Introduction

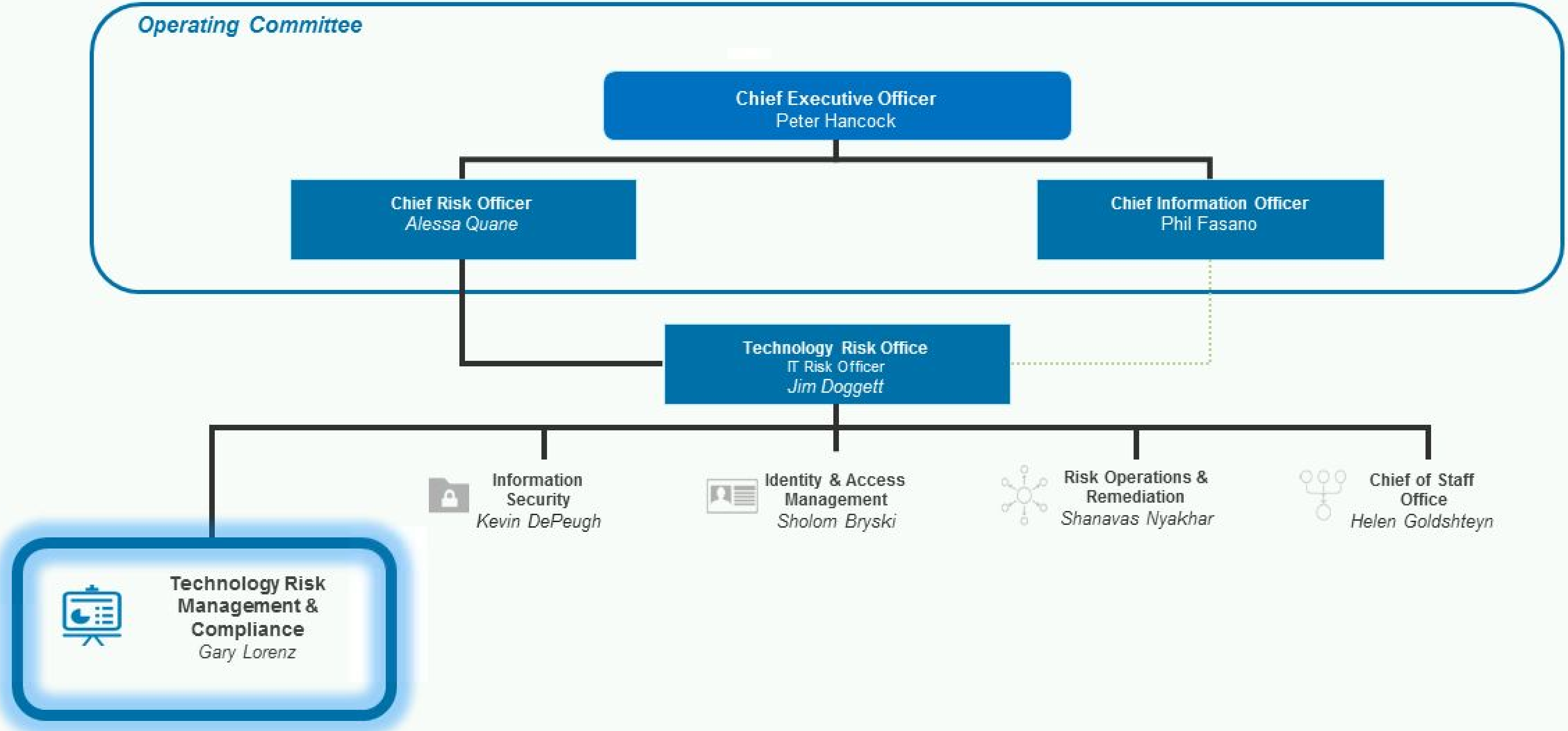
Gary Lorenz

Agenda

- Introduction to TRM – Gary Lorenz
- Govern – Lissa Edmondson
- Evaluate – Stephen Jarrett
- Act – Russell Lewis
- GRID – Amit Shrimavle / Vamshi Muppidi

How do we fit in?

The following diagram provides a high-level organizational structure of TRO, emphasizing TRM's position



Operating Committee

Chief Executive Officer
Peter Hancock

Chief Risk Officer
Alessa Quane

Chief Information Officer
Phil Fasano

Technology Risk Office
IT Risk Officer
Jim Doggett

Technology Risk Management & Compliance
Gary Lorenz

Information Security
Kevin DePeugh

Identity & Access Management
Sholom Bryski

Risk Operations & Remediation
Shanavas Nyakhar

Chief of Staff Office
Helen Goldshteyn

Four levers drive 2016 priorities

Automate	+	Eliminate	+	Consolidate	+	Simplify	=	2016 Priorities
Give our clients automated options for improved and cost-efficient access.		Eliminate outdated or unnecessary procedures.		Consolidate duplicate roles and processes.		Simplify how we work and clarify decision rights.		Rationalized, consolidated technology risk management.

TRM goals

1 Govern

- Simplify and consolidate committee structure, integrate with ERM governance
- Improve exception management process

2 Evaluate

- Simplify and automate 3rd party workflow for profiling / assessment processes
- Eliminate low-value risk assessments

3 Act

- Consolidate IT risk register / flows into ERM RR
- Enhance risk treatment oversight (remediation)
    - Reduce extensions for:
        - Open audit items
        - ExReq
- Reduce risk through oversight of Data Security Program

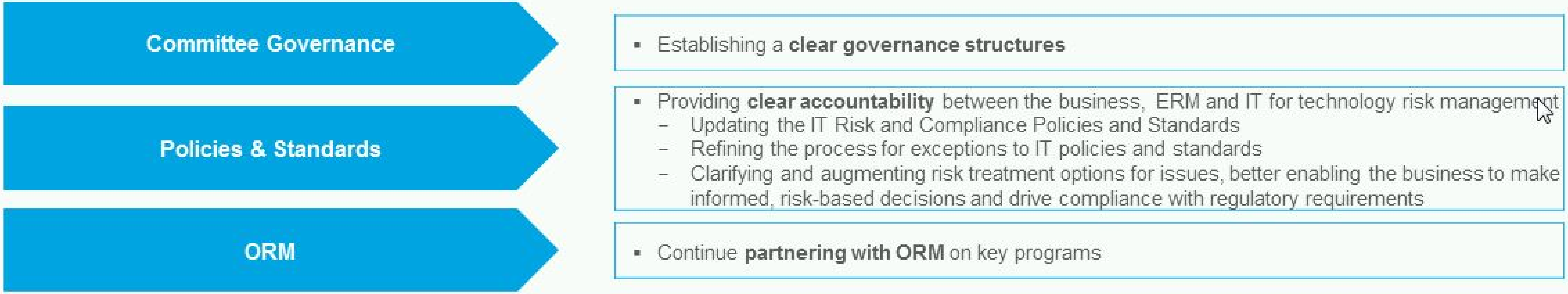
Governance Overview

- **Background**
  - Many financial services organizations have been broadening the scope of risk governance and management to include technology
  - This awareness is growing in the wake of highly publicized identity theft incidents and other security breaches, as well as legislation aimed at managing financial, market, and operational risk exposures
  - Technology Risk Management (TRM) is actively forming a cohesive risk-focused organization to monitor these incidents, while adding value to the business and working closely with the rest of ERM and IT

- **Components of TRM's governance to highlight today include:**
  1. **Committee Governance**
  2. **Policies & Standards**
  3. **Coordination with Operational Risk Management**

- **Other components to be discussed at a later date include:**
  - Regulatory guidance
  - Assessments

- **Upcoming initiatives include:**



Committee Governance

- Establishing a **clear governance structures**

Policies & Standards

- Providing **clear accountability** between the business, ERM and IT for technology risk management
  - Updating the IT Risk and Compliance Policies and Standards
  - Refining the process for exceptions to IT policies and standards
  - Clarifying and augmenting risk treatment options for issues, better enabling the business to make informed, risk-based decisions and drive compliance with regulatory requirements

ORM

- Continue **partnering with ORM** on key programs

Committee Governance: Overview

- **Background**
  - The IT Risk Committee (ITRC) was a legacy Committee established to manage IT risk management activities across AIG under the delegated authority of the Operational Risk Committee (ORC)
  - As a result, both committees were responsible for managing and overseeing technology risk at AIG

- **Approach**
  - Reduce the number of committees to establish a single committee that manages technology and operational risk to streamline processes and gain efficiencies, tentatively called the **Technology, Operational Risk & Control Committee (TORCC)**
  - Establish a global working group feeding into this committee, the **Technology Risk Steering group (TRS)**, which will meet a minimum of quarterly to facilitate discussion and issue resolution at a level below a committee
  - Partner with ORM and Legal to ensure the structure follows the precedents set by the current committee rationalization and Integrated Risk and Control Framework

- **Key Contributors**
  - Members / Contributors for the TORCC and the TRS are still being vetted
  - Members and key contributors for both groups will include participants from the businesses, IT, ORM, TRO, and Compliance as well as other groups

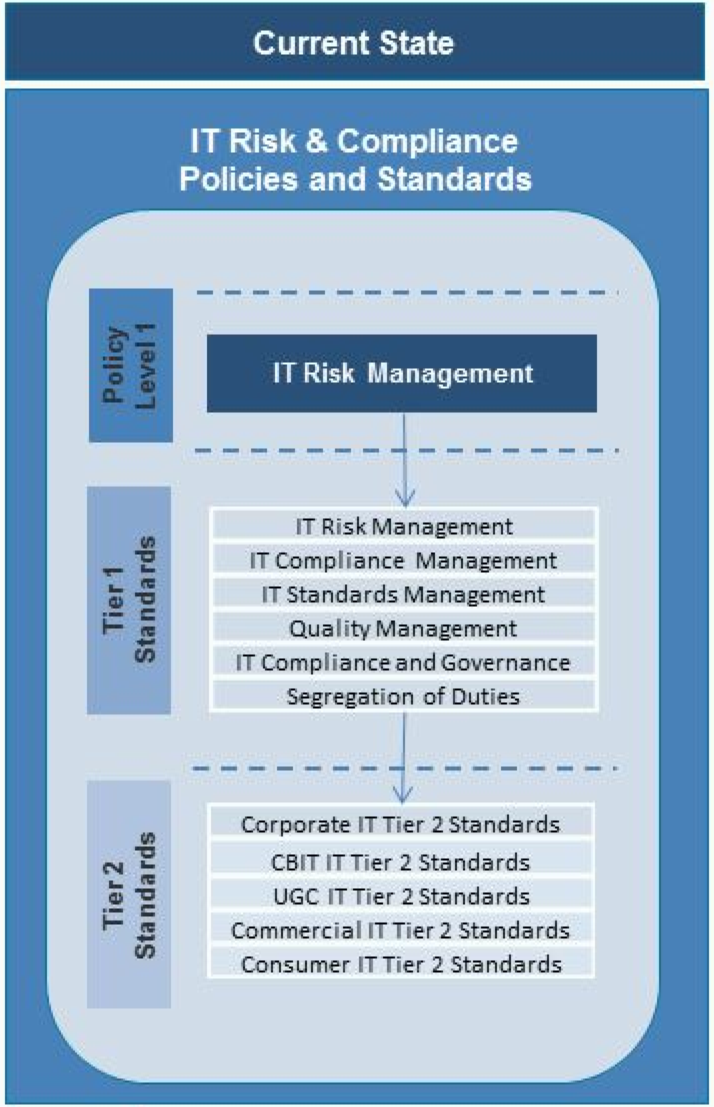
Committee Governance: Technology Risk Steering Group (TRS) Overview

- **Governance**
  - TRS receives authority from the Technology, Operational Risk & Control Committee (TORCC) and is intended to be the central working group for all of TRO
  - This group will be composed of senior management from TRO, ORM, IT, and the BUs

- **The diagram below outlines TRS' place in AIG's overall governance structure**

Committee	Responsibilities
Risk & Capital Committee (RCC)	• The governance committee of the AIG Board, which reports to and assists the Board in oversight of ERM • Provides strategic guidance to management regarding capital, approves issuances, investments, dispositions and other transactions in line with its authority
Group Risk Committee (GRC)	• AIG's senior risk and capital committee to assess all significant risk issues globally to protect AIG's financial strength, optimize its intrinsic value and to protect its reputation among key stakeholders • The GRC oversees AIG risk management committees as well as the risk management responsibilities delegated to AIG's business units and / or functions
Technology, Operational Risk & Control Committee (TORCC)	• Oversees the Technology & Operational Risk Frameworks and Architectures • Identifies Emerging Risks, Trends and Issues • Assesses and Evaluates AIG's Control Environment • Prioritizes Activities and Remediates Issues • Advances a Strong Risk Culture
Technology Risk Steering group (TRS)	▪ Review and monitor **technology risk tolerances and limits** ▪ Review the **TRO frameworks and governance** ▪ Review and monitor **escalated risk and policy exception** decisions ▪ Monitor **emerging technology risks, information security threats and compliance violations** throughout the organization ▪ Review all Technology Risk **policies & standards**

Policies and Standards



Current State

IT Risk & Compliance Policies and Standards

Policy Level 1

IT Risk Management

Tier 1 Standards

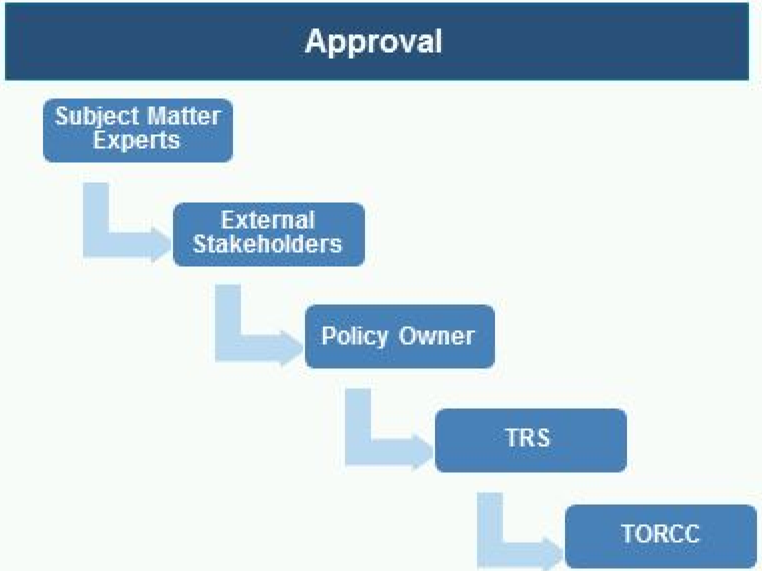
- IT Risk Management
- IT Compliance Management
- IT Standards Management
- Quality Management
- IT Compliance and Governance
- Segregation of Duties

Tier 2 Standards

- Corporate IT Tier 2 Standards
- CBIT IT Tier 2 Standards
- UGC IT Tier 2 Standards
- Commercial IT Tier 2 Standards
- Consumer IT Tier 2 Standards

Rationalization

- Simplify the structure
- Drive global adoption
- Eliminate Tier 2 Standards
- Align with Process Risk and Control (PRC) framework



Approval

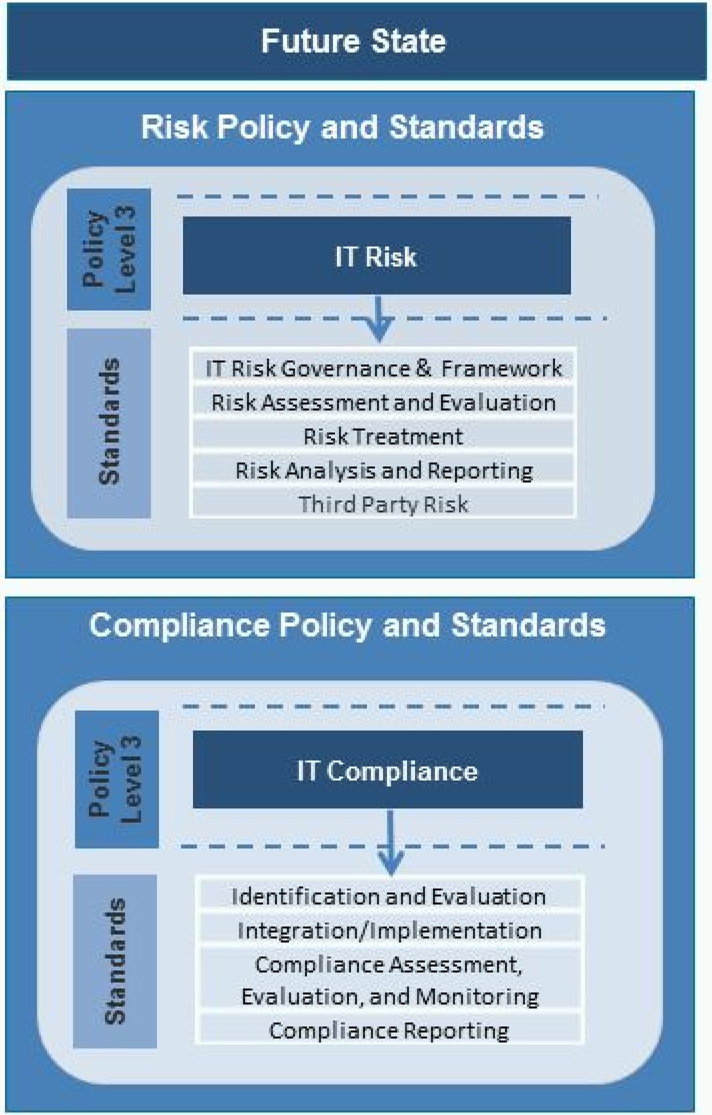
Subject Matter Experts

External Stakeholders

Policy Owner

TRS

TORCC



Future State

Risk Policy and Standards

Policy Level 3

IT Risk

Standards

- IT Risk Governance & Framework
- Risk Assessment and Evaluation
- Risk Treatment
- Risk Analysis and Reporting
- Third Party Risk

Compliance Policy and Standards

Policy Level 3

IT Compliance

Standards

- Identification and Evaluation
- Integration/Implementation
- Compliance Assessment, Evaluation, and Monitoring
- Compliance Reporting

Policy & Standards: Exceptions

- **Background**
  - If Business Units or Corporate Functions do not expect to comply with TRO policies or standards, they must request an exception
  - Exceptions are approved for a specified duration of time, with a maximum of one year to remediate the underlying issue

- **Key Issues**
  - The existing request process for exception requests is inefficient, has no consistent criteria to risk rate and approve an exception, and results in a high number of exceptions
  - Exception requests are often poorly documented, missing critical information to determine the risk
  - This process has traditionally relied on one person as the final reviewer, with no backup in the case of an emergency
  - Further, the business rarely is asked to approve the exceptions

- **Proposal to Address Issues**
  - Add new reviewers so that there are at least two people responsible for each initial / final reviewer role
  - Establish crisp guidelines for when an exception should and should not be created
  - Provide guidance on exception submission requirements
  - Establish clear and consistent risk review criteria for both rating & approving each exception across all BUs / functions
  - Establish closer relationships with the business to facilitate their approval

Coordination with ORM

- **Background**
  - Technology risk is a subset of overall operational risk management
  - **Operational Risk** *(Solvency II)* is the risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and **systems**, or from external events (including legal risk), differ from the expected losses

- **The table below outlines ORM's company wide programs, and where TRM fits into the bigger picture**

#	ORM Initiatives	Description	TRM Responsibilities
1	**Risk Events**	Materialization of operational risk leading to financial or non-financial impacts including unintended economic losses or gains, reputational harm due to negative publicity, censure from supervisory agencies, operational and business disruptions, and / or damage to customer relationships	Review, analyze and monitor IT risk events
2	**Risk & Control Self-Assessment (RCSA)**	RCSA is a risk assessment program conducted across AIG that provides Management with a framework to identify, assess, mitigate and escalate operational risk exposures consistently across the organization.	Oversight of IT RCSA
3	**Fraud Assessment**	Overall assessment of the fraud risks that the firm is exposed and how well these risks are identified, assessed and managed by the business and the different control functions involved in the overall Fraud Risk Framework of AIG	Data Theft
4	**Top Risks**	ORM reporting on key risks across AIG	Reports on IT risks distributed to operational risk quarterly as part of the DCCF reporting process
5	**Scenario Analysis**	An organized approach for employing expert opinion to calculate the level of risk for a particular type of event	Analyze 3 scenarios: Japan, Consumer Americas, and Cyber Security
6	**Integrated Risk & Control Framework**	Clarify the control framework for AIG, including the role of business and control functions, and to increase efficiencies and reduce unnecessary touch points with the business	Plan and communicate assessments and other activities to be aligned with other control functions, ultimately working to a goal to "assess once, use many"

Evaluate

Stephen Jarrett

Refine the approach to risk assessment

Opportunities exist to drive risk-based assessments, consistent with ‘AIG levers for change’.

For example, retaining and consolidating existing IT Assessment activities in TRM

- Align and simplify disparate assessment activities across IT
- Consolidate coverage of internal and external stakeholder requirements
- Eliminate testing duplication, i.e. ‘test-once, use-many’
- Automation of assessments and reporting (where practicable)
- Ensure alignment with enterprise programs and leverage of enterprise enablers
- Consolidate results for determining residual risk - prioritize/rationalize remediation investments
- Reduce impact of assessment activities on IT and business

Stakeholders		Example Assessment Activities
Regulators*	→	IT Regulatory Inspections – assessment requirements and responses
Investors	→	IT General Control Testing for 420+ IT SOX Applications globally
Customers, Vendors, and Business Partners	→	Coordinate Customer Assessments of AIG IT (e.g. SSAE16s, AT101s)
	←	Execute 1800+ AIG Vendor/Business Partner assessments/year globally
	→	Monitoring of annual PCI (Shared Infrastructure) Attestation Results
Management	→	Global coordination of 65+ IT RCSAs (7000+ controls) annually
Audit	→	QA/Testing of IT control remediation for IAD issues/actions

TRO portfolio

Identity and Access Management (Bryski)

- Identity Access Management Global Program
    - myAIGaccess Birthright
    - myAIGaccess Portal
    - myAIGaccess Fulfillment
    - myAIGaccess Certification
    - myAIGaccess Administration
    - myAIGaccess Privileged Access
    - Foundational Activities

Information Security (DePeugh)

- Logging and Monitoring /GCDC Program
    - Application Logging and Monitoring (Re Plan)
    - global Cyber Risk Defense Center
    - Database Logging & Monitoring
    - Next Generation SIEM
- Threat Counter Measures & Defenses Program
- Threat Intelligence Integration
- IT Security Capabilities Maturity Assessment
- Microsoft Compromise Assessment

Risk Management (Lorenz)

- Data Security Program
    - Data Loss Prevention Tactical Program (DLP)
    - Global Network DLP Prevent Implementation
- Application Risk Assessment Transformation

IT Compliance (Lorenz)

- TRO Policy and Standards Enhancement
- IT Compliance Future State Operating Model
- Third Party Risk Phase2

Risk Operations & Remediation (Nyakhar)

- ROAR Phase 1A: GRID Development & Configuration

Other

- Active Directory
    - Active Directory Consolidation
    - Active Directory Security

Background

Thematic Data Security Issues:

- Inconsistency in Data Loss Prevention (DLP) technology platforms and coverage
- Lack of a defined DLP strategy
- Ineffective DLP governance, management and operational processes (including investigation)
- Ineffective DLP exception management (including high number of open exceptions)
- Open access to sensitive data across file shares

- Program Inputs -

Address Federal Reserve Bank of New York (FRBNY)

- Implement data loss prevention (DLP) solutions that addresses the themes documented in the letter

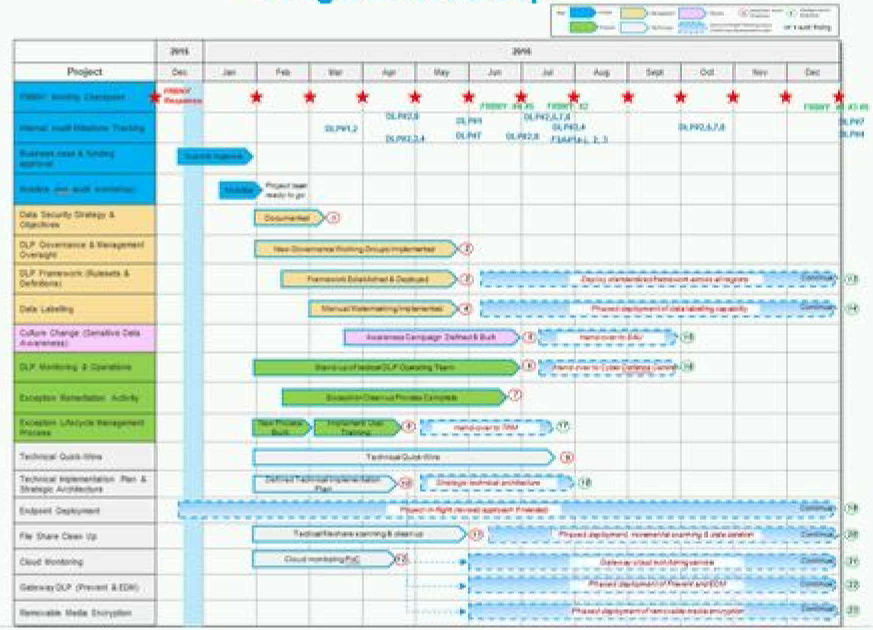
Internal Audits

- Implement DLP solutions that address open findings identified during the 2015 DLP Internal Audit
- Address findings from the File Share audit

Mature capabilities based on data security assessment results

- In addition to compliance driven activities, build data security solutions that manage risk to the environment and enhance the maturity of the data security program

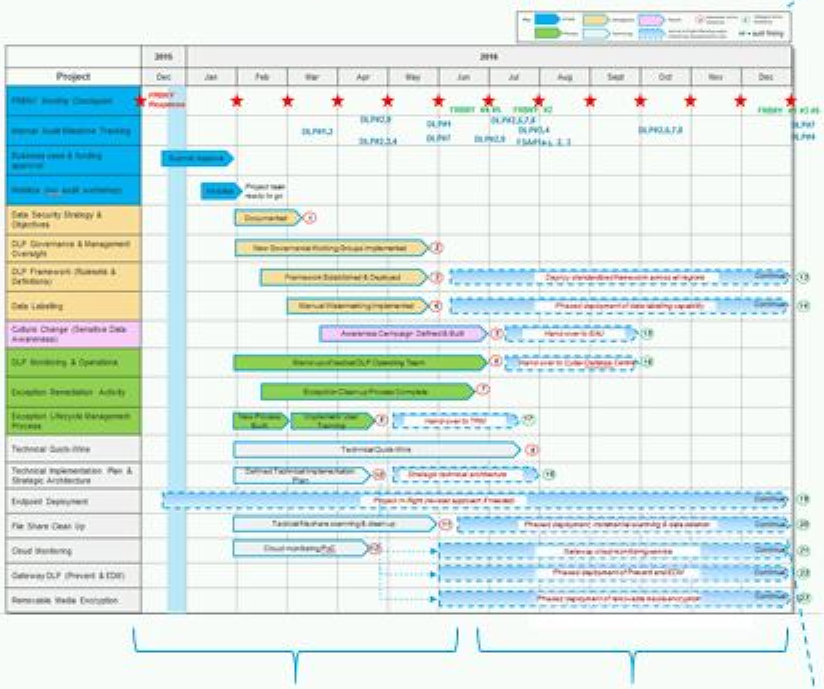
- Program Roadmap -



AIG

Program roadmap & project summary

- Program Roadmap -



Rapid mobilization of 12 immediate projects. These projects begin to address specific audit findings, consolidating current in-flight tactical remediation activities and build the foundation for the subsequent wave of strategic projects.

A secondary wave of strategic projects build on the immediate actions, expanding scale and enhancing capability across AIG's global estate.

- Project Structure -

Management

Objective

To define and communicate AIG's data security strategy and objectives and to implement the supporting governance structure.

Projects

#1 Data Security Strategy & Objectives
#2 DLP Governance & Management Oversight
#3 DLP Framework (Rulesets & Definitions)
#4 Data Labelling

People

Objective

To build and enhance user awareness of the importance of protecting AIG sensitive information.

Project

#5 Sensitive Data Awareness

Process

Objective

To re-engineer and enhance the DLP monitoring and operating procedures and integrate DLP operations with the newly defined governance structure.

Projects

#6 DLP Monitoring & Operations
#7 Exception Remediation Activity
#8 Exception Lifecycle Management Process

Technology

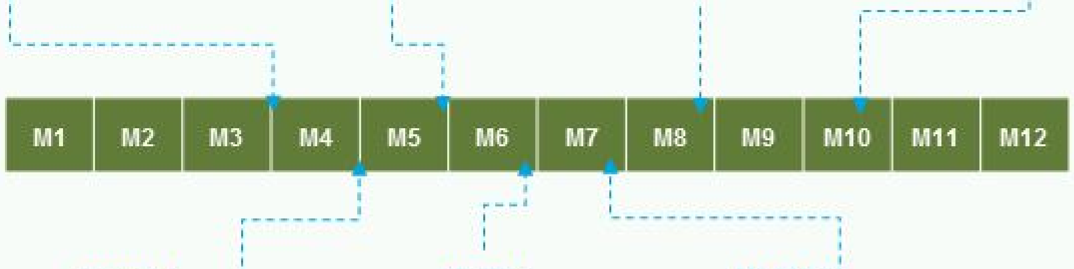
Objective

Enhance and implement expanded DLP technology to enable AIG to monitor, detect and reduce the occurrence of sensitive data loss.

Projects

#9 Technical Quick-Wins
#10 Technical Implementation Plan & Strategic Architecture
#11 File Share Clean Up
#12 Cloud Monitoring

Monthly risk reduction - summary



MONTH 3

(1) Data Security Strategy and supporting objectives approved, signed off and communicated to AIG users

MONTH 4

(8) A new DLP exception lifecycle process is defined and implemented

(10) A detailed technical implementation plan has been defined. Technical implementation projects mobilized

(12) Cloud monitoring PoC completed

MONTH 5

(2) A new DLP governance and management oversight committee is in operation. A DLP management working group is defined and implemented.

(3) AIG 'crown jewels' are defined and documented. A DLP framework is created to set out the definition of each crown jewel, it's business context and the thresholds associated with inappropriate use, storage or transmission

(4) Tactical implementation of manual watermark's on key sensitive data types

MONTH 6

(7) DLP exception clean-up process is complete

(11) Tactical file share & clean up activity completed

MONTH 7

(5) A user awareness campaign has been defined and built. The campaign has been initiated across AIG's US locations and a plan is defined to extend the campaign to all global locations (as a BAU activity)

(6) A tactical monitoring team is in place, with a defined plan to transition monitoring to the strategic Cyber Defense Centre (CDC). DLP operating processes have been re-designed to improve efficiency, performance and reporting.

(9) A series of technical quick wins have been completed (specific to IA findings). (Note: some of these are already in flight)

MONTH 8

(18) Strategic technical architecture and supporting design principles and templates documented and implemented

MONTH 10

(15) Sensitive data awareness campaign running as ongoing BAU activity

(16) DLP operating capability transitioned to strategic Cyber Defense Centre (dependency on CDC timeframes)

Month 12+

(13) Standardized rule sets deployed across all existing DLP platforms (inc. manual watermarking on specific documents)

(14) Data labelling process and technical solution (s) implemented

(19) In-flight endpoint project running with revised approach (if needed*)

(20) File share capability expanded with ongoing clean-up and data deletion activity

(21) Cloud monitoring capability deployed (assumes successful PoC and business case approval)

(22) Gateway DLP capability extended to blocking ('Prevent') & Exact Data Matching (EDM)

(23) Removable media encryption process and technical solution (s) implemented

Key:

(X) Immediate project

(X) Strategic project

AIG

Act

Russell Lewis

Refine the approach to risk assessment

Opportunities exist to drive risk-based assessments, consistent with ‘AIG levers for change’.

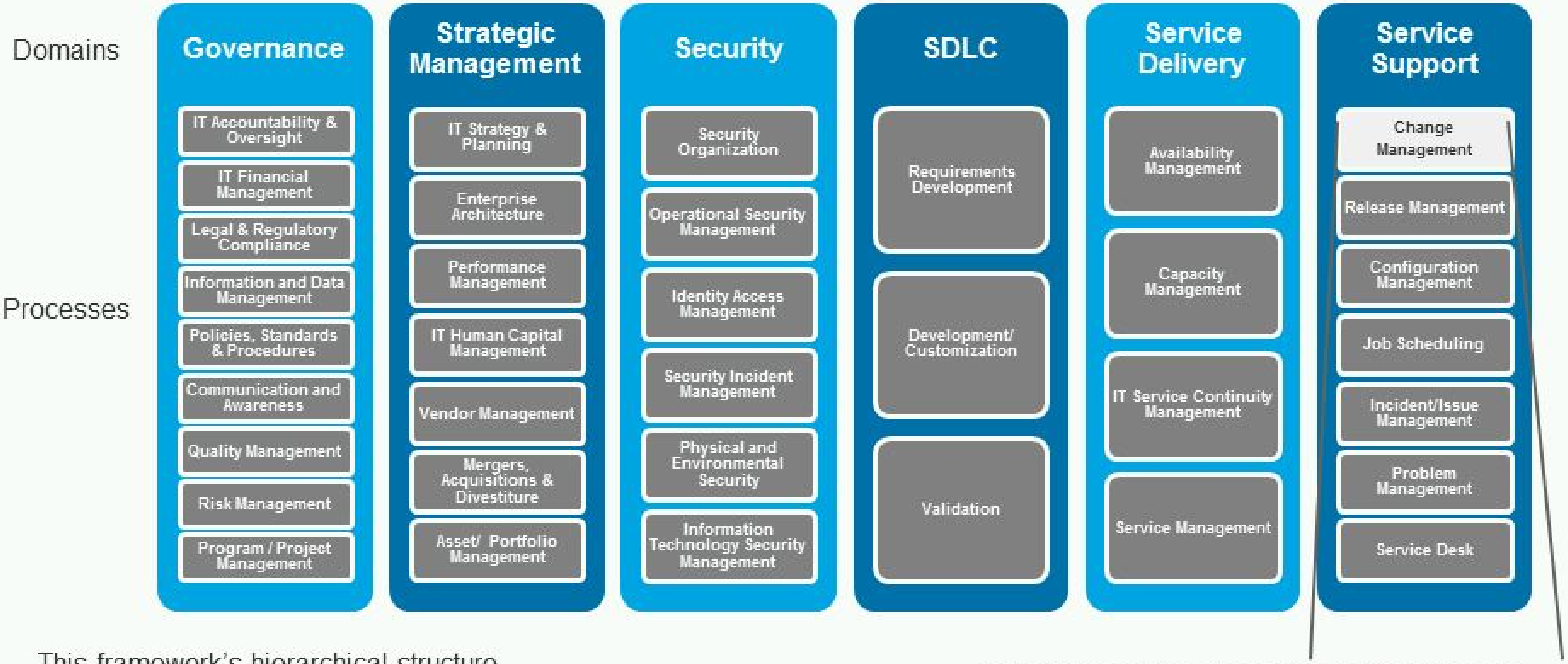
For example, retaining and consolidating existing IT Assessment activities in TRM

- Align and simplify disparate assessment activities across IT
- Consolidate coverage of internal and external stakeholder requirements
- Eliminate testing duplication, i.e. ‘test-once, use-many’
- Automation of assessments and reporting (where practicable)
- Ensure alignment with enterprise programs and leverage of enterprise enablers
- Consolidate results for determining residual risk - prioritize/rationalize remediation investments
- Reduce impact of assessment activities on IT and business

Stakeholders		Example Assessment Activities
Regulators*	→	IT Regulatory Inspections – assessment requirements and responses
Investors	→	IT General Control Testing for 420+ IT SOX Applications globally
Customers, Vendors, and Business Partners	→	Coordinate Customer Assessments of AIG IT (e.g. SSAE16s, AT101s)
	←	Execute 1800+ AIG Vendor/Business Partner assessments/year globally
	→	Monitoring of annual PCI (Shared Infrastructure) Attestation Results
Management	→	Global coordination of 65+ IT RCSAs (7000+ controls) annually
Audit	→	QA/Testing of IT control remediation for IAD issues/actions

IT Process, Risk and Control Framework Coverage

Shown below is a conceptual model of the domains and technology processes within the PRC framework.


Domains
Processes
Governance
IT Accountability & Oversight
IT Financial Management
Legal & Regulatory Compliance
Information and Data Management
Policies, Standards & Procedures
Communication and Awareness
Quality Management
Risk Management
Program / Project Management
Strategic Management
IT Strategy & Planning
Enterprise Architecture
Performance Management
IT Human Capital Management
Vendor Management
Mergers, Acquisitions & Divestiture
Asset/ Portfolio Management
Security
Security Organization
Operational Security Management
Identity Access Management
Security Incident Management
Physical and Environmental Security
Information Technology Security Management
SDLC
Requirements Development
Development/ Customization
Validation
Service Delivery
Availability Management
Capacity Management
IT Service Continuity Management
Service Management
Service Support
Change Management
Release Management
Configuration Management
Job Scheduling
Incident/Issue Management
Problem Management
Service Desk

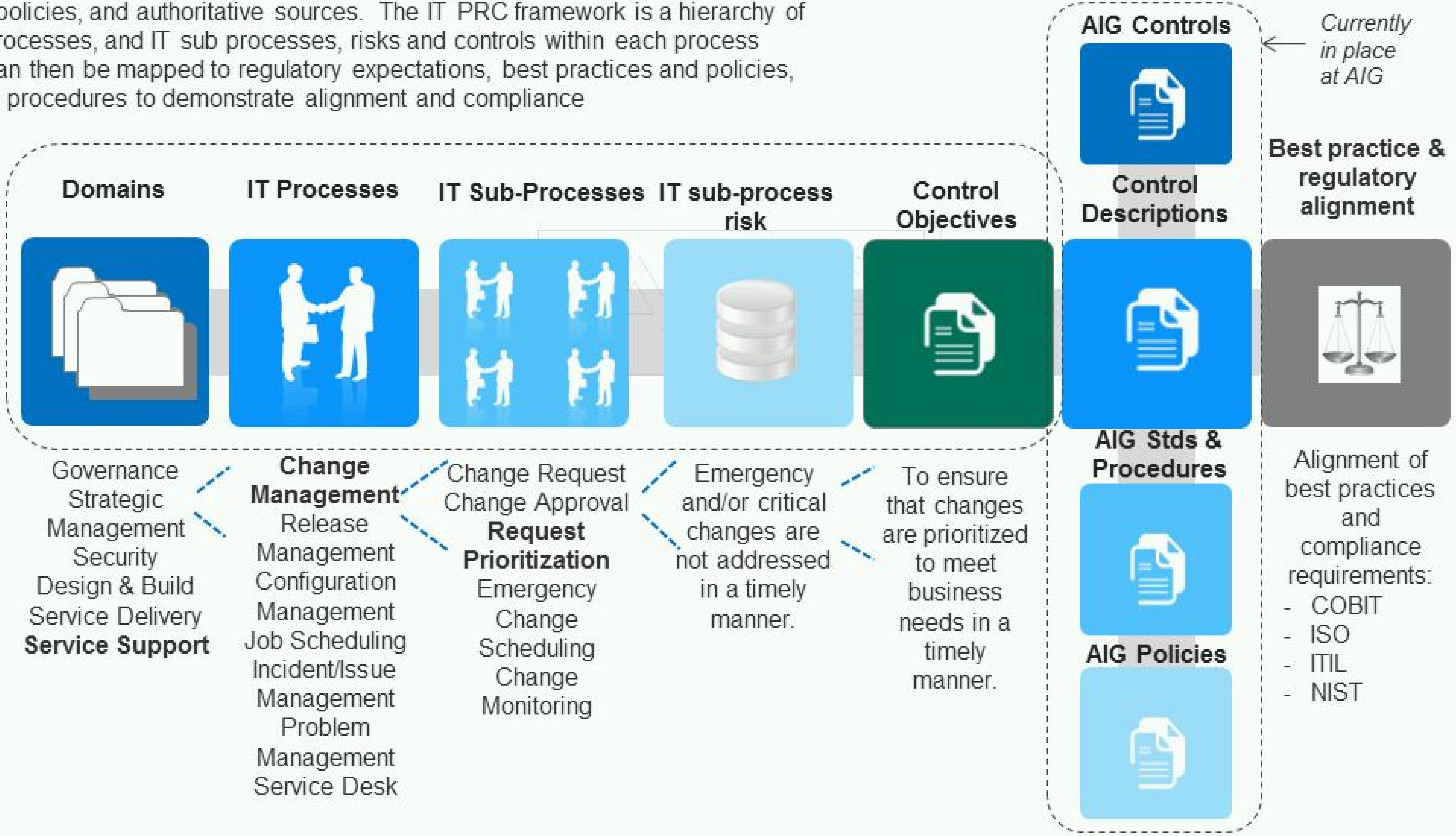
This framework's hierarchical structure facilitates roll-up reporting by logically grouping risk and controls according to their associated IT processes and helps drive accountability

Each process has associated sub-processes

Change Request	Emergency Change Scheduling
Change Approval	Change Monitoring
Request Prioritization	

IT PRC alignment to internal controls, policies, and authoritative sources

This below demonstrates the conceptual alignment between the IT PRC framework and AIG controls, policies, and authoritative sources. The IT PRC framework is a hierarchy of domains, IT processes, and IT sub processes, risks and controls within each process area. These can then be mapped to regulatory expectations, best practices and policies, standards and procedures to demonstrate alignment and compliance



Currently in place at AIG

AIG Controls

Domains

Governance
Strategic Management
Security
Design & Build
Service Delivery
Service Support

IT Processes

Change Management
Release Management
Configuration Management
Job Scheduling
Incident/Issue Management
Problem Management
Service Desk

IT Sub-Processes

Change Request
Change Approval
Request Prioritization
Emergency Change
Scheduling
Change Monitoring

IT sub-process risk

Emergency and/or critical changes are not addressed in a timely manner.

Control Objectives

To ensure that changes are prioritized to meet business needs in a timely manner.

Control Descriptions

AIG Stds & Procedures

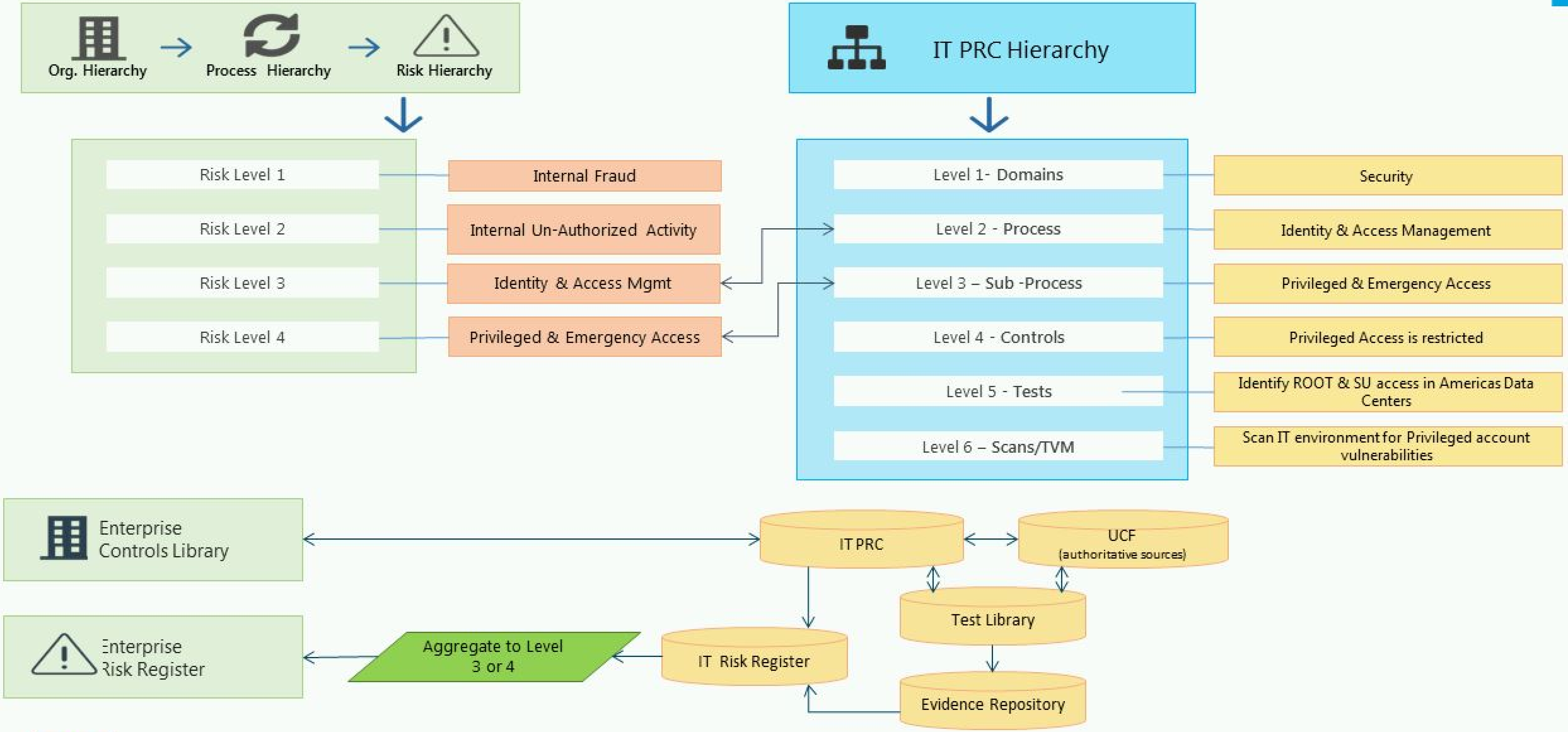
AIG Policies

Best practice & regulatory alignment

Alignment of best practices and compliance requirements:

- COBIT
- ISO
- ITIL
- NIST

Example integration with Enterprise Program and GRC



Org. Hierarchy → Process Hierarchy → Risk Hierarchy

Risk Level 1 — Internal Fraud

Risk Level 2 — Internal Un-Authorized Activity

Risk Level 3 — Identity & Access Mgmt

Risk Level 4 — Privileged & Emergency Access

IT PRC Hierarchy

Level 1- Domains — Security

Level 2 - Process — Identity & Access Management

Level 3 – Sub -Process — Privileged & Emergency Access

Level 4 - Controls — Privileged Access is restricted

Level 5 - Tests — Identify ROOT & SU access in Americas Data Centers

Level 6 – Scans/TVM — Scan IT environment for Privileged account vulnerabilities

Enterprise Controls Library

IT PRC

UCF (authoritative sources)

Test Library

Evidence Repository

IT Risk Register

Aggregate to Level 3 or 4

Enterprise Risk Register

Third party risk model – information security

With the enhanced TRO Third Party Risk Model, we can effectively evaluate Information Security and Business Continuity inherent risk(s), enabling AIG to focus its assessment efforts on the highest risk relationships.

The Information Security risk level depends on the classification of the data 3rd Party has access to and how that data is accessed.

Legend

🟥	High Information Security Risk
🟧	Elevated Information Security Risk
🟨	Medium Information Security Risk
🟩	Low Information Security Risk

>2000 Records

	Type of Data					
Access to Data	Firm Confidential	Sensitive Personal Information	Personal Information	Restricted	Publicly Accessible	N/A - No Access to AIG data
None OR Third Party on AIG premises or remote using AIG equipment only (e.g. Staff augmentation, professional services)	🟩	🟩	🟩	🟩	🟩	🟩
Third Party using non-AIG equipment to access AIG data (onsite at AIG or remote)	🟥	🟥	🟧	🟨	🟩	🟩
Third Party only provides physical transport services and/or storage of physical media (e.g. data storage, archiving or destruction)	🟨	🟨	🟨	🟨	🟩	🟩

Physical Security assessment performed on relationships meeting the criteria within the black box.

Note: Given the limited impact to AIG, if <2000 records are held by the Third Party, the scope of the required IS control assessment will be adjusted and a physical security assessment will not be necessary.

Third party risk model – business continuity

The Business Continuity review depends on when a major disruption at the Third Party may begin to adversely impact AIG and the level of adverse impact experienced as defined by the ORM Matrix.

	Impact Level (based on ORM Matrix)			
Timing of Adverse Impact	Low	Moderate	Elevated	High
0 – 3 Days	🟩	🟨	🟥	🟥
3 – 7 Days	🟩	🟨	🟧	🟥
7 – 30 Days	🟩	🟩	🟨	🟧
Greater than 30 Days	🟩	🟩	🟩	🟨
No Adverse Impact	🟩	🟩	🟩	🟩

Note: *Relationships with High Business Continuity Risk will be considered for the* ***"Enterprise Critical"*** *designation.*

Legend

🟥	High Business Continuity Risk
🟧	Elevated Business Continuity Risk
🟨	Medium Business Continuity Risk
🟩	Low Business Continuity Risk

Assumptions:

- High and Medium Business Continuity Risk levels will trigger a full BCM assessment.
- For Medium Business Continuity Risk, BCM assessment need will be considered during scoping. Generally, a separate BCM assessment should not be required.
- A BCM assessment is not required for Low Business Continuity Risk.

Frequency and depth of assessments

A risk-based approach will be used to drive the depth and frequency of the third party assessment cycle.

	Remote Assessments			
	Information Security			
	High	Elevated	Medium	Low
Frequency	1 year	3 years	5 years	N/A
	Business Continuity			
	High	Elevated	Medium	Low
Frequency	1 year	1 year	N/A	N/A

Onsite Assessments		
Information Security	High	
Business Continuity	High	Elevated
Frequency	1 year	1 year

Legend

🟥 High
🟧 Elevated
🟨 Medium
🟩 Low

Risk Based Onsite Approach

- Critical relationships (High Business Continuity Risk) are assessed annually via an on-site visit.
- Onsite reviews are conducted every other review cycle for relationships that are high for Information Security AND elevated for Business Continuity. In years where an onsite review is not completed a remote review will be conducted.

Global Risk Intelligence Database (GRID): An Overview

GRID (Global Risk Intelligence Data warehouse is a platform that enables users / stakeholders to rapidly create applications, manage workflows and process data through a centralized management platform. GRID provides users with a single source for risk reporting , metrics and automates the 'gathering', refreshing of multiple sources of IT risk metrics and data to improve efficiency ensure analysis and reporting is accurate. It aims to provide a comprehensive end-to-end risk analysis by business, product, platform and geography, where possible.

Stakeholders

- Consumer
- Commercial
- Claim & Ops
- UGC
- IT
- Crop Services
- EMEA
- APAC
- Japan

GRID

GRID

IT Risk Metrics

IT Risk Metrics displays KRI score card across top 10 IT risk focus areas with drill down capability to granular details

Labor Free

With GRID. Workflow management & Data Solutions, you can free yourself from the labor and system-intensive processes of creation of forms, workflow & data aggregation, cleansing and delivery

Data Collection

GRID. collects data from more than <70> leading data providers on a daily basis.

Data Analysis

GRID. automates the 'gathering' and refreshing of data to improve efficiency, ensure analysis and reporting is against a common source data and will facilitate a more consistent risk opinion.

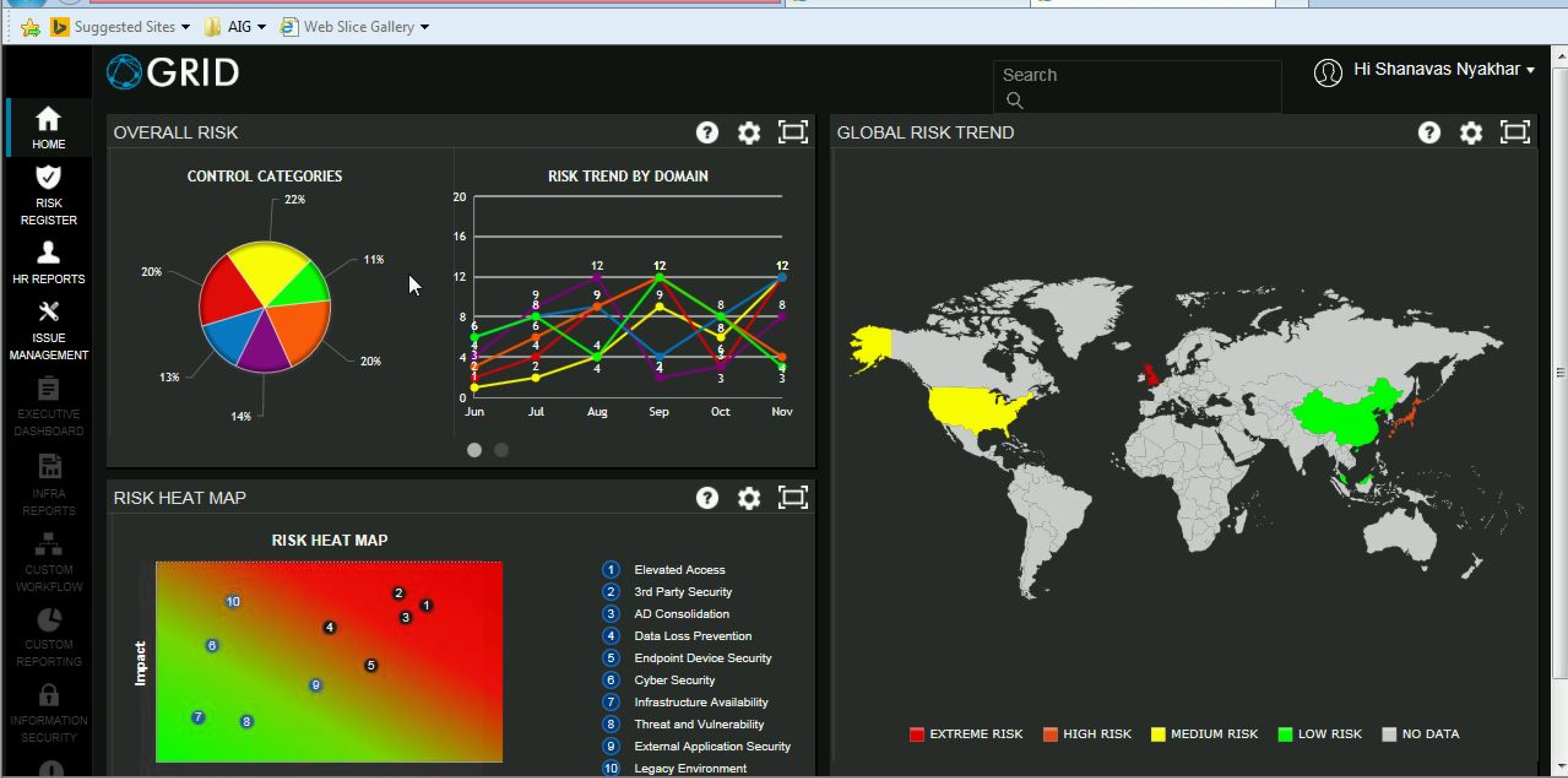
Data Enrichment

Data enrichment where data from multiple sources is added to the existing data set to enhance the quality and richness of the data.

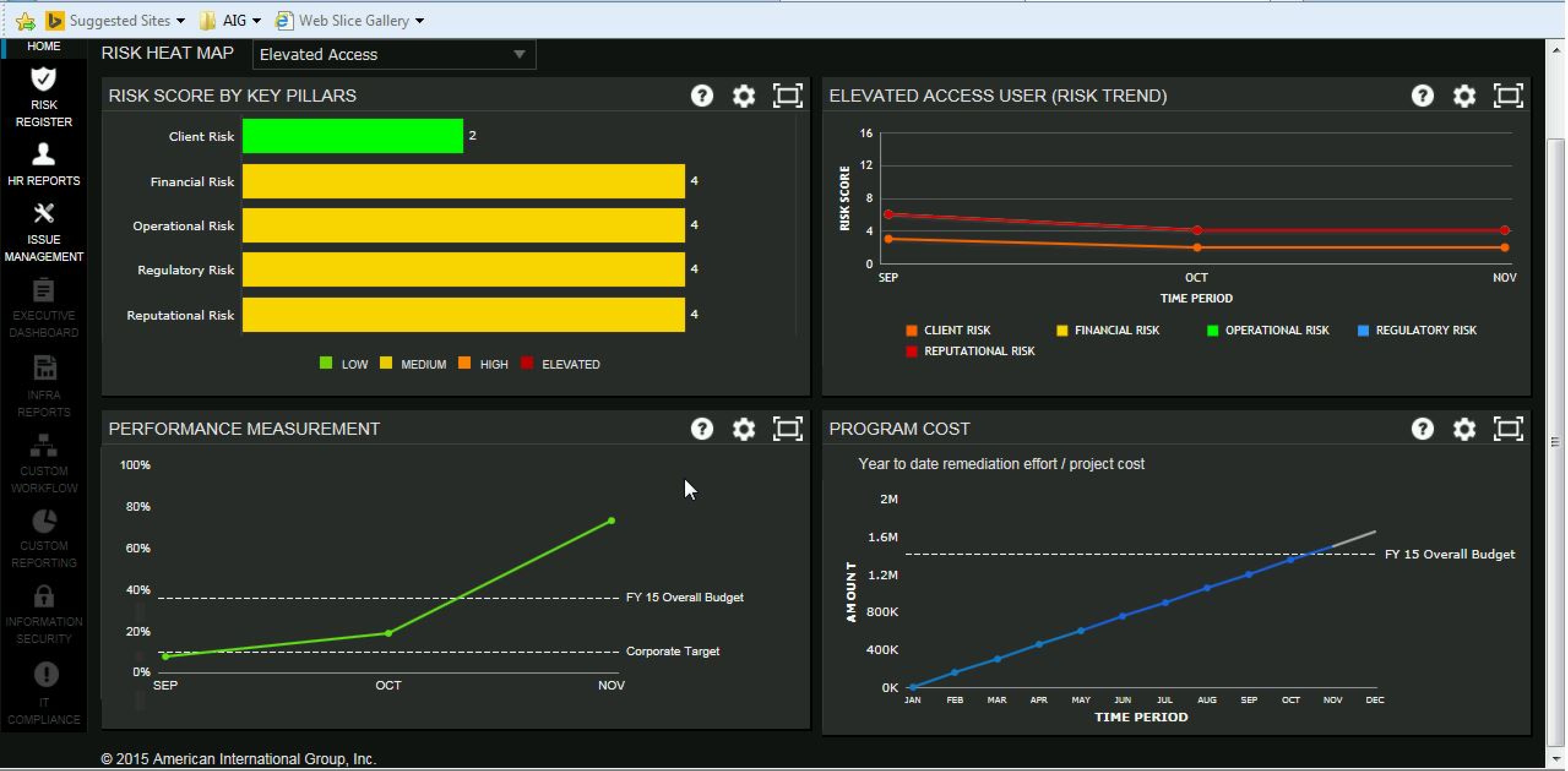
Data Sources

- CMDB
- GEAR
- Archer
- Active Directory
- SAP FI
- Qualys
- McAfee
- RITA/Open Page
- Manual data sources

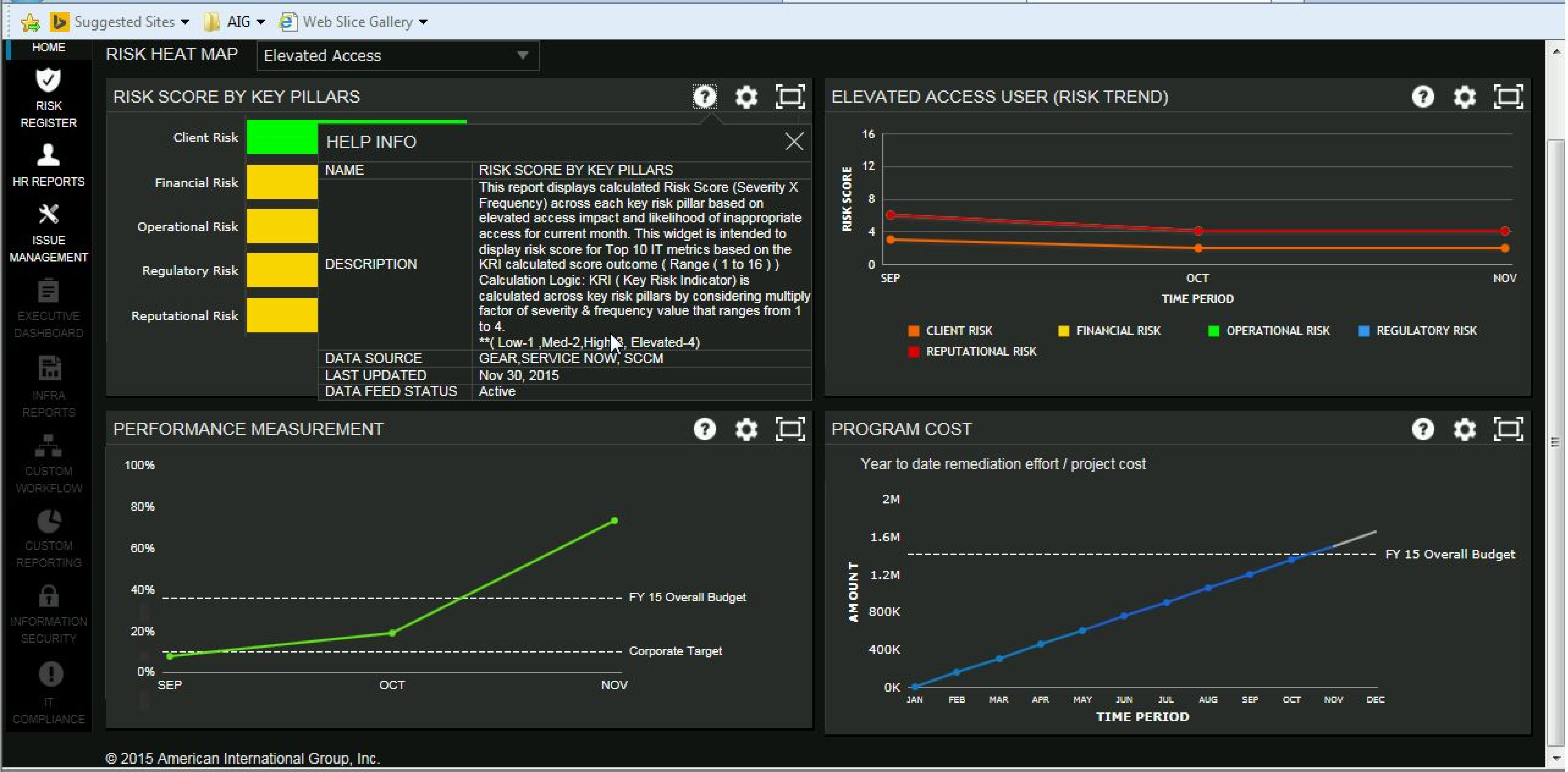
Active **70+** data sources



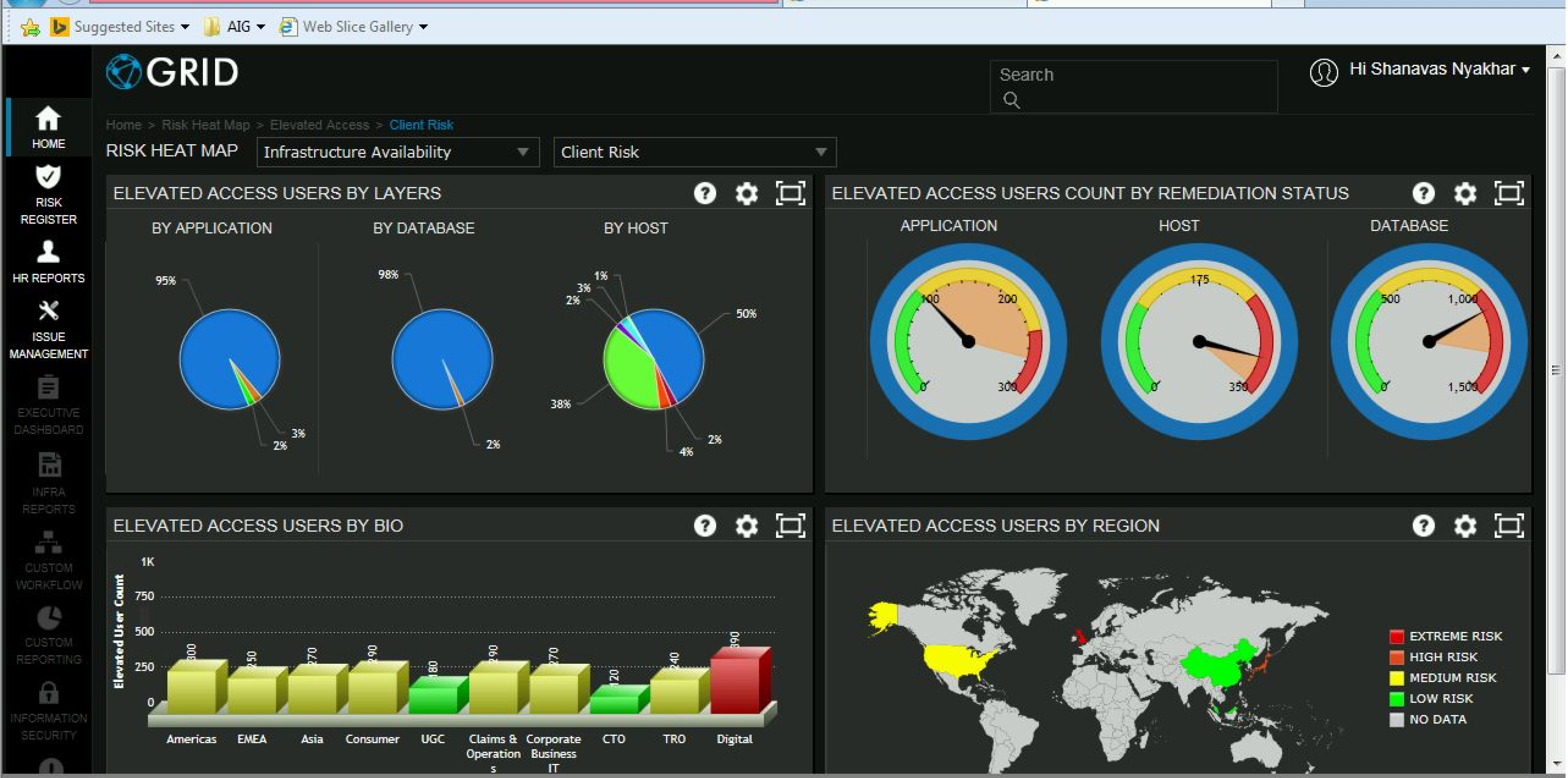
1. Elevated Access
2. 3rd Party Security
3. AD Consolidation
4. Data Loss Prevention
5. Endpoint Device Security
6. Cyber Security
7. Infrastructure Availability
8. Threat and Vulnerability
9. External Application Security
10. Legacy Environment



© 2015 American International Group, Inc.

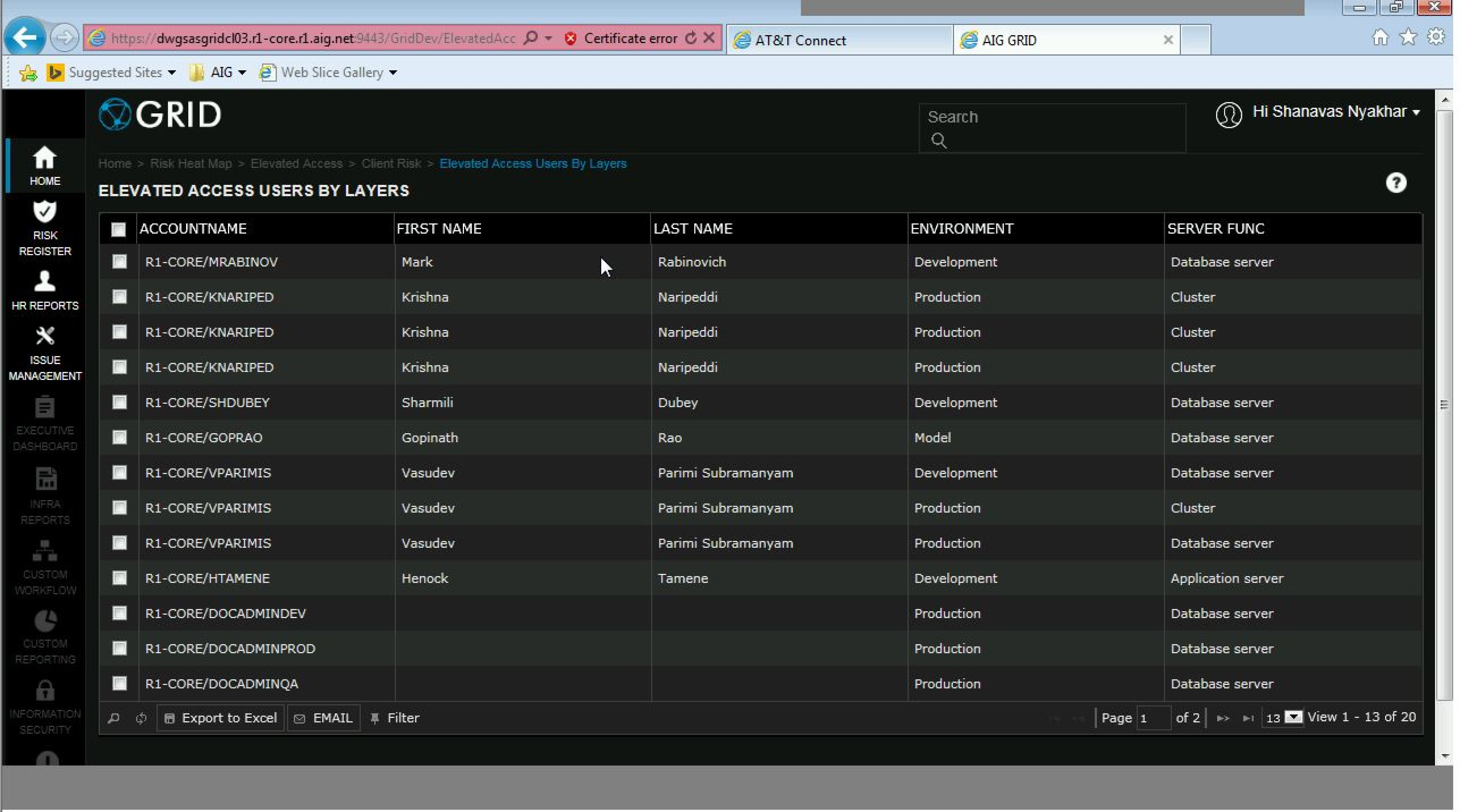


NAME	RISK SCORE BY KEY PILLARS
DESCRIPTION	This report displays calculated Risk Score (Severity X Frequency) across each key risk pillar based on elevated access impact and likelihood of inappropriate access for current month. This widget is intended to display risk score for Top 10 IT metrics based on the KRI calculated score outcome (Range (1 to 16)) Calculation Logic: KRI (Key Risk Indicator) is calculated across key risk pillars by considering multiply factor of severity & frequency value that ranges from 1 to 4. **(Low-1 ,Med-2,High-3, Elevated-4)
DATA SOURCE	GEAR,SERVICE NOW, SCCM
LAST UPDATED	Nov 30, 2015
DATA FEED STATUS	Active



Home > Risk Heat Map > Elevated Access > Client Risk

RISK HEAT MAP: Infrastructure Availability | Client Risk



Home > Risk Heat Map > Elevated Access > Client Risk > Elevated Access Users By Layers

ELEVATED ACCESS USERS BY LAYERS

□	ACCOUNTNAME	FIRST NAME	LAST NAME	ENVIRONMENT	SERVER FUNC
□	R1-CORE/MRABINOV	Mark	Rabinovich	Development	Database server
□	R1-CORE/KNARIPED	Krishna	Naripeddi	Production	Cluster
□	R1-CORE/KNARIPED	Krishna	Naripeddi	Production	Cluster
□	R1-CORE/KNARIPED	Krishna	Naripeddi	Production	Cluster
□	R1-CORE/SHDUBEY	Sharmili	Dubey	Development	Database server
□	R1-CORE/GOPRAO	Gopinath	Rao	Model	Database server
□	R1-CORE/VPARIMIS	Vasudev	Parimi Subramanyam	Development	Database server
□	R1-CORE/VPARIMIS	Vasudev	Parimi Subramanyam	Production	Cluster
□	R1-CORE/VPARIMIS	Vasudev	Parimi Subramanyam	Production	Database server
□	R1-CORE/HTAMENE	Henock	Tamene	Development	Application server
□	R1-CORE/DOCADMINDEV			Production	Database server
□	R1-CORE/DOCADMINPROD			Production	Database server
□	R1-CORE/DOCADMINQA			Production	Database server

Page 1 of 2 13 View 1 - 13 of 20