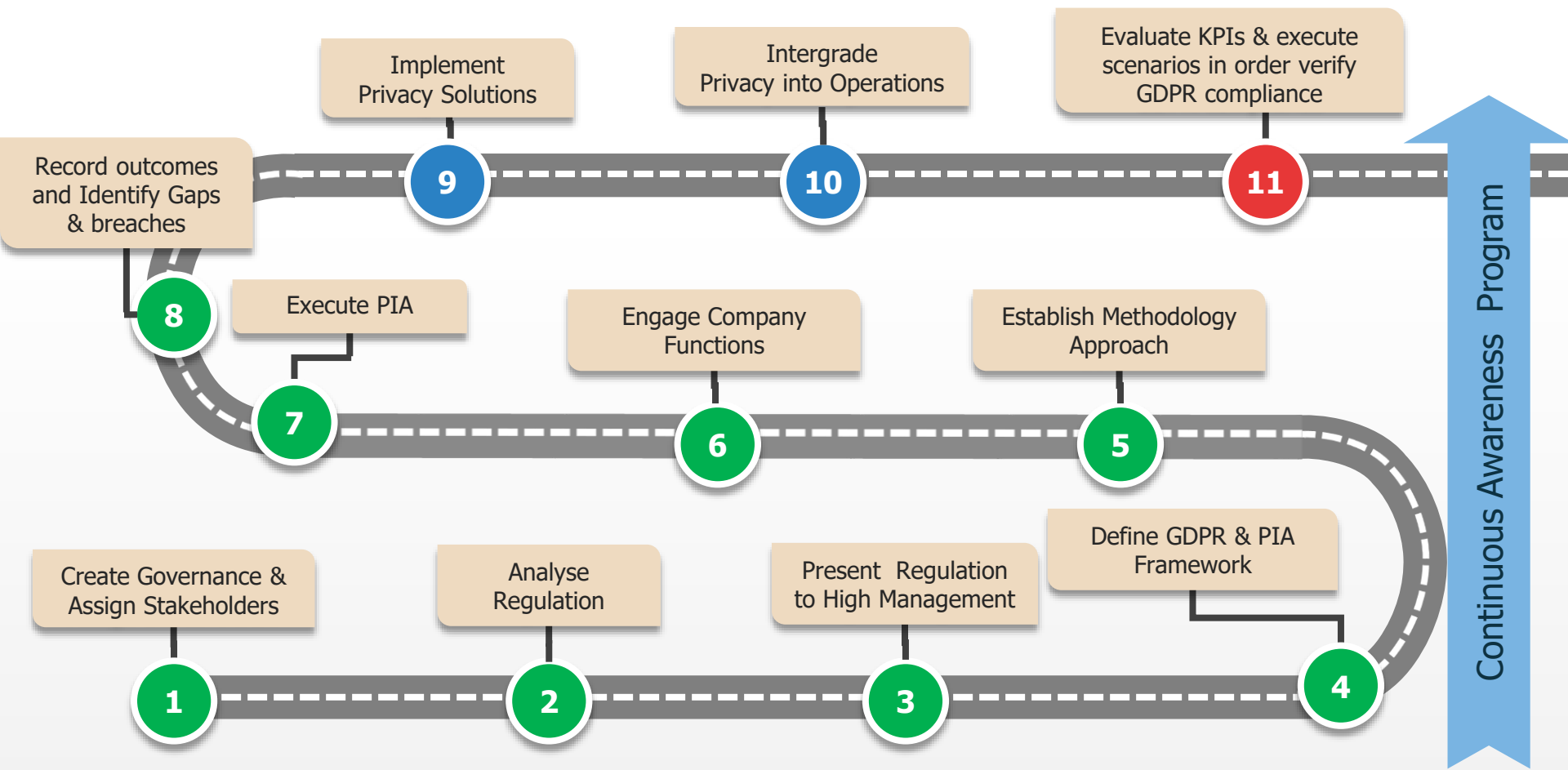
INTERAMERICAN

GDPR: Is it just another regulation or a great opportunity for operational excellence?

Athens , February 2018

GDPR Roadmap

INTERAMERICAN



Maturity Status (PIA Results)

INTERAMERICAN

Personal Data Processing Basic Principles — Level 2

Safeguarding Data Subject's Rights — Level 2

Personal Data Breach Notification — Level 3

Organizational Structure — Level 3

Policies and Procedures — Level 3

Audit and Continuous Improvement — Level 2

Security — Level 3

Legend

- 1 –Initial
- 2 –Managed
- 3 –Defined
- 4 –Measured
- 5 –Optimized

Based on CMMI Maturity Model

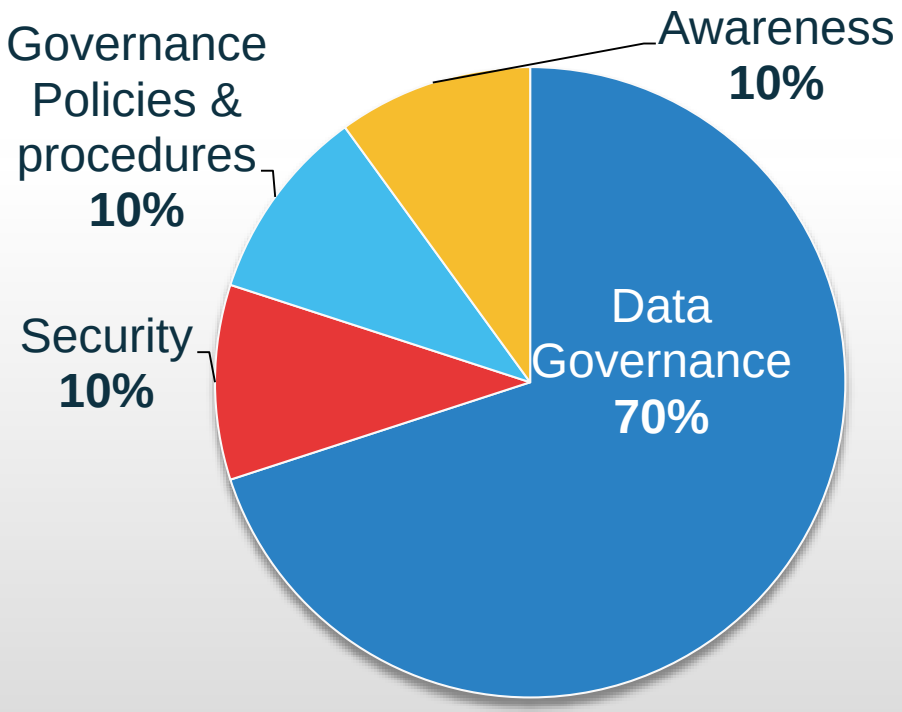
GDPR Findings

INTERAMERICAN

Consent	Requests for consent for different purposes are not distinguished.	Consent is opt-out
Retention	Retention periods for personal data are not clearly defined.	
Portability	No policy for satisfying requests for personal data portability.	
Security	USB ports are enabled on all corporate PCs and Laptops.	Emails containing personal data are not encrypted
Forgetness	There are no mechanisms for personal data erasure.	
Collection Purpose	Not all data collected, stored, transferred etc. are necessary for the purposes of personal data processing	
Contracts	The template contract between IAG and an insurer partner is not updated based on GDPR provisions	
Audit	The scope and criteria of the internal audit process does not include personal data protection requirements.	
Data Breach	The security incidents records do not include all the required information regarding personal data breaches.	

INTERAMERICAN

GDPR : Effort Diagram



Approaching GDPR (Governance & Policies)

INTERAMERICAN

- Assign the role of Data Protection Officer (DPO) and appoint responsibilities
- Document a corporate Data Protection Policy
- Create DPO HUB (DPO, Info Sec, BCM, Legal, Compliance, Risk, IT Sec)
- Define KPIs for the measurement of GDPR performance
- Establish communication with Data Protection Authority
- Review and update contracts & agreements with processors

Approaching GDPR (Security)

INTERAMERICAN

- Implement Data Protection Policy security controls
- Strengthen DLP functionality
- Encrypt or Mask personal information depending on purpose
- Review the removable storage media policy & procedure
- Review, adjust & enhance processes to satisfy requests from data subjects
- Secure Application environment & encryption in corporate mobile devices

Approaching GDPR (Awareness)

INTERAMERICAN

- Educate/Train people according to GDPR principles
- Create internal site for Security & GDPR Awareness
- Uploading Videos & Quizzes in portal, Posters, Manuals & Guidelines
- Executing periodical Clean Desk Assessment
- Reward employees who comply GDPR requirements
- Live Presentations across all different business functions

Approaching GDPR (Data Governance)

INTERAMERICAN

- Strengthen corporate Data Governance Policy incorporating GDPR requirements
- Enhance Data Lineage (Data Processes & Flows)
- Create a personal data processing register
- Tagging personal and sensitive identifier (PII , SII , VII)
- Enhance Data Remediation processes
- Create common data glossary

Approaching GDPR (Data Governance)

INTERAMERICAN

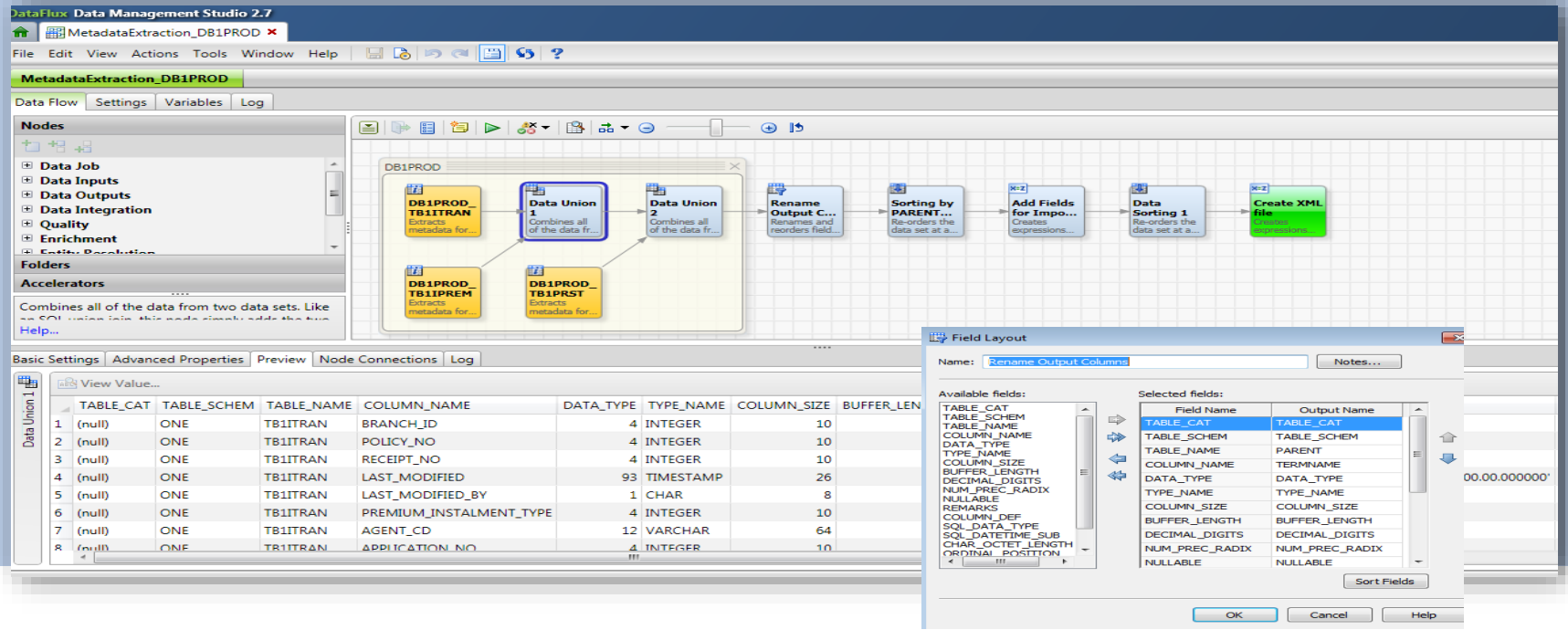
- Assign the role of Data Traffic Controller and appoint responsibilities
- Confirm existence of Data Owner per data category within framework
- Adjust current Retention Policy
- Data Disposal either hardcopy or electronic
- Create Internal Data Request Center
- Adjust Data Collection possesses according to GDPR requirements

Data Governance: Data Manipulation

Metadata Management

INTERAMERICAN

SAS® Data Management Studio

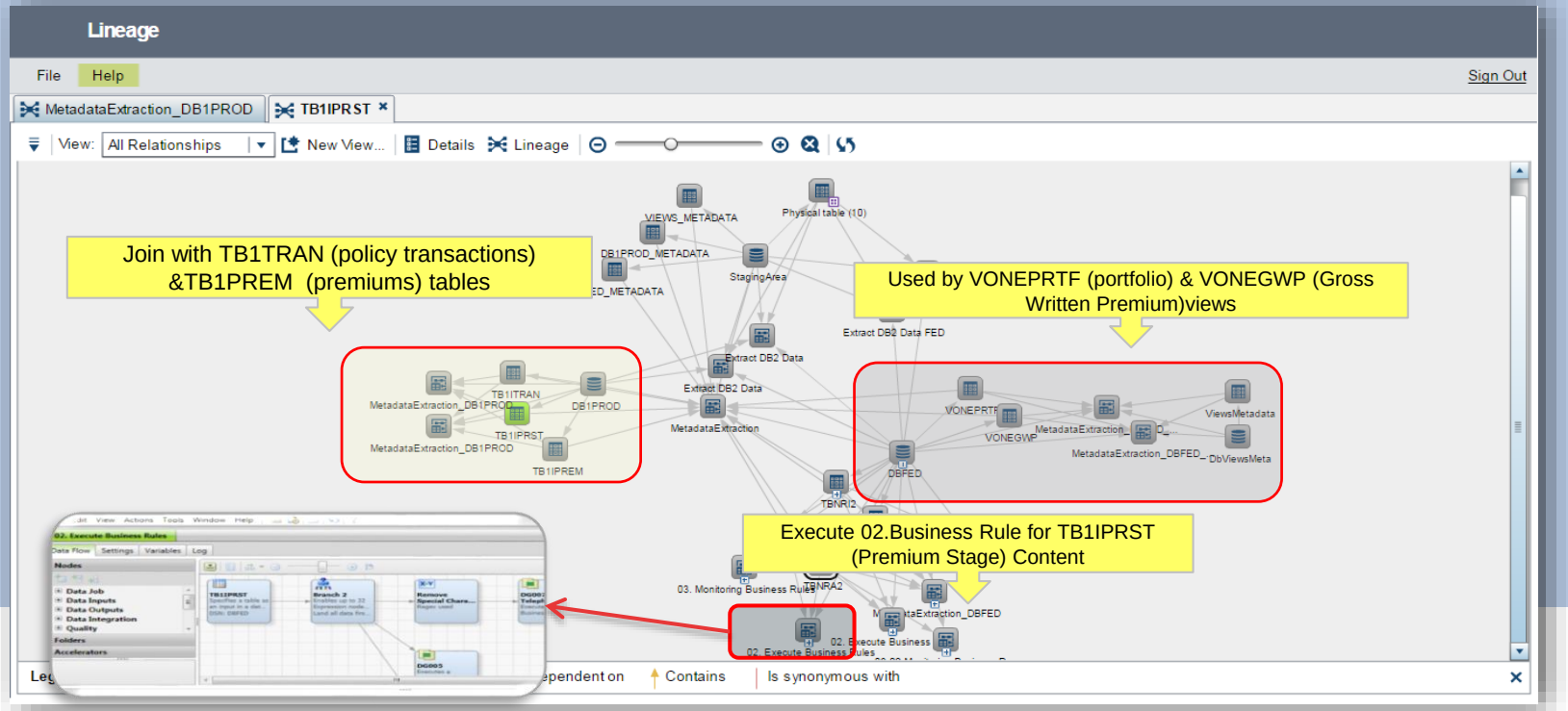


Data Governance: Data Management

Enterprise Data Lineage

INTERAMERICAN

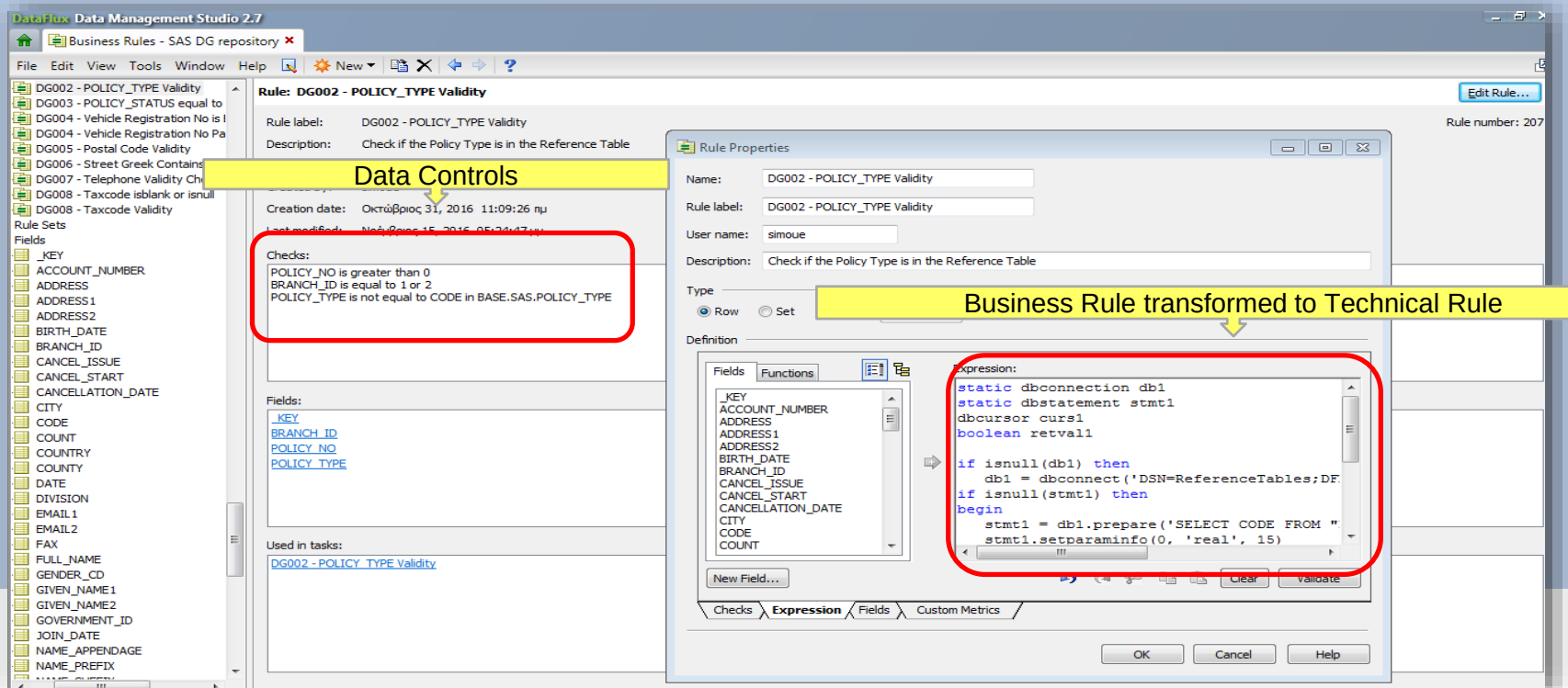
SAS® Data Lineage



Data Governance: Data Framework

INTERAMERICAN

SAS® Data Management Studio

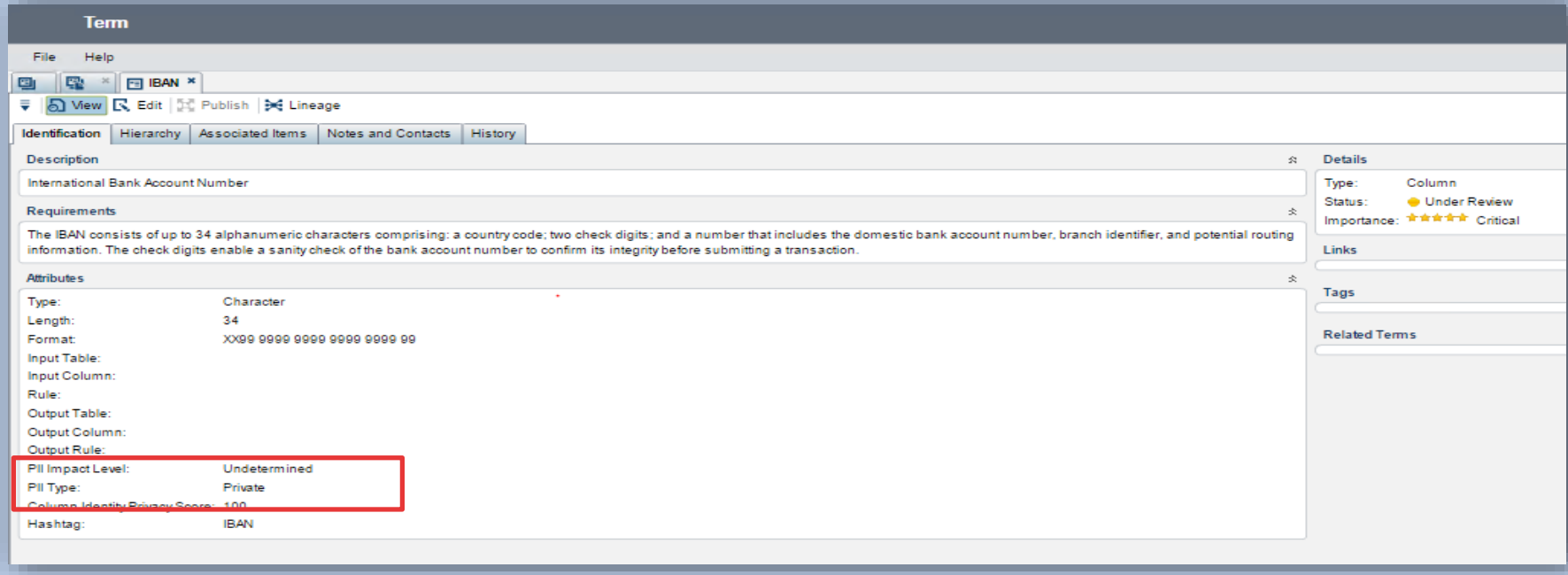


GDPR New Principles

Personal Identity Information -PII

INTERAMERICAN

SAS® Data Management Studio

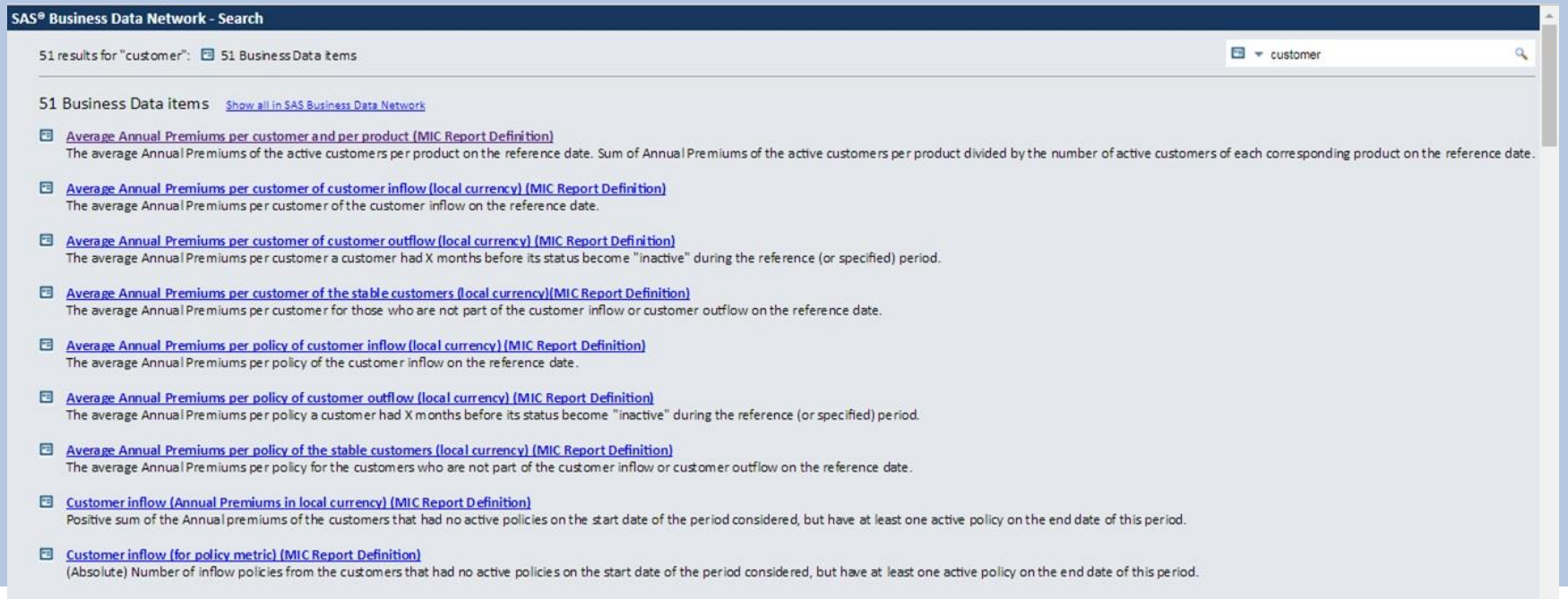


Data Governance: Data Framework

Wiki-Like Search

INTERAMERICAN

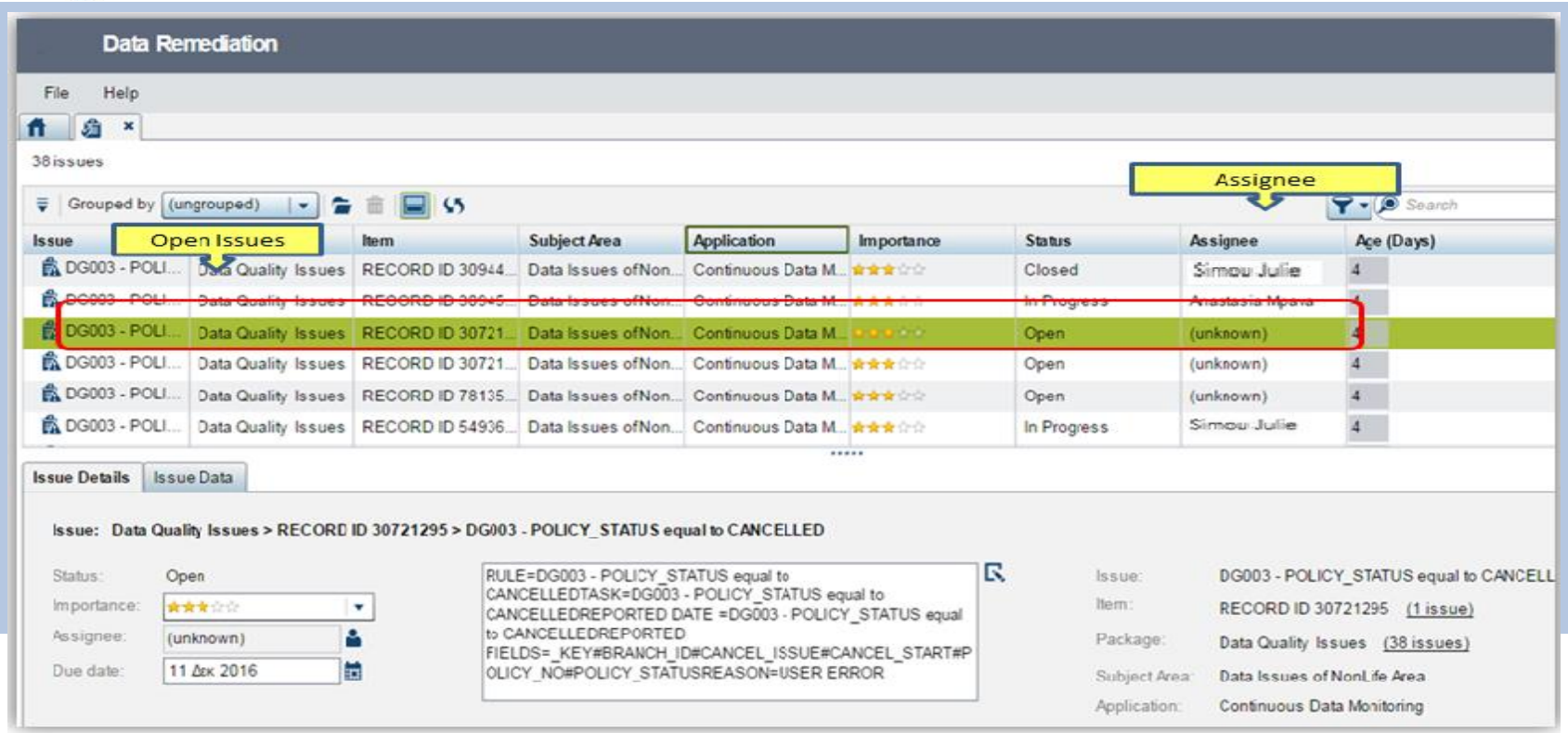
SAS® Business Glossary



Data Governance: Data Framework

Data Remediation

SAS® Data Management Studio

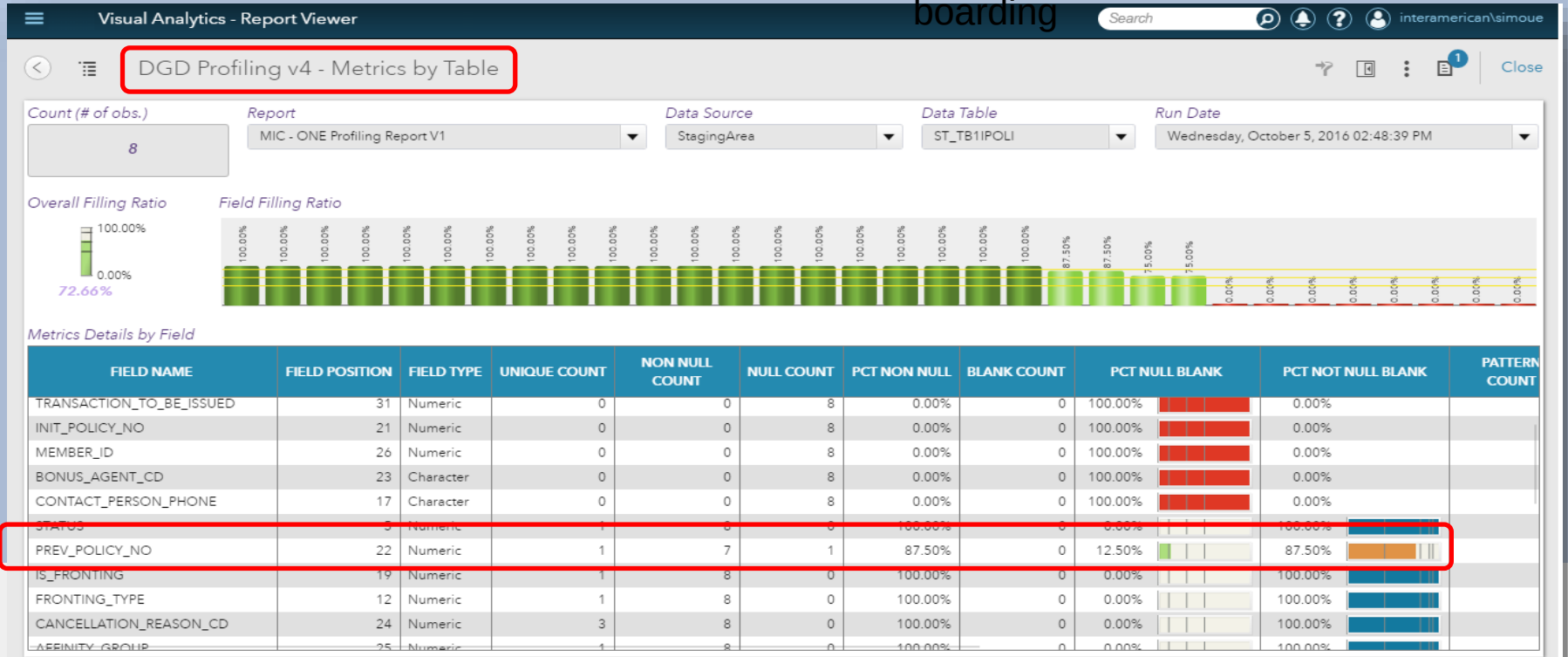


Data Governance: Data Framework

Data Monitoring and Dash boarding

INTERAMERICAN

SAS® Data Monitoring & Dash boarding

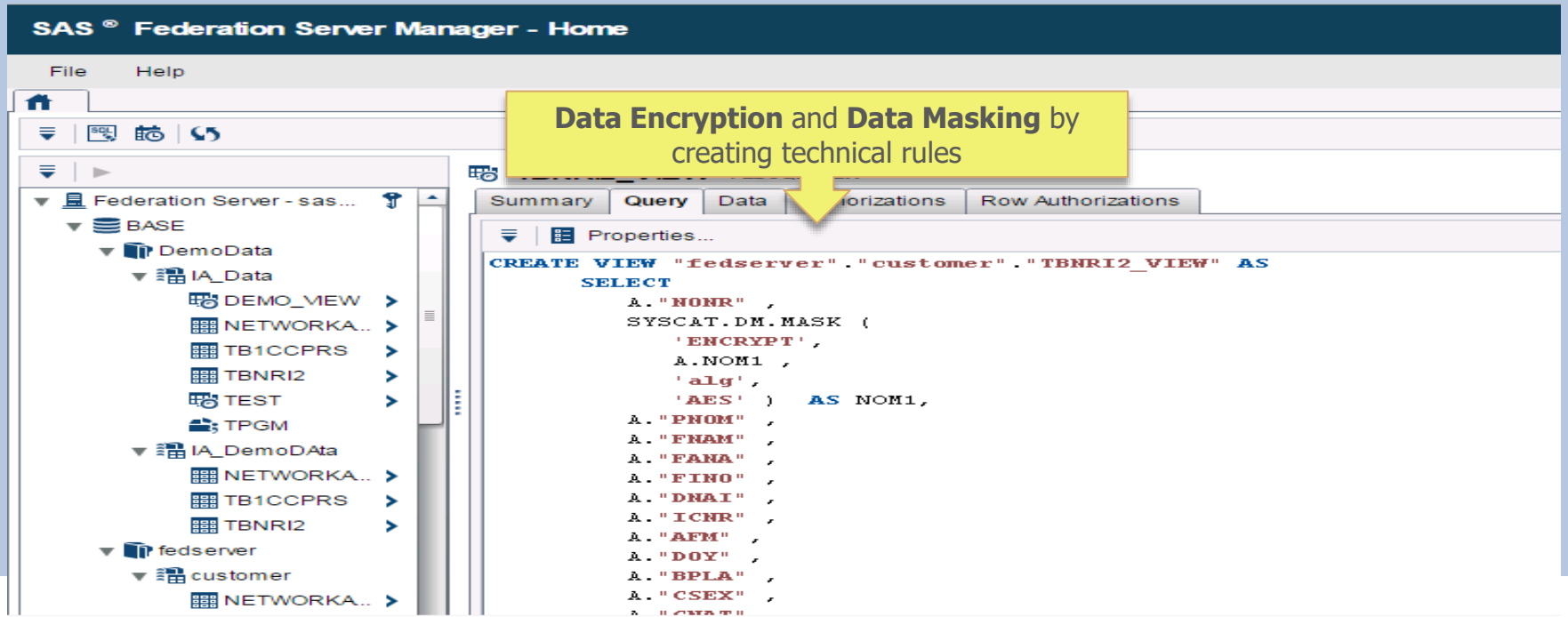


FIELD NAME	FIELD POSITION	FIELD TYPE	UNIQUE COUNT	NON NULL COUNT	NULL COUNT	PCT NON NULL	BLANK COUNT	PCT NULL BLANK	PCT NOT NULL BLANK	PATTERN COUNT
TRANSACTION_TO_BE_ISSUED	31	Numeric	0	0	8	0.00%	0	100.00%	0.00%	
INIT_POLICY_NO	21	Numeric	0	0	8	0.00%	0	100.00%	0.00%	
MEMBER_ID	26	Numeric	0	0	8	0.00%	0	100.00%	0.00%	
BONUS_AGENT_CD	23	Character	0	0	8	0.00%	0	100.00%	0.00%	
CONTACT_PERSON_PHONE	17	Character	0	0	8	0.00%	0	100.00%	0.00%	
STATUS	5	Numeric	1	8	0	100.00%	0	0.00%	100.00%	
PREV_POLICY_NO	22	Numeric	1	7	1	87.50%	0	12.50%	87.50%	
IS_FRONTING	19	Numeric	1	8	0	100.00%	0	0.00%	100.00%	
FRONTING_TYPE	12	Numeric	1	8	0	100.00%	0	0.00%	100.00%	
CANCELLATION_REASON_CD	24	Numeric	3	8	0	100.00%	0	0.00%	100.00%	
AFFINITY_GROUP	25	Numeric	1	8	0	100.00%	0	0.00%	100.00%	

GDPR New Principles

INTERAMERICAN

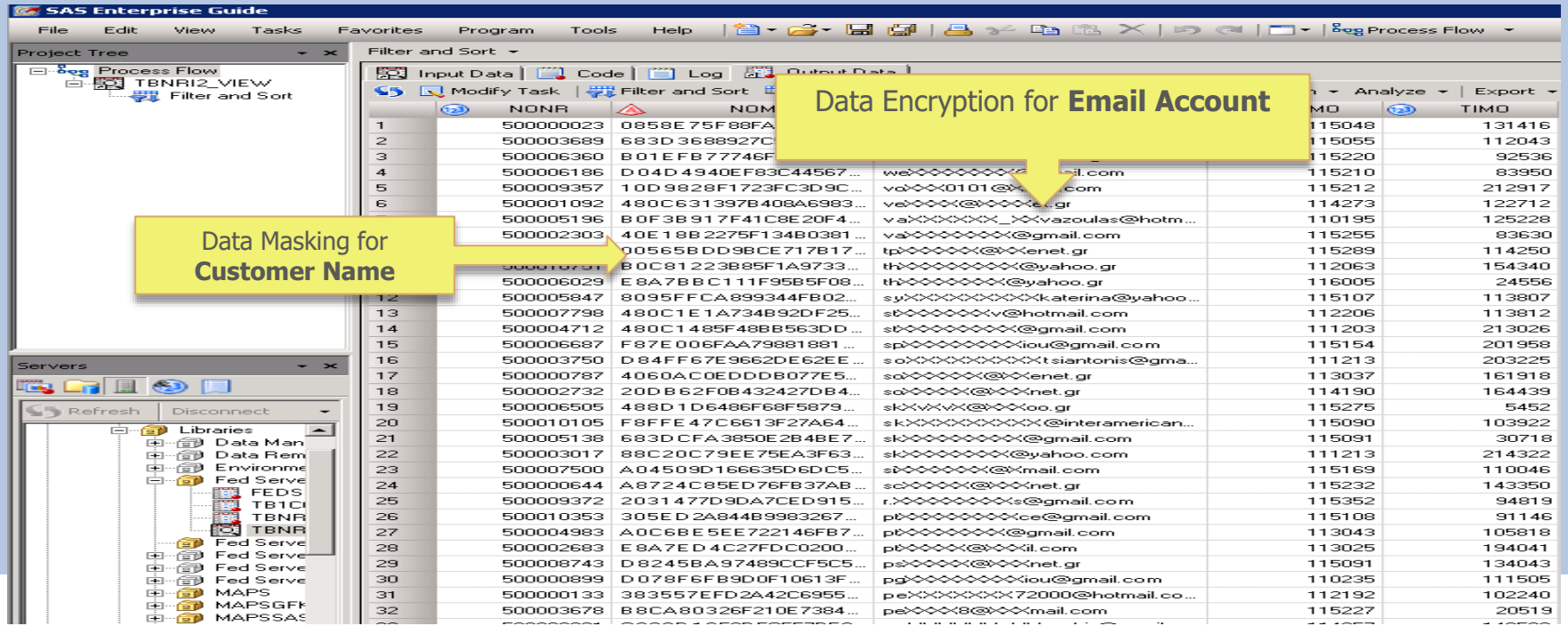
SAS® Federation Server



GDPR New Principles

INTERAMERICAN

SAS® Federation Server

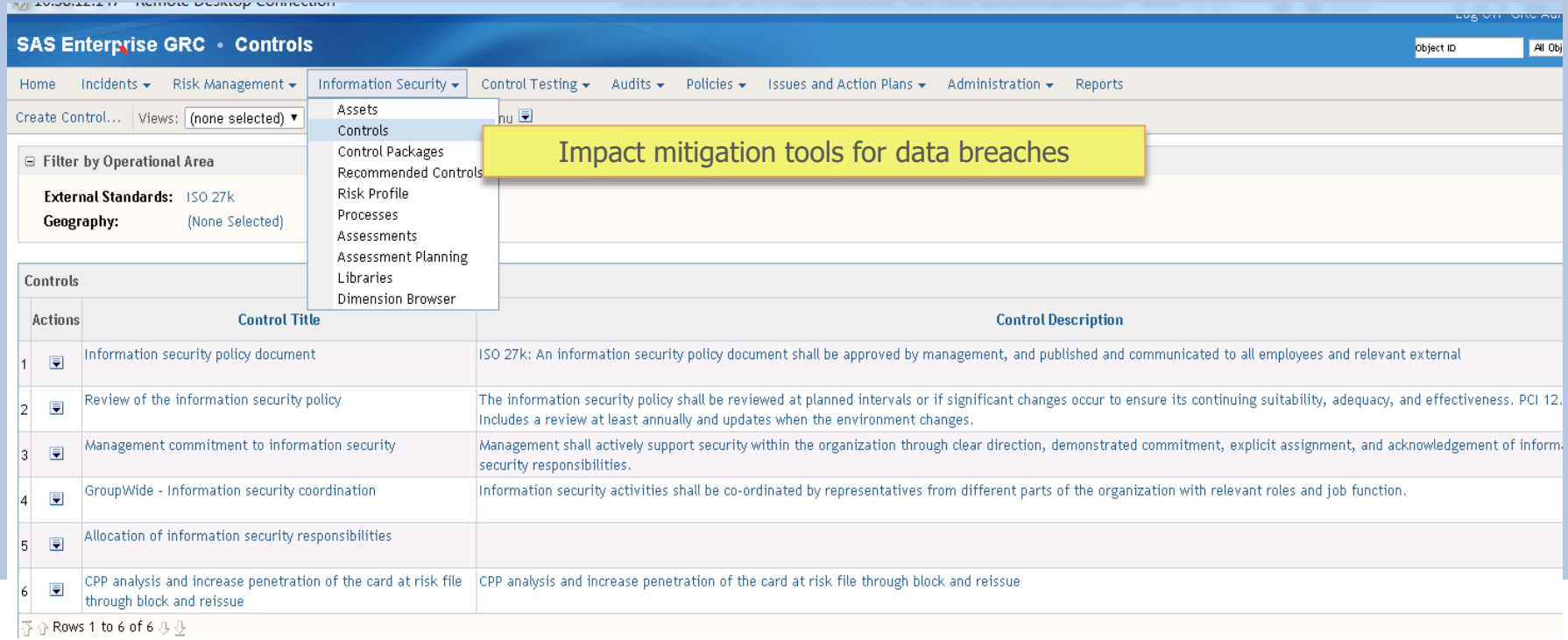


GDPR New Principles

INTERAMERICAN

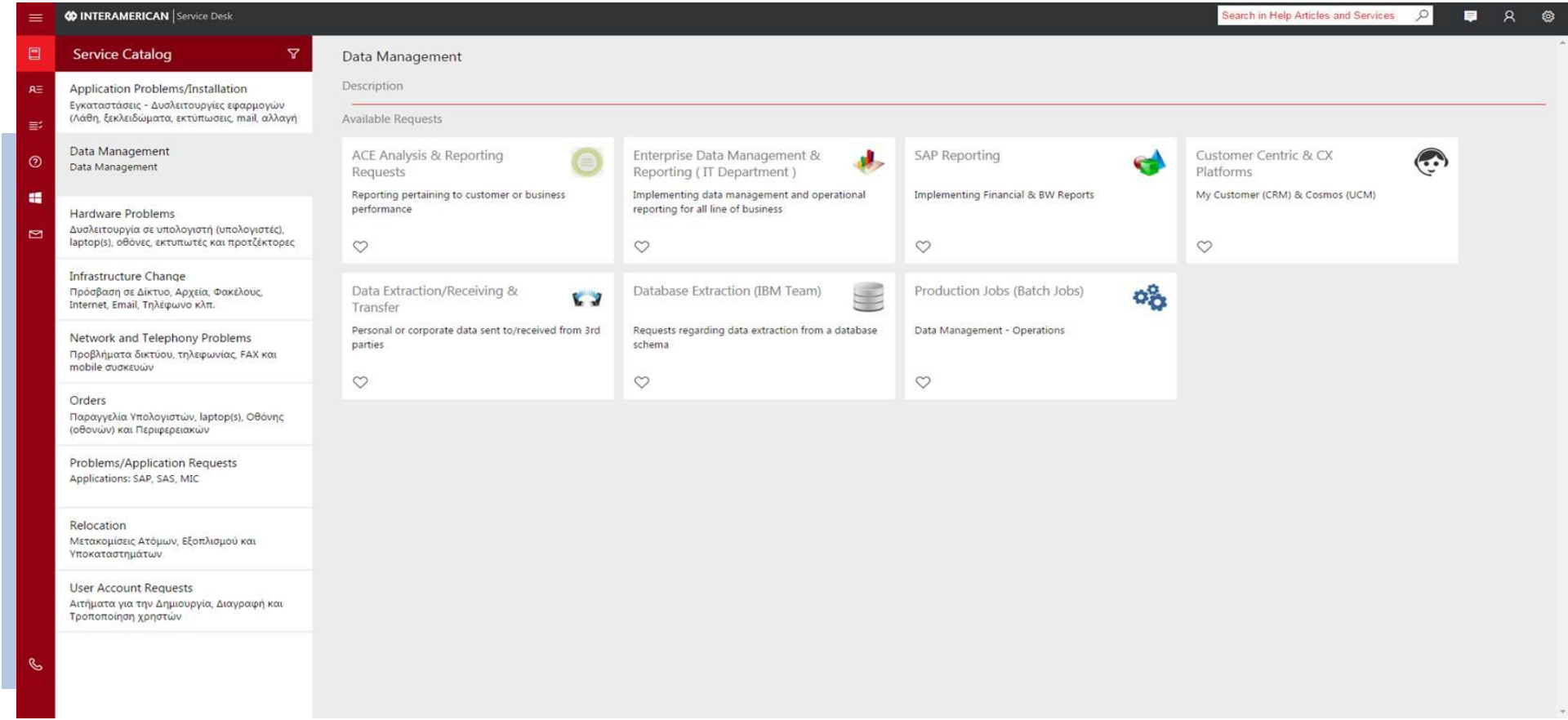
Enterprise, Govern, Risk and Compliance (EGRC)

SAS® Enterprise GRC



Data & Reporting Request Center

INTERAMERICAN



Last but not least ….

- Set up a Clean Desk policy
- Ensure paper documents are safely stored and disposed of
- Classify Unstructured data
- Employee involvement through continuous awareness
- Verify Processors' compliance
- Control requests for data
- Expected additional guidelines from Data Protection Authority & Hellenic Insurance Union

GDPR : Post implementation Benefits

INTERAMERICAN

- ✓ **Strengthen** customer trust and customer relationships, resulting in loyalty
- ✓ Enhance market **reputation** & business **cooperation**
- ✓ Competitive **market advantage**
- ✓ Strengthen **security** & minimized security Incident
- ✓ Digital benchmark through **PIA**
- ✓ **Smart** Big Data leads to better, safer, faster processing
- ✓ **Elimination** of redundant or duplicate data leads to reduced costs & faster processes

INTERAMERICAN

…is not just another framework or regulation

but a great opportunity to enhance operational excellence!