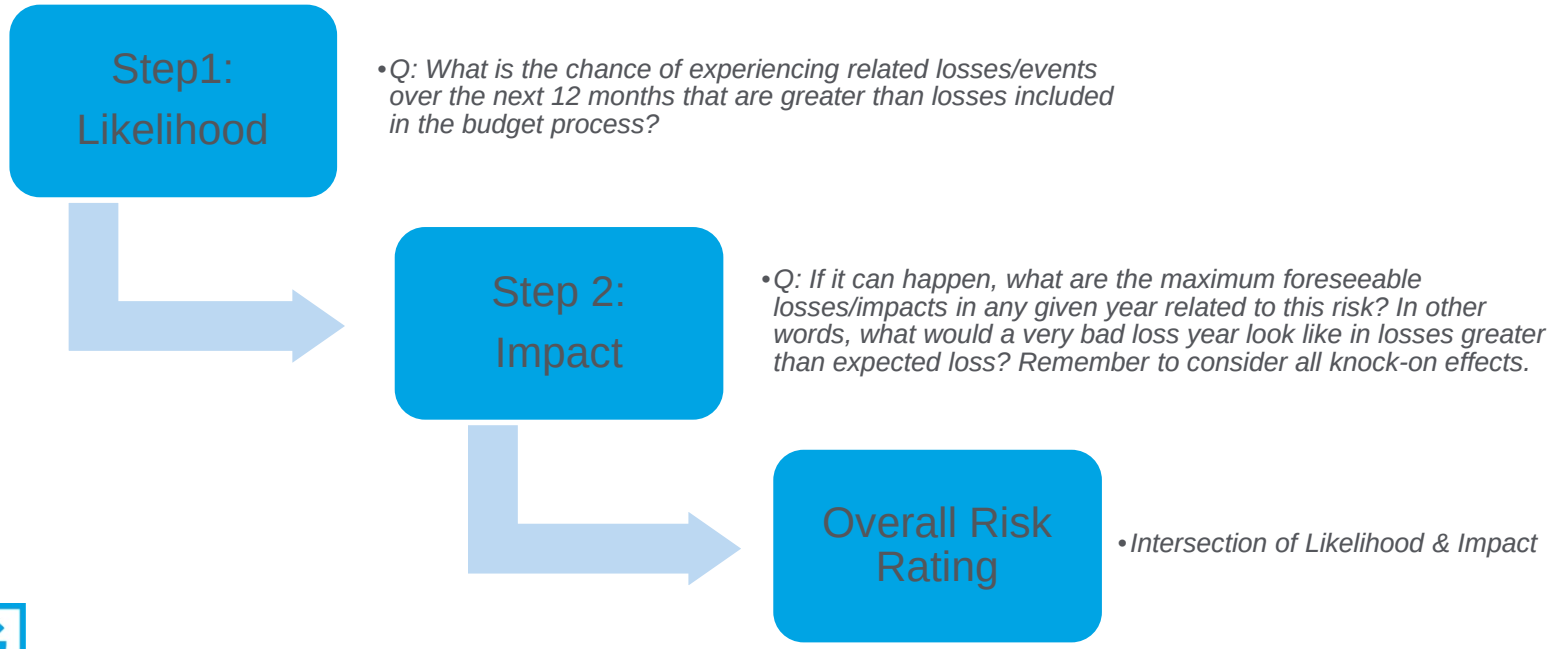
"Pre-Work" (Input into Initial Risk Assessment)	1. Identify & Assess Inherent Risk	2. Identify & Evaluate Controls	3. Assess Residual Risk	4. Risk Treatment - Identify Issues and Actions
• Review and understand the policies and procedures for the business (if various Lines of Business, have reviewed each one of them) • Review SOX & Audit reports • Review internal and external risk events	• Identify risks by critical process, leveraging standard PRC. Identify other materials risks per risk rating methodology.	• Evaluate controls for Elevated and High inherent risks using the standard PRC. • Identify control gaps.	• Review results of controls evaluations. • Evaluate effectiveness of controls environment in mitigating each risk.	• Identify issues and action plans. • Determine target dates for remediation

Inherent Risk Assessment

Inherent Risk

Inherent Risk is the pure risk exposure that exists prior to consideration of any controls or other mitigating factors. Alternatively, inherent risk can be viewed as the exposure assuming all controls fail. Higher inherent risks generally pose greater threat to the organization should the risk materialize and, therefore, require a stricter level of controls and monitoring of the effectiveness of controls.

- The *ORM Risk Rating Matrix* is used to perform an inherent risk assessment via a step process; (1) likelihood of a risk occurring and (2) the potential impact/losses that could be incurred. Impacts are determined taking in both qualitative and quantitative factors.
- RCSAs prioritize Top Risks which have previously been determined as material to the organization. Therefore, these risks are defaulted as "High". However, considering that assessments are conducted at various levels and areas of the organization, Top Risks materiality may vary and a review of the local inherent risks rating can be performed to ensure effective prioritization control evaluation. Any deviations from a "High" rating requires a rationale in Archer.
- The inherent risk assessment serves as guide for identifying additional material risks (Elevated/High) not included in Top Risks.



Control Assessment

Control Evaluation

Understanding Control Design and Effectiveness:

Controls are processes designed to provide reasonable (not 100%) assurance regarding the achievement of objectives relating to business operations, reporting and compliance with internal policies, procedures and external regulations. Properly designed and functioning Controls are integral to mitigate known inherent risks in the Business. As such, the proper evaluation of control design and operating effectiveness must be reviewed as part of the RCSA.

- Controls are evaluated for design effectiveness (DE) and operating effectiveness (OE)
  - **Control Design**: Is the control design appropriate for mitigating the Risk?
  - **Operating Effectiveness**: Is the control being executed as intended?
- Assessing the DE is the first step in the control evaluation process. If the design is deemed Ineffective, the overall control rating will be Ineffective.
- If the DE is Effective, the second step is to review the OE to ensure the control is executed per the design.
- The evaluation of a control's OE does not require formal testing of controls. Other methods including observation of the process and control operation can be leveraged to support a reasonable conclusion as to the OE of the control.
- Upon completion of the DE and OE evaluation, an overall control rating is determined.

Effective

- Control is well established, relevant and deemed reliable in mitigating the risk of loss
- The control is appropriately designed and executed as intended

Partially Effective

- There is only partial fulfilment or adherence with the control as stated (i.e. the control is not being performed with full effectiveness, is being performed inconsistently or with irregular frequency)
- Control design needs some improvement (may not be fully effective in mitigating risk), or the design might be manual (where automated controls would be more effective)

Ineffective

- Control does not mitigate the risk that is inherent in the key business process:
  - The control either does not exist or, if in place does not mitigate the portion of the risk for which it is designed (the control design is inadequate in mitigating the risk and requires significant redesign), or
  - The control is performed improperly or not at all

AIG

Residual Risk Overview

Residual Risk

Residual Risk estimates the remaining or actual risk exposure that an organization faces based on the strength of the current control environment. Residual risk is assessed after all mitigating controls are evaluated to determine how effective they are in mitigating the risk to an acceptable level (currently defined as “Moderate” risk). Higher residual risk ratings are used to prioritize control gaps requiring remediation.

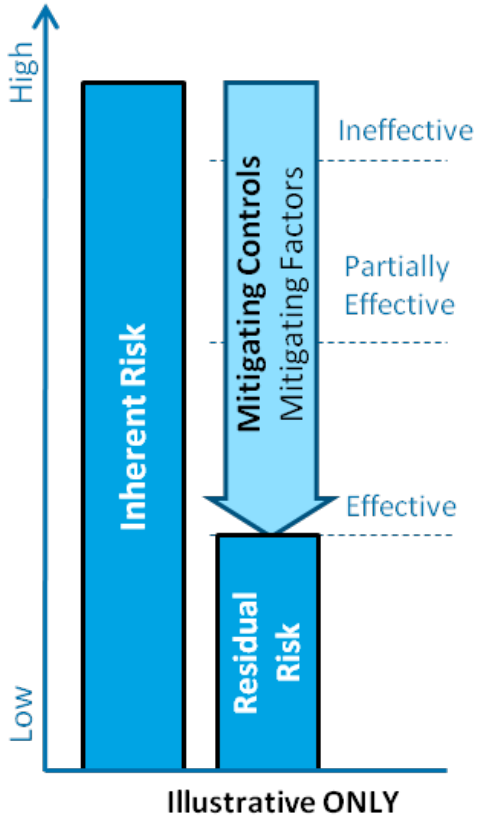
NOTE: The steps for assessing residual risk are very similar to inherent risk with one major difference, the current control environment is taken into consideration when determining impact and likelihood.

Determining Residual Risk and Subsequent Actions

- Using the *ORM Risk Rating Matrix* in conjunction with the supplemental guide on the next slide, assessors evaluate **Residual Risk Impact** and **Residual Risk Likelihood** for each risk and determine **Residual Risk Rating.**
- Residual risks rated as **High** or **Elevated** require creation of issues and action plans to remediate control gaps and reduce residual risk to an acceptable level (M or L).

Considerations on Residual Risk Ratings and Rationales

- For any given risk, Residual Risk should be less than, or equal to, Inherent Risk
- It should not be assumed that **residual risk impact** would be the same as **inherent risk impact**. Unlike inherent risk, residual risk takes into account controls. Therefore, impact may be less severe. For example:
  - Controls in place may reduce the volume of transactions or records (e.g.. policies, claims, customers) impacted
  - Controls may detect a failure before inherent extent of impact is realized
- Ineffective and partially effective mitigating controls would not be expected to result in a substantial reduction to residual risk
- Residual risk ratings rationales should be clear and concise explaining in detail how the effectiveness of corresponding controls led to the residual risk rating determination.
- Issue and action plans are created at the control level since it is the control(s) that requires remediation to mitigate the risk.



Issues and Action Plans

Risk Treatment

- Issues are identified to explain a problem for a risk that is not adequately mitigated.
- For **High** and **Elevated** residual risks noted during RCSA, the process owner and management must identify issues and create action plans addressing control gaps to reduce residual risk.
- Issues and Action Plans follow the RCSA Standard which should be referred.

Issues

- Issue descriptions should contain sufficient detail to allow individuals unfamiliar with the specifics to understand the issue, risks and potential impact. Identify the issue and either create an action plan to reduce the residual risk to Moderate or Low or file a risk acceptance for management review and approval of the residual risk
- Facilitators must ensure that all issues have been reviewed with key impacted stakeholders, not just the issue owner so that consideration is given to action plans required to mitigate risk.

Action Plans

- Action plans are created to describe the action that will be taken to address each issue.
- If remedial actions will not be put in place or will not sufficiently address an issue, they should be discussed with the respective CRO/2nd Line and escalated to the appropriate business leader and committee to ensure they are comfortable with the approach.
- Action plans should contain sufficient detail of the high-level mitigating actions required to reasonably and effectively address the Issue. Each action plan should also identify the owner and target due date.
- Action plans should be reviewed with impacted stakeholders and target dates should be reviewed and approved by the appropriate management levels.

Summary of RCSA Process Changes

Highlighted below are the key changes for the Risk and Control Self-Assessments (RCSAs) across AIG.

Changes are being Implemented to truly drive first line ownership of the risk and control environment, with ERM's focus being on review and challenge.

Area	Process Changes
Risk and Control Self-Assessment (RCSA) Standard	▪ Business Unit/Corporate Functions to define an approach and governance for executing their RCSA program. ▪ BU ERM to provide support and review and challenge. ▪ BU ERM will ensure that the minimum RCSA standards noted below are met. ▪ Business implemented RCSA program will, at a minimum: – Define the approach and governance for the RCSA. – Use ERM Process Risk and Controls (PRC). – Select processes for assessment with supporting rationale. – Perform risk and control evaluations. – Aggregate and present results of RCSA to senior management and business leadership. – Log issues and track progress of remediation.
RCSA Coverage	▪ Business to select significant/ key processes for assessment with supporting rationale, taking into consideration all business processes and risks associated with each. – ERM's role will shift from being prescriptive about which RCSAs the business completes to instead review and challenge what the business prioritizes for assessment.

Summary of RCSA Process Changes

Area	Process Changes
Common Taxonomies	▪ Standardized PRC with reduced process-risk-control combinations implemented in 2Q 2018, allowing for a more steady-state, user-friendly PRC. ▪ Where needed, users can augment existing PRC to include process-risk-control combinations more reflective of current business environment.
RCSA Output / Reporting	▪ Business to present results of RCSA to senior management and business leadership (e.g. legal entity or risk committee) to inform of key risks and articulate how control gaps are being addressed.
System and Tools	▪ RCSAs can be documented by the business in standard template provided by Corp Center ERM, or the business may select another documentation format/method it deems appropriate, as long as minimum documentation requirements are met. ▪ Risks rated inherently high and elevated, and with identified control deficiencies/gaps, must be logged in Archer along with associated issues and action items.

Thank you!

eGRC Archer Program

10/10/2019

Richard O'Brien
Head of Governance and Operational Controls
ERM
+1 212 458 1669
Richard.O'Brien@aig.com

Damian Matthews
eGRC Strategic Program
ERM
+1 212 770 3841
Damian.Matthews@aig.com

Stella Xu
eGRC Strategic Program
ERM
+1 212 770 9175
Stella.Xu@aig.com

eGRC Archer Program

Instructors Bio

- **Richard O'Brien**

Richard O'Brien serves as Head of Operational Controls & Governance at AIG and is a member of the ERM team. He is based in New York. He joined AIG in New York in 2007 in a regional capital management role and was based in Hong Kong from 2008 until 2010. From 2011 until 2016 he was the Chief Risk Officer for AIG in the Asia Pacific region, based in Singapore. He was responsible for Enterprise Risk Management across all of AIG's businesses in the region. Between 2016 and 2018, he was Global CFO for Property & Special Risks at AIG. Prior to joining AIG, Richard worked for General Motors' Treasury Department in New York, with rotations through capital management, debt capital markets, and pension funding. Additionally, he has worked for Morgan Stanley in its UK M&A group. Richard has a degree in Finance from the National University of Ireland, Cork, and an MBA from Cornell University.

- **Damian Matthews**

Damian Matthews manages the GRC Strategic Program which focuses on the implementation of governance, Risk and Compliance practices on the RSA Archer platform. He joined AIG in June 2004 as manager of an IT development team in London before moving to ERM in 2014 holding various roles in Operational Risk and Risk Architecture. Damian holds a bachelor's degree in business information systems from the University of Portsmouth and is currently working towards his master's degree in Risk Engineering at Clemson.

Agenda

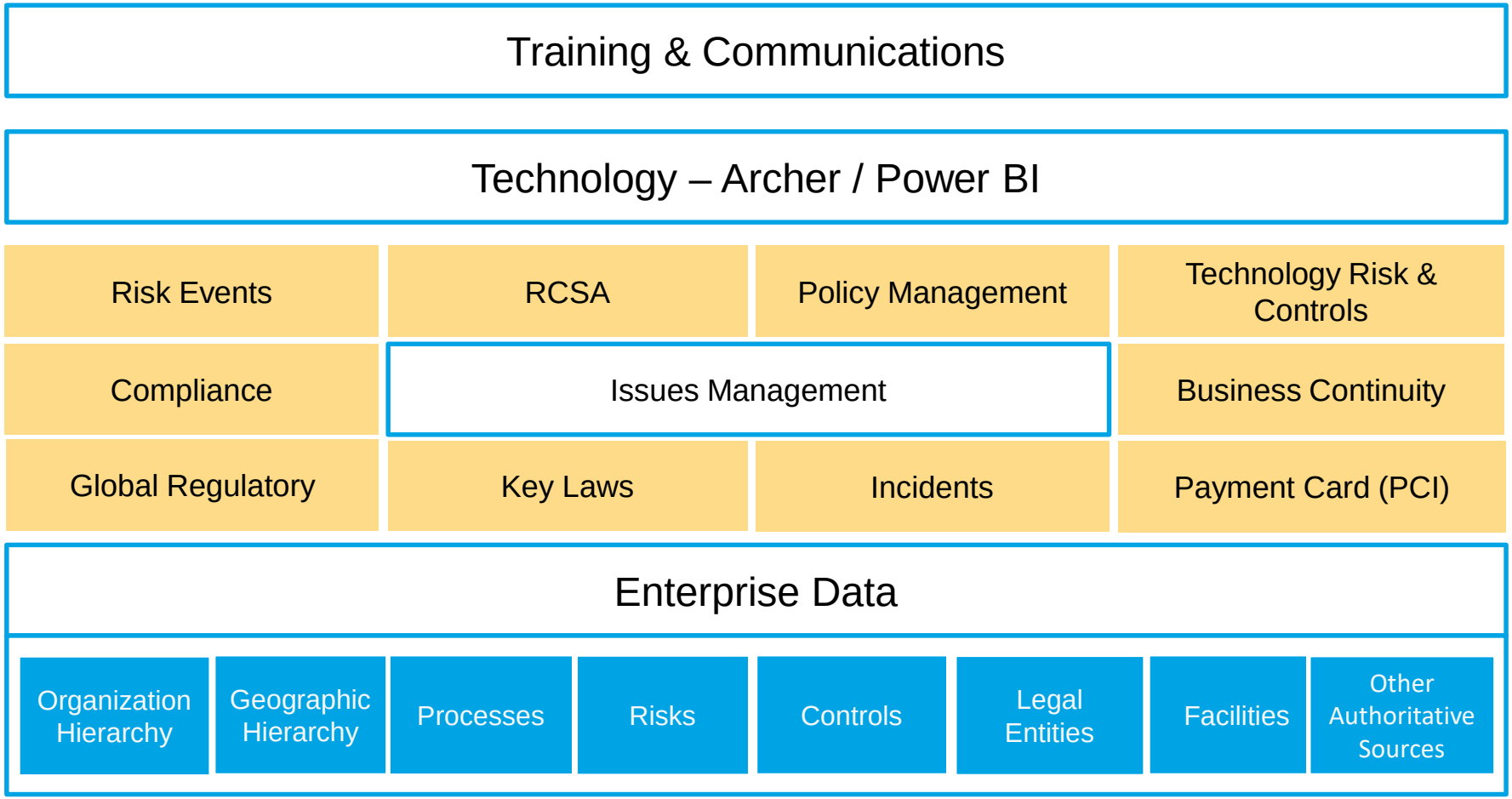
- eGRC Program
- eGRC Framework
- Archer Platform
- Platform Optimization
- GRC Data Warehouse and BI Reporting
- GRC Data Warehouse and BI Reporting – High Level Architecture
- Customized GRC Reporting
- Customized 1st Line Dashboards

eGRC Program

The Enterprise Governance Risk and Compliance program consolidates individual governance, risk and compliance practices on an integrated platform (Archer)

Work Stream	Owner
BCM	Stephen Jarrett
Compliance (Monitoring & Testing, Risk Assessments)	Richard Dapcic
Compliance (Incidents, Inquires, Conflicts of Interest)	Katherine Segersten
Data Maturity Management	David Williams
Global Regulatory / Key Laws	Patrick O'Neal
Issues Management	Kim Fix
Operational Risk Management – Risk Events, RCSA	Kim Fix
Payment Card Industry (PCI)	Bruce Sussman
Policy Management	Guy Kulman
Savings Tracker	Eric Gordon
TRC - Risk Assessments, Application Rating, Software Security Assessments	Mohit Raut

eGRC Framework



*Data Maturity Management and Savings tracker are not GRC processes

Archer Platform

Enhances Risk Visibility

RSA Archer Suite consolidates risk data from across an organization and uses risk analytics to provide organizations with a comprehensive and integrated picture of risk.

Improves Efficiency

With RSA Archer solutions, organizations are able to rationalize and automate a wide variety of governance, risk and compliance processes, leading to cost savings and other efficiency gains.

Accelerates Decision-Making

The risk taxonomy built into RSA Archer gives organizations a framework for collecting timely, actionable information that helps to drive more informed, risk-based decisions.

Drives Accountability for Risk

Customers say RSA Archer solutions enable them to drive a strong culture of risk management across their enterprises by driving clear accountability to front line managers.

Features a Best-Practices Approach

Designed with built-in industry standards and best practices, RSA Archer allows customers to quickly implement effective risk management processes.

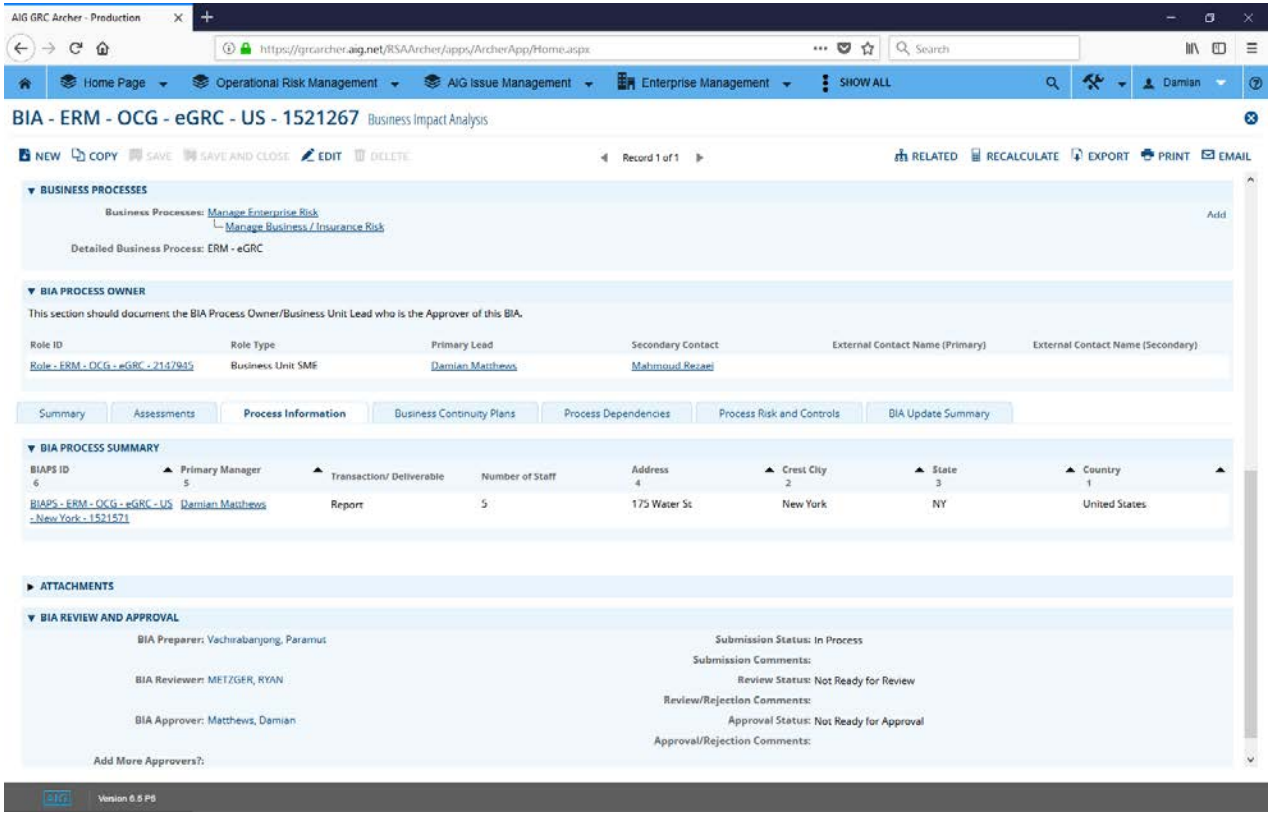
Provides a Proven Solution

Gartner has repeatedly recognized RSA Archer in the “Leaders” quadrant of its Magic Quadrant reports for integrated risk management, IT risk management and more.

AIG

Archer Platform

Since initial deployment in 2016, platform upgrades have provided numerous improvements to the user interface



Platform Optimization

- Established Governance and Change management process for Enterprise Data
- Development of GRC Data Warehouse
- Integration of BI Reporting (Power BI)
- Improved Communication
- System
  - Improved performance
  - User Interface refresh
- RCSA Simplification (In Progress)
  - Improved ease of data entry
- Issues Simplification (In Progress)
  - Simplification of workflow, roles and standardization of statuses

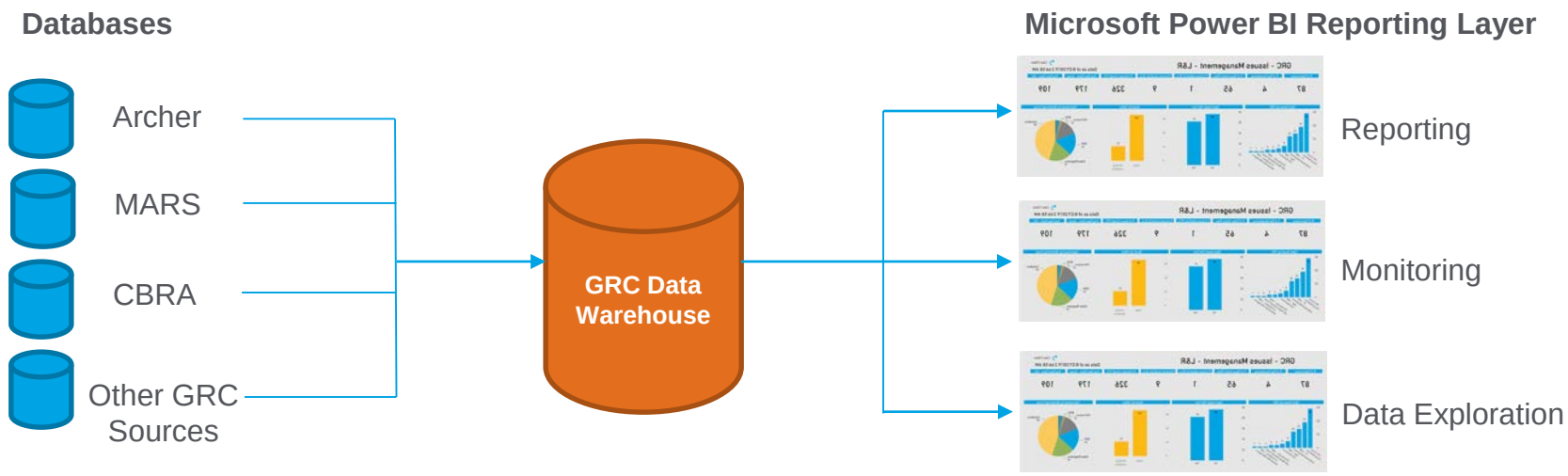
AIG

GRC Data Warehouse / BI Reporting

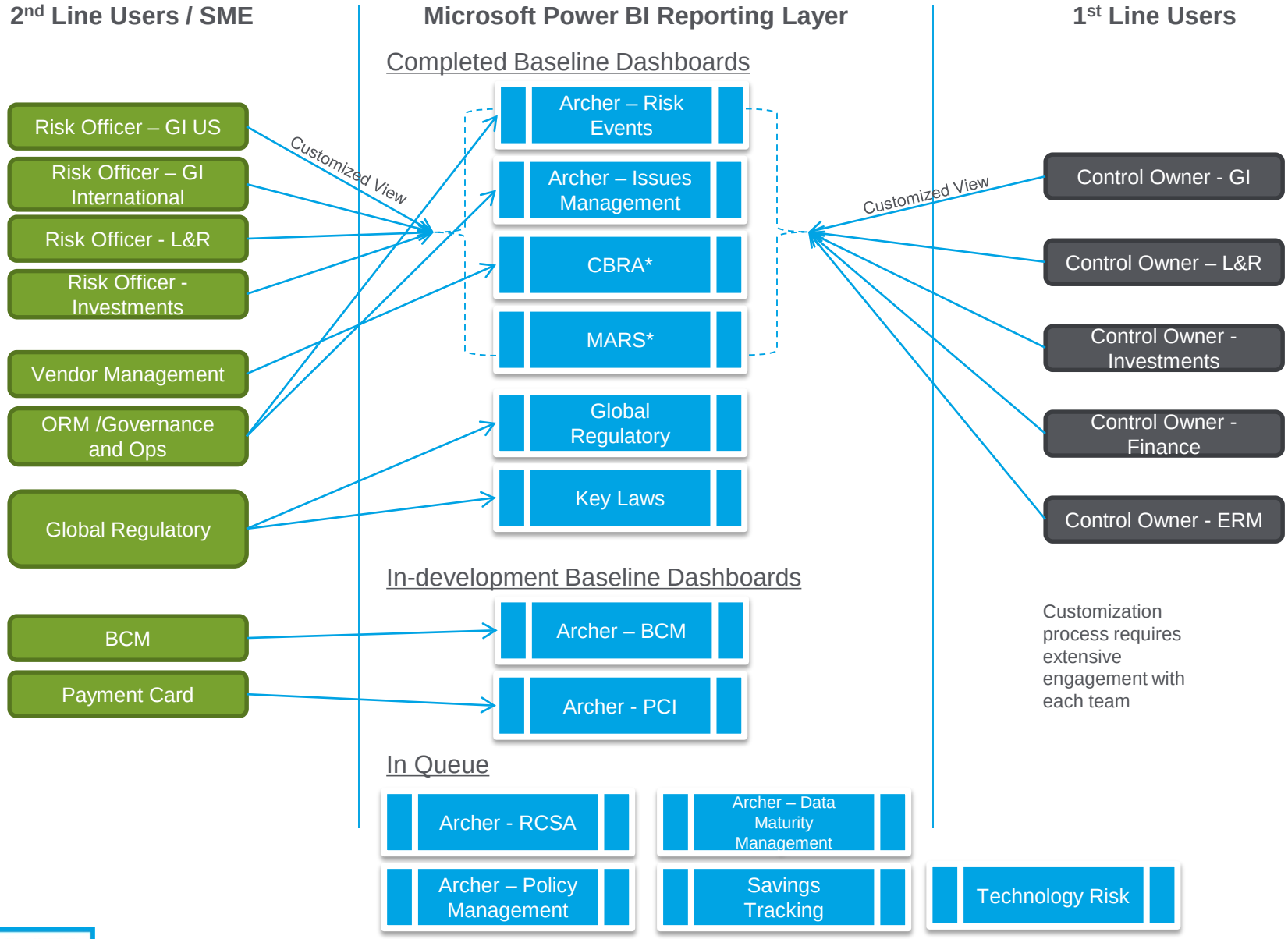
- Comprehensive reporting on all GRC data sources
- Integrated GRC Reporting (PRC and other taxonomies)
- Drill through hierarchies and taxonomies for custom viewpoints
- Point-in-Time reporting
- Quick navigation to archer solutions
- Automated and customized to stakeholders needs

GRC Data Warehouse / BI Reporting – High Level Architecture Diagram

- GRC Data Warehouse provides the opportunity to build out integrated reporting from all GRC data sources with current and historical point-in-time snapshots

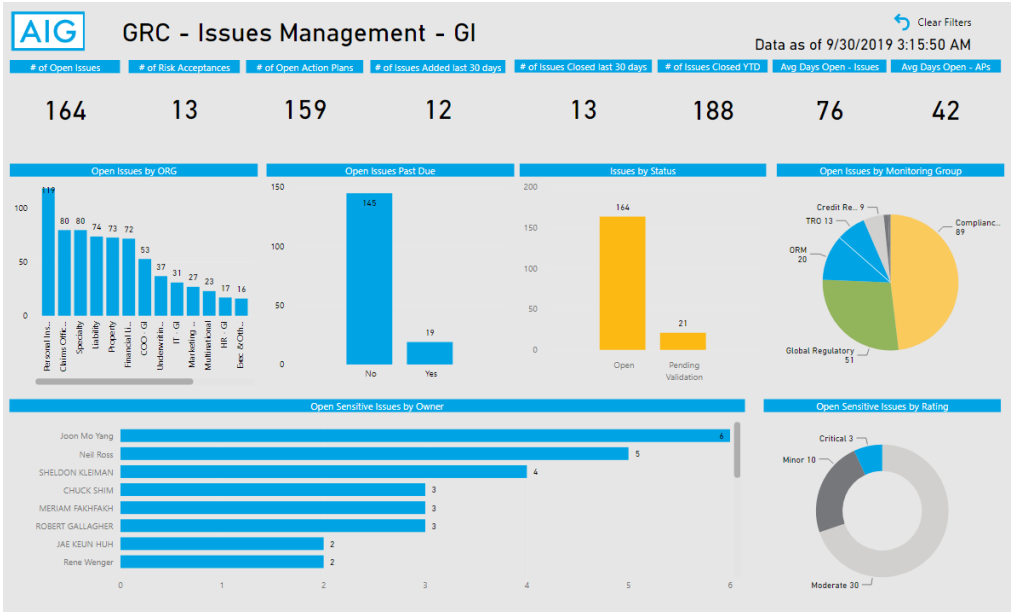


Customized GRC Reporting



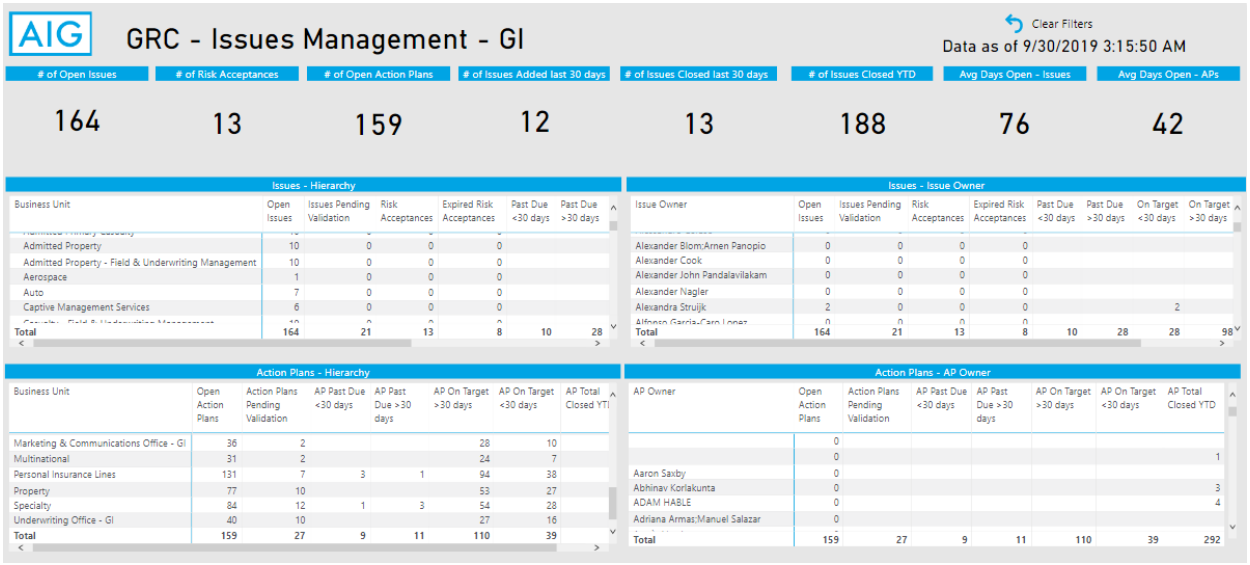
Legend: (*) Did not have prior reporting interface

Customized 1st Line Dashboards

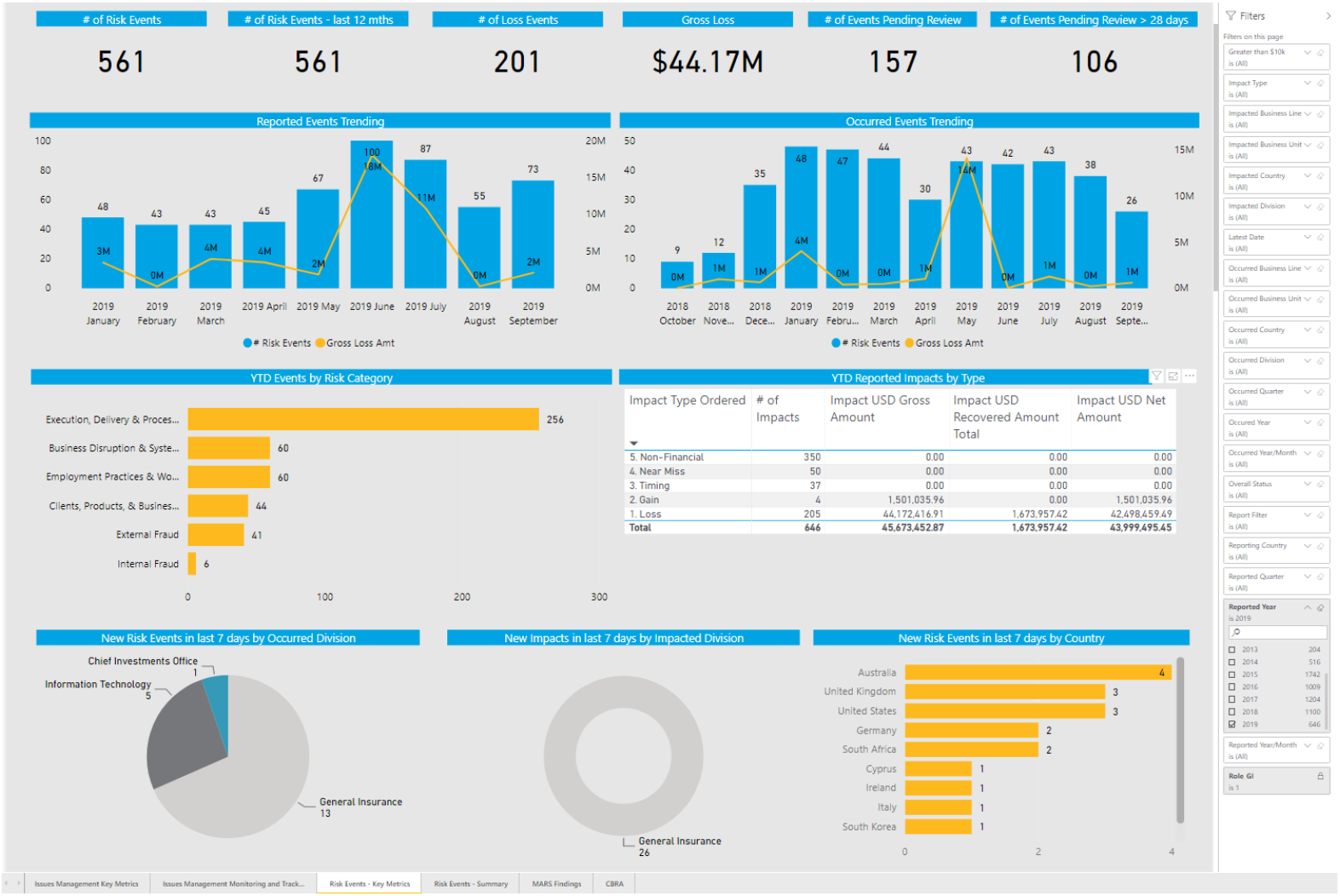


Reporting

Monitoring



Customized 1st Line Dashboards



Customized 1st Line Dashboards

Thank you!

Third Party Risk Management

October 10th, 2019

Kimberly Fix, Managing Director
Operational Risk Management
AIG Enterprise Risk Management

212.770.6752
kimberly.fix@aig.com
175 Water St., NY, NY

Victor Miller, SVP
Third Party Risk Management Program Head
AIG Enterprise Risk Management

704.553.5120
Victor.miller@aig.com
Charlotte, NC

Third Party Risk Management
Instructors Bio

- **Kimberly Fix**

Kimberly Fix is the Head of AIG Operational Risk Management and Third-Party Risk Management and co-leads Enterprise Business Resiliency. Kimberly joined AIG's Enterprise Risk Management team in 2012 in preparation for SIFI designation, leading initiatives to enhance risk management focus across global corporate control functions. She was also responsible for implementing the risk management program in the shared service centers for claims and operations globally. Prior to joining AIG, Kimberly spent 21 years at Citigroup, where she was responsible for numerous enterprise-wide product, system and process implementations, including the launch of web-based bank account management products, electronic on-boarding for corporates and the creation of an Information Technology information security program & organization. Kimberly has held certifications from Carnegie Mellon University's Software Engineering Institute in the reengineering methodology for software process improvement and attended New York University.

- **Victor Miller**

Victor Miller heads the Third-Party Risk Management function and has stewardship of the third-party risk assessment process and associated toolset in partnership with AIG Control Groups and serves as the interface for regulatory reviews and examinations. Other activities include: risk aggregation and escalation, risk analysis and metrics, and training in relation to TPRM requirements as well as the rollout of tools and related processes. He has been with AIG since October 2015. Victor holds an MBA from Webster University and a BS in Mechanical Engineering. He completed certifications in Six Sigma as a Black belt (ASQ) , "Agile" Scrum Master, and ITIL operational effectiveness.

Agenda

- TPRM - Where we are today?
- Policy and Standards Update
- Operating Model Overview
- Entry Points
- Process Overview
- Due Diligence Requirements by Category
- Due Diligence: Initial & Refresh Requirements
- Adoption
- Appendix

Where we are today

- ✓ Mandatory risk assessment based on business defined standards and corporate policy
- ✓ Due Diligence activities are determined based on the level of exposure to third party risks
- ✓ Integrated IT's review & challenge process (IRIS) for onboarding/renewing technology with procurement, IT security and TPRM for all technology requests globally
- ✓ Control groups and business (Contract Owner) are responsible to complete the required due diligence activities, plus Exit Strategy when required
- ✓ Expanded coverage of technology control assessment for all third parties
- ✓ Transparency provided by CBRA ensures risk assessments are completed (risk related decision points) prior to contract
- ✓ Fewer high risk rated third parties; realistic category based risk assessments
- ✓ Regulatory compliance (GDPR, NYDFS, MAS, FSA, FCA)

AIG

TPRM Policy & Standards Key Points

- Revised TPRM Policy and Standards effective as of December 2017 and anchored to New York Department of Financial Services (NYDFS) Regulation.

- Leveraged categorization of third parties and focus on what they do for or on behalf of AIG when assessing and monitoring risk
  - To that effect, businesses lead the definition of and will drive adoption of Standards by Third Party Category, which include:

Category	TPRM Standard Owner (Organization)
Vendors	Michael O'Malley (GS&PS)
Affinity Sponsors	Laurie Tribuiani (GI);
Brokers, Independent Agents, and Travel Agents	Steve Grabek (GI) & Kimberly Hutkowski (GI); Mark Childs (L&R)
Managing General Agents, Program Administrators, and Delegated Underwriting Authority	Jeffery Miller (Lexington – Personal Lines) /TBD
Third Party Administrators (including Claims)	Wendy Boyd (GI) & Nicola Dodd (GII); Mark Childs (L&R)
Third Party Risk Management (Other)	Victor Miller
Reinsurance	Michael Zeller

- Focuses on risk management of third parties and excludes business related activities such as Business Performance Monitoring (SLAs, Business Reviews, etc.)

Third Party Risk Management (TPRM) Operating Model Overview

TPRM

TPRM defines AIG's third party regulatory obligations via Policy & Standards, has stewardship of the third party risk assessment process and associated toolset in partnership with AIG Control Groups, and serves as the interface for regulatory reviews and examinations. Other activities include: risk aggregation and escalation, risk analysis and metrics, and training in relation to TPRM requirements as well as the rollout of tools and related processes.

First Line:

AIG **Business Units and Functions*** are accountable for owning and managing the risks that exist in their respective areas per defined third party risk management framework (e.g. TPRM Policy and Standards).

*Business Units and Functions:

- General Insurance,
- Life & Retirements,
- Investments,
- Corporate Functions

Control Groups:

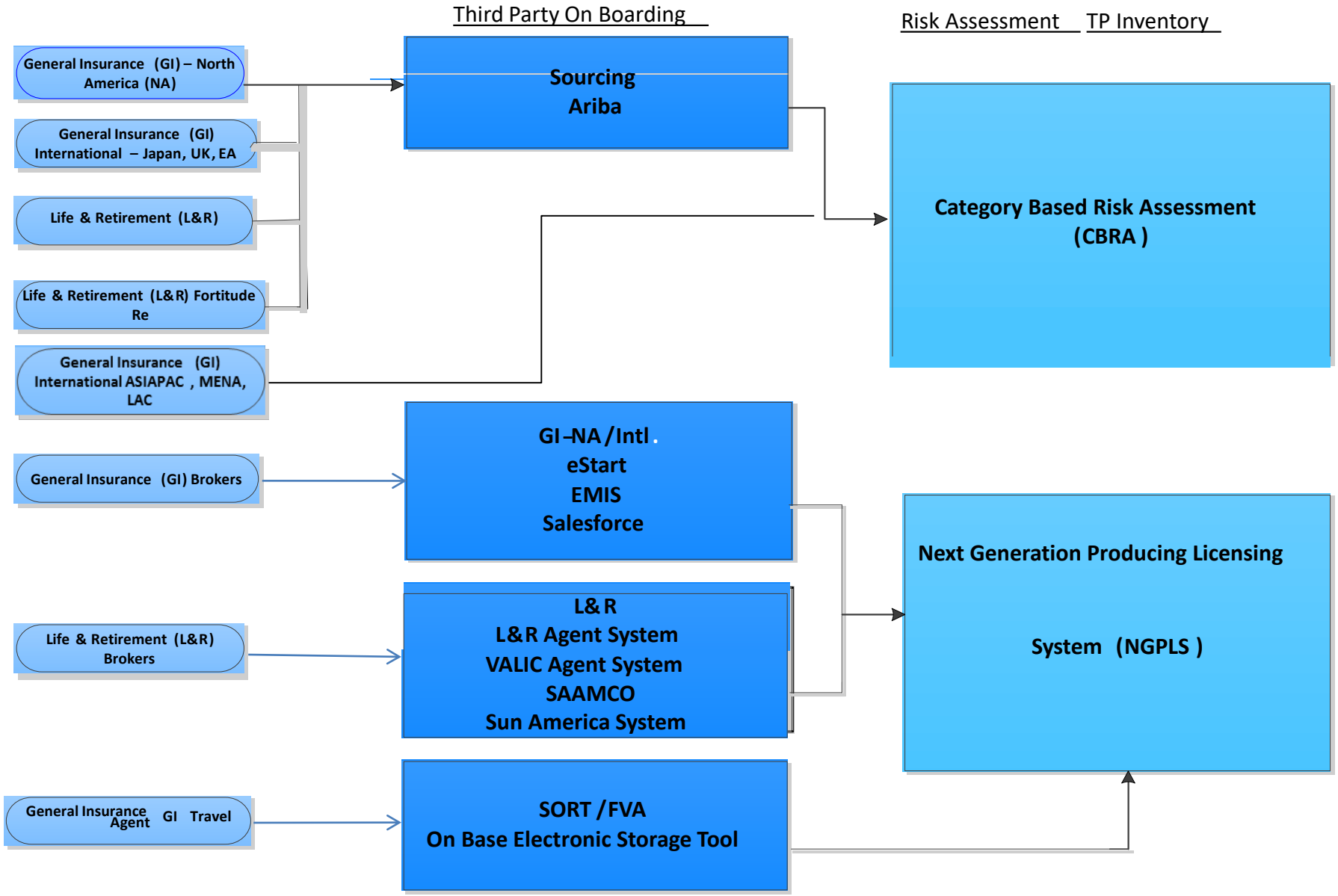
BU/GF Third Party Governance teams and Procurement in partnership with **Third Party Category Owners*** support and are accountable for overseeing and challenging the first line in the effective management of their risks and driving convergence of TPRM requirements across regions.

*Third Party Category Owners:
Vendors, MGAs/PAs/DUAs, TPAs (Claims & Non-Claims), Affinity Sponsors, and Brokers/Independent Agents/Travel Agents
Reinsurance

Control Groups* are responsible for providing guidelines for assessing and managing exposure for their specific risk area. They partner with TPRM to define and tailor risk assessment questions based on changes to regulatory landscape.

*Control Groups:
Compliance and Legal, Information Security, Business Continuity, Global Security, and Financial Viability

TPRM Entry Points



TPRM Process Overview

***Brokers, Independent Agents, and Travel Agents are high volume and highly compliant third party types that do not go through the CBRA process**

Business-Driven Pre-Risk Assessment Onboarding Activities

Minimum Requirements

C Risk Assessment — Determine sub-exposure inherent risks and identify which due diligence activities must be performed; notify/instruct the user and appropriate control groups as necessary.

Due Diligence, Ongoing Due Diligence, Exit Strategy, and Risk Acceptance

Due Diligence including Ongoing (determined by risk)

- C • Sanctions Screening
- Financial Viability Assessment
- Information Security Assessment
- Business Continuity Assessment
- IRIS Approval (New Technology)
- Software Security Assessment

Control Group Driven Activity
Notifications sent to request submitter, on-behalf of (where applicable), and Control Group to perform identified due diligence, including refresh

- Background Checks
- Licensing Validation
- Anti-Money Laundering
- Anti-Corruption
- Third Party Code of Conduct

C Exit Strategy (High-Elevated Risk)

C Risk Acceptance (where applicable)

Contract Related — All contracts with third parties must be reviewed and approved by legal or utilize an existing template pre-approved by legal.

C Third Party Inventory — All third parties must be recorded and managed as part of an inventory. CBRA maintains an inventory of third parties that have been risk assessed via CBRA. All legacy third parties must be risk assessed via CBRA over time. The policy provides more details regarding legacy third party requirements.

Business Oversight & Performance Monitoring — The Contract Owner and business are responsible for ongoing performance monitoring of their third parties, particularly those that are High or Elevated risk. The business should determine what factors to consider in performance monitoring, for example including Service Level Agreement's customer complaints, defect, risk events etc. C

Independent Reviews — Independent Reviews of High and Elevated third parties should be periodically performed to ensure effective performance monitoring and risk management of the third party by the business. Your business management should determine options for conducting the independent review.

AIG

C Denotes activity or artifact executed or captured in CBRA

TPRM Policy & Standards: Due Diligence Requirements by Category

Due Diligence	Third Party Category (Type)						
	Vendor	Affinity Sponsor	Broker, Independent Agent, Travel Agent	MGA / PA / DUA	TPA	Reinsurance	Other
Information Security*	✓	✓	✓	✓	✓	✓	✓
Business Continuity*	✓	✓	NR	✓	✓	✓	✓
Financial Viability Assessment*	✓	✓	NR	✓	✓	✓	✓
Background Checks	✓	✓	✓	✓	✓	✓	✓
OFAC/Sanctions Screening	✓	✓	✓	✓	✓	✓	✓
Third Party Code of Conduct	✓	✓	✓	✓	✓	✓	✓
Anti-Money Laundering	✓	✓	✓	✓	✓	✓	✓
Anti-Corruption	✓	✓	✓	✓	✓	✓	✓

*When specified for a Category, due diligence is driven by level of risk and will be detailed on the next slide.
NR – Not Required

TPRM Policy Due Diligence: Initial & Refresh Requirements

Control Groups	Due Diligence (Initial)					
TCO	Information Security*	Information Security Inherent Risk	High	Elevated	Moderate	
	Business Continuity	Business Continuity Inherent Risk	High	Elevated		
FVA	Financial Viability Assessment	Overall Inherent Risk	High	Elevated		
IT Security	Software Security*	Prompted based on responses to specific Software Security questions.				
Global Security	Background Checks	Mandatory for all third parties unless the local laws/regulations prohibit or if they have a background check waiver (e.g. Waived Vendor Program).				
Global Compliance	OFAC/Sanctions Screening	Completed during submission of CBRA				
	Third Party Code Of Conduct	Must be issued for every engagement				
	Anti-Money Laundering	Applicable to third party distributors, who are defined as individuals and entities with which AIG has a formal, written agreement to market and distribute AIG's products and services to customers.				
	Anti-Corruption	Applicable to any individual or entity with whom AIG enters into a business relationship (other than an arms-length transaction) involving the sale of personal lines insurance to a customer. Third Parties do not include joint venture partners and vendors providing AIG with goods of a modest value or routine office.				
Control Groups	**Ongoing Due Diligence (Refresh)**					
TCO	Information Security*	Information Security Inherent Risk	High	Elevated	Moderate	Low
		Refresh Frequency	1-year	3-years	5-years	N/A
	Business Continuity	Business Continuity Inherent Risk	High	Elevated	Moderate	Low
		Refresh Frequency	1-year	1-year	N/A	N/A
IT Security	Software Security Assessment	Inherent Risk	High	Elevated	Moderate	Low
		Refresh Frequency	Once every 2 years	Every 3-5 years	Every 5+ years	Ad-Hoc requests accommodated
FVA	Financial Viability Assessment	FVA Risk Rating (Initial Due Diligence)	High	Elevated	Moderate	Low
		Refresh Frequency	1-year	2-years	N/A	N/A
Global Security	Background Checks	Mandatory for all third parties unless the local laws / regulations do not allow these checks				
		Refresh Frequency	Must be refreshed every five years for active Third Parties (i.e. inforce contracts)			
Global Compliance	OFAC/Sanctions Screening	Periodic sanctions screening is required				
		Refresh Frequency	Preferably on a monthly basis. Event driven frequency is prior to sending payments to third parties, or when third party information (i.e. name or address) changes			
	Third Party Code of Conduct	Required to be reissued only if there is a change involving the third party (e.g. Acquisitions)				
	Anti-Money Laundering	Applicable to third party distributors, who are defined as individuals and entities with which AIG has a formal, written agreement to market and distribute AIG's products and services to customers.				
		Refresh Frequency	1-year for L&R Agents and Annuity Brokers			
	Anti-Corruption	Applicable to any individual or entity with whom AIG enters into a business relationship, other than an arms-length transaction involving the sale of personal lines insurance to a customer. Third Parties do not include joint venture partners and vendors providing AIG with goods of a modest value or routine office services.				

Exit Strategy is required for ALL overall high or elevated inherent risk engagements and refreshed annually.

Adoption

- All new engagements / contracts to use CBRA for risk assessment effective December 2017.

- Legacy Third Party Remediation:

  - Previously risk assessed (via any method) as high or elevated risk OR never previously assessed (unknown risk) – CBRA risk assessment was required by December 31, 2018

  - Previously risk assessed (via any method) as moderate,– CBRA risk assessment required by December 31, 2019

  - All auto-renewal contracts or “evergreen” contracts – CBRA risk assessment required by December 31, 2019

  - Previously risk assessed (via any method) as low risk – CBRA risk assessment required upon contract renewal

Thank you!

AIG

AIG

Third Party Risk Management

CBRA Model Third Party Consolidated Insurance Segmentation View

October 2019

Third Party Risk Management - CBRA Model Third Party Consolidated Insurance Segmentation View

Instructors Bio

Kimberly Fix

Kimberly Fix is the Head of AIG Operational Risk Management and Third-Party Risk Management and co-leads Enterprise Business Resiliency. Kimberly joined AIG's Enterprise Risk Management team in 2012 in preparation for SIFI designation, leading initiatives to enhance risk management focus across global corporate control functions. She was also responsible for implementing the risk management program in the shared service centers for claims and operations globally. Prior to joining AIG, Kimberly spent 21 years at Citigroup, where she was responsible for numerous enterprise-wide product, system and process implementations, including the launch of web-based bank account management products, electronic on-boarding for corporates and the creation of an Information Technology information security program & organization. Kimberly has held certifications from Carnegie Mellon University's Software Engineering Institute in the reengineering methodology for software process improvement and attended New York University.

Victor Miller

Victor Miller heads the Third-Party Risk Management function and has stewardship of the third-party risk assessment process and associated toolset in partnership with AIG Control Groups and serves as the interface for regulatory reviews and examinations. Other activities include: risk aggregation and escalation, risk analysis and metrics, and training in relation to TPRM requirements as well as the rollout of tools and related processes. He has been with AIG since October 2015. Victor holds an MBA from Webster University and a BS in Mechanical Engineering. He completed certifications in Six Sigma as a Black belt (ASQ) , "Agile" Scrum Master, and ITIL operational effectiveness.

Table of Contents

Third Party Segments: Insurance – Underwriting: MGA / PA / DUA

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Managing General Agent / Program administrator				
Sub-Segment	Delivery Type	Class of Service	Definition	Inherent Risk Range
Underwriting	Retail	Underwriting, Policy Administration, and Claim Administration, Handling, & Settlement	An Individual or business entity appointed by the Company to solicit applications from agents or applicants for insurance contracts, Underwrite risks and negotiate insurance contracts on behalf of the Company and, if authorized by the Company to bind and countersign insurance contracts. Depending on the type of service appointment, a MGA / PA may perform one of many functions that are normally performed by the hiring Company such as but not limited to: • Sub-contracting with independent agents for business placements • Negotiate commissions, • Issue polices • Process endorsements • Collect policy premiums • Complete regulatory reporting	**ELEVATED to HIGH**

Third Party Segments: Insurance – TPA: Administration / Claims

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Third Party Administrator				
Sub-Segment	Delivery Type	Class of Service	Definition	Inherent Risk Range
Administration	Store/Call Center	Underwriting-quoting and /or Binding	An entity acting as intermediary that provides: policy quoting, binding, premium calculation, policy endorsement, new/renewal application inspection, bordereaux transactions, mid-term adjustments including policy proposals and submissions.	**ELEVATED to HIGH**
Policy Administration & Fulfillment	Store/Call Center	Policy Issuance and / or Premium Collection & Refunds Mid Term Adjustments / endorsements-Financials	An entity that primarily provides administrative services such as: • review of premium lapses, renewals and reinstatements, premium audits and customer survey and also support policy related printing, data entry and imaging, policy technical help desk, address change and complaint handling. • premium collection, remittances, review of premium lapses and premium audits and also supply customer survey, policy technical help desk, billing support and payment processing. • financial based policy endorsements, mid-term adjustments, address change, review of premium lapses, renewals and reinstatements and also support premium audits, customer survey and policy technical help desk.	**ELEVATED to HIGH**
Policy Administration & Fulfillment	Store/Call Center	Mid Term Adjustments / Endorsements-Non Financials and / or Administration-Imaging / printing/ and / or Data Entry	An entity that primarily provides administrative services such as: • non-financial policy endorsements, mid-term adjustments, address change, renewals and reinstatement and also supply premium audits, customer survey, policy technical help desk and complaint handling. • Renewals, reinstatements and policy related printing, imaging and PDFs. • data entry for premium collection, remittances, billing, payment processing, and compliant handling.	**LOW to MODERATE**

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Third Party Administrator				
Sub-Segment	Delivery Type	Class of Service	Definition	Inherent Risk Range
Policy Administration & Fulfillment	Store/Call Center	Support Services – Compliant Handling	A company who on our behalf conducts compliant handling and dispute resolution.	**ELEVATED to HIGH**
Policy Administration & Fulfillment	Store/Call Center	Support Services – Customer Support Help lines	A company providing technical and customer support to policy holders on the various aspects of the product.	**LOW to MODERATE**
Assist Services – Medical Clinics	Retail Store	Specialty Services	A Company with whom we enter into a relationship to provide *medical assistance* services for our insureds.	**LOW to MODERATE**
Assist Services -Other	Retail Store	Specialty Services	A Company with whom we enter into a relationship to provide *management assistance* services for our insureds.	**LOW to MODERATE**
Repair Network - Warranty	Retail Store	Specialty Services	An agreement entered into with an approved network of service providers to provide repairs/ replacement of equipment, applies to: • *Auto* • *Warranty*	**LOW to MODERATE**
Technical Consultancy Services	Retail Store	Specialty Services	The firm or Individual assigned to support underwriting areas to provide technical services in the following categories: • Medical expert • Risk assessment / management/Loss control/ Actuaries • Salvagers • Surveyors / Appraisers/ Engineers • UW Independent Loss Assessor / Adjustor	**LOW to MODERATE**

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Third Party Administrator (Claims)				
Sub-Segment	Delivery Type	Class of Service	Definition	Inherent Risk Range
Claims Administration	Store/Call Center	Claim Handling	A Third Party Administrator who is contracted by AIG to receive, adjudicate and settle insurance claims made against the various policies issued by our company within certain defined levels of authority and in accordance to specified service level standards. The TPA is not issuing payments. Payments are referred to AIG for processing.	**ELEVATED to HIGH**
Claims Services	Store/Call Center	First Notice of Loss and Claim administration	A Program Administrator may perform one of many tasks normally performed by the Company. These include but are not limited to, sub-contracting with independent agents for placement of business, negotiating commissions, issuing policies, processing endorsements, collecting policy premiums or being responsible for completion of regulatory reports.	**LOW**
Claims Services	Store/Call Center	Claims Repair Network	An agreement entered into with an approved garage network of service providers to provide repairs/ replacement, applies to: • Auto • Warranty	**LOW**
Claims Services	Store/Call Center	Claims Specialist services – Technical Consultancy services	Claims specialist services – includes the following: Independent Loss assessor Salvagers Surveyors / appraisers / engineers Medical experts	**LOW**
Preferred Provider Organization Networks	Store/Call Center	PPO Networks	PPO Networks contract financial discounts with Medical providers, reducing the amount due from the billed amount or due under law or regulation for the medical services provided to claimants.	**LOW**

Third Party Segments: Insurance – Distribution Partners: Brokers / Independent Agents / Travel Agents / Affinity Partners

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Independent Agent				
Sub-Segment	Delivery Type	Class of Service	Definition	Risk Range
Distribution Partner	Direct Marketing/ Indirect Marketing	Sales	Independent Agents are primarily distributors of insurance products for various insurers in the Retail market place to their customers and clients. • essentially "matchmakers" who match the risk mitigation insurance needs of their customers with appropriate matching insurance products of insurers. • a key role in providing underwriting information to insurers and also support in the post insurance sale customer service functions.	**LOW to MODERATE**

SEGMENT: Introducer Representative				
Sub-Segment	Delivery Type	Class of Service	Definition	Risk Range
Distribution Partner	Direct Marketing/ Indirect Marketing	Sales	Independent Agents are primarily distributors of insurance products for various insurers in the Retail market place to their customers and clients. They play a key role in providing underwriting information to insurers and also support in the post insurance sale customer service functions.	**LOW**

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Travel Agent				
Sub-Segment	Delivery Type	Class of Service	Definition	Risk Range
Distribution Partner	Direct Marketing/ Retail Store	Sales	A licensed retailer or supplier that sells, furnishes, arranges and provides tourism related services, including packaging tours and/or offering travel insurance for trip protections.	**LOW**

SEGMENT: Affinity Sponsor				
Sub-Segment	Delivery Type	Class of Service	Definition	Risk Range
Distribution Partner	Direct Marketing/ Retail Store	Sales	An organization that has a proprietary customer base to which they provide goods and/or services, such as a bank, retailer, utility, mortgage lender, or credit card issuer. The Sponsor typically has brand affinity with its customer base and a mechanism for collecting payments. AIG contracts with Sponsors to gain access to their customer base via a variety of sales channels (e.g., direct mail, telemarketing, in-branch, customer service, internet channels) for the purpose of cross-selling insurance products. (A typical sponsor agreement will cover such terms as commission structure, roles and responsibilities of the parties, use of the data, customer ownership, runoff rights, marketing rights to the policy holder data, term and termination of the contract.)	**LOW to MODERATE**

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Broker				
Sub-Segment	Delivery Type	Class of Service	Definition	Risk Range
Distribution Partner	Direct Marketing/ Retail Store	Sales	An insurance broker is a person or entity which acts as an independent intermediary to bring parties seeking insurance together with insurance providers. They solicit, negotiate or sell an insurance contract on behalf of an insured. Unlike a Managing General Agent or Program administrator, a broker is not granted underwriting authority: therefore they may not obligate an insurer to provide coverage prior to the insurer's consent.	**LOW to MODERATE**

Third Party Segments: Insurance – Reinsurance

Category Based Risk Assessment (CBRA) Model

Third Party Segments: Insurance – Consolidated View

SEGMENT: Reinsurers - Reinsurance Companies				
Sub-Segment	Delivery Type	Class of Service	Definition	Risk Range
Reinsurer	Direct Marketing/ Retail Store	Sales	A Reinsurance Company is an entity that provides reinsurance to an insurance company. AIG purchases reinsurance from reinsurance companies to diversify risk consistent with risk and profitability objective and to improve capital fungibility.	**LOW to MODERATE**
Reinsurance Intermediary	Direct Marketing/ Retail Store	Sales	An unaffiliated entity that solicits, negotiates or places reinsurance cessions or retrocessions on behalf of a ceding insurer without the authority to bind reinsurance on behalf of the insurer. Unlike a Managing General Agent, a Reinsurance Intermediary is not granted the authority to bind coverage; therefore they may not obligate an insurer to cede reinsurance prior to the insurer's consent.	**LOW to MODERATE**

Third Party Segments: Vendor – Consolidated View

Proposed: Vendor Risk Profiles

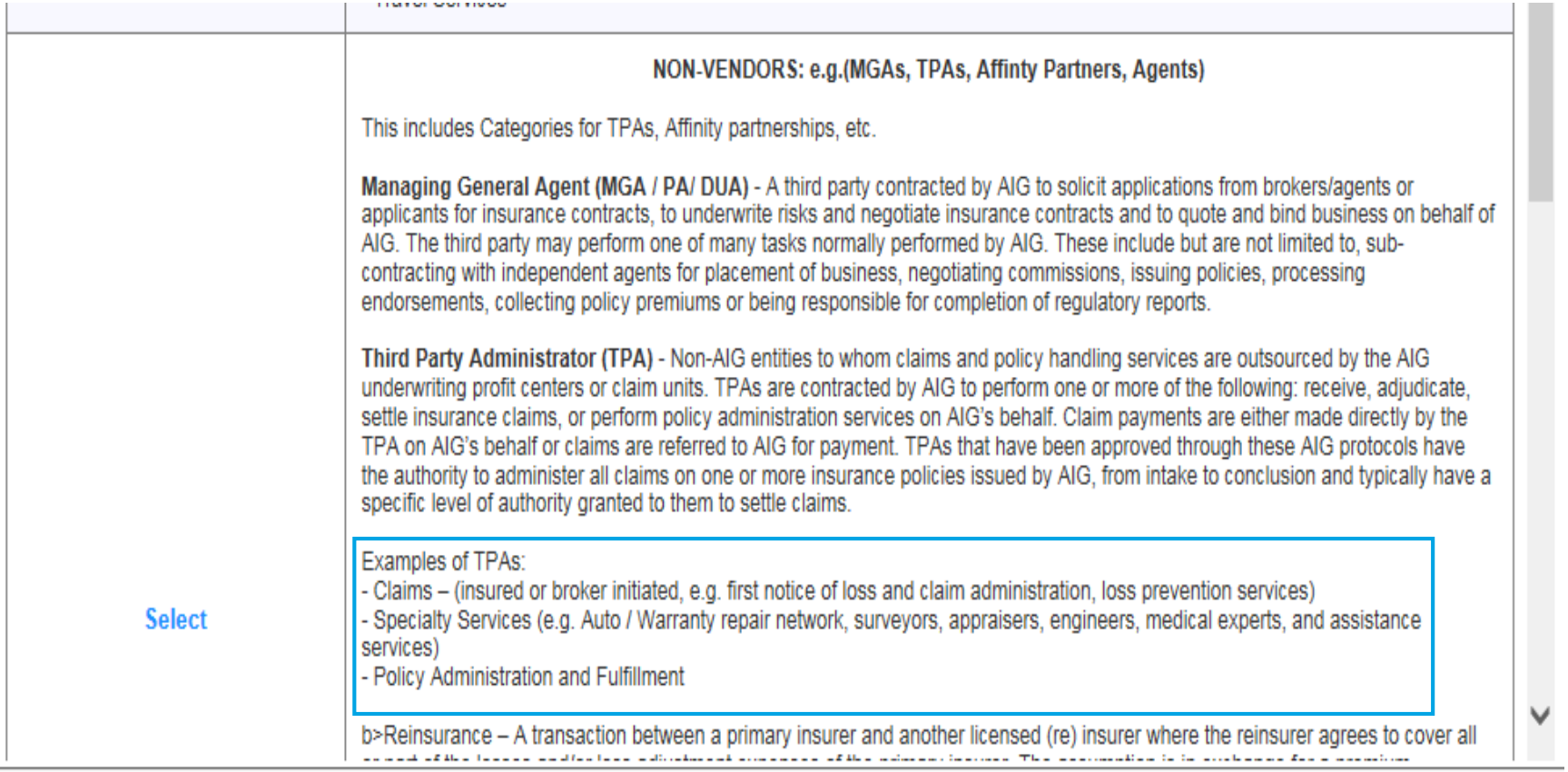
Risk Profile Attributes				
Category	**Sub-Category**	**Service Area Segmentation**	**Service Delivery Mechanism**	**Risk Probability Range (Low, Moderate, Elevated, High)**
Client Services Hardware Market Data Prof Svcs Non Tech	• Document storage services-Data archiving services • Records Management Services-Document destruction services • Data Center Hosting/Outsourcing Svcs-Data center services • Insurance & Compliance Information (AIG) - Market data-Insurance & Compliance Information • Finance, Tax & Accounting Svcs-Banking and investment • HR Services-Healthcare Services	Supplier (Non-Preferred)	• Retail store / Off-site handling– not AIG premises • Online web platform–Third Party controlled • On-site attendance / Data Handling • Service center	**Elevated to High**
Client Services, Hardware, Legal, Market Data, Network/Telecomm, Prof Svcs Non Tech, Prof Svcs Tech, Software,	• Legal Support / Attorney • Preferred Provider Organization (PPO) Network • All excluding the above Sub-Categories for Client Services, Hardware, Market data and Prof Svcs Non Tech	Supplier (Non-Preferred)	• Retail store / Off-site handling – not AIG premises • Online web platform – Third Party controlled • On-site attendance / Data Handling Service center	**Low to Elevated**
Client Services, Contingent Resource Mgmt, Marketing Services, Real Estate Services, Travel	All	Supplier (Non-Preferred)	• Retail store / Off-site handling – not AIG premises • Online web platform – Third Party controlled • On-site attendance / Data Handling • Service center	**Low**

Source: The Federal Reserve Regulatory Group (FRRG); the National Association of Insurance Commissioners (NAIC); The Federal Insurance Office (FIO)

Third Party Segments: System Screen shots

Third Party Segments: System Screen shots

New CBRA request page – Starting point



NON-VENDORS: e.g.(MGAs, TPAs, Affinty Partners, Agents)

This includes Categories for TPAs, Affinity partnerships, etc.

Managing General Agent (MGA / PA/ DUA) - A third party contracted by AIG to solicit applications from brokers/agents or applicants for insurance contracts, to underwrite risks and negotiate insurance contracts and to quote and bind business on behalf of AIG. The third party may perform one of many tasks normally performed by AIG. These include but are not limited to, sub-contracting with independent agents for placement of business, negotiating commissions, issuing policies, processing endorsements, collecting policy premiums or being responsible for completion of regulatory reports.

Third Party Administrator (TPA) - Non-AIG entities to whom claims and policy handling services are outsourced by the AIG underwriting profit centers or claim units. TPAs are contracted by AIG to perform one or more of the following: receive, adjudicate, settle insurance claims, or perform policy administration services on AIG's behalf. Claim payments are either made directly by the TPA on AIG's behalf or claims are referred to AIG for payment. TPAs that have been approved through these AIG protocols have the authority to administer all claims on one or more insurance policies issued by AIG, from intake to conclusion and typically have a specific level of authority granted to them to settle claims.

Select

Examples of TPAs:
- Claims – (insured or broker initiated, e.g. first notice of loss and claim administration, loss prevention services)
- Specialty Services (e.g. Auto / Warranty repair network, surveyors, appraisers, engineers, medical experts, and assistance services)
- Policy Administration and Fulfillment

b>Reinsurance – A transaction between a primary insurer and another licensed (re) insurer where the reinsurer agrees to cover all

Third Party Segments: System Screen shots

Category selection: TPA (Policy & Admin)

Commodity:

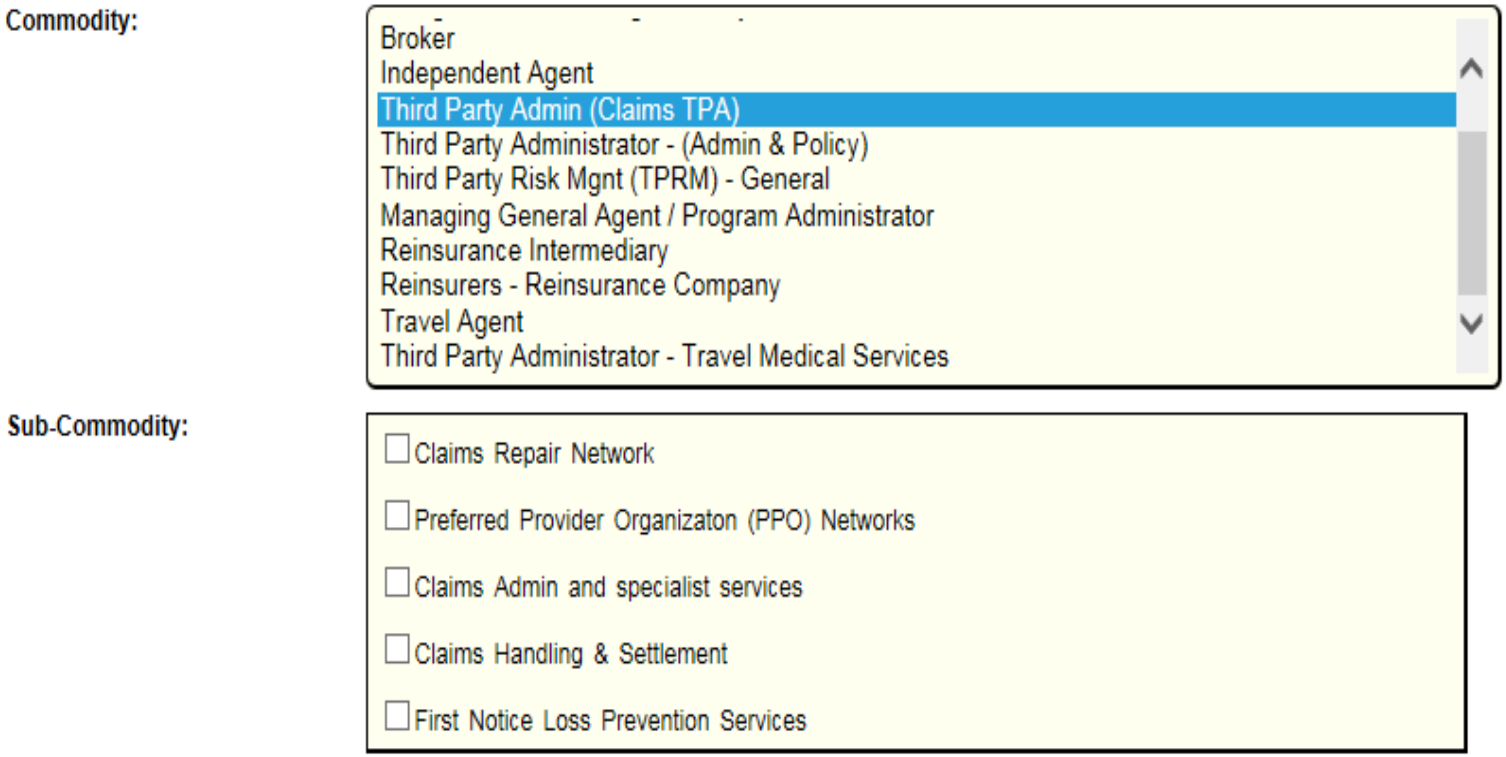
- Broker
- Independent Agent
- Third Party Admin (Claims TPA)
- **Third Party Administrator - (Admin & Policy)**
- Third Party Risk Mgnt (TPRM) - General
- Managing General Agent / Program Administrator
- Reinsurance Intermediary
- Reinsurers - Reinsurance Company
- Travel Agent
- Third Party Administrator - Travel Medical Services

Sub-Commodity:

- ☐ Administration & Fulfillment: Administration - Data Entry
- ☐ Administration & Fulfillment: Mid Term Adjustments / Endorsements - Financial & Non-Fin
- ☐ Administration & Fulfillment: Policy Issuance
- ☐ Administration & Fulfillment: Premium Collection, Refunds & Billing
- ☐ Administration & Fulfillment: Support Services
- ☐ Specialist Technical Services: Auto Repair Network
- ☐ Specialist Technical Services: Medical Experts
- ☐ Specialist Technical Services: Risk Assessment / Management
- ☐ Specialist Technical Services: Surveyors / Appraisers / Engineers
- ☐ Specialist Technical Services: Warranty Repair Network
- ☐ Technical Consultancy Services-UW Independent Loss Assessor / Adjustor

Third Party Segments: System Screen shots

Category selection: TPA (Claims)




AIG

Thank you!

AIG