

# Lloyd's Market Briefing: SAP GRC for Risk, Fraud and Cyber

Dr. Neil Patrick, COE GRC (EMEA), SAP  
4<sup>th</sup> July 2016



# © 2016 SAP SE or an SAP affiliate company. All rights reserved.

---

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://global12.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

# Key themes: solutions for GRC and security from SAP



Access governance

**Audience:**

- CIO or director of IT
- CFO
- CISO



Cyber security risk and governance

**Audience:**

- CIO
- CFO
- CISO



Three lines of defense

**Audience:**

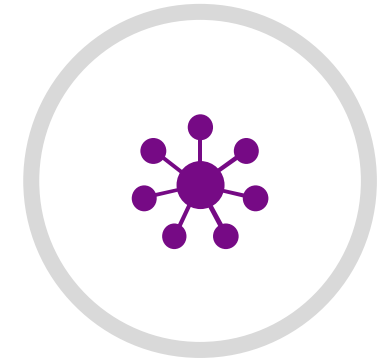
- CxO (CFO, CRO, CCO, or CAE)
- Director of IT and access management



International trade management

**Audience:**

- VP of supply chain
- Director of trade compliance
- CFO



Fraud management and screening

**Audience:**

- CAE
- Director of internal audit
- LoB VP (Procurement)
- Legal

# SAP solutions for governance, risk, and compliance (GRC)

Simplify, gain insight, and strengthen



## SAP Access Control

Enable business-driven access governance



## SAP Access Violation Management by Greenlight

Identify and quantify the impact of actual access risk violations



## SAP Dynamic Authorization Management by NextLabs

Secure applications, protect application data, and simplify role management



## SAP Regulation Management by Greenlight, cyber governance edition

Manage cyber-related regulatory requirements and align with internal controls



## SAP Process Control

Maintain effective controls and ongoing compliance



## SAP Regulation Management by Greenlight

Manage regulatory requirements and align with internal control activities



## SAP Risk Management

Preserve and grow value with enterprise risk management



## SAP Audit Management

Transform auditing and move beyond assurance



## SAP Fraud Management

Detect and prevent fraud better



## SAP Business Partner Screening

Grow your business network with confidence



## SAP Global Trade Services

Optimize global trade and screen restricted parties



## SAP Technical Data Export Compliance by NextLabs

Automate trade compliance for digital goods and technical data



## SAP Electronic Invoicing for Brazil

Meet electronic invoicing requirements for Brazil

# Solutions for security from SAP

---



## SAP Enterprise Threat Detection

Detect, investigate, and respond to anomalies



## SAP Single Sign-On

Authenticate once to access all business applications



## SAP Identity Management

Know your users and what they can do



## SAP Cloud Identity

Manage the identity lifecycle in the cloud



## SAP NetWeaver AS, add-on for code vulnerability analysis

Analyze code for security risks



## SAP Mobile Secure

Manage cyber risks for mobile devices

# Cyber-Attack: Enterprise Defence

# Overview: This is Your Digital Transformation Future

---

**In the last two years:**

**90%**

Of the world's data has been generated<sup>1</sup>

**40%**

Growth in adoption of business networks<sup>2</sup>

**7-fold**

Increase of MTM patents through WIPO 2010 to 2014

**6**

Devices per person on-line by 2025 (50 billion)<sup>3</sup>

**205**

Average days to realize there is a cyber breach

**51%**

Of workload processed in the cloud in 2014<sup>4</sup>

---

<sup>1</sup> *ScienceDaily*, May 22, 2013.

<sup>2</sup> *Technology Adoption Report on Business Networks*, Ardent Partners, 2014.

<sup>3</sup> *Ericsson*

<sup>4</sup> *Cisco Global Cloud Index: Forecast and Methodology for 2013–2018*, Cisco Systems Inc., November 11, 2014.

# Trends in Attack

## Evolution of Fraud - Visa Europe

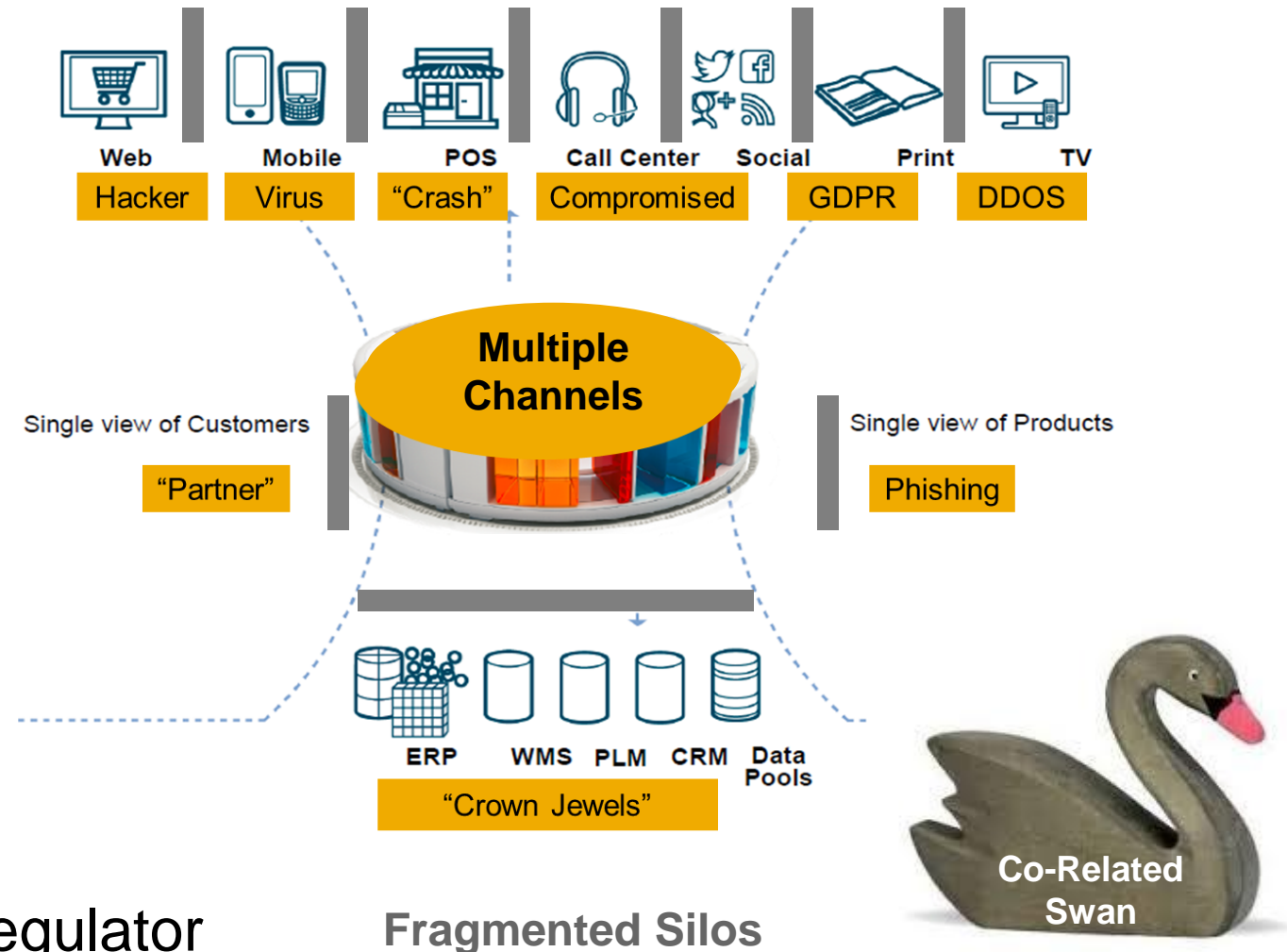
	2000	2015
Fraudsters	Local crime rings	Global crime rings Decentralized
Target	Large retailers	Payment Industry
Technique	ID Theft, Phising Rudimental data	Cross Border, Online, ID, Phising Hacking: Cyber crime
Type	Mass market credit cards	All types of cards Bank Accounts
Resources	Technical know how	Audacity Technical expertise Global connections

**Operates as a big business**



# Silo Defence vs Joined-up Attack

- Many more channels
- Criminals – organise to exploit channels
- Growth of internal fraud/criminal behaviour
- Fragmented & complex employee & partner community
- Increasingly intrusive and punitive regulator



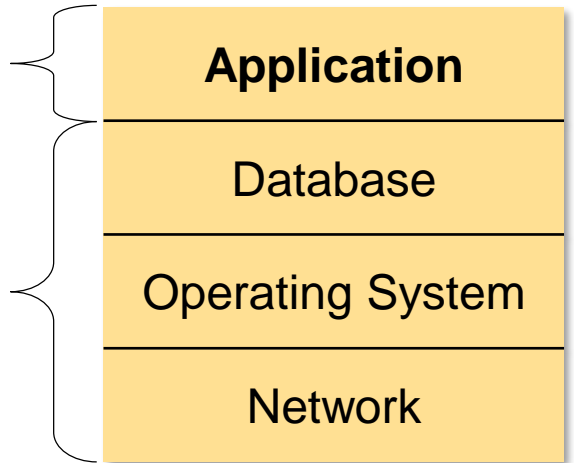
# Focus on Where the Important Data Resides

## SAP Enterprise Threat Detection:

- **Applications** keep the **crown jewels**, yet they are often neglected
- Analysis of **application** log pinpoints activities **not visible** or understandable in other analyses
- Correlation of event **context** across logs and across systems, and not just “expected” threats
- Complexity and processing **speed** and power from HANA is significant

Focus of Enterprise Threat Detection

Focus of SIEM systems



Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

WE **PARTNER** WITH SIEM SOLUTIONS

# Broader Perspective: SAP Cyber Risk Defence Approach

Risk assess value of assets,  
determine cost of protection

**Risk Management**

Control access to approved  
visitors

**Access Control**

Detection of intruders

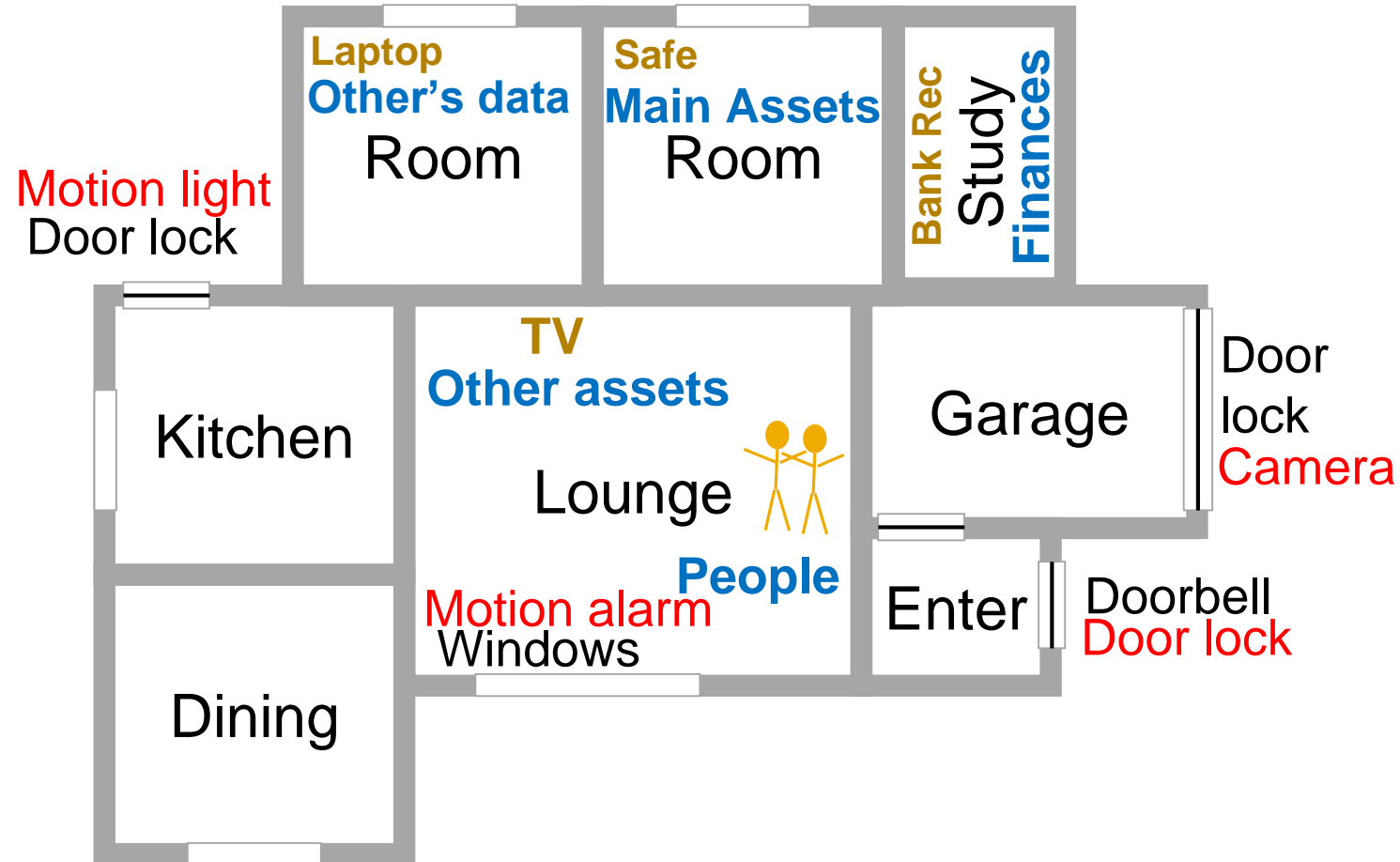
**Enterprise Threat Detection  
Fraud Management**

Routines to 'make safe' at night,  
when away (BAU)

**Process Control  
Code Vulnerability Analysis**

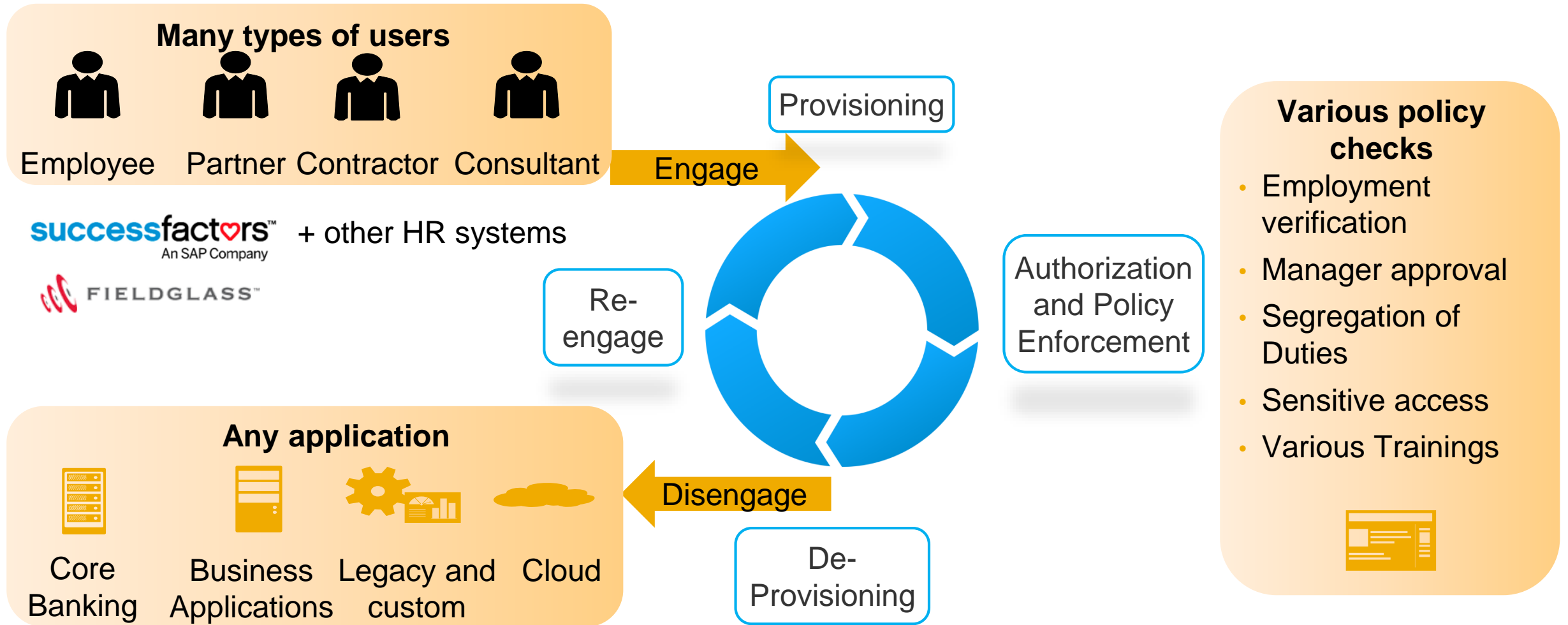
Read news for latest scams,  
am I protected?

**Cyber Regulation Management**



# HR/AD Integrate to Provisioning

# Access Governance via HR System: Manage Legitimate Access



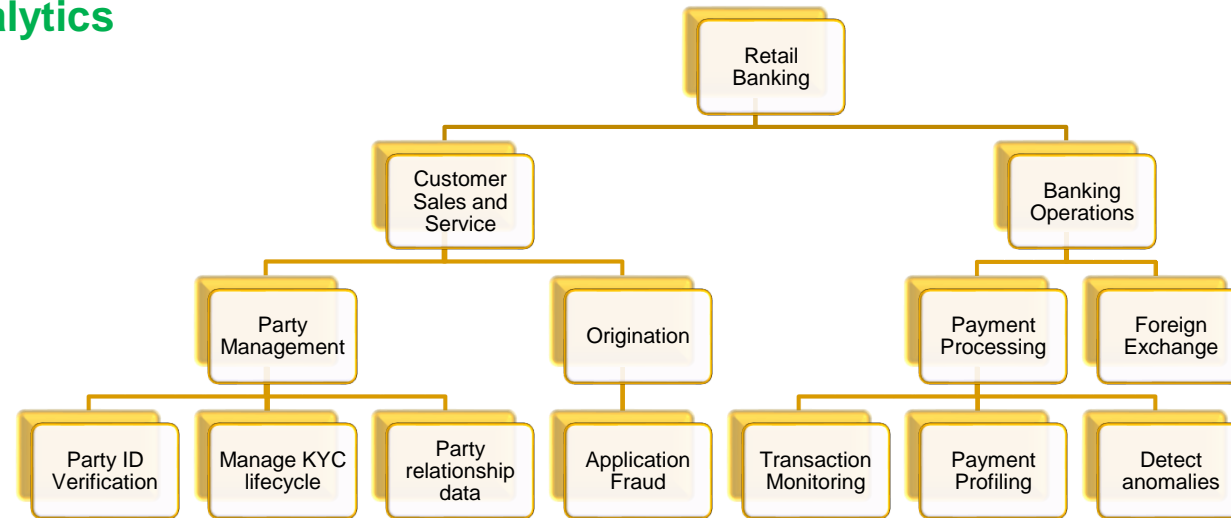
# Policy, Process, Regulations

# Policy + Controls + Processes + Tests + Audit Trail

Organization and Process .... **and Automation**

Support decisions and promote accountability with insightful **analytics** and **sign-off**

Document **controls and policies** centrally; **map to key regulations** and impacted organizations



Perform **automated, exception-based monitoring** of ERP systems (includes non-SAP)

Evaluate control **design and effectiveness**; raise and remediate issues

Perform **periodic risk assessments** to determine scope and test strategies

# Define Business as Usual Controls, Link to Org Structure + Policy

My Processes

Regulation: All

- All
- ABAC Regulation (ABAC)
- CAPA Regulation (CAPA)
- Financial Regulation (FIN)
- HR Regulation (HR)
- IT Regulation (IT)
- Operational Regulation (OPS)

Policies

Show Year 2014 Apply Advanced Create Open Copy Actions

Name	Type
Policy Hierarchy	Policy Hierarchy
General Corporate	Policy Group
CIA Agreement	Policy
EH&S Policy and Guidelines	Policy
External Communications Policy	Policy
R&S Investment Policy	Policy
Anti-Bribery and Corruption Policy	Policy
Employee Code of Ethics	Policy
Finance and Accounting	Policy Group
Human Resources	Policy Group
Information Technology	Policy Group
Industry-Related Policies	Policy Group
Anti-Money Laundering	Policy

Anti-Bribery and Corruption Policy

### Introduction

The purpose of this policy is to establish controls to ensure compliance with all applicable anti-bribery and corruption regulations, and to ensure that the Company's business is conducted in a socially responsible manner.

Bribery is the offering, accepting, or soliciting of an advantage as an inducement for action which is illegal or a breach of trust. A bribe is an inducement or reward offered, promised, or provided in order to gain any commercial, contractual, regulatory or personal advantage.

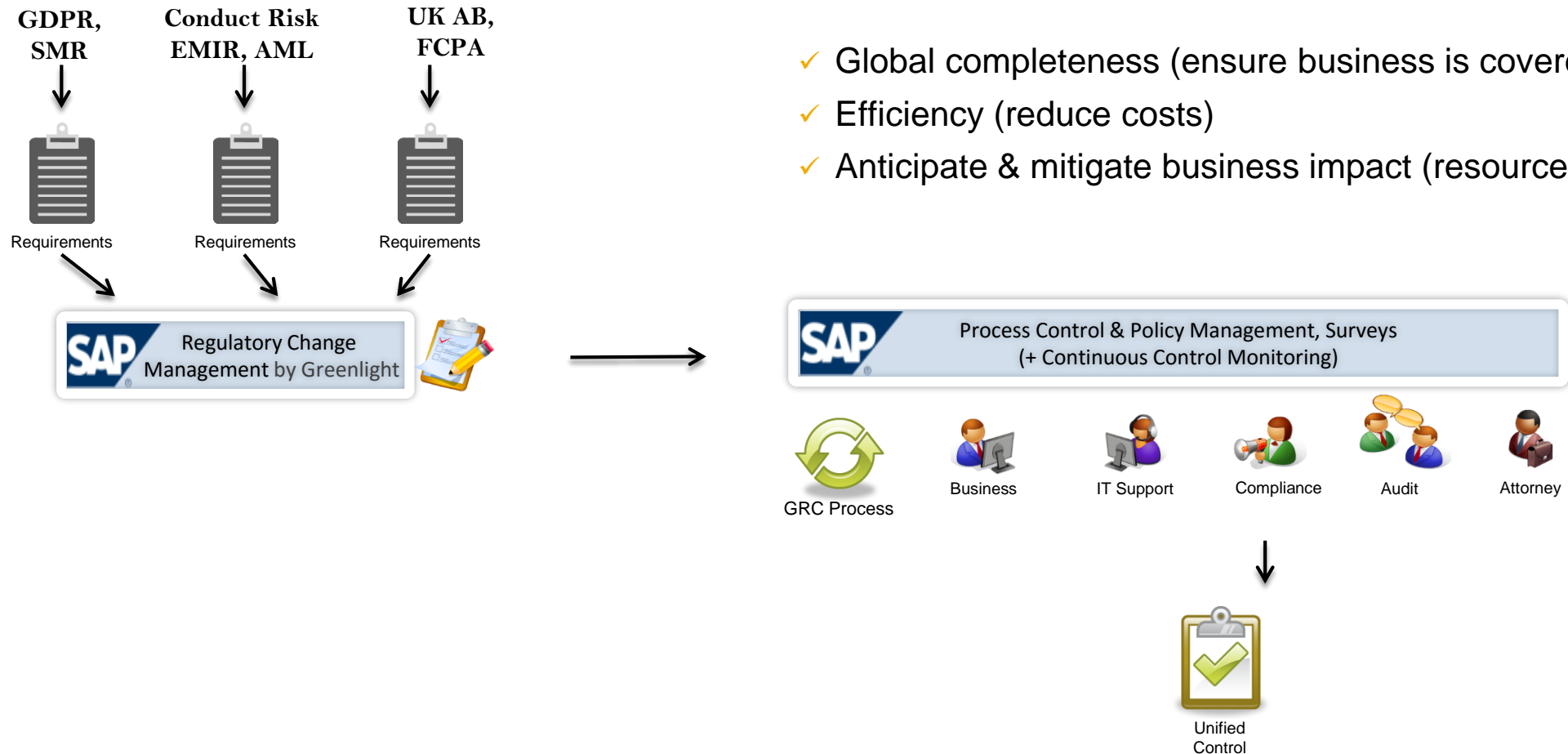
It is our policy to conduct all of our business in an honest and ethical manner. We take a zero tolerance approach to bribery and corruption. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships. We are committed also to implementing and enforcing effective systems to counter bribery and to uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate.

### Scope

In this policy, third party means any individual or organization you come into contact



# RegTech – Reduce Cost of Regulatory Compliance



- ✓ Global completeness (ensure business is covered)
- ✓ Efficiency (reduce costs)
- ✓ Anticipate & mitigate business impact (resource Mgt)

# Putting it Together with Profiling

# Achmea: Focus on Insurance Fraud



## Company

Achmea

## Industry

Insurance

## Employees

22,000

## Revenue

25B Euro

## Customers

7M

## Other details

Gross Written

Premiums 20,223M €

- One of the largest financial service providers in NL
- Providing about half of all Dutch households with health, life, and non-life insurance.
- 60 FTEs in Fraud Investigation
- Business Case:
  - >3% of claims believed fraudulent
  - P&C
    - 1M claims p.a. (Auto, Homeowner, ..)
  - Health
    - Largest cases w/ health care services providers

*"SAP Fraud Management enables Achmea to be successful in her fight against fraud in insurance"*

Sjoerd van der Klaauw, Achmea

## Focus on Real Fraud

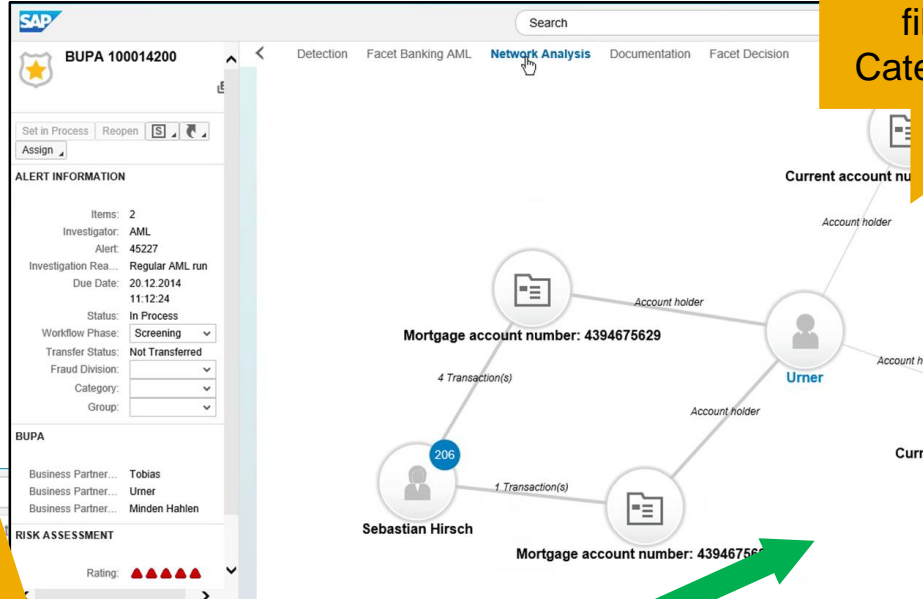
- **Business Benefit #1: Single End-To-End FM Platform**  
Ability to detect/prevent claim fraud across mult. LOBs (Phase 1 P&C, Phase 2 Health)
- **Business Benefit #2: Minimize Fraud Losses**  
Minimizing payments on illegitimate claim requests & directly impacting company's loss ratio. Detection: Legacy (<1%); SAP (>1%)
- **Business Benefit #3: Fraud Investigator's Direct Control Over Rules**  
Quality (and ease of adjustment) of rules, resulting in speed to reduce # false positive hits

# Pattern Spike based on Type, Threshold, new Vulnerability

**1** Rules-based alert, real-time, calibrated.  
Financial, Maritime-Cyber  
Business user maintained

**2** Investigate alert for malicious activity. Geo, nationality, bank files, transfer agencies. Categorise. Attach evidence.

Patterns over time, contextualised data for 360° viewpoint  
**3** Conclude investigation. Calibrate strategy effectiveness. Feed back to design



**Detection Strategies (1)**

Detection Strategy	Description	Detected On	Score	Threshold
EXTFR-STRATEG...	Fraud suspicion in current account	21.01.2015 11:57:13	115	100

**Detection Methods (4)**

Detection Method	Description	Risk Score	Contribution	Evaluation	Parameters
EXTFR_AM_HIGMAX_02	Amount higher than max amount of previous period	30	26,09 %	Previous highest amount: 1948.00€ Transactions in 01/2015 above highest amount: -> Transaction ID "553368" with amount of 50000.00€	Analyzed premonths for calculation : 2 Threshold percent : 100
EXTFR_LOGIN_LANG	Login Language different to Nationality / Domicile	35	30,43 %	Nationality: Turkish, Domicile: German -> Last Login Language is Russian. Transactions: 25. Amount: 67000.00€.	
EXTFR_AGE_CUSTOMER	Customer older than threshold	30	26,09 %	Customer is 71 years old. Birthday is: 1942-July-07	Business Partner older than X years : 40
EXTFR_LIMIT_CHANGE	Check for limit change on account level	20	17,39 %	Account limit has been changed by 900%.	Account limit change in % : 10

**Alert Items (2)**

Detection Object	Lifecycle Status	Reason for Closing	Finding	Financial Outcome
Bank Account - 4394675627	In Process			
Bank Account - 4394675629	In Process			

**Bank Account - 4394675627**

\*Summary: Clear evidence of AML violation because of...

\*Finding: Confirmed

\*Reason: Proof by files

Financial Outcome: 2400000.00 EUR

# User Changes Payment Routing Data: ETD Application-level Alert

1 Admin user account compromised, fraudster changes file details (e.g. destination account)

2 ETD scanning Application logs real-time, alert: rule threshold exceeded

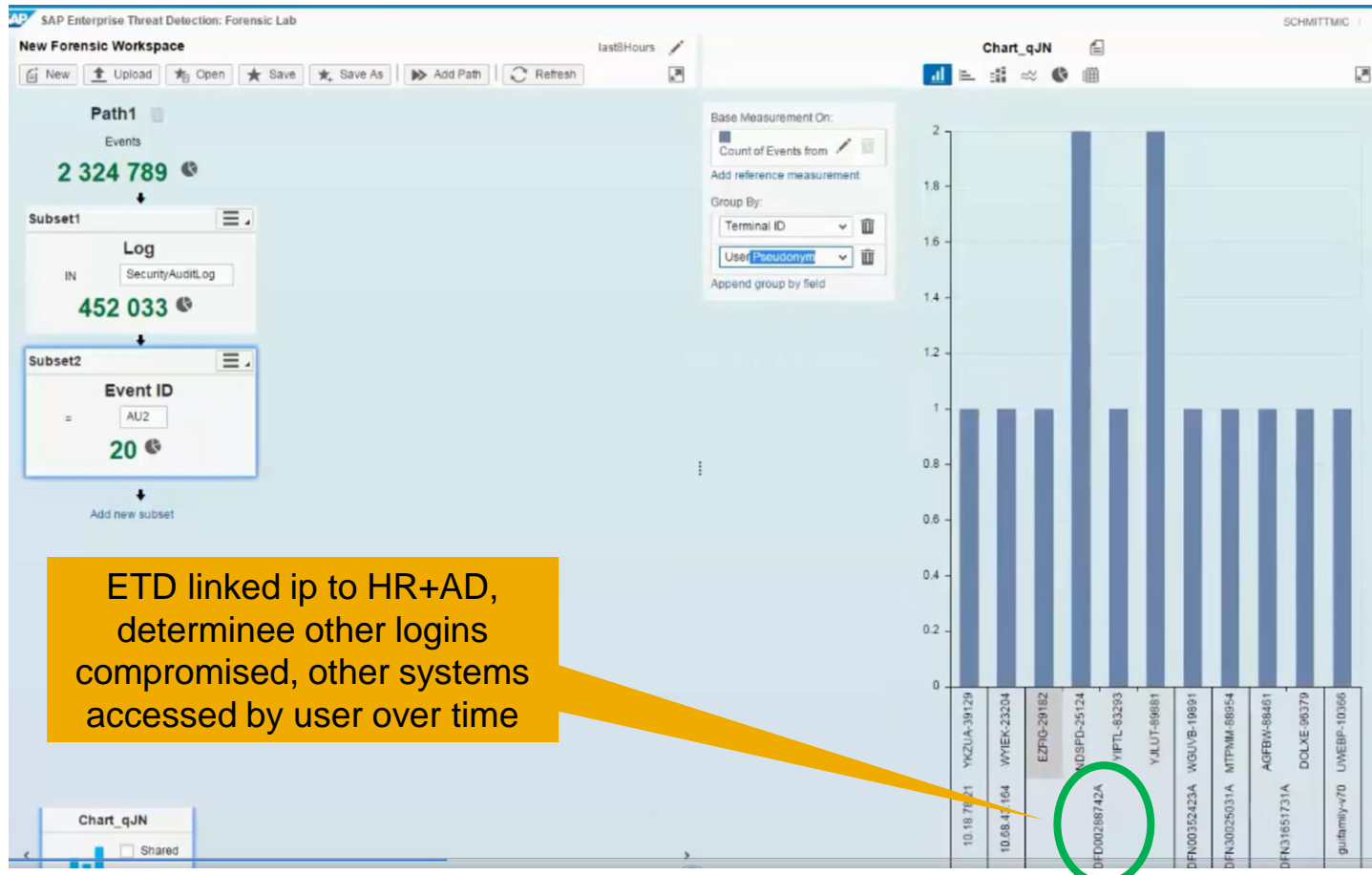
Cyber-attack Application changes raise alerts for analysis and investigation

3 ETD investigation team view data change script, determine malicious is true

The image displays three main components of the SAP Enterprise Threat Detection (ETD) interface:

- Top Dashboard:** Shows various monitoring charts and event lists. A green circle highlights a bar chart with the value '1' for ID 'Q7KQ0-85442', indicating a rule threshold exceeded.
- Bottom Left Table:** A memory analysis table with columns: S., Variable, V., Val., C., Hexadecimal Value, Technical Type, Absolute Type. The 'RECIPIENT' row shows a change from 'Ds. Teletex, Eesti' to a hexadecimal value.
- Bottom Middle Workspace:** Shows 'OUTLIER DETECTION' with 'Path4' and 'Path5' each having 1,204 events. Below are 'Event (Semantic)' blocks with counts of 1 and 4.
- Bottom Right Table:** A log table with columns: Timestamp, SystemId, UserPseudonym, LogType, MessageText. It lists three entries for 'SystemLog' with messages about field content changes (RECIPIENT, IBAN, PURPOSE).

# Collaboration using Data - Deeper Contextual Analysis

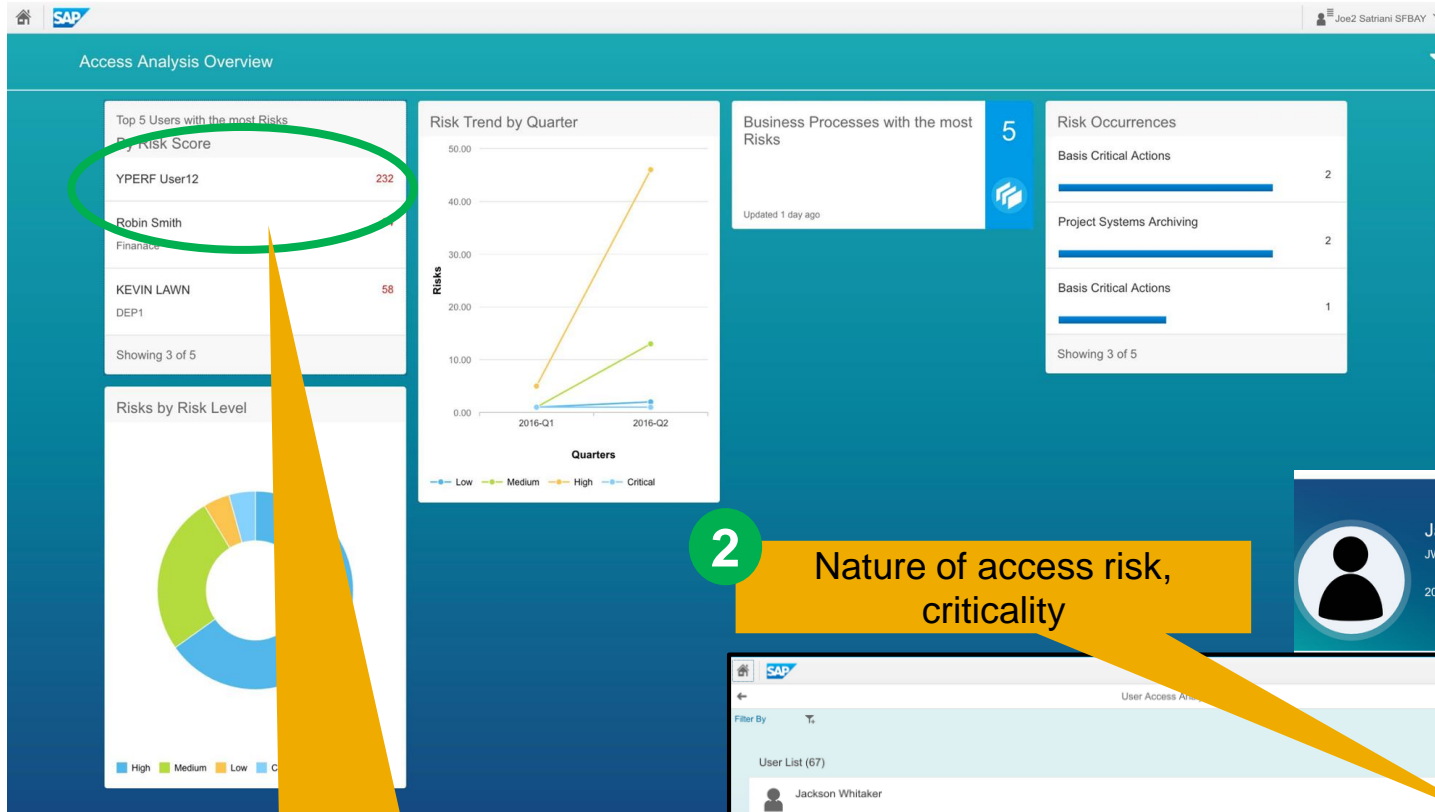


Compromised account may have performed other suspicious activity on other platforms, other applications. Pattern can be over several months.

Unusual user behaviour:

- Sending emails with time threshold (e.g., after hours).
- >1 attachment/spike in volume of emails.
- Typical use is 9-5 Monday-Friday, weekend spike is unusual.

# Example Dashboarding (System Access Violations)



Example central console for risk associated with data access, remediation.

Same can be achieved for financial transactions, combined reporting.

**3 Remediate**

**2 Nature of access risk, criticality**

**1 Simple console for Access Permissions Violations**

**Jackson Whitaker**  
 JWHITAKER  
 2016\_Q1\_REVIEW

**16 Risks** | **14 SoD Risks** | **2 Critical Access Risks** | **0 Risks Mitigated** | **0 Access Refined**

**0%** Access Compliance | **22%** Access Effectiveness

User Access Overview

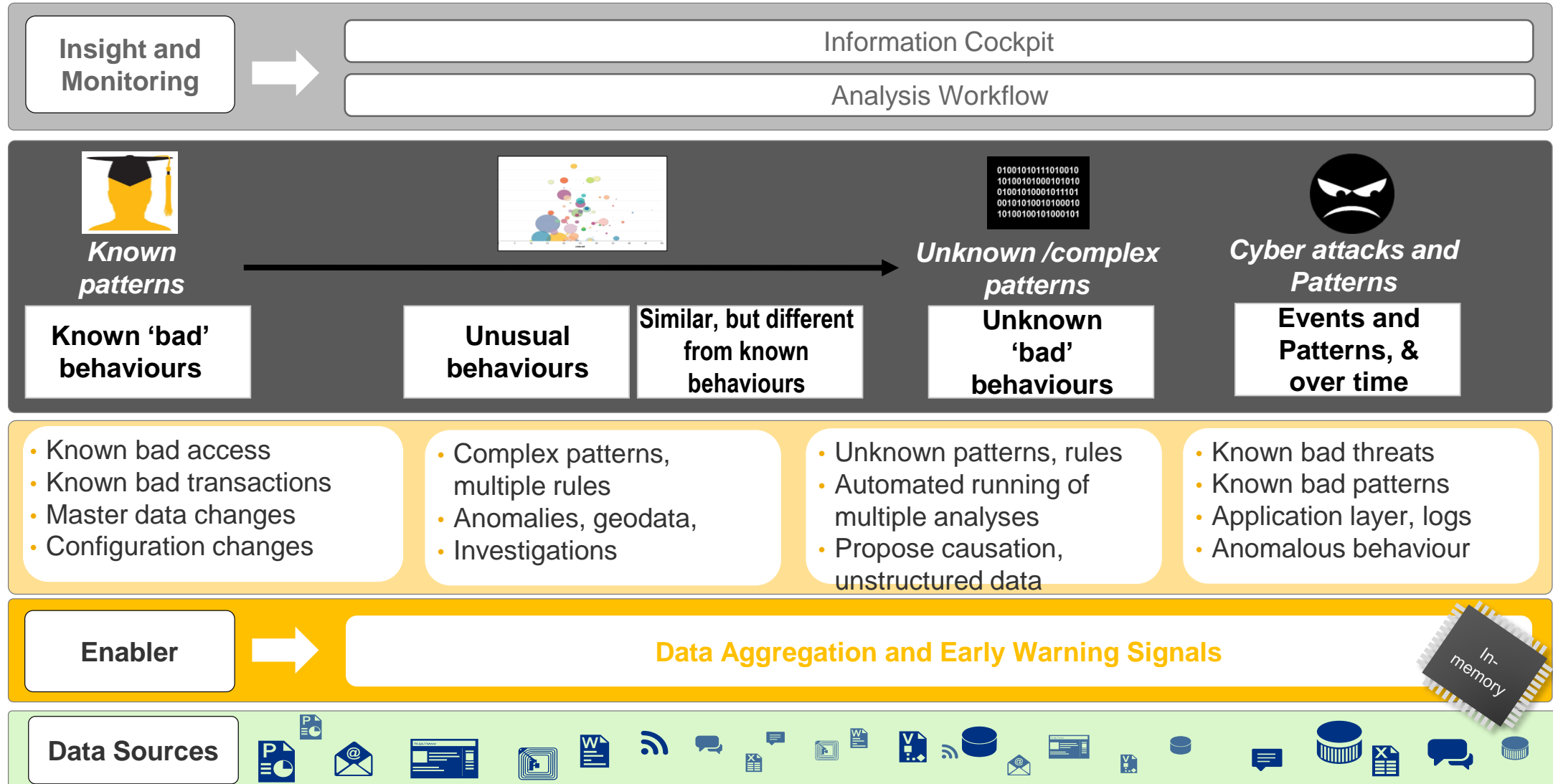
Filter By

User List (67)

Jackson Whitaker	Email: Jackson.Whitaker@grc.com	Department: Finance	SoD Risks: 14	Critical Access Risks: 2
Jane SMITH	Email: Julia.Smith@grc.com	Department: Finance	SoD Risks: 5	Critical Access Risks: 2
SGIVE				

Type	System	Assigned Until	Usage	Last Used	Risks
Role	GH7CLNT600	Dec 31, 9999	4	Apr 8, 2016	0
Role	GH7CLNT600	Dec 31, 9999	4	Apr 8, 2016	11
Role	GH7CLNT600	Dec 31, 9999	2	Apr 8, 2016	1
Role	GH7CLNT600	Dec 31, 9999	2	Mar 8, 2016	5
Role	SuccessFactor	Jan 1, 9999	0		0
Role	SuccessFactor	Jan 1, 9999	0		0
Role	GH7CLNT600	Dec 31, 9999	2	Apr 8, 2016	10
Role	GH7CLNT600	Dec 31, 9999	0		13

# Platform Approach Adds Value, Agility, Assurance, Governance







# Thank you



**Dr. Neil Patrick**  
COE GRC (EMEA)  
SAP Governance, Risk and Compliance

[neil.patrick@sap.com](mailto:neil.patrick@sap.com)  
[www.sap.com/grc](http://www.sap.com/grc)