University of Innsbruck
School of Management
Information Systems

Performance Measurement in Cross-Organizational Security Settings

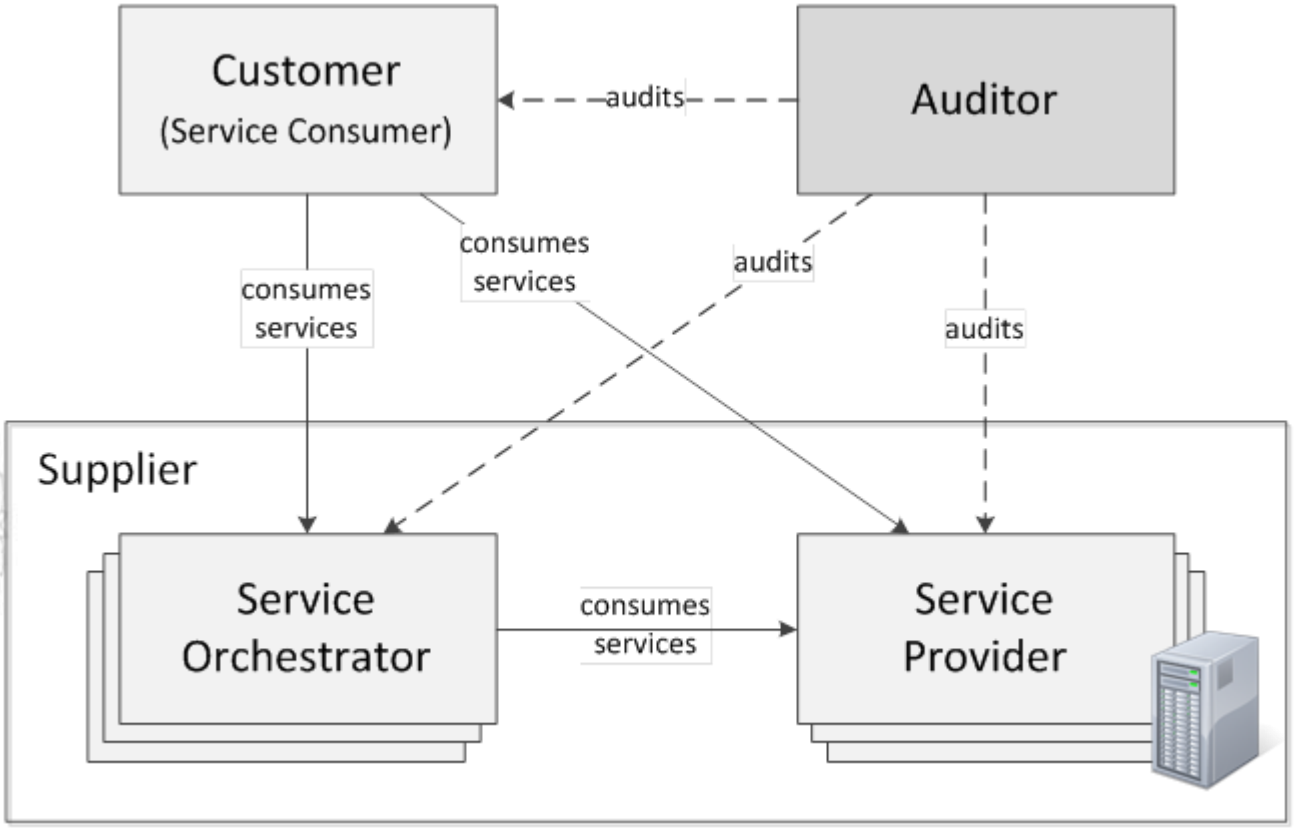
7th International Workshop on
Security Measurement and Metrics
Banff, Alberta

Lukas Demetz, Stefan Thalmann, Daniel Bachlechner, Ronald Maier

Overview

- Motivation
- Empirical Foundation
- Results
- Conclusion & Outlook

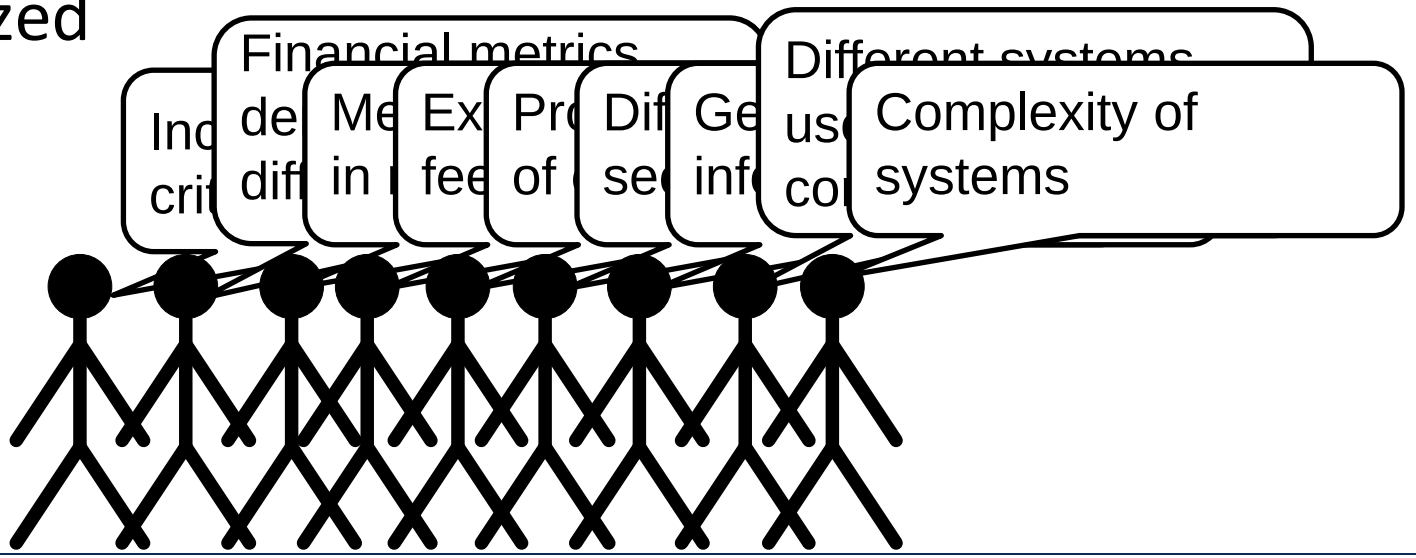
Motivation



What are suitable metrics for determining a service supplier's level of security and compliance?

Empirical Foundation

- Two series of interviews with 28 information security professionals focusing on
  - Intra-organizational settings
  - Cross-organizational settings
- Interviews recorded, transcribed and qualitatively analyzed



Results

- Service Consumer
  - Quality of service supplier
    - # of security and compliance violations per service provider
  - Integration of existing landscape
  - Monitoring supplier
  - Skilled employees
    - # of employees able to integrate outsourced services
  - Trust for service providers
    - avg. probability of security incidents per supplier
- Service Supplier
  - Taking changes in technology into account
    - avg. time to plan for changes
  - Providing audit compliance
    - time/costs spent on audit activities
  - SLAs covering provided services
    - % of SLAs with assigned account manager
  - Cost of missing security
  - Customer satisfaction

Conclusion & Outlook

- Interviewees are able to judge whether processes are well performed, however, struggle to identify KPIs
- Interviewees face several challenges when trying to define suitable KPIs
- Based on the interviews and a thorough literature review exemplary KPIs could be proposed
- The evaluation of the success of a software tool focusing on achieving and maintaining secure and compliant IT infrastructures will be based on the proposed KPIs

Acknowledgments

The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129) and through the COSEMA project which is sponsored by the Tyrolean business development agency.

PoSecCo
Policy and Security Configuration Management

http://www.posecco.eu

COSEMA
Collaborative Security Management

http://www.cosema.org/en

Contact

Lukas Demetz
Lukas.Demetz@uibk.ac.at

Stefan Thalmann
Stefan.Thalmann@uibk.ac.at

University of Innsbruck
School of Management
Information Systems I
Universitätsstraße 15
6020 Innsbruck, Austria

Backup

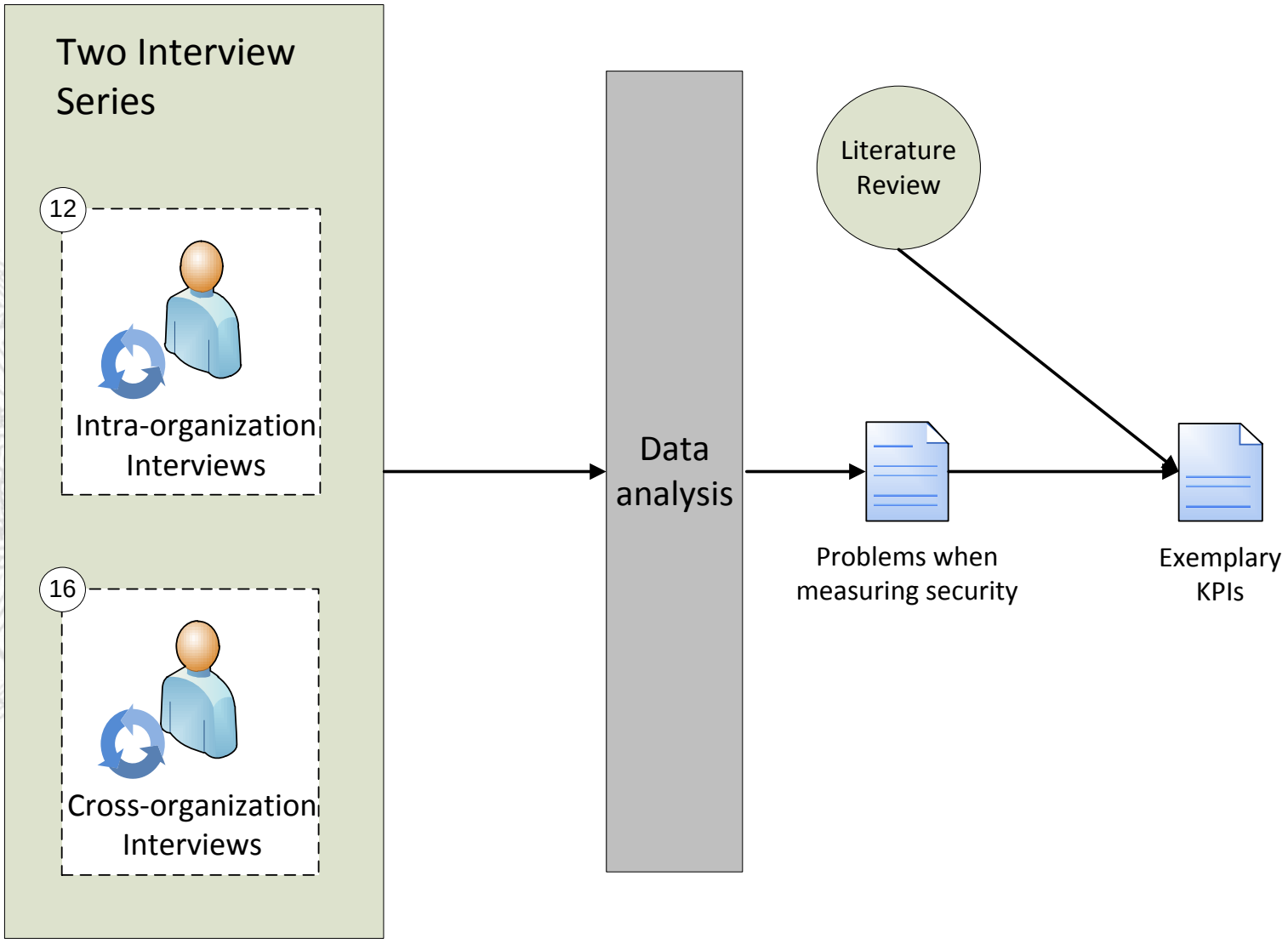
KPIs – Service Consumer

Quality of service supplier	# of security and compliance violations per service provider
Integration of existing landscape	avg. time to realize changes of the existing IT landscape avg. costs to realize changes of the existing IT landscape
Monitoring supplier	avg. time needed for auditing an (outsourced) service avg. costs needed for auditing an (outsourced) service % of service providers meeting defined security, compliance requirements and SLAs
Skilled employees	# of employees able to integrate outsourced services # of employees able to negotiate technical details # of employees being able to monitor service provider
Trust for service providers	avg. probability of security incidents per supplier

KPIs – Service Supplier

Taking changes in technology into account	avg. time to plan for changes avg. costs of change implementation
Providing audit compliance	time/costs spent on audit activities # of audits successfully completed % of systems with security certifications
SLAs covering provided services	# of SLAs per service % of service levels that are measured % of SLAs with assigned account manager
Cost of missing security	cost of security incidents per service
Customer satisfaction	% of stakeholders satisfied with quality of IT security

Study Procedure



Open Questions

- How would you proceed to measure security in a cross-organizational security setting?
- Have you already done something similar?
- Do you have any recommendations?
- Do you know any best practices in this domain?