IBM Security

Integration of the Three Lines of Defense

GRC and Regulatory affairs integration using SAP GRC

Victor Garcia Rodriguez

IBM Security – Associate Partner – Europe CoC Lead for SAP Security & SAP GRC

Milano, June 18th 2019

IBM

Table of Contents

Integration of the Three Lines of Defense

1. Introduction to the Debate…

Regulatory Compliance vs. IT Security

1. Introduction to the Debate…

Regulatory Compliance vs. IT Security: How to reconcile both areas?

Regulatory Compliance

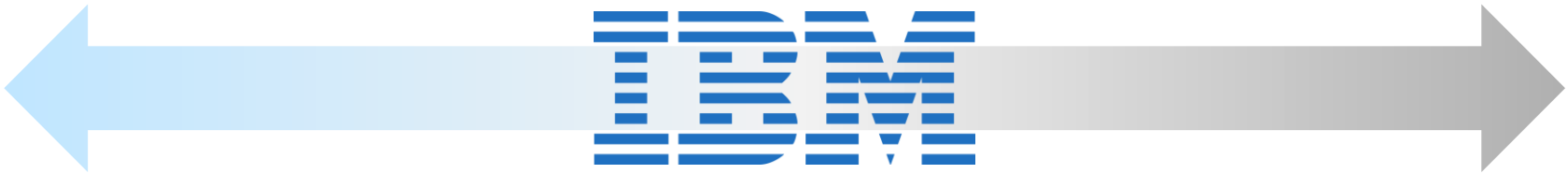
- **Audit** centric
- **Risks** driven (COSO)
- Driven largely by **regulatory requirements**
- **Sample** based
- Scope limited by **audit domain**
- Evaluated on a **quarterly or annual basis**

IT Security

- **Business** centric
- **Policies and Controls** based (COBIT)
- Driven by **business requirements**
- **Scope is Holistic**
  - Enterprise and extended community (E.g. 3rd parties, suppliers, partners, etc.)
- Evaluated on a **near-real time basis**

Mainly is a **Big4 / Audit firms** world…

Mainly is an **IT / Technical companies** world…



1. Introduction to the Debate…

Scope of this session: **GRC**, **Regulatory** and **Business CCM**

1. Governance	**Internal Control**, **Internal Audit**, **Enterprise Risk** and **Regulation Affairs**: Integration and Automation of the Three Lines of Defense
2. Access Management	**Segregation of Duties, Identity and Role Management**: User Access complying with Regulatory Requirements (E.g. SOX)
3. Data Privacy	**GDPR** (and others): Data Retention and Data Deletion, Data Portability, Data Field Masking, Access Logging to Personal Data
4. Business-IT Monitoring	**Continuous Control Monitoring (CCM)**: Configurable and Transactional controls // Fraud Scenarios // RPA // Predictive Risk Analytics
5. Authentication	**Unified Access to SAP systems**: Single Sign-On // **Double Factor Authentication** (Two-Factor) // **Secured Communication**
6. Application Security	**Custom Source Code**: Automated analysis to Identify potential Security Breaches // Optimize Performance using SAP best-practices
7. Application Server	**SAP Server configuration**: Security Parameters of all Clients // Secured Services // Patching Level // OSS Notes
8. Database Security	**SAP HANA**: Secured access to SAP HANA Views and Schemas // Integration with data lakes // Ensure no open paths to access data
9. Data Encryption	**Data Volume Encryption** (SAP HANA) // Usage of SAP **Cryptographic Libraries** // Secured Socket Layer // Public Key Infrastructure
10. Network and Communications	**Pen Testing**: **Securization of RFCs** (Remote Function Calls) // **Support from SAP** // Management of **Web connections**
11. Vulnerability Assessment	**Pen Testing**: **OS users** (broad privileges) // **SAP log analysis** and integration with SIEM solution // Integration of **antivirus** into SAP
12. Infrastructure Security	**Pen Testing**: **Configuration of physical / logical devices**: Firewall and Gateways // OS and Applications Logs
13. Physical Security and Hosting	**Standard Controls Coverage** (SOC reports) // **Compliance Level** of each Cloud platform // Ad-hoc Security audits // Physical hacking

2. Evolution of SAP GRC in the last 15 years

Descriptive, Predictive and… Prescriptive?

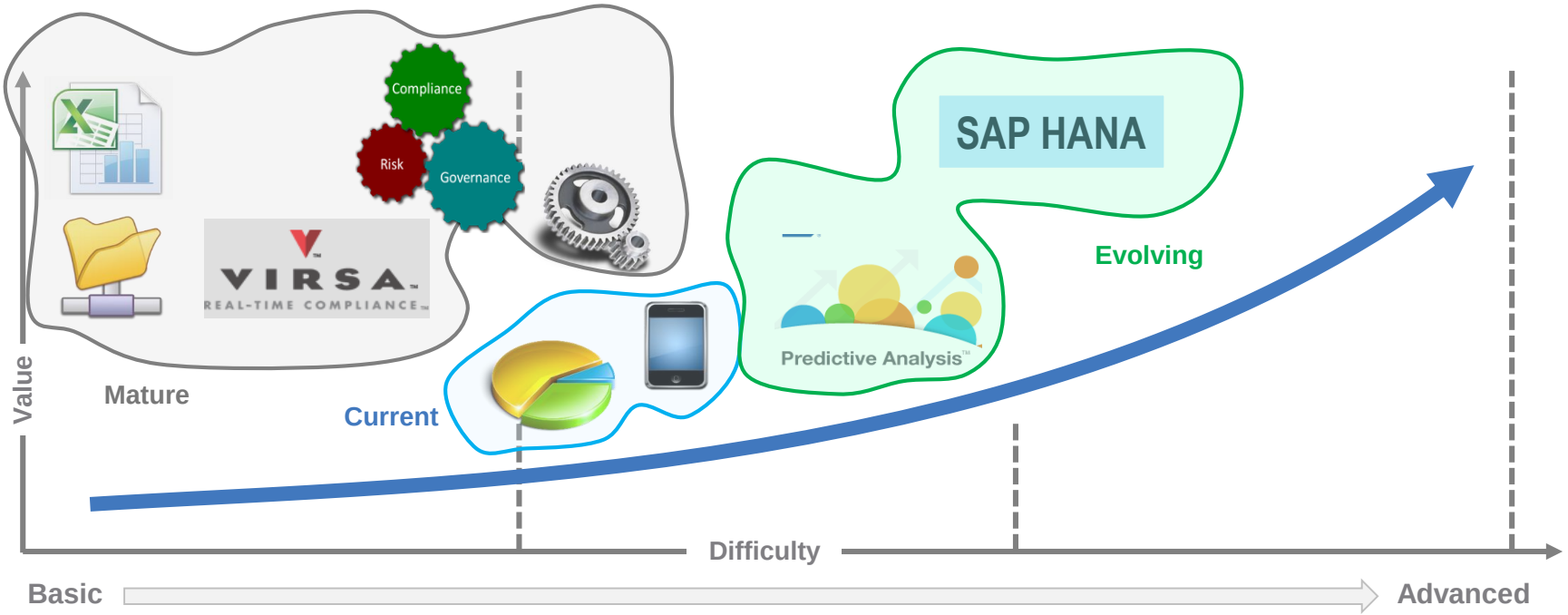
2. Evolution of SAP GRC in the last 15 years

Descriptive, Predictive and Prescriptive scenarios

Descriptive
Data mining over historical data to report, visualize and understand
what happened

Predictive
Usage of historical data to calculate likelihood of an event can happen in the future and know…
what's going to happen

Prescriptive
Determines, in real time, what action and / or decision brings the best and most efficient result
prescribes the best option

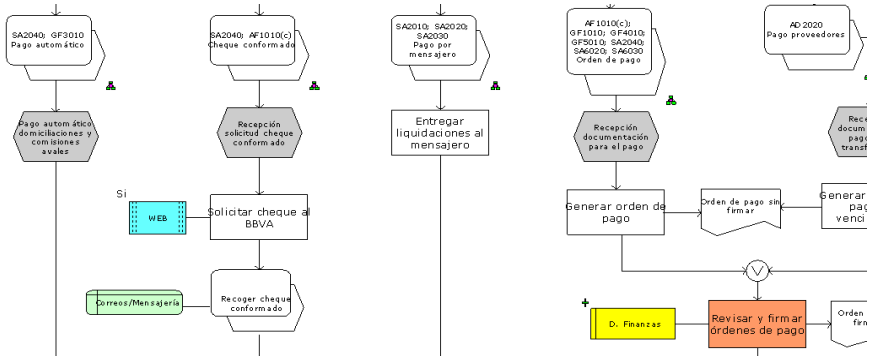


2. Evolution of SAP GRC in the last 15 years

Manual Descriptive (Until 2007)

Actividades Operativas

Nombre	Código	Responsable	Descripción/Definición	Actividad de Control	Tipo de Actividad	Subciclo
Solicitar cheque al BBVA	GF6010.1	Director de Finanzas	Una vez que la Dirección de Finanzas recibe la solicitud de emisión de un cheque conformado por la Unidad solicitante, procede a la solicitud de emisión de este cheque al BBVA (único banco con el que se tiene contratado este servicio) a través de la página web del mismo.	No	Manual	Subciclo de pago y registro
Recibir cheque conformado	GF6010.2	Director de Finanzas	El cheque es recibido por la Dirección de Finanzas.	No	Manual	Subciclo de pago y registro
Enviar a la Unidad Solicitante	GF6010.3	Director de Finanzas	Una vez recibido el cheque éste es enviado a la Unidad Solicitante del mismo.	No	Manual	Subciclo de pago y registro
Entregar liquidaciones al mensajero	GF6010.4	Director de Finanzas	La Dirección de Finanzas le entrega al mensajero las liquidaciones de los impuestos para el pago en el banco.		Manual	Subciclo de pago y registro

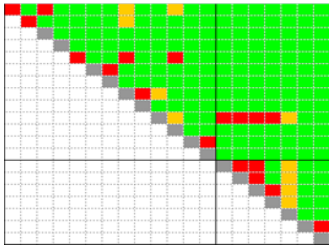


Manual Descriptive

- There is **no automation**
- **No data unicity**
- Big effort spent in perform **manual and repetitive tasks**
- **Low value-added** tasks
- The global compliance picture is **difficult to achieve**
- **Slow data capture**
- **Ineffective follow-up** of process status

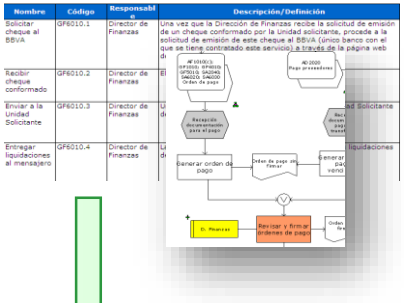
2. Evolution of SAP GRC in the last 15 years

Automatic Descriptive (2007 to 2012)



SoD analysis

SAP GRC
Access Control



CCM

SAP GRC
Process Control

SAP GRC
Risk Management

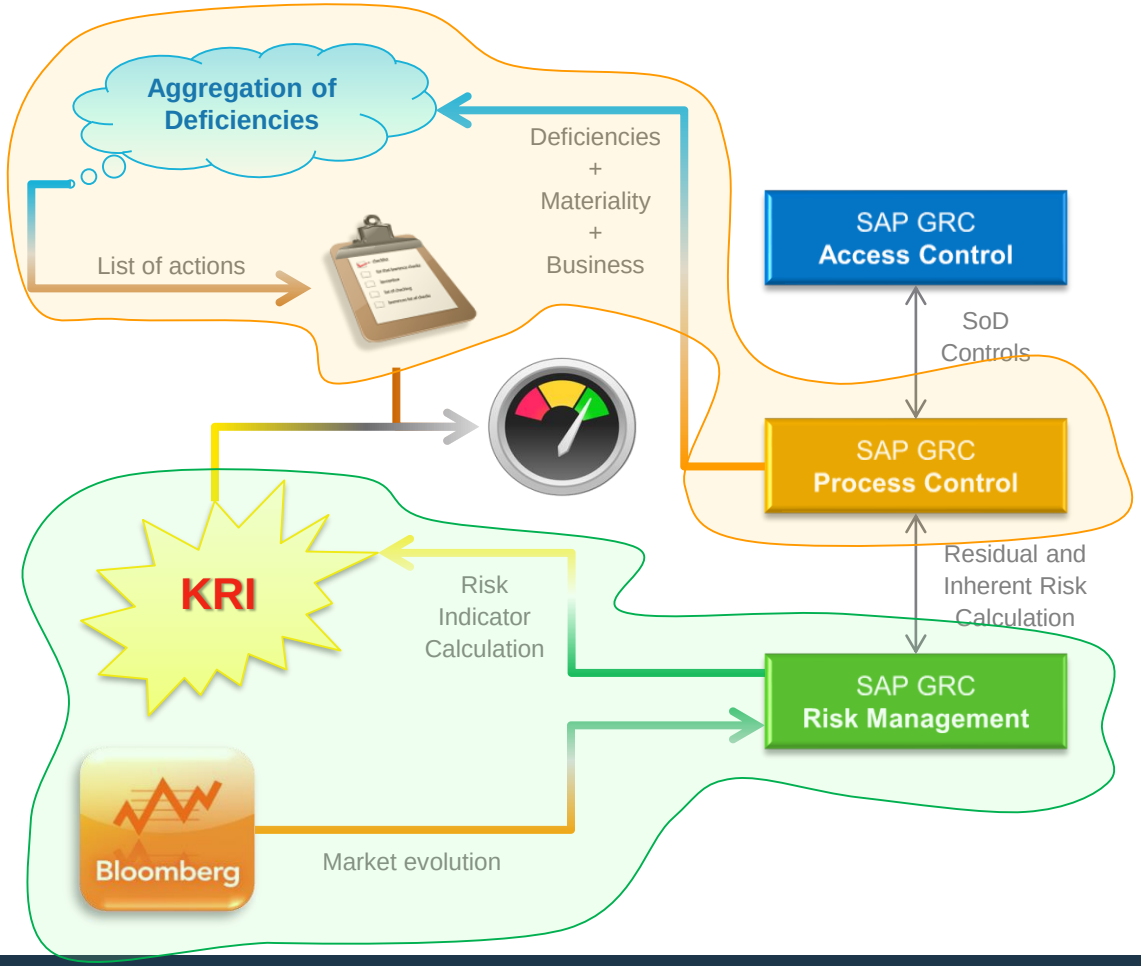
Automatic calculation: Risks & KRIs

Automatic Descriptive

- **Data model** managed with a GRC solution
- Compliance activities **managed through GRC solutions**
- Starting with **off-line models** (data risk download to corporate repositories)
- **Expansion to on-line models** that connect to the data source and exploit the data locally using automations
- **Matrix reporting**
- **Slight solutions integration**

2. Evolution of SAP GRC in the last 15 years

Early Predictive (2013 to 2015)

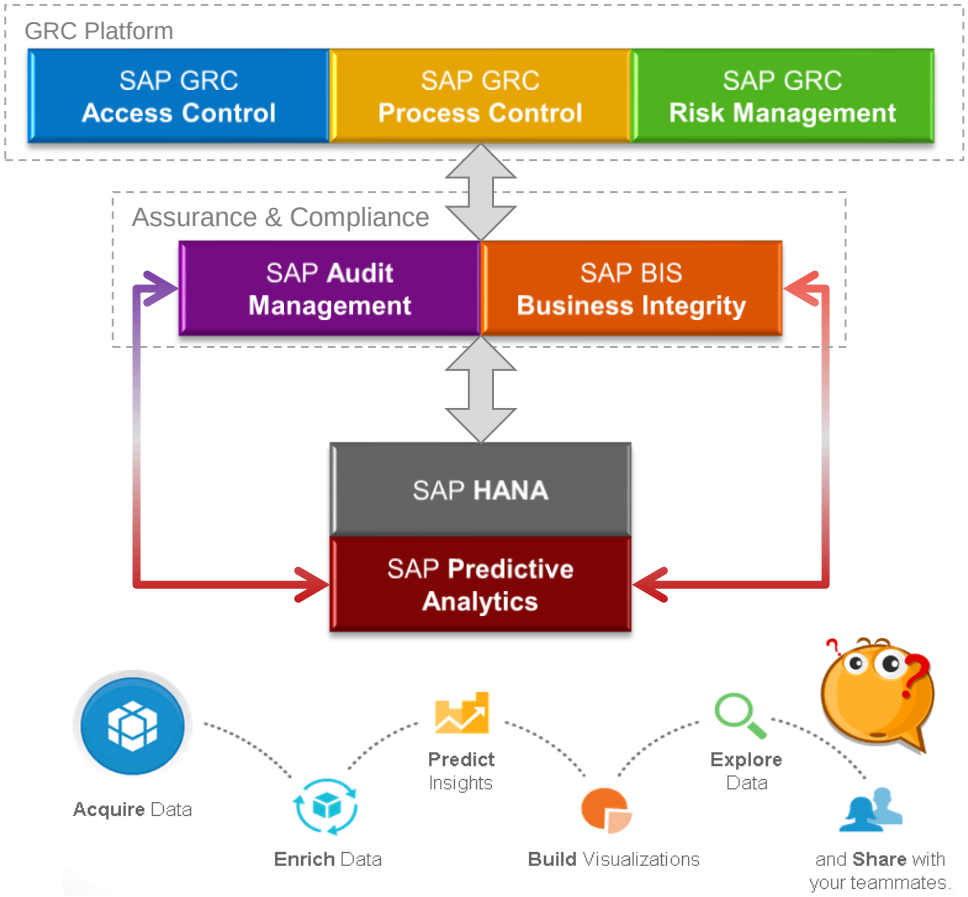


Early Predictive

- All **risk data is automated in GRC solutions**
- The different **GRC tools work in an integrated way**
- **Advanced reporting** (using BI/BO with drill-down capabilities)
- **Data aggregation functions in place**, and data extraction **for decision making** based on basic calculations
- Starting to **integrate with external sources** in an automated way

2. Evolution of SAP GRC in the last 15 years

Predictive Audit (2016 to 2018) – SAP Assurance & Compliance platform



Predictive Audit

- Identify patterns or tendencies that can be formalized as **future controls**
- Anticipate **"outbreaks" of fraud**
- Introducing the concept of **"predictive audit"** based on a "self-service" model
- Estimate the **risk evolution** that can impact in the future business
- **Real-time**, thanks to the usage of "in-memory" technologies / capabilities

2. Evolution of SAP GRC in the last 15 years

Predictive (2017 to 2018)

GRC Platform

SAP GRC **Access Control**

SAP GRC **Process Control**

SAP GRC **Risk Management**

Assurance & Compliance

SAP **Audit Management**

SAP BIS **Business Integrity**

SAP HANA - PAL (Predictive Analytics Library)

SAP **Predictive Analytics**

PAL Algorithms

- Clustering (**12**)
- Classification (**16**)
- Regression (**7**)
- Association (**4**)
- Time Series (**15**)
- Pre-processing (**12**)
- Statistics (**12**)
- Social Networks (**1**)
- Various (**2**)
- **Total: 81**

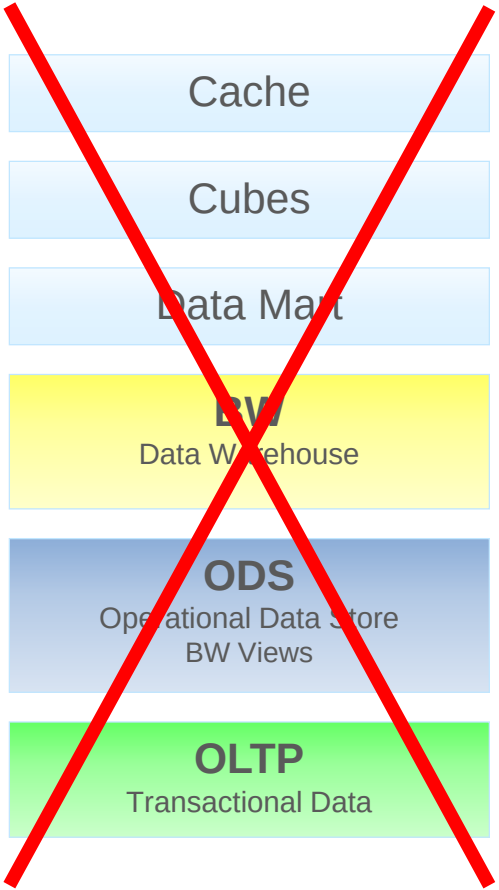
Source: SAP HANA PAL Functions

3. Next steps proposed by IBM in your companies

The reality of companies is far than technology allows today

3. Next steps proposed by IBM in your companies

Importance of SAP HANA → Transformation into GRC / Risk Analytics



SAP HANA

Attribute
View

Analytical
View

Calculation
View

Single Source of Data

Reduces or drops:

- Data Replication,
- Data Aggregation,
- Indexing,
- Mapping,
- Caches and BWA

Data

Transactional = Analytical

3. Next steps proposed by IBM in your companies

Challenges that companies must face in the GRC space

SAP Technological change

- **SAP ECC end of support in 2025** → It will imply a journey to SAP S/4HANA that should start soon
- **SAP GRC 10.1 end of support in 2020** → It will imply migrate to SAP GRC 12.0

Transactional Controls

- **Compliance / GRC moves towards CCM** (Continuous Control Monitoring)
- The usage of **SAP HANA, makes possible tackle transactional controls** that are not possible in Oracle databases
- Having an **SAP S/4HANA system** implies that **all the enterprise transactional is running "in memory"**, and that implies embedded analytics in the business daily activities, including activities related to Compliance and Corporate Governance.

Easier integration with non-SAP systems

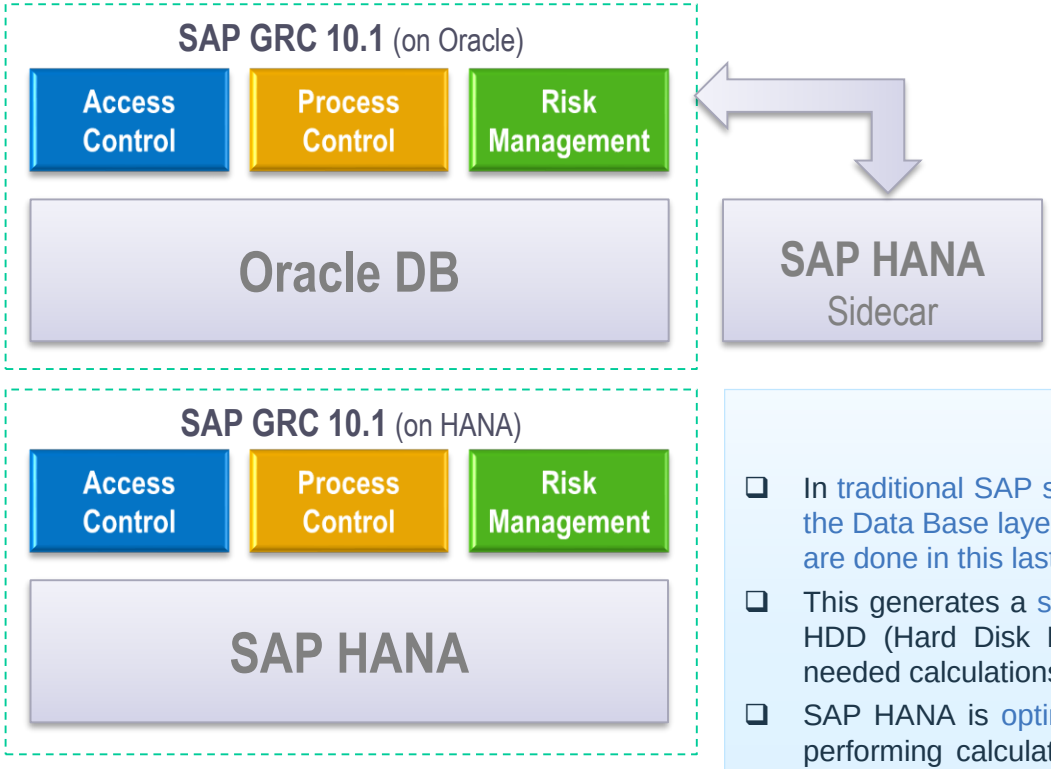
- SAP HANA includes advanced real-time ETLs methods: **SAP Lansdscape Transformation (SLT) Replication**
- No more integration with non-SAP systems via data file upload, or managing automatic controls as manual ones using a testing plan and a set of evidences to be provided to ensure control effectiveness
- SLT allows **non-SAP data replication in specific SAP HANA views per each application**, providing access permission to view, modify and / or execute programmed queries using data included in that SAP HANA views

Integration with data-lakes (E.g. Hadoop)

- SAP HANA integration, using SAP Vora, with Apache Spark (Hadoop component for managing of data clusters) allow the usage of data hierarchies or analytical modelling typical in in SAP HANA, over Hadoop data

3. Next steps proposed by IBM in your companies

Comparison of SAP GRC 10.1 Oracle vs. SAP GRC on HANA (native or using a sidecar)



SAP HANA Sidecar

- The company can continue using their SAP GRC System on Oracle "as-is", while using a secondary SAP HANA "database" to speed-up the execution of some automatic controls
- It allows us test which would be the potential performance improvement obtained for those controls that would use the HANA technology

Oracle vs. SAP HANA

- In traditional SAP systems SAP (on Oracle), the data are transferred from the Data Base layer to the Application layer, and the calculations over data are done in this last layer.
- This generates a significant latency time in the transfer process, from the HDD (Hard Disk Drive) to the RAM memory, in order to perform the needed calculations at application level.
- SAP HANA is optimized to perform massive parallelized processing and performing calculation only at the "database layer", that in addition runs "in-memory", in this way **only the result of calculations are sent to the application layer**.

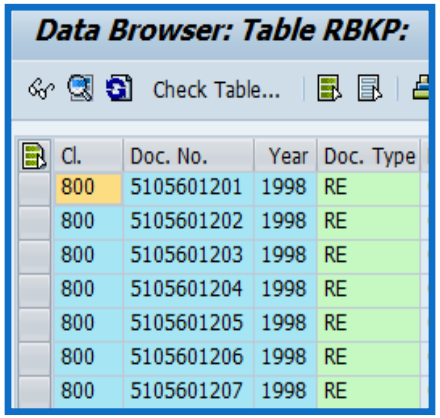
3. Next steps proposed by IBM in your companies

Automatic Controls over “Transactional Data” → **Time consuming programmed queries on SAP HANA**

- The automation of controls using **SAP Process Control with SAP HANA** allows the analysis of the entire testing universe, consuming a very low time-frame, and providing a real-time reporting for transactional controls.

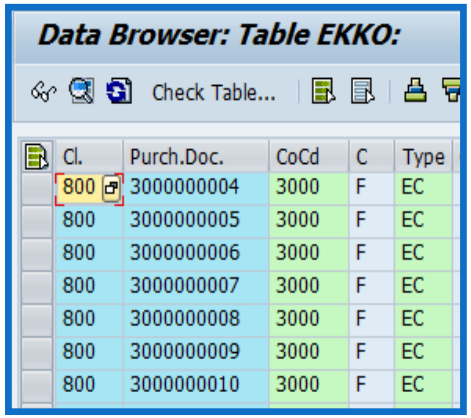
Functional Control: Total amount of invoice cannot exceed the total of the purchase order in any case
Review of **all cases of testing universe**

Technical Approach: JOIN of SAP Tables: **RBKP** (Invoices) and **EKKO** (Purchase Order)



> 5 Millions

JOIN



> 13 Millions

> 65 * 10^{12} reg.

65 Billions!!!

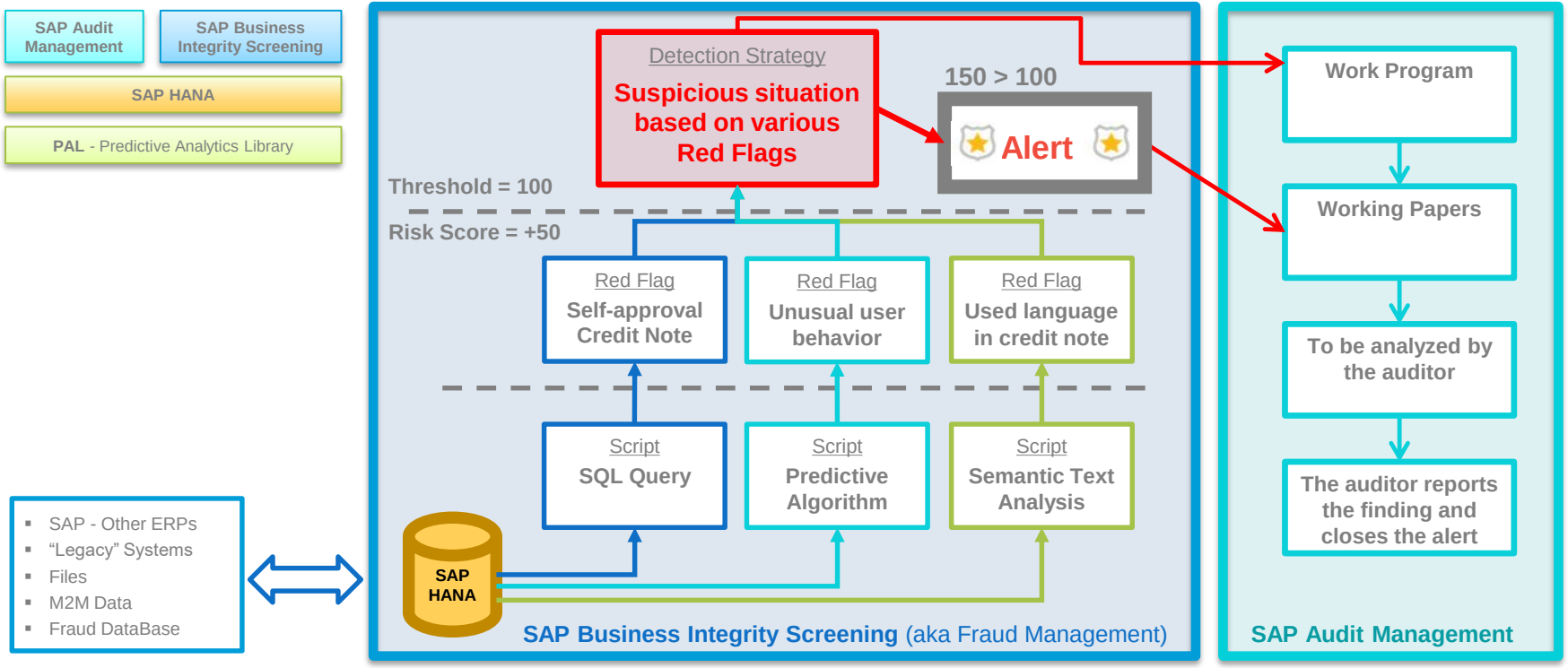
>24 Hours
(Traditional SQ01 query on Oracle DB)

3 minutes
(Programmed query on SAP HANA)

3. Next steps proposed by IBM in your companies

Automatic Controls over “Transactional Data” → **Fraud scenario analysis on SAP HANA**

- The automation of controls using **SAP Business Integrity Screening** allows the combination of more than one automatic control in the same scenario, combining all of them based on weights, and **enabling the option to block the execution of the SAP t-code in live**.



3. Next steps proposed by IBM in your companies

1. Continuous Control Monitoring (CCM) → Transactional Controls with HANA

1. IT General Controls (ITGCs) — **In-scope for clients with SAP "on Oracle"**

- Basically a set of "**Configurable**" controls. Check of a "parameter" in a table with a maximum of hundreds of records + check of "Log" to ensure that nobody changed that parameter in the audited period.
- No need of "in-memory" capabilities (as SAP HANA). **Can be implemented using a SAP Process Control system on Oracle**.

2. Business Financial Controls (Configurable Controls)

- Same approach than ITGCs… but for Financial Controls. **Can be implemented using a SAP Process Control system on Oracle**.

3. Semi-automatic controls (SAP Reports)

- Identification of SAP standard reports that cover business requirements, and that can be semi-automated as SoD controls.

4. SoD Automatic Controls (Linkage with SAP Access Control rule-set)

- **A SoD risk analysis can invoked from SAP Process Control**.
- This type of control would be a kind of semi-automatic control, due that SAP Access Control will perform the risk analysis and will present a report with the SoD conflicts identified. **The control owner will review the report and decide** about if all the users that have potential access to the SoD are approved by the organization (by business needs, or impossibility to segregate both functions).

5. Transactional controls (Requires the usage of SAP HANA)

- **Process Control** (on SAP HANA): Controls that require the join of two or more tables with hundreds of thousand, or millions of records, in order to check all the audit universe.
- **Business Integrity Screening** (on SAP HANA): Combination of transactional automatic controls, with different weights assigned to each one of them, to model a potential fraud scenario. **Can block the execution of a SAP transaction in on-line**.
- **Non-SAP controls** (on SAP HANA): Identification of non-SAP systems, creation of SLT replicator and synchronization of the data in the HANA database to execute automatic controls over that. **It's not a real-time automatic control.**

In-scope ONLY for clients with SAP "on HANA"

3. Next steps proposed by IBM in your companies

Regulation Affairs: SAP Regulation Management → Data Import from SAP Process Control

GRC Platform

SAP GRC **Access Control**

SAP GRC **Process Control**

SAP GRC **Risk Management**

Process Control Sync

Name *

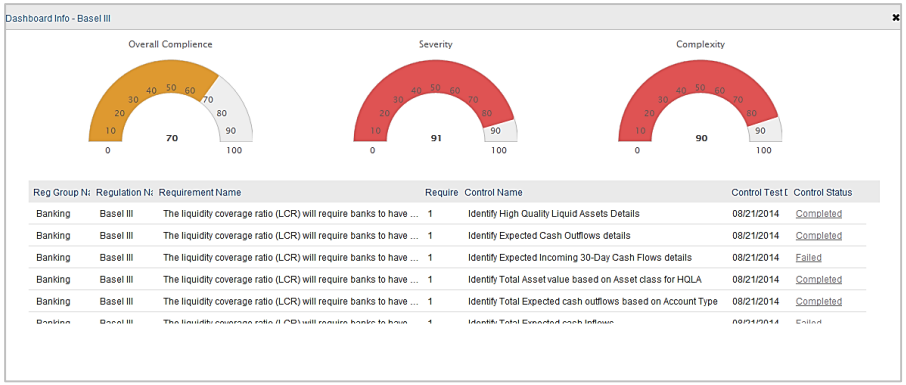
Name	Priority
Organization	1
BusinessProcess	2
BusinessSubProcess	3
BusinessOrgAssociation	4
RegulationGroup	5
Regulation	6
Requirement	7
Control	8

1. SAP RM "reads" the compliance data from GRC PC

SAP **Regulation Management** by Greenlight

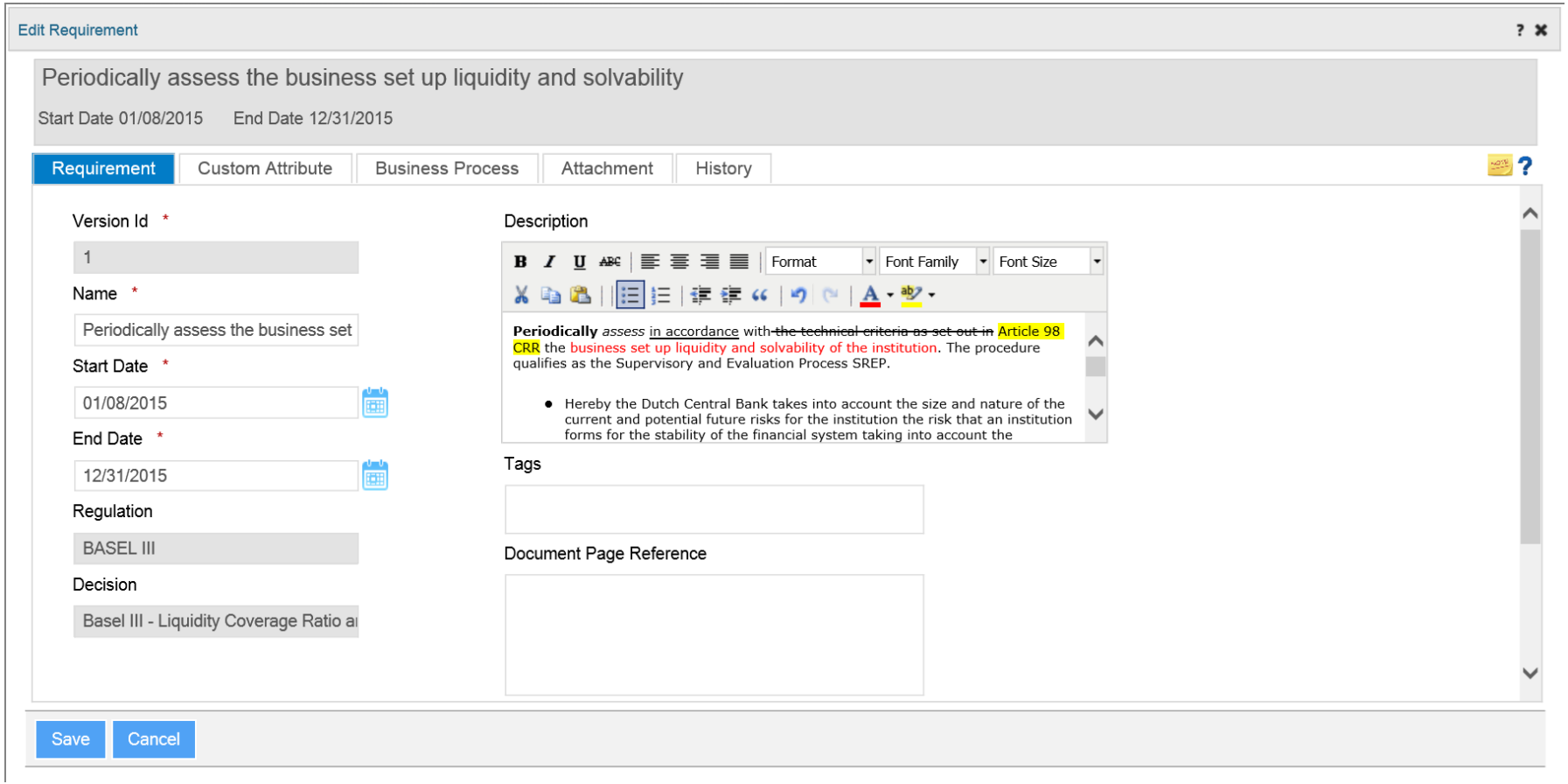
2. SAP RM exploits this information using the "requirements" defined in GRC PC, and consolidating the results in drill-down reports and dashboards

1. Regulation Group
2. Regulation
3. Requirement



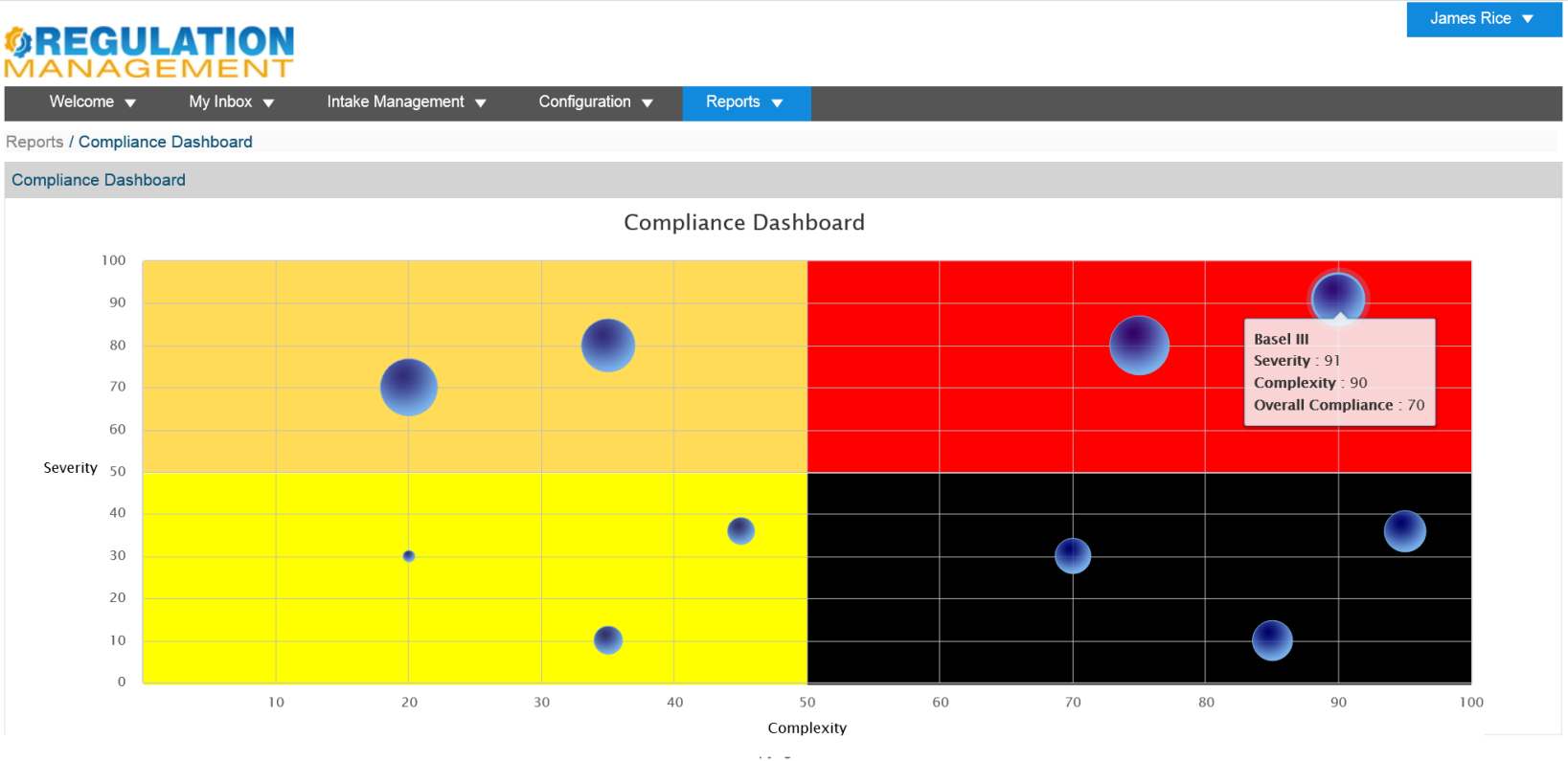
3. Next steps proposed by IBM in your companies

Regulation Affairs: SAP Regulation Management → Requirements Change (Tracking)



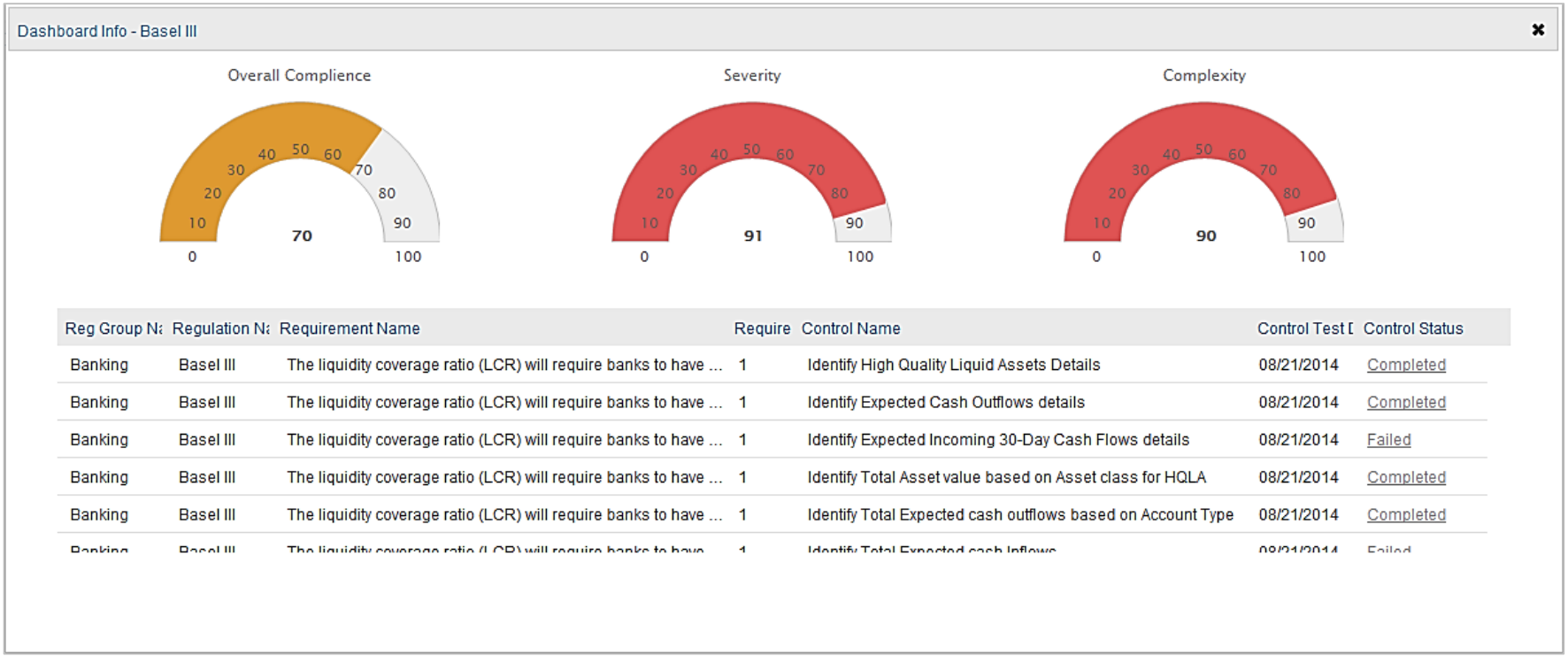
3. Next steps proposed by IBM in your companies

Regulation Affairs: Compliance Dashboard → Drill-down capabilities



3. Next steps proposed by IBM in your companies

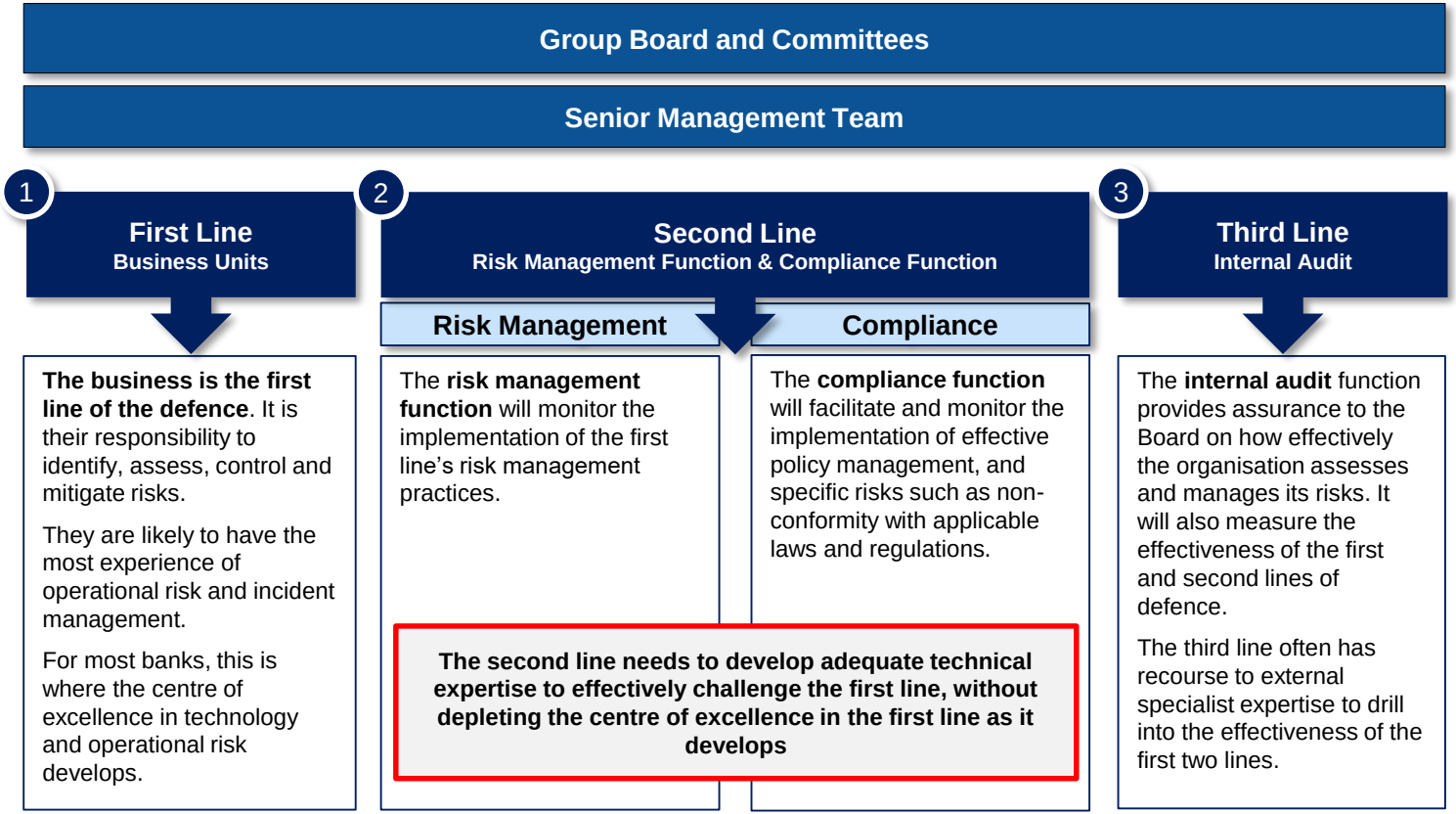
Regulation Affairs: Regulation Dashboard → “Requirement” and “Control” linkage



Reg Group Na	Regulation Na	Requirement Name	Require	Control Name	Control Test D	Control Status
Banking	Basel III	The liquidity coverage ratio (LCR) will require banks to have ...	1	Identify High Quality Liquid Assets Details	08/21/2014	Completed
Banking	Basel III	The liquidity coverage ratio (LCR) will require banks to have ...	1	Identify Expected Cash Outflows details	08/21/2014	Completed
Banking	Basel III	The liquidity coverage ratio (LCR) will require banks to have ...	1	Identify Expected Incoming 30-Day Cash Flows details	08/21/2014	Failed
Banking	Basel III	The liquidity coverage ratio (LCR) will require banks to have ...	1	Identify Total Asset value based on Asset class for HQLA	08/21/2014	Completed
Banking	Basel III	The liquidity coverage ratio (LCR) will require banks to have ...	1	Identify Total Expected cash outflows based on Account Type	08/21/2014	Completed
Banking	Basel III	The liquidity coverage ratio (LCR) will require banks to have ...	1	Identify Total Expected cash Inflows	08/21/2014	Failed

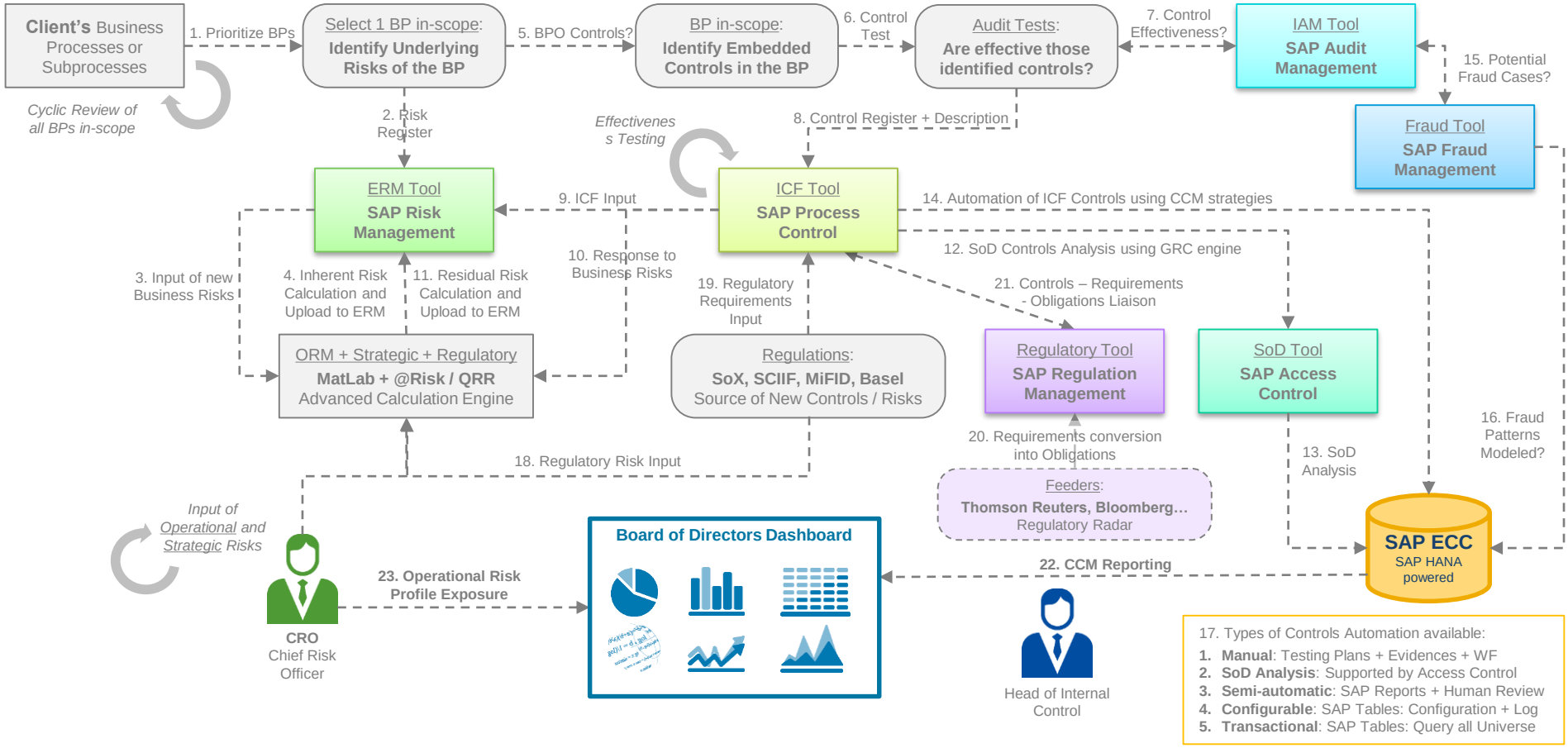
3. Next steps proposed by IBM in your companies

The Three Lines of Defense: Main Actors and Stakeholders involved



3. Next steps proposed by IBM in your companies

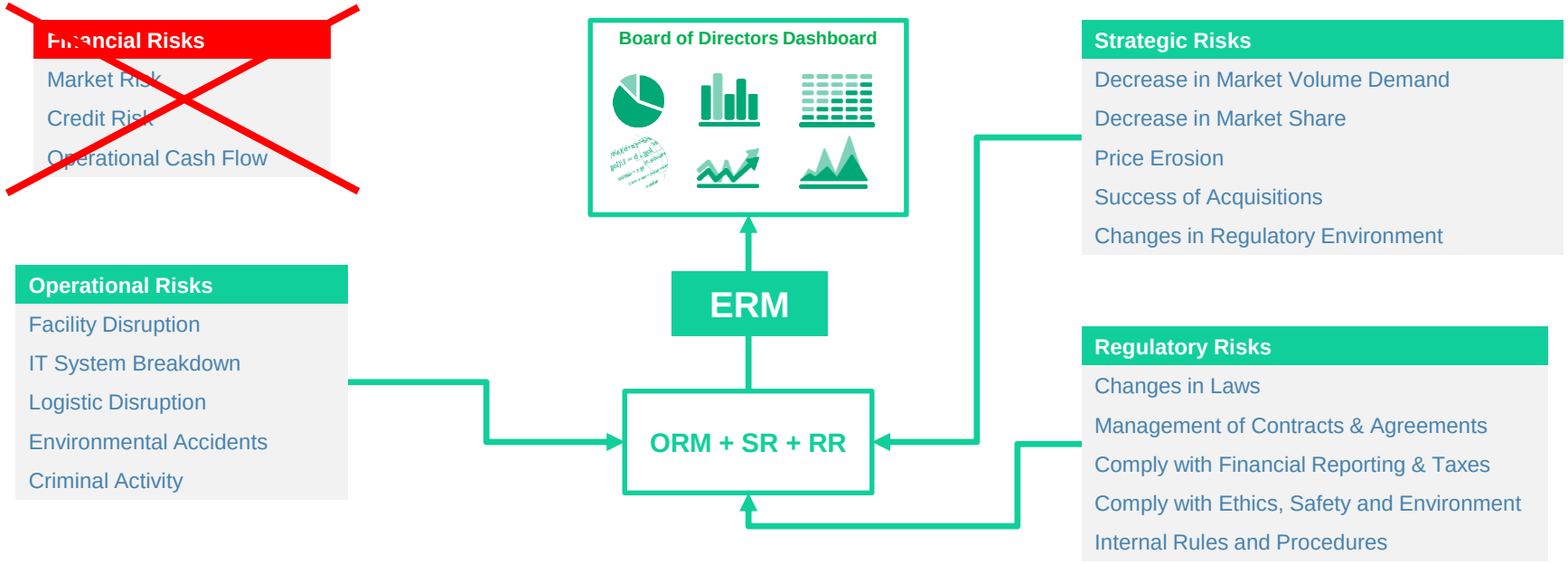
The Three Lines of Defence Automation → A Risk-driven approach



3. Next steps proposed by IBM in your companies

ORM (Basel III): The rigor of banking quantitative risk models applied to other sectors

Many (non financial / banking) companies are starting to include to their current Strategic Risk model, the addition of the Operational Risks and Regulatory Risks, whose scenarios are quantifiable from a financial / operational point of view, to **build an extended ORM model**, that will provide the **Operational Risk Exposure profile level per BU, BL and Consolidated** to the Company Group level, that will be reported to the Board of Directors.



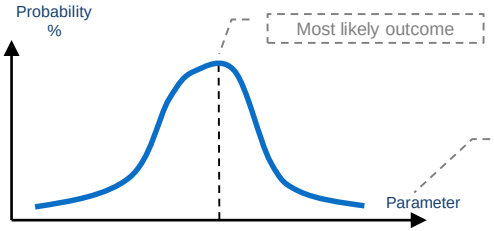
3. Next steps proposed by IBM in your companies

ORM (Basel III): Quantification based on Probability Distribution and Impact on Cash Flow

Improvement of the Enterprise Risk Management models moving from a deterministic approach based on expert criteria of the key BU's stakeholders to a brand new **hybrid stochastic model** where main Financial KPI's will be the base for a mid-term / long-term calculation

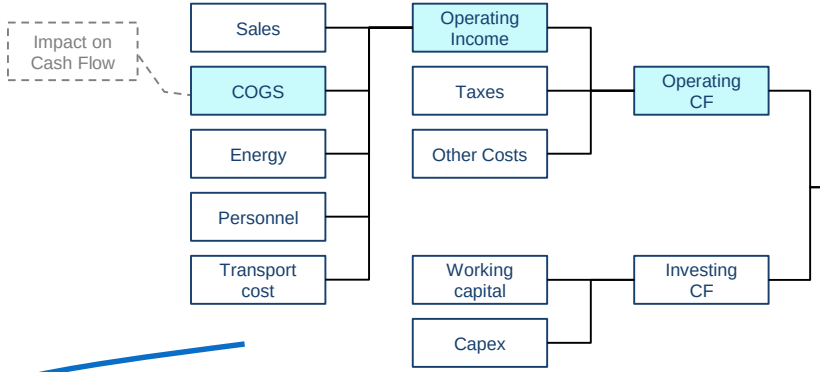
Main Risk → **Driver Chosen**

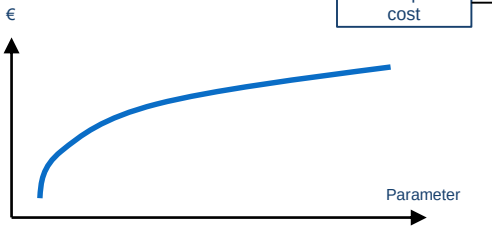
- **Probability Distribution**
- **Impact's "Location"**
- **Impact on Cash Flow**
- **Correlations**



With the assistance of the BU's management expert input this curve and it's evolution over time

Metric that measures impact on Cash Flow





With the assistance of the BU's management expert input this curve and it's evolution over time

With the assistance of the BU's management opinion on correlations between drivers and/or main risks, where required

4. The Rabid Future of GRC

Machine Learning

4. The Rabid Future of GRC

Machine Learning

- Although many companies are in a pretty immature status yet, the **controls automation via CCM** is, from a technical perspective, **a goal more than achieved**.
- Some people is talking about ~~**making RPA in GRC**~~. That's a wrong concept, because GRC don't automate processes itself, only automates the testing of the processes, identifying the issues.
- The next step that is coming, is **embed Machine Learning, in our GRC / Compliance**.
- SAP is doing a significant investment on the **SAP API Business Hub**, where there is a consumable pre-trained models, as well as customizable models.

  https://api.sap.com/package/SAPLeonardoMLFunctionalServices?section=Artifacts
- At this moment, **SAP is developing models that can be applied to different business process**, and that are used to self-learn (unsupervised learning).
- The SAP GRC solution that will integrate these models is **SAP Business Integrity Screening**.
- SAP is also doing an effort to integrate SAP HANA with other statistical programming platforms, as "R"

  https://help.sap.com/doc/6f2ff4c50f7e4e4d90b93aa33652d063/2.0.03/en-US/SAP_HANA_R_Integration_Guide_en.pdf

5. Q&A

Questions & Answers

5. Q&A

Questions and Answers

IBM Contacts

Victor Garcia Rodriguez
- Associate Partner
- Phone: +34 682 38 44 08
- Mail: victor.garcia.rodriguez@ibm.com

Raffaella Cannone
- Managing Consultant
- Phone:+39 349 6075255
- Mail: raffaella.cannone@it.ibm.com

IBM Security

THANK YOU!

FOLLOW US:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube.com/user/ibmsecuritysolutions

IBM