



REALM -- Regulations Expressed As Logical Models

Christopher Giblin, Alice Y Liu, Samuel Müller, Birgit Pfitzmann, Xin Zhou

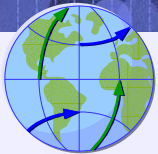
IBM Research

June 22, 2005



Disclaimer

- ▶ IBM's customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

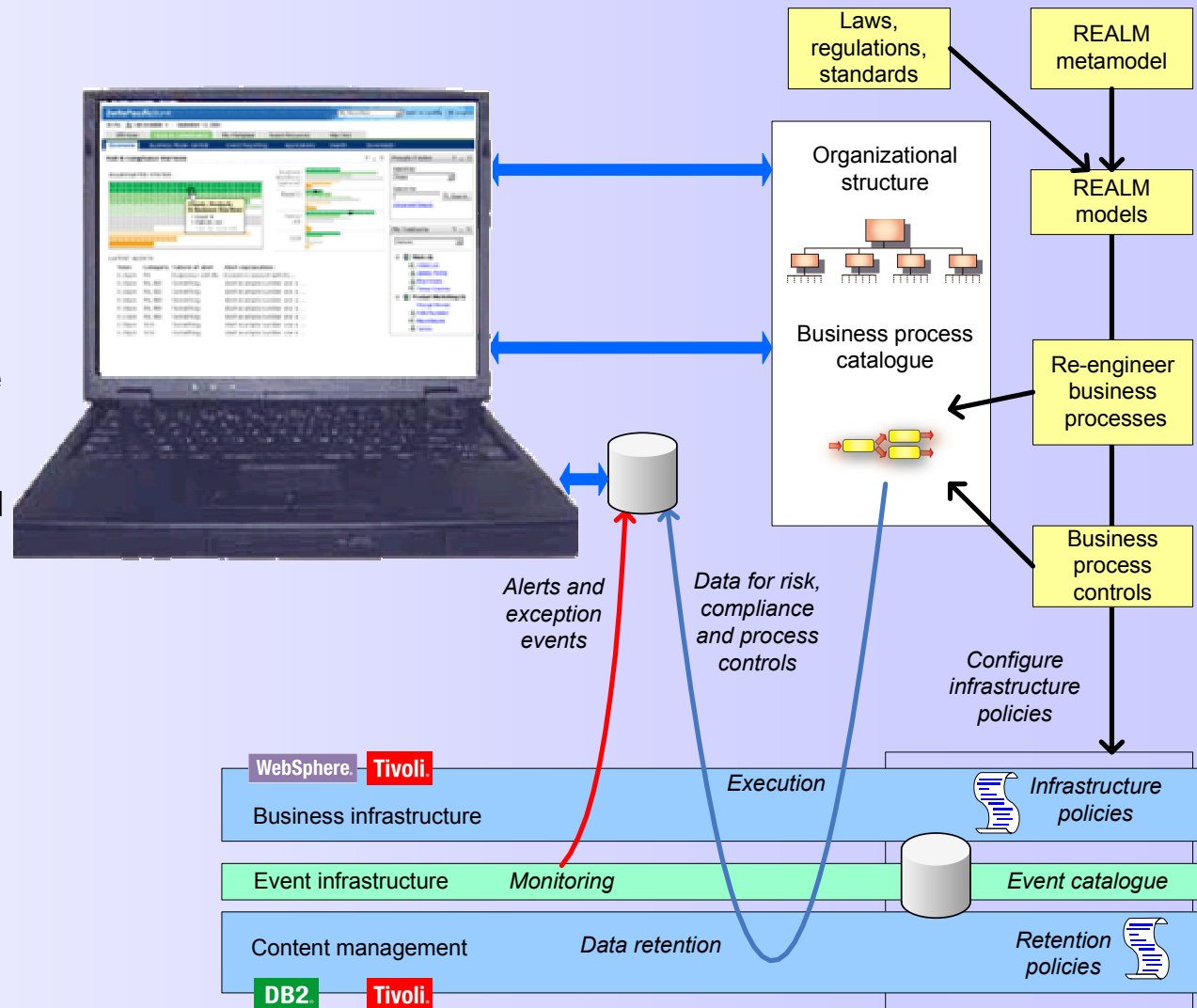


IBM Research on Risk & Compliance

Vision: An Enterprise R&C Framework enabling a unified treatment of all types of risk and compliance across applications and processes

This requires:

- **Visualization**, which allows the various stakeholders to see meaningful and actionable representations of both risk and compliance
- **Regulation Modeling** for treating regulations like policies (REALM)
- **Risk calculations**, in particular for operational risk
- **Architecture** for tying everything together; this must be an aspect to overall business and IT architectures

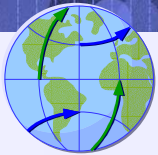




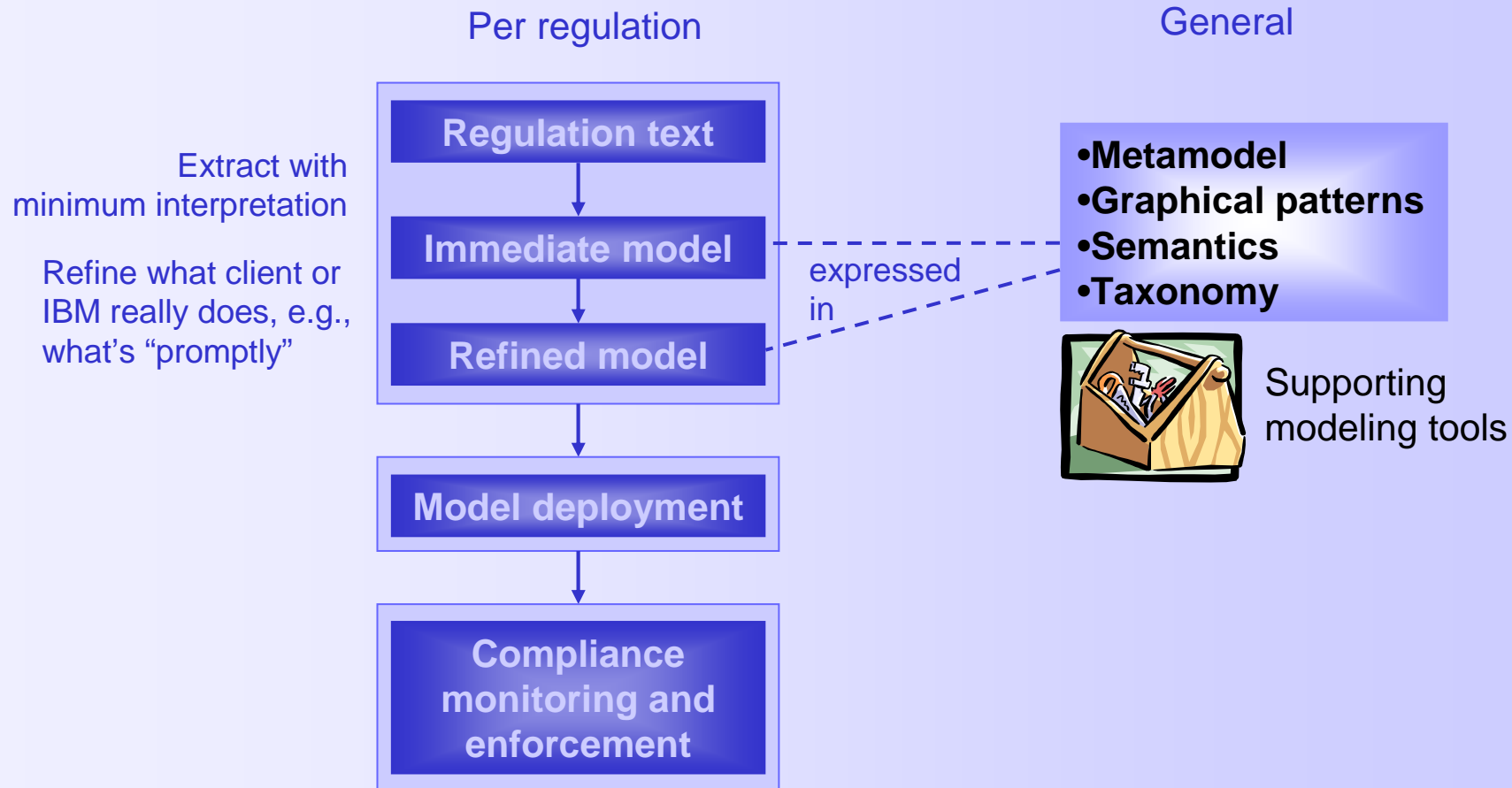
Goals with REALM (Regulations Expressed As Logical Models)

- ▶ A systematic approach to regulatory compliance management.
 - Model-driven
 - Uniform
 - Temporal logic with modern object concepts

- ▶ Policy-based Compliance Management
 - End-to-end lifecycle from law → policy → runtime
 - Integration with existing modeling standards (UML2.0,CBM, BOM, IFW)
 - Automated policy deployment
 - Continuous monitoring and enforcement



Compliance Management Process



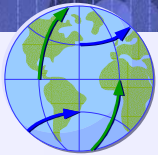
▶ Recall disclaimer: This is not legal advice by IBM. It is only a technique for tracing requirements and bringing them closer to business process models and IT.



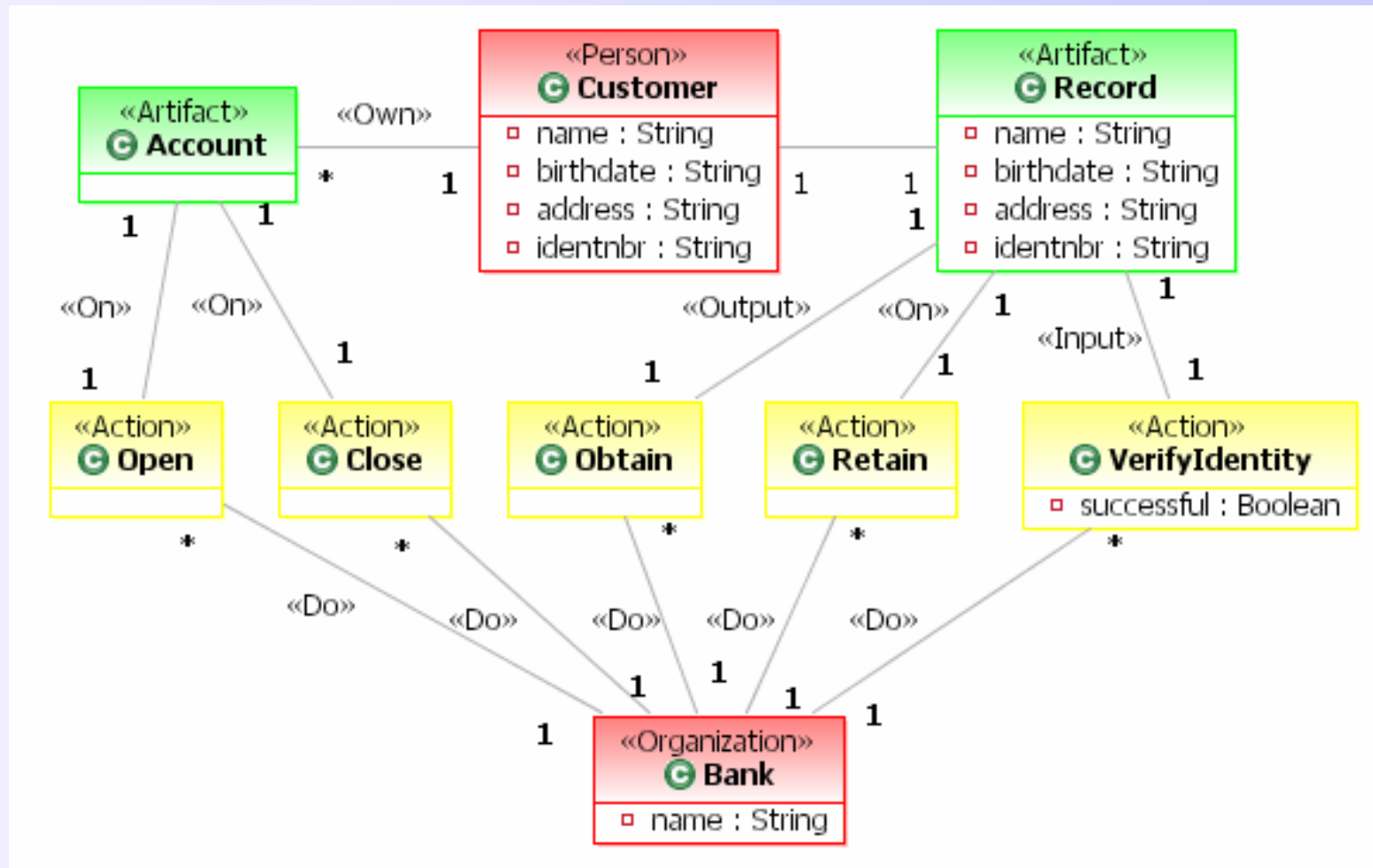
Example Regulation Text

Simplified version of Patriot Act: SEC. 326. VERIFICATION OF IDENTIFICATION.

- ▶ Banks must implement risk-based procedures for verifying the identity of each customer. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. The bank must further implement procedures that specify the identifying information that will be obtained from each customer. At a minimum, the bank must obtain the following information prior to opening an account:
 - Name;
 - Date of birth;
 - Residential Address;
 - Identification number.
- ▶ The bank must verify the identity of each customer, using the information obtained in accordance with the above requirements, within a reasonable time after the account is opened.
- ▶ The bank must also implement procedures for responding to circumstances in which the bank cannot form reasonable belief that it knows the true identity of the customer. These procedures should describe when the bank should close an account, after attempts to verify the customer's identity have failed.
- ▶ The bank must implement procedures for making and retaining a record of all information obtained according to the above requirements.
- ▶ The bank must retain the recorded information for five years after the date the account is closed.

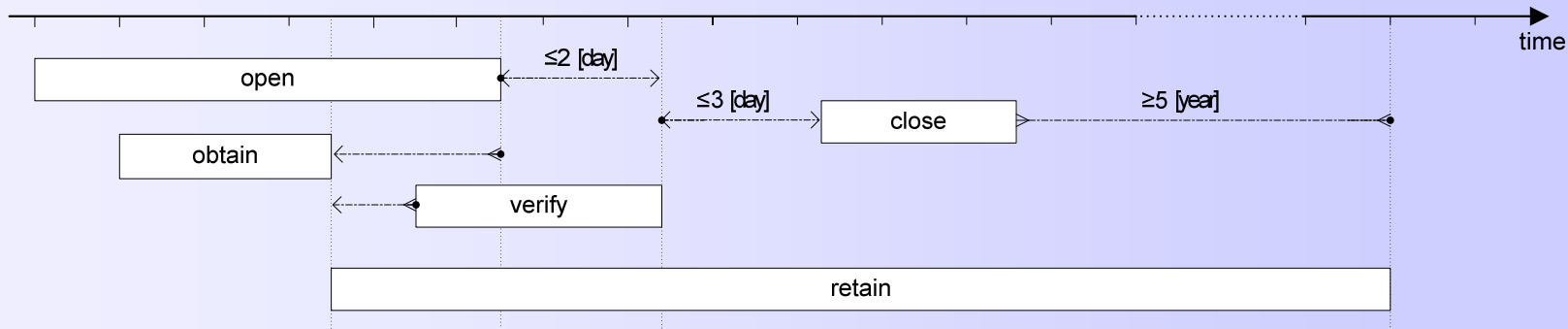


Domain Model (using REALM UML Profile)





Time Constraint View from this Text



Example formula (real-time logic over object model – note OCL referencing):

$$\begin{aligned}
 &\forall \text{ bank} \in \text{Bank}, \text{ open} \in \text{Open}, \text{ a} \in \text{Account}, \exists \text{ verify} \in \text{VerifyIdentity}: \\
 &\quad t_{\text{open}} \cdot \text{DoOn}_F(\text{bank}, \text{open}, \text{a}) \\
 &\quad \rightarrow \diamond t_{\text{verify}} \cdot \text{DoInput}_F(\text{bank}, \text{verify}, \text{a.customer.record}) \\
 &\quad \quad \wedge t_{\text{verify}} - t_{\text{open}} \leq 2[\text{day}]
 \end{aligned}$$



Summary

- Data, Processes, Privacy, and Information Security are increasingly governed by Regulations.

- IBM Research REALM project (Regulations Expressed As Logical Models):
 - ◆ Regulation Modeling (Immediate Model, Refined Model, Patterns) by real-time temporal object logic
 - ◆ Integration with UML2.0 as UML profile; planned integration IBM BOM
 - ◆ Planned deployment of regulation models into various technologies

- Benefits of a Compliance Metamodel:
 - ◆ Bounds number of translations and ensures common understanding.
 - ◆ Quick and uniform adaptation to new regulations and regulatory changes.
 - ◆ Lifecycle model