Continuous Auditing and Risk Management in Cloud Computing

Marcus Spies
Chair of Knowledge Management
LMU University of Munich
Scientific / Technical Director of EU Integrated Research Project MUSING

Cloud computing – computing services beyond perimeters visible to the client

- Cloud Service Models
  - cloud infrastructure as a service (IaaS) – provider facilities, hardware, network transparent
    - storage, computation, service management
  - cloud platform as a service (PaaS) – operating system, messaging, … transparent
    - BI, X-Enterprise Service Bus, Collaborative Development
  - cloud software as a service (SaaS) – implementation, internal operation abstracted
    - Financial, HR, Content & Document Mgmt, …

NIST Cloud Deployment Models

- *Private cloud*
  - cloud infrastructure is operated *for* a single organization –
  - may be managed by the organizations or a third party
  - may exist on premise or off premise
- *Community cloud*
  - like private, but cloud is shared by several organizations and supports a community with shared concerns
- *Public cloud*
  - cloud infrastructure is made available to the general public or a large industry group
  - owned by an organization selling cloud services
- *Hybrid cloud*
  - **cloud** infrastructure is a composition of two or more **clouds**
  - component clouds linked for data and application portability

Cloud Computing Benefits

- NIST has identified the key technical and business benefits of cloud services
  - On-demand self-service –
    - customer driven provisioning of services
  - Broad network access –
    - network access via a broad range of protocols and devices
  - Resource pooling –
    - Scalability and Fault-Tolerance through virtualization of resources
  - Rapid elasticity –
    - dynamic (re-)allocation of resources
  - **Measured Service**
    - ***Continuous monitoring and reporting capabilities*** allow for economies of scale

Cloud Services Threats – The other side of the coin

- The Cloud Security Alliance (CSA) has identified the key threats …
  - **Threat #1:** Abuse and Nefarious Use of Cloud Computing
  - **Threat #2:** Insecure Interfaces and APIs
  - **Threat #3:** Malicious Insiders
  - **Threat #4:** Shared Technology Issues
  - **Threat #5:** Data Loss or Leakage
  - **Threat #6:** Account or Service Hijacking
  - **Threat #7:** **Unknown Risk Profile**

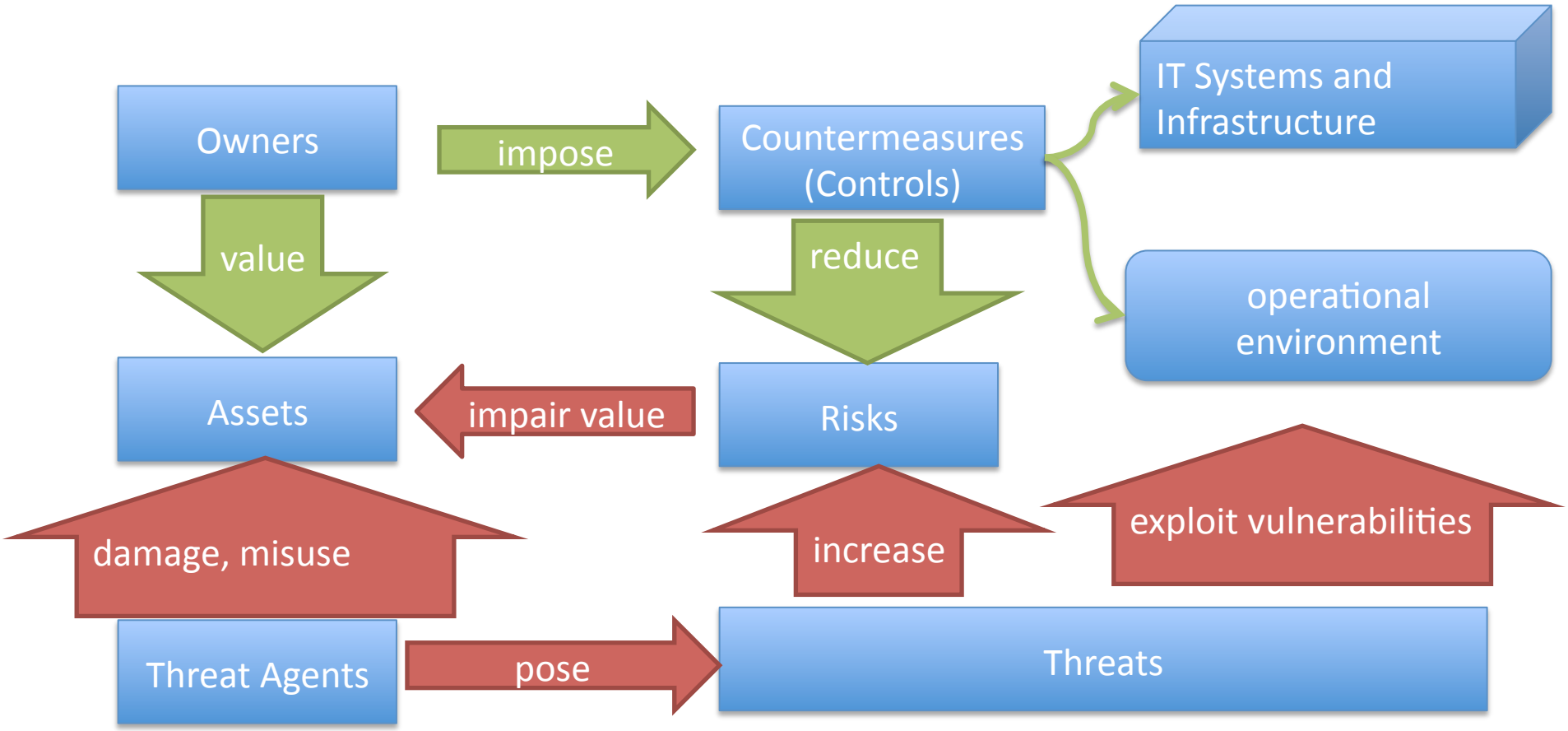
Cloud Computing and Continuous Auditing

- Cloud computing (CC)
  - builds on recent advances in continuous reporting, but
- CC challenges continuous auditing in many ways
  - auditing targets may not exist at the time of auditing –
    - even if high resolution time scales are chosen
  - to be audited organizations can be complex networks both on the provider and on the client side
    - (see multi-tenancy)
- let us examine the challenges in more detail …

Analysis Framework -- Common Criteria for Information Technology Security Evaluation

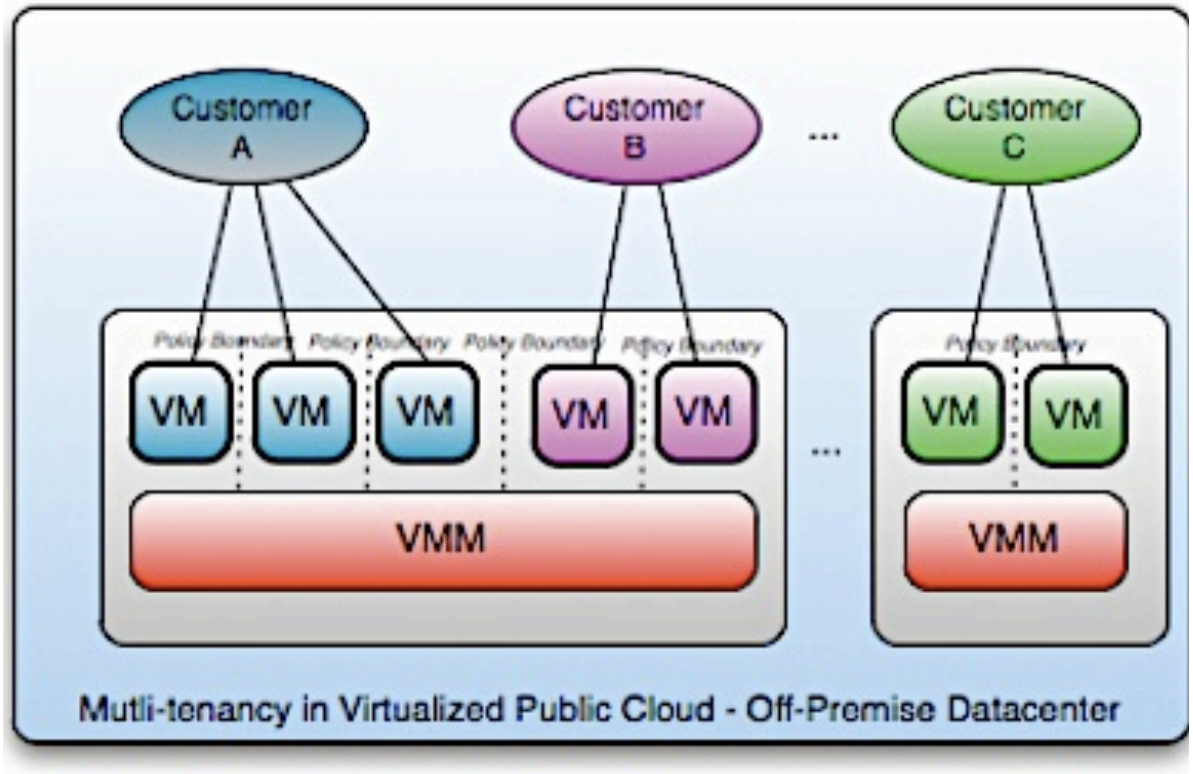
- Security target (ST) – defines
  - security problem definition (Threats)
  - security objectives (Countermeasures)
  - security requirements (IT / operational environment)
    - functional
    - assurance
- Common Criteria focus on countermeasures evaluation for sufficiency and correctness
  - ST – for specific targets of evaluation (TOE)
  - Protection Profiles (PP) – generic requirements for types of TOE
  - both ST / PP refer to specific components according to the SFRs
- Common Criteria assurance evaluation

Overview – The Common Criteria general model



Cloud Computing Property / Issue Multi-Tenancy

- Multi-Tenancy introduces policy boundaries between VMs managed by a single or several hypervisor instances



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

from CSA Guide Version 2.1, p. 18

Criteria to be refined in Cloud Services

- Whose Cloud is it?
  - Ownership of parts of IT infrastructure?
  - owners' responsibilities can be delegated
    - to the cloud provider or a provider to the cloud provider …
- Who is it in the Cloud?
  - Identification of Threat Agents?
  - authentication and access control can be abstracted – provisioned identities (IDaaS)
- Which cloud am I in?
  - Ownership of Operational Environment?
  - storage location does not imply physical or legal ownership

Challenges for Continuous Auditing in Cloud Services

- Entities and Events relevant for auditing
  - are spread across multiple businesses (CSPs and client organizations)
  - with highly fluctuating supply network structures
- Integrated model of cloud services auditing requirements is difficult to set up
  - Boundaries of responsibilities and overall responsibility
  - Contractual and Policy details and boundaries
- Risk profiles for CSPs are not standardized, often even not existing

Cloud Computing Auditing – The need for Standards

- in order to improve this situation we need standards for defining / describing CC …
  - security targets, threats, control activities
  - audit objects and objectives
  - operational and compliance risk profiles
- related standards exist, but in a fragmented way …
  - example – Policies (X-ACML), Security Assertions (SAML), Service Provisioning ML
  - Specific security evaluation standards Common Criteria, ISO 27001/2 and related frameworks for auditing

Two important and related Standardization initiatives

- Cloud Security Controls Matrix
  - Cloud Security Alliance (CSA)
  - additional specs for Metrics …
- Governance, Risk, Compliance (GRC) XML
  - Open Compliance and Ethics group (OCEG), Technology Council
  - broader scope than CC
- Both OCEG and CSA represent key vendor and customer enterprises and aim at integrating existing standards

Security in the Cloud – the Cloud Security Alliance

- Existing IT security frameworks need extensions
  - Cloud Computing needs security models adapted to multi-organisational operation environments
  - user related security requirements are complicated in cloud computing through provisioned identities
  - Cloud Hypervisor software works like a meta-operating system – lots of additional security objectives
- CSA is addressing Cloud Computing Specific Security Issues through
  - dedicated Research
  - Technical Specifications

CSA Guide Cloud Security Domains

- Governance Domains
  - Governance and Enterprise Risk Management
  - Legal and Electronic Discovery
  - Compliance and Audit
  - Information Lifecycle Management
  - Portability and Interoperability

- Operational Domains
  - Traditional Security, Business Continuity and Disaster Recovery
  - Data Center Operations
  - Incident Response, Notification and Remediation
  - Application Security
  - Encryption and Key Management
  - Identity and Access Management
  - Virtualization

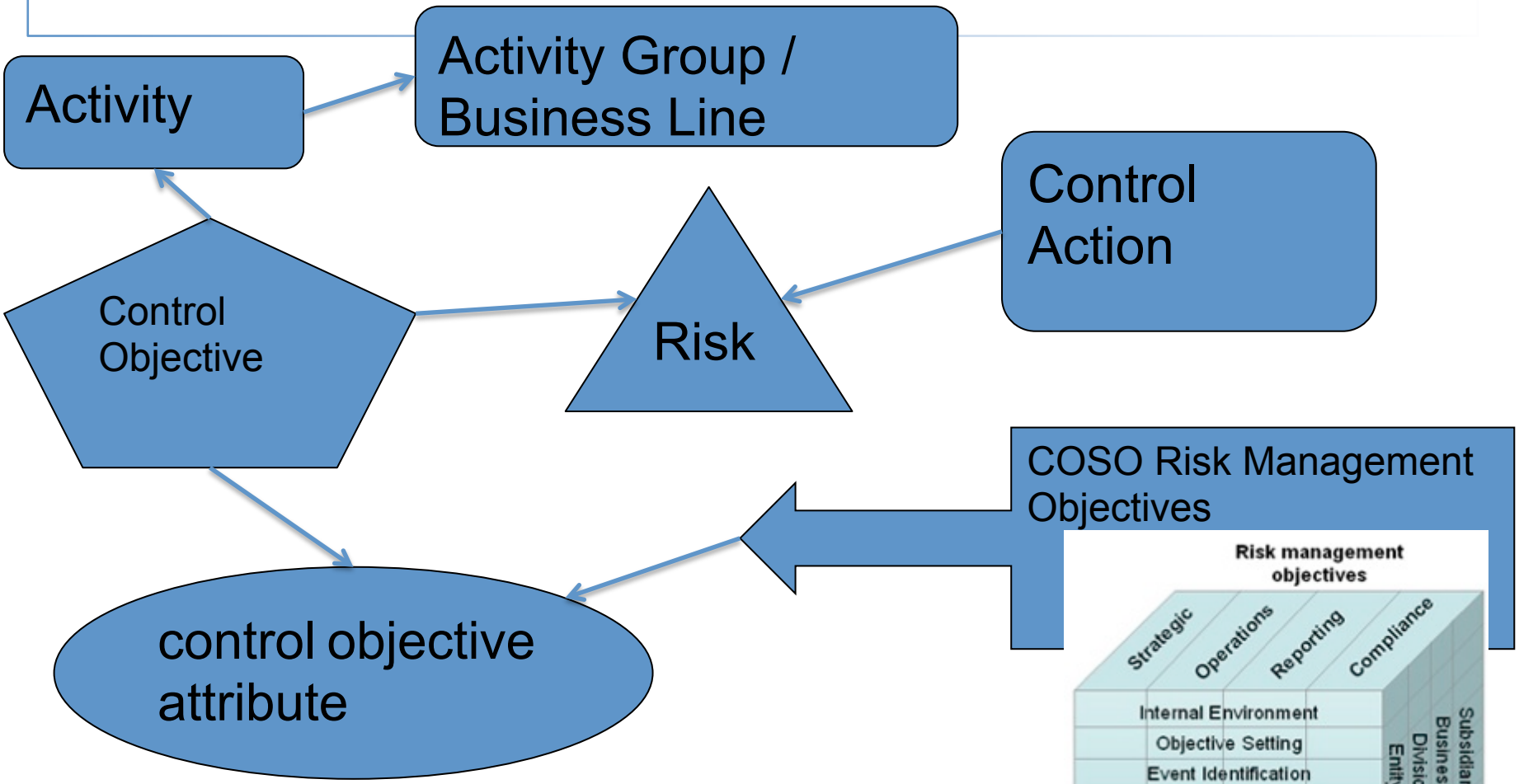
CSA Cloud (Security) Controls Matrix

- CSA CCM
  - currently available in MS-Excel
  - two level taxonomy of control areas
    - related to the CSA Guide document Cloud Security domains
  - textual description of control activities
    - specific issues both for IT infrastructure and operational environments
  - references to numerous IT Risk Management and Information Security standards
    - including ISACA and AICPA
- consensus process to ensure key concerns are addressed
  - detailing control activities w.r.t. assurance
  - top 100 concerns captured in question list
  - each question needs at least one mapping in the control activities
- audit questionnaires

OCEG GRC-XML

- based on the extensible Business Reporting Language (XBRL) – Global Ledger
  - benefit – specify GRC entities / relationships INTEGRATED with suitable formats for
    - reporting / auditing documents
    - data tables structured for analytical applications (dimensions)
- Overall goal is to build a full representation of the OCEG GRC capability framework
  - OCEG Red book – conceptual framework and questionnaires
  - OCEG Burgundy book – data analysis including analytics and benchmarking facilities for authorized enterprise members
- essential categories in the alpha1 version of 2009 (see OCEG GRC-XML white paper by S. Tabet) are outlined on the next slide

GRC-XML alpha1 2009 Conceptual Overview



Specification led by Said Tabet

THE ADDITIONAL CHALLENGE – CAPTURING THE SEMANTIC LAYER IN CLOUD SERVICES

Cloud Computing Audit data generation and analysis

Common Criteria SFRs

- Security audit data generation (FAU_GEN)
  - Level definitions of auditable events
  - Data list definition for each audit record
- Security audit analysis (FAU_SAA)
  - Potential violation analysis on the basis of a fixed rule set
  - Profile based anomaly detection on the basis of usage patterns by profile target group
  - Simple attack heuristics by detecting "signature events" that represent a significant threat to enforcement of SFRs
  - Complex attack heuristics -- represent and detect multi-step intrusion scenarios (poss. produced by diff. users / groups)

Cloud Computing Challenges

- Security audit data generation (FAU_GEN)
  - Level definitions **contracted** and **compliant**
  - Data list definition **contracted** a. **compliant**
- Security audit analysis (FAU_SAA)
  - violation analysis needs **adaptable** rule sets and service **composition analysis**
  - usage patterns by profile target group may be invisible to CSP, **typical anomalies** may be invisible to client
  - "signature events" occur in the cloud and the **identity** of the **causing entity** may be provisioned – needs being **traced**
  - Complex attack heuristics -- **represent** and detect multi-step intrusion scenarios **exploiting Cloud APIs and provisioned Ids**

Cloud Computing Audit reviews and audit events

Common Criteria SFRs

- Security audit review (FAU_SAR)
  - capability to read information from audit records
  - restricted access to audit review information
  - selectable audit review
- Security audit event selection (FAU_SEL)
  - Selective audit based upon attributes specified in PP/ST
- Security audit event storage (FAU_STG)
  - protected audit trail storage
  - guarantee of audit data availability
  - action in case of possible audit data loss
  - prevention of audit data loss

Cloud Computing Challenges

- Security audit review (FAU_SAR)
  - capability **to integrate information from audit records by multiple organizations**
  - **complex access rules** for X-tenants / CSPs access to audit review information
  - selectable X-tenants / CSPs audit review
- Security audit event selection (FAU_SEL)
  - Selective audit based upon attributes specified **across** PP/ST **interoperably**
- Security audit event storage (FAU_STG)
  - **Agreed** Protection levels X service network
  - **Agreed** guarantee of audit data availability
  - **coordinated** actions ag. audit data loss
  - **coordinated** prevention of audit data loss

So there are additional challenges for continuous auditing across the clouds …

- This detailed analysis suggests SFRs are insufficient to fully capturing information needed for auditing, in addition, we need
  - semantic interoperability – ensure that data definition, access restrictions and policies are described such that a broad variety of CSPs and customers can be audited against them
  - automated consistency and verification checks should be enabled to master the complexity of all the GRC elements involved

Interoperability of Audit elements descriptions

- it would be unrealistic to require all existing related languages to be re-versioned
- key issue is semantic relationship
  - control activities address risks / vulnerabilities
    - hard to cast this to a relationship bw entities
- so we need an interoperability layer on a semantic level
  - can relate policy X of vendor A to data definition element Y of customer B …
  - a joint meta-data model with transformations from / to, e.g.,
    - SAML, X-ACML,
    - WS-Policy, WS-Federation

Automated Consistency Checks and Verifications – Use cases

- Governance
  - infer applicable regulatory requirements
  - verify adequateness of control activities
- Risk
  - check probable threats and infer suitable control activities
  - set up sufficient metrics systems for specific cloud services
- Compliance
  - match vendor's policies against required controls
  - verify operational environment / IT infrastructure against regulatory / statutory requirements

Solution Approach

- one solution to both requirements is introducing an ontology layer –
  - give a precise an actionable meaning to all domain concepts and their relationships
  - domain specific (formal) language
    - comprising suitable taxonomies and concept associations
  - special focus on logical structure
    - integrate a rules representation language
    - integrate capability to compute logical inferences
    - integrate capability to solve constraint satisfaction problems

A related approach from EU research – Next Generation BI for Risk Management

- EU MUSING project (www.musing.eu)
- Multi-Industry Semantics Based Next Generation Business Intelligence
- goal – combine the strengths of AI and BI
  - represent knowledge and infer facts and rules
  - blueprint new generation of analytics services

Next Generation
Business Intelligence

Feasibility of a Semantic Layer – Conclusions from the MUSING project

- MUSING focussed on integrating structured with unstructured data in Risk Analysis
  - textual data from business analysts, public sources, trusted information services
  - service flow integrated with Data Mining
- MUSING delivered a comprehensive set of domain ontologies
  - using specific semantic web approaches (RDF, OWL)
  - restricting inferences to decidable cases
- MUSING delivered a set of service oriented risk management pilots integrating all these technologies

Conclusion and Outlook

- Cloud Computing is an important field for CA&R
  - CA&R should be supported by definition
  - need to integrate auditing with advanced security modelling and GRC management
- innovative challenges for auditing automation and monitoring
  - can be extended to cover ever more GRC capability elements
  - interest in pursuing this by prominent standardization organizations active in CC and GRC
  - first steps in setting up suitable projects are being made

Thank you for your attention!