SEcure Cloud computing
for CRitical Infrastructure IT

Techno-Legal Motivation

Ass. iur. Silvia Balaban

24/11/2015

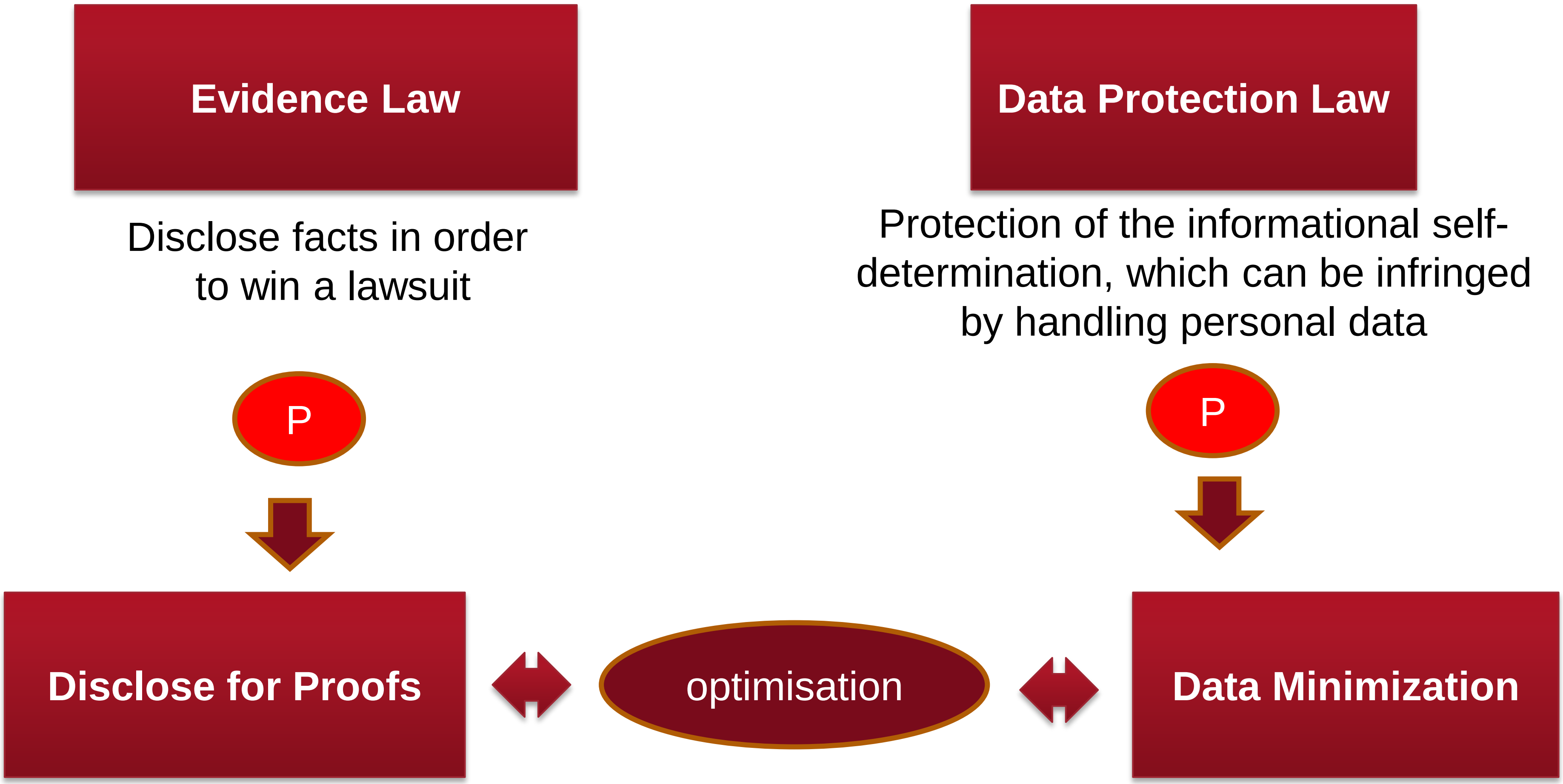
AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

Introduction - Objective

- What are the legal requirements in cloud computing cases?
- How can the technical properties of cloud computing comply with the legal requirements?

Why?: **techno-legal assessment** from the very beginning in order to foster the **conformance** of the system with **regulatory constraints („Compliance by Design“)**

Introduction – Law Fields



Evidence Law

Disclose facts in order to win a lawsuit

P

Disclose for Proofs

Data Protection Law

Protection of the informational self-determination, which can be infringed by handling personal data

P

Data Minimization

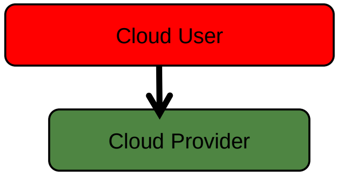
optimisation

What are the legal requirements in cloud computing cases?

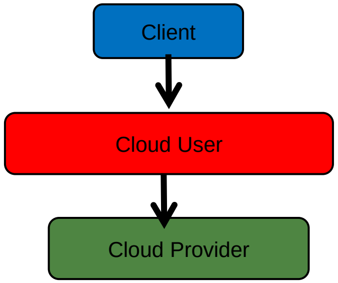
Evidence Law

Current Situation – Evidence Law

- First Case: A cloud user (A) has a contract with a cloud provider (B), that one commits a breach of duty and the cloud user has a damage. The cloud user wants to get his damage compensated, so he sues the cloud provider.



- Second Case: The cloud user has a contract with a client and requires for the fulfillment of the contract a cloud-based solution. He has for this a contract with the cloud provider. That one commits a breach of duty and it is the client of the cloud user who has a damage. Client sues the cloud user.

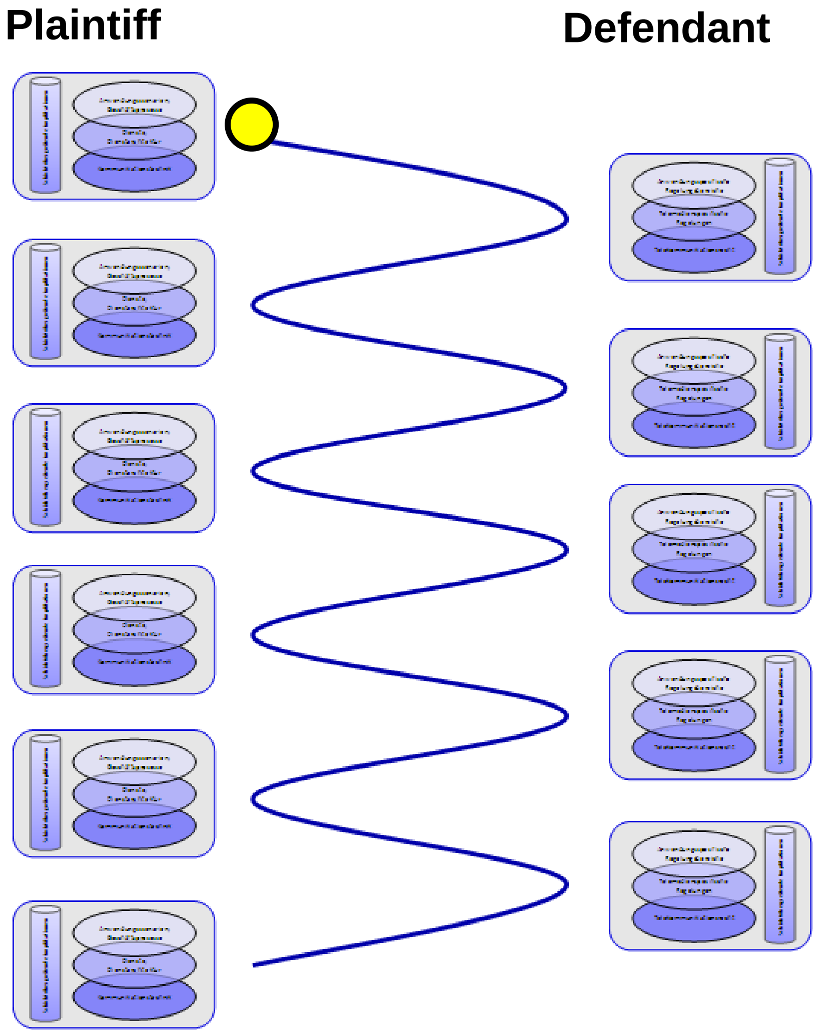


Evaluating the first Case

	Contract	Fault	Default	Damage
Cloud USER	Document	Legal inspection/expert evidence/witness/ document		Legal inspection/expert evidence/witness/ document
Cloud PROVIDER			Document/ Witness/Expert Evidence	

Current Situation – Evidence Law

Contract, fault, damage, causal link between damage and fault



default

Evaluating the first Case

- Cloud User: Contradict non-default of provider?
  - Legal inspection
    - Own perception difficult as past incident
  - Witness
    - Only in sphere of the provider, employee of the provider
  - Document
    - All documents in sphere of the provider, no insight view
  - Expert evidence
    - Difficult to retrace what caused the fault
    - Only assess documents of provider → NOT NEUTRAL

- Cloud user loses lawsuit – lack of useable proofs

Evaluating the Second Case

- Client:
  - documents, legal inspection, witness proof
- Cloud user:
  - prove that he did not act negligent
  - prove that provider did not act negligent
- What caused the damage? Cloud user, made passwords accessible?
  - Proving situation of first case → wasn‘t provider, still cloud user needs to disprove own possible negligent behavior
  - Prove of existence of damage proves fault

Evaluating the Second Use Case

- For proving that it was not the cloud user:
  - Witness: needs to testify about negative facts
  - Document cannot prove all possible non acting/acting situations
  - Expert evidence: difficult to retrace negligent behavior

- Cloud user‘s own default remains unclear: cloud user loses lawsuit
- Provider‘s fault: Cloud user loses lawsuit
  - Third party notice for second lawsuit in order to gain a title against provider

Evidence Law Challenges

- **Usual evidence** in court presumably not suitable in cloud scenarios because of **multiplicity** of acting parties and technical **complexity**
- Cloud user has no inside view → can hardly prove default
- Cloud user has **no access** to required evidence
- Cloud user's legal position is weak!

Data Protection Law

Current situation - Data Protection Law

- Protection of the informational self-determination, which can be infringed by handling personal

Data Subject → personal data: information relating to an identified or identifiable natural person (data subject)

Controller → determines the purposes and means of the processing of personal data

Processor → processes personal data on behalf of the controller

Processing: collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

Current Situation – Data Protection Law

- Data subject has **access rights**, **information rights** etc.
- Only against **cloud user (processing on behalf of the controller)**
- Cloud provider and cloud user are counting as one unit, provider is only „**processor**”

	Data Subject	Cloud User	Cloud Provider
Personal data	X	-	has the data
Information about location of data	wants to know	?	?
Rights	correction, deletion, blocking	has to fulfill	-
Problems		Cannot fulfill because: not transparent, no control	- takes recourse on other providers - can transmit data to others

Current Situation – Data Protection Law

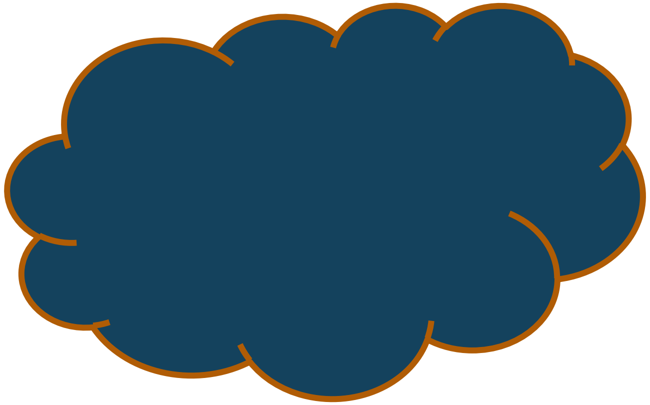
- Data subject has rights which user needs to fulfill
- Cloud user has to control cloud provider
- → merely done by certification
- Is based on trusting the cloud provider
- How to solve fulfillment of data subjects right by user if no inside view is given
- → Lack of transparency, lack of control

How can the technical properties of cloud computing comply with the legal requirements?

Cloud-specific Givens…

…leading to legal problems:

Black Box Nature:



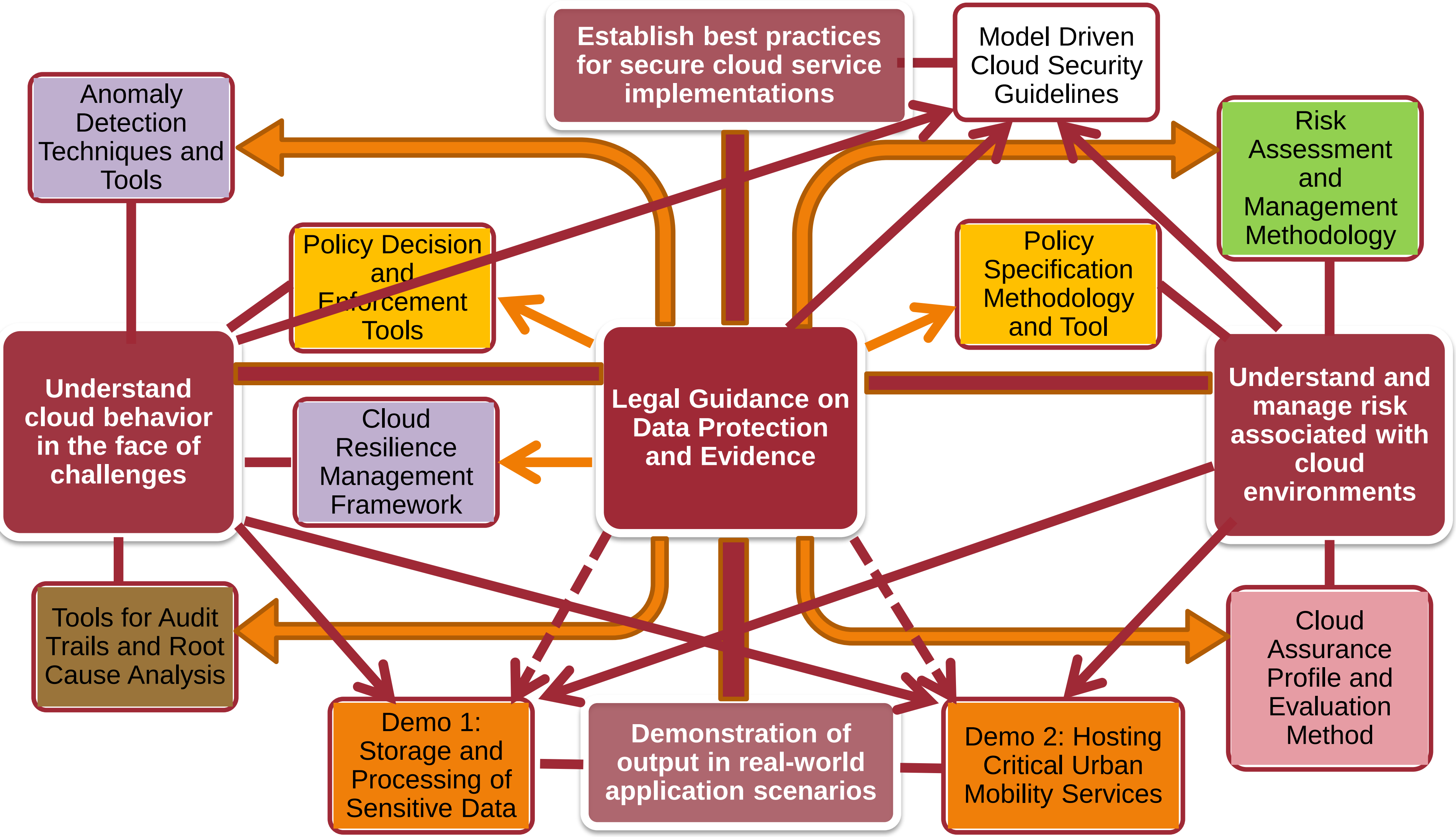
Data processing is not visible!

Evidence Law

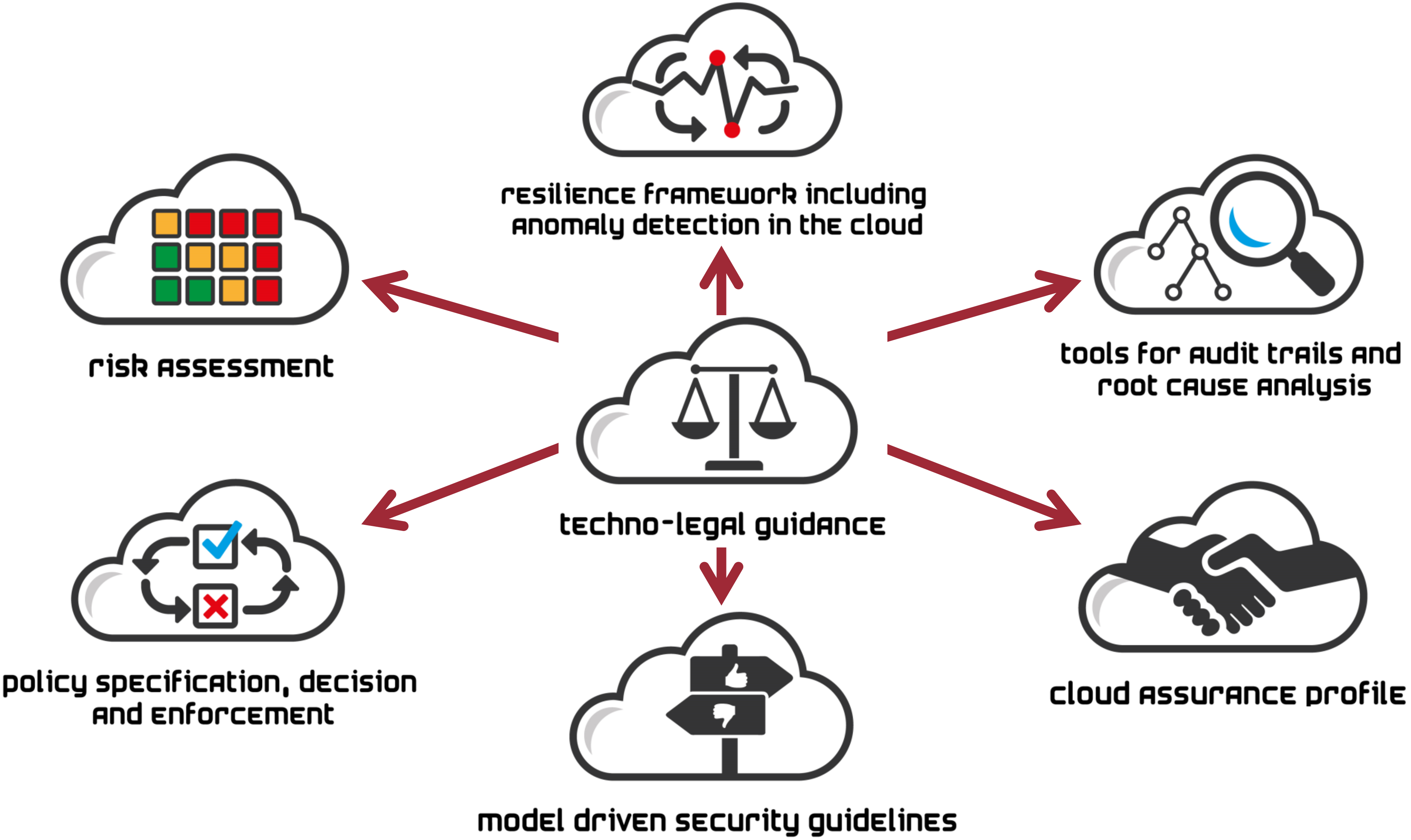
Data Protection Law

Fulfilling the legal requirements…

SECCRIT
SEcure Cloud computing for CRitical infrastructure IT


Establish best practices for secure cloud service implementations
Model Driven Cloud Security Guidelines
Anomaly Detection Techniques and Tools
Risk Assessment and Management Methodology
Policy Decision and Enforcement Tools
Policy Specification Methodology and Tool
Understand cloud behavior in the face of challenges
Legal Guidance on Data Protection and Evidence
Understand and manage risk associated with cloud environments
Cloud Resilience Management Framework
Tools for Audit Trails and Root Cause Analysis
Cloud Assurance Profile and Evaluation Method
Demo 1: Storage and Processing of Sensitive Data
Demonstration of output in real-world application scenarios
Demo 2: Hosting Critical Urban Mobility Services

SECCRIT Outputs



techno-legal guidance

resilience framework including anomaly detection in the cloud

risk assessment

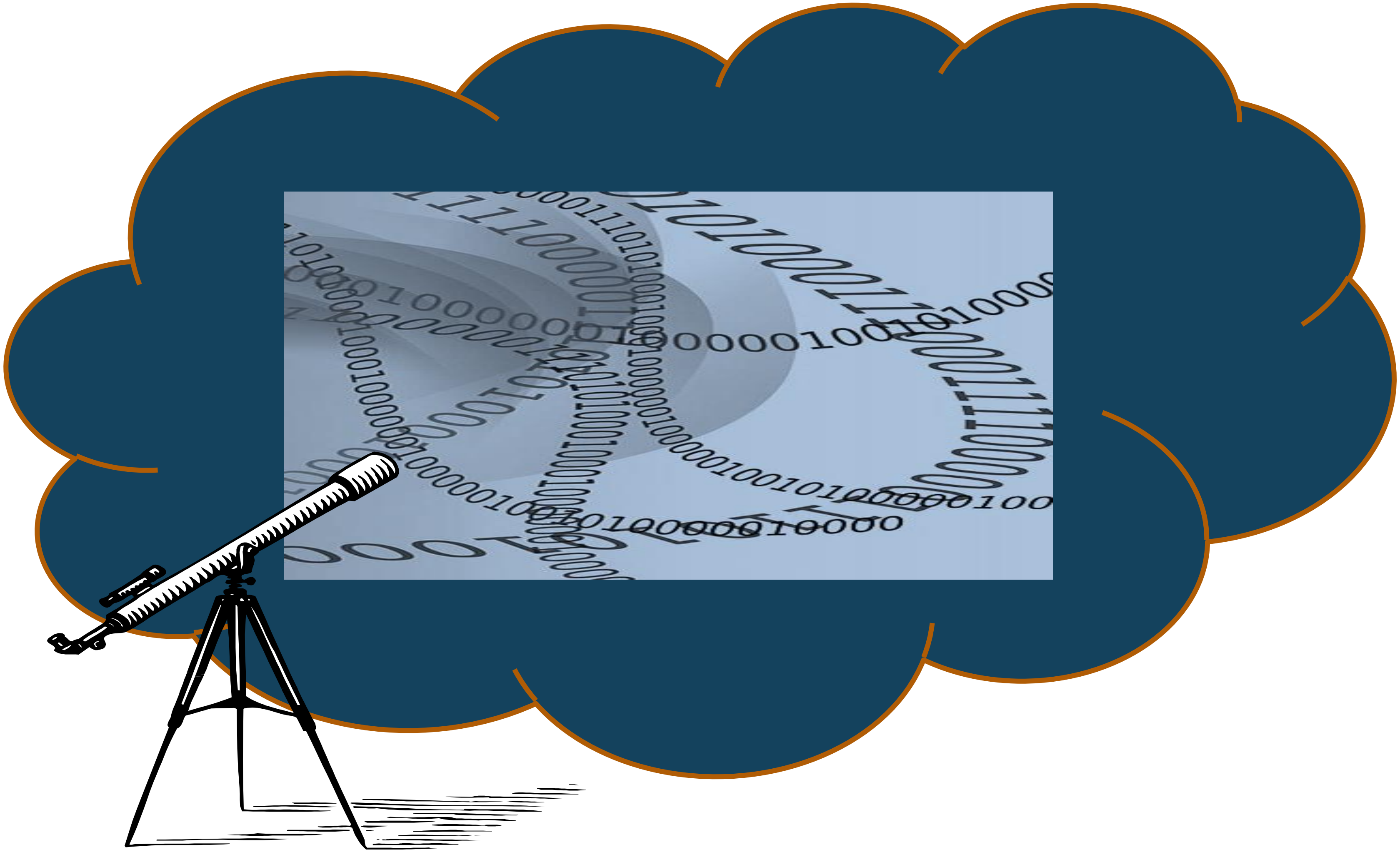
tools for audit trails and root cause analysis

policy specification, decision and enforcement

cloud assurance profile

model driven security guidelines

Summary



Contact

Ass. iur. Silvia Balaban
KIT, Center for Applied Legal Studies
(silvia.balaban@kit.edu)