Bottom-Up approach for Compliance: The MASTER position

Emmanuel Pigout, Philip Miseldine
18/11/2009

MASTER

SEVENTH FRAMEWORK PROGRAMME

THE BEST-RUN BUSINESSES RUN SAP™

SAP®

Compliance is important … but expensive

"No matter how you look at it, the price of compliance is minimal compared to the costs of non-compliance. As the saying goes, 'pay now or pay a lot more later.' Devoting resources to compliance is simply the right business decision. If a firm does not have a strong compliance ethic, if it places the interests of the firm before its clients, it is only a matter of time before it loses the confidence of its clients. A compliance failure can lead to bad publicity and embarrassment which can permanently damage a firm's reputation and ultimately lead to an erosion of its client base. The end result will be lower profitability and private law suits. In short, a weak and ineffective compliance system can spell disaster."

Paul F. Roye, former director of the SEC Division of Investment Management.

"Firms are anticipating significant increase in regulatory developments with accompanying costs to cope with the surge of changes. Of the 280 global compliance professionals that responded to the survey 66 per cent expected that, largely as a result of recent market failures, there will be a significant increase in the amount of time they will have to spend liaising and communicating with regulators and exchanges in 2009."

Complinet: Cost of Compliance Survey 2009

Industrial Challenges 1/2

What are the challenges of compliance management facing a modern enterprise?

A motivating example from the Healthcare Sector: Health Insurance Portability and Accountability Act (HIPAA-1996)

- ““Ensure protection of personally identifiable health information held or disclosed by a covered entity in any form including orally, written and electronically” .

Patient data is a critical aspect of medical business processes

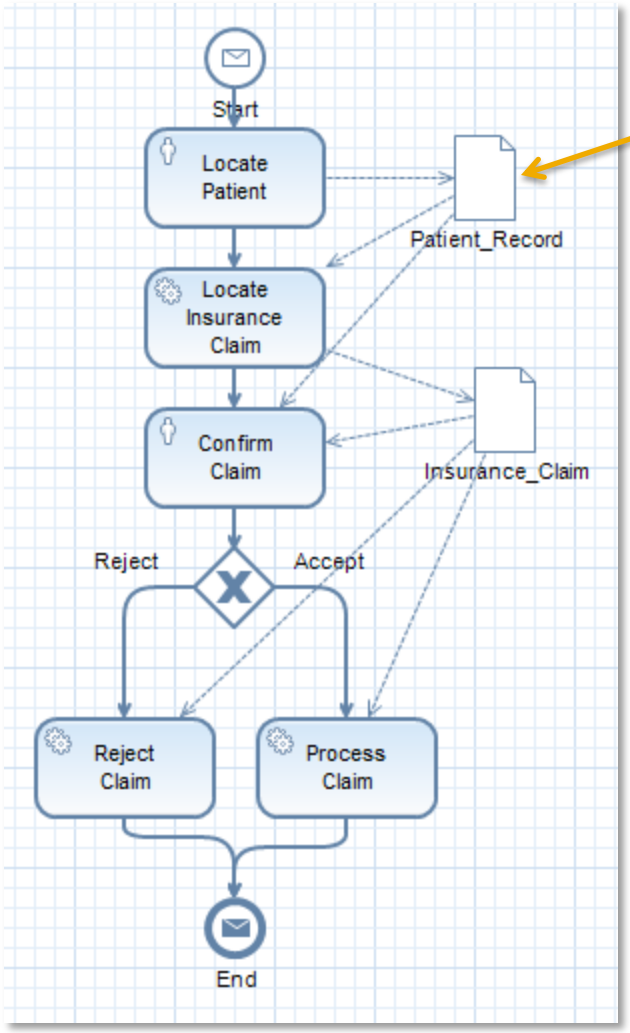
- Processing patient medication, insurance claims, hospital stays

Could pass through multiple systems

- Implemented via a wide range of services
  - Process Modeling: SAP NetWeaver BPM, IBM WebSphere Business Integration Modeler, BEA’s AquaLogic BPM, ARIS …
  - Enterprise Services: Automated Services
  - Human Interaction: Silverlight, Adobe Flash, Flex, JavaFX, Quicktime
  - External Services: Outsourcing

© SAP AG 2009 / Page 3

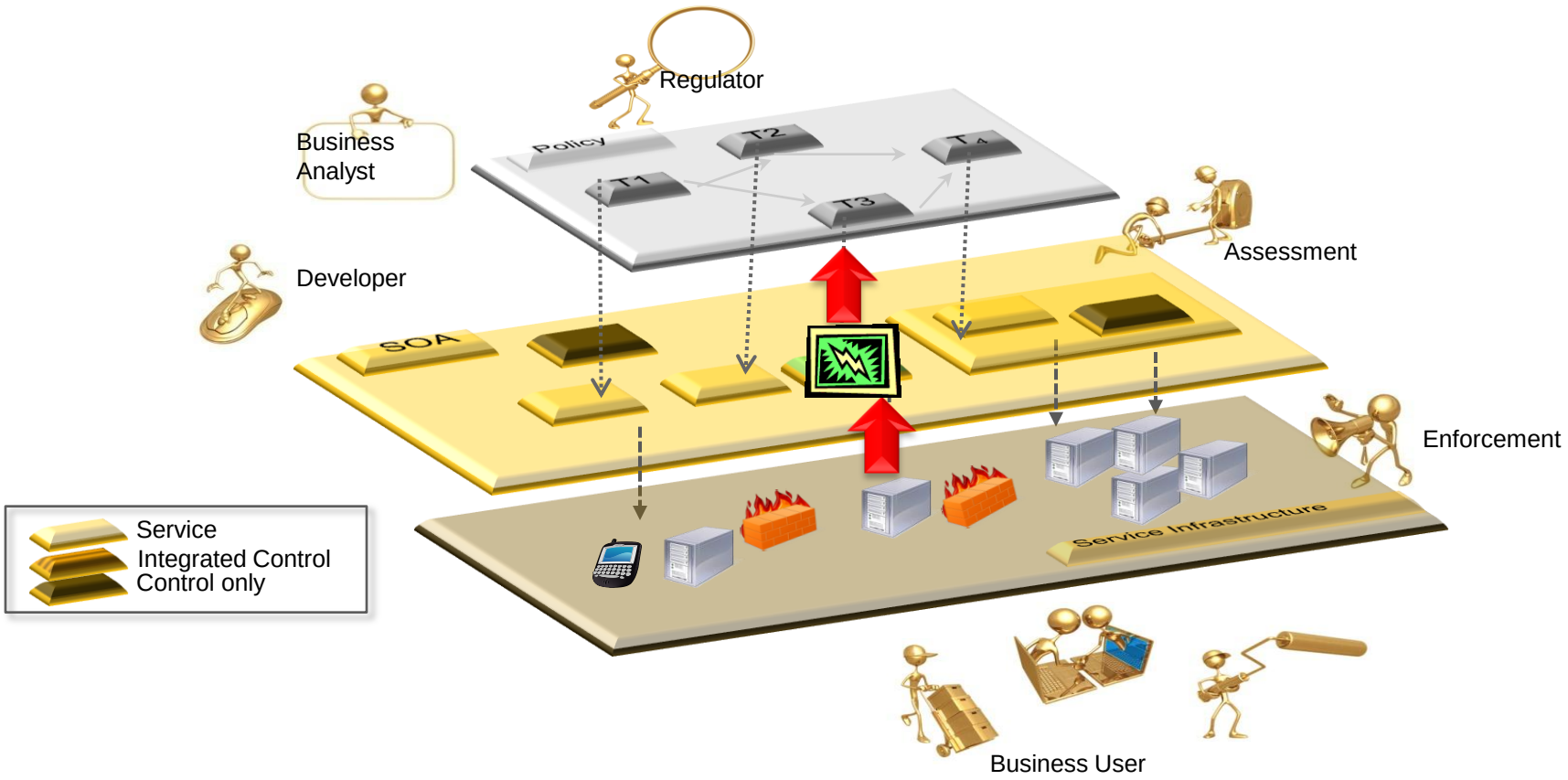
Industrial Challenges 2/2



This object is the patient record

- To be compliant to HIPAA, we need to
  - Constrain it (i.e. requirements for anonymisation)
  - Assess it (i.e. prove its usage)
  - Enforce it (obfuscate)

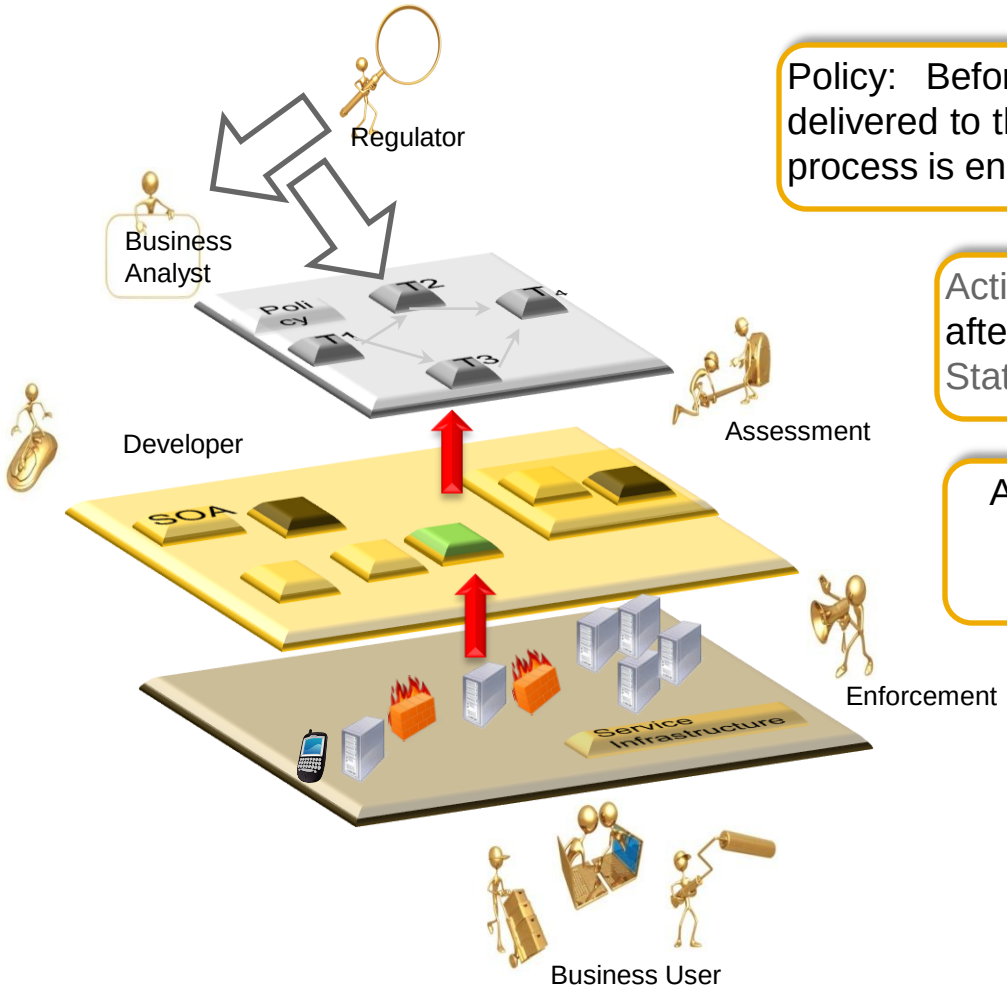
MASTER Position: Bottom-Up Approach



Master's solution proposal

- The Master's evidence model allows a service to describe itself by providing the following information:
  - Actions a service performs
  - States each single action supports
  - Events on the action states
  - Enforcement actions possible on the service
- Evidence model allows to express security requirements in the same vocabulary as the service descriptions
  - By combination of ontology vocabulary with the formal description of the requirements
- Has been selected for the MASTER standardization plan.

MASTER Position: Simple Use-Case



Policy: Before showing the drugs prescribed and/or delivered to the patient, the system checks if the retrieval process is ended with success *[C.A. 12.02.02]*

Action Display on DrugInfo can only happen after Action Retrieve on DrugInfo has reached State CompletedSuccessfully

Always(Display(DrugInfo) implies
Retrieve(DrugInfo) ∧
Retrieve.State=CompletedSuccessfully)

THANK YOU !

“I have the answers ! Who have the questions ?”: Woody Allen