Conceptual Framework and Architecture for Privacy Audit

Ksenya Kveler, Kirsten Bock, Pietro Colombo, Tamar Domany, Elena Ferrari, Alan Hartman

IBM Haifa Research Laboratory – KK, TD, AH

Unabhaengiges Landeszentrum fuer Datenschutz - KB

University of Insubria – PC, EF

Agenda

- Motivation
- Tool Enhanced Audit Process
- Data Protection Goals
- Data Privacy Compliance Metrics
- Architecture For Privacy Audit

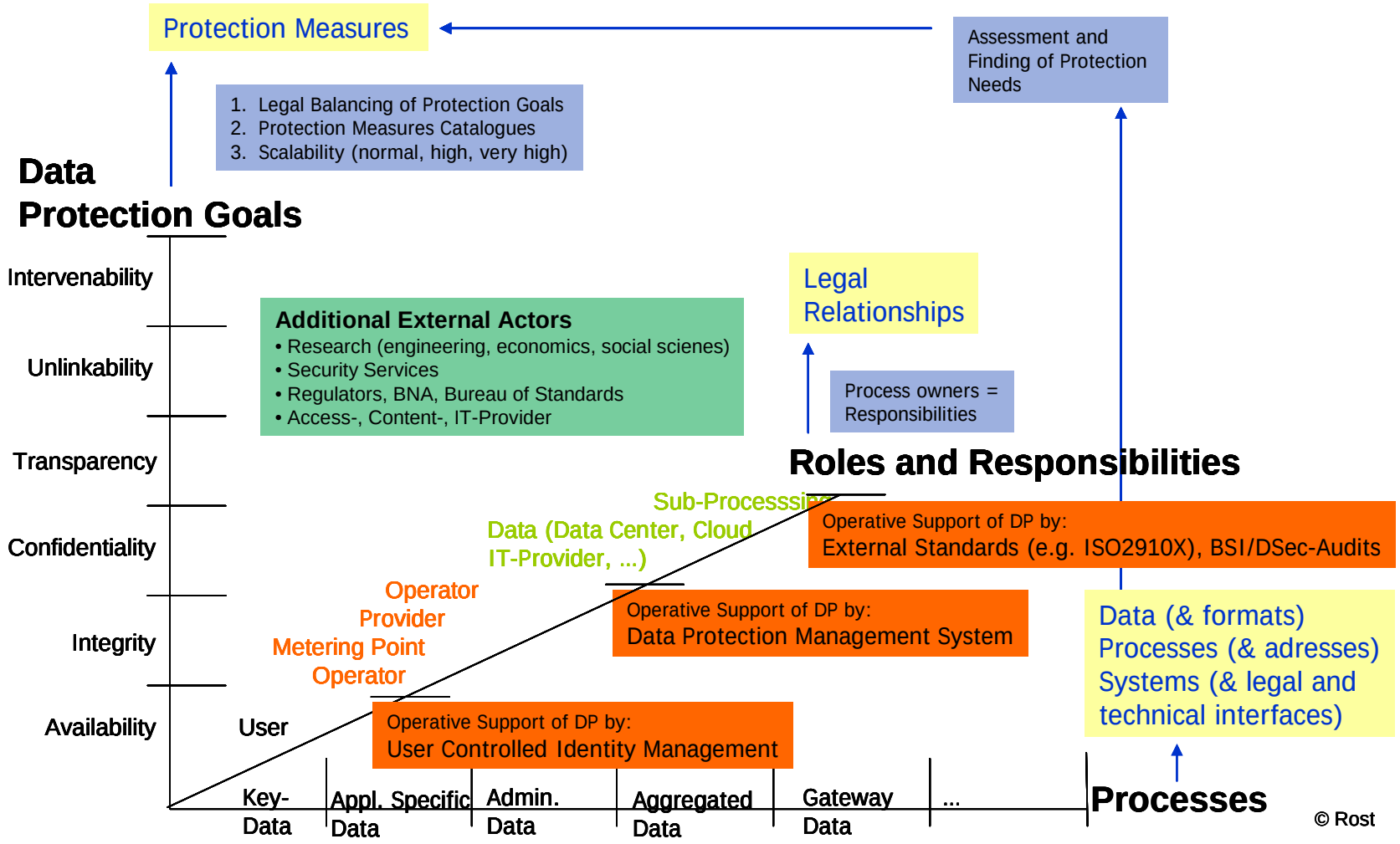
Motivation

- Many organizations collect a lot of private data
- Most of them want to comply with the law BUT
  - The privacy protection laws are complex and heterogeneous
  - Privacy compliance audits are expensive

Tool Enhanced Audit Process

- Stage 1: Determine targets of evaluation
  - Based on data protection goals – rather than laws
  - Analysis of data collection and storage processes
  - Analysis of the types of data collected
- Stage 2: Design metrics
  - Create a UML representation of the privacy requirements
  - Map the processes and IT artifacts onto the model
  - Derive metrics related to the DPG
- Stage 3: Build assessment tools
  - Separate metric assessor plugins for each metric

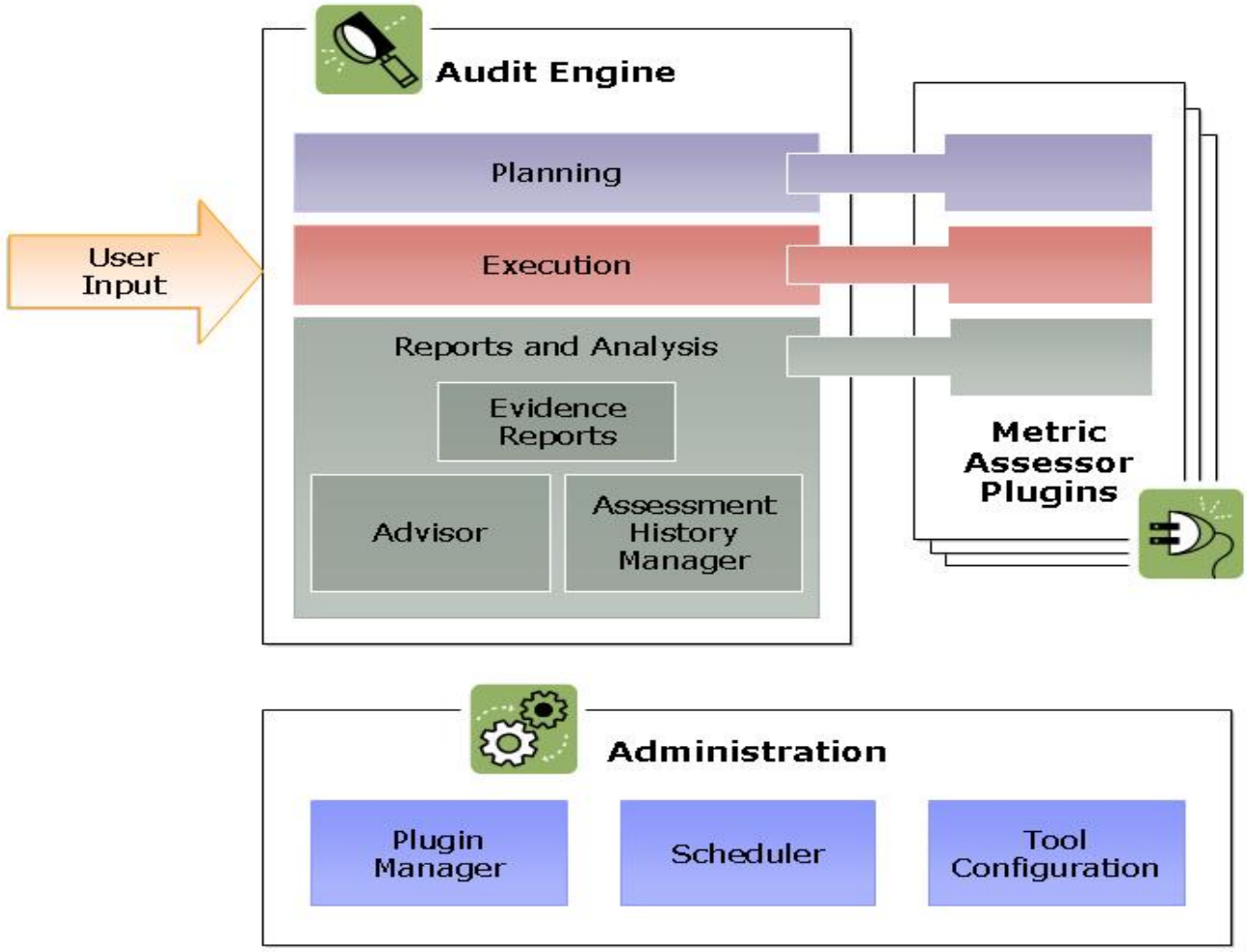
Data Protection Goals



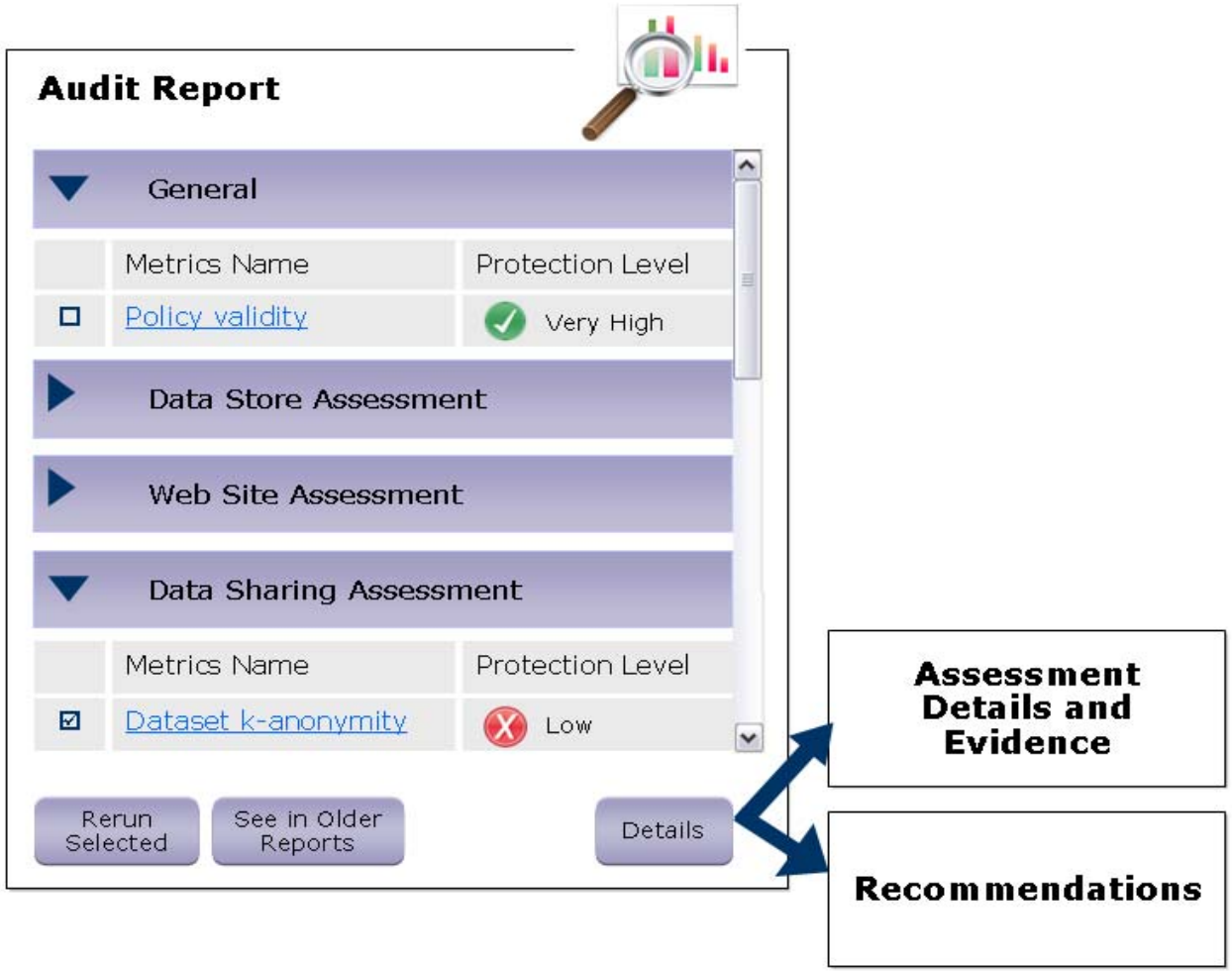
Data Privacy Compliance Metrics

- Privacy conceptual model defines a language for expressing privacy requirements
- Constraints on the model are weighted by the assessor, and associated with Data Protection Goals
- The system under assessment is mapped onto the privacy requirements model
- Metrics are derived from the weighted sum of constraints satisfied by the system under assessment

Architecture for Data Privacy Audit



Sample Audit Report



Main contributions

- Linkage between data protection goals and privacy compliance metrics
- Conceptual model for privacy requirements including a set of UML classes and constraints
- Extensible and transparent architecture for privacy compliance assessment tools