How can ISO Management System Standards contribute to mitigate business risks?

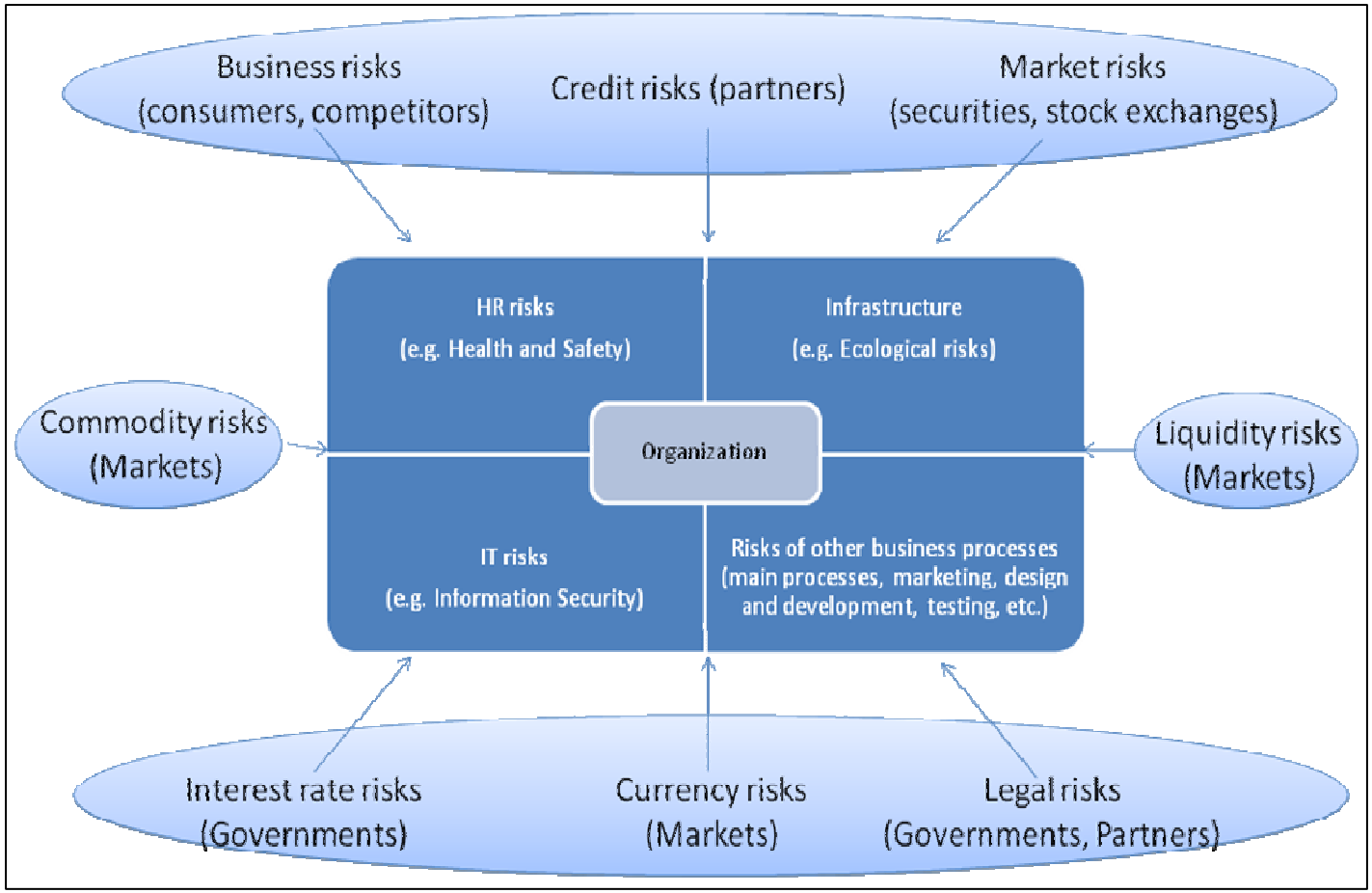
Valentin Nikonov, PhD (Economics), PMP IPMA,
Director General, Growth Trajectory Consulting Company

Irena Kogan, Partner,
Growth Trajectory Consulting Company

Issues of practical implementation

- ‘Nobel prize lectures’ vs. ‘buy low, sell high’, and ‘generic risk management process’
- Everybody manages risks – no need to convince
- How to make risk management efficient and effective?
  - Risks are timely identified and no risks are missed
  - Risk are properly evaluated
  - Risk management strategies are implemented effectively
  - Etc.

Too many risks to manage: standards come from different spheres

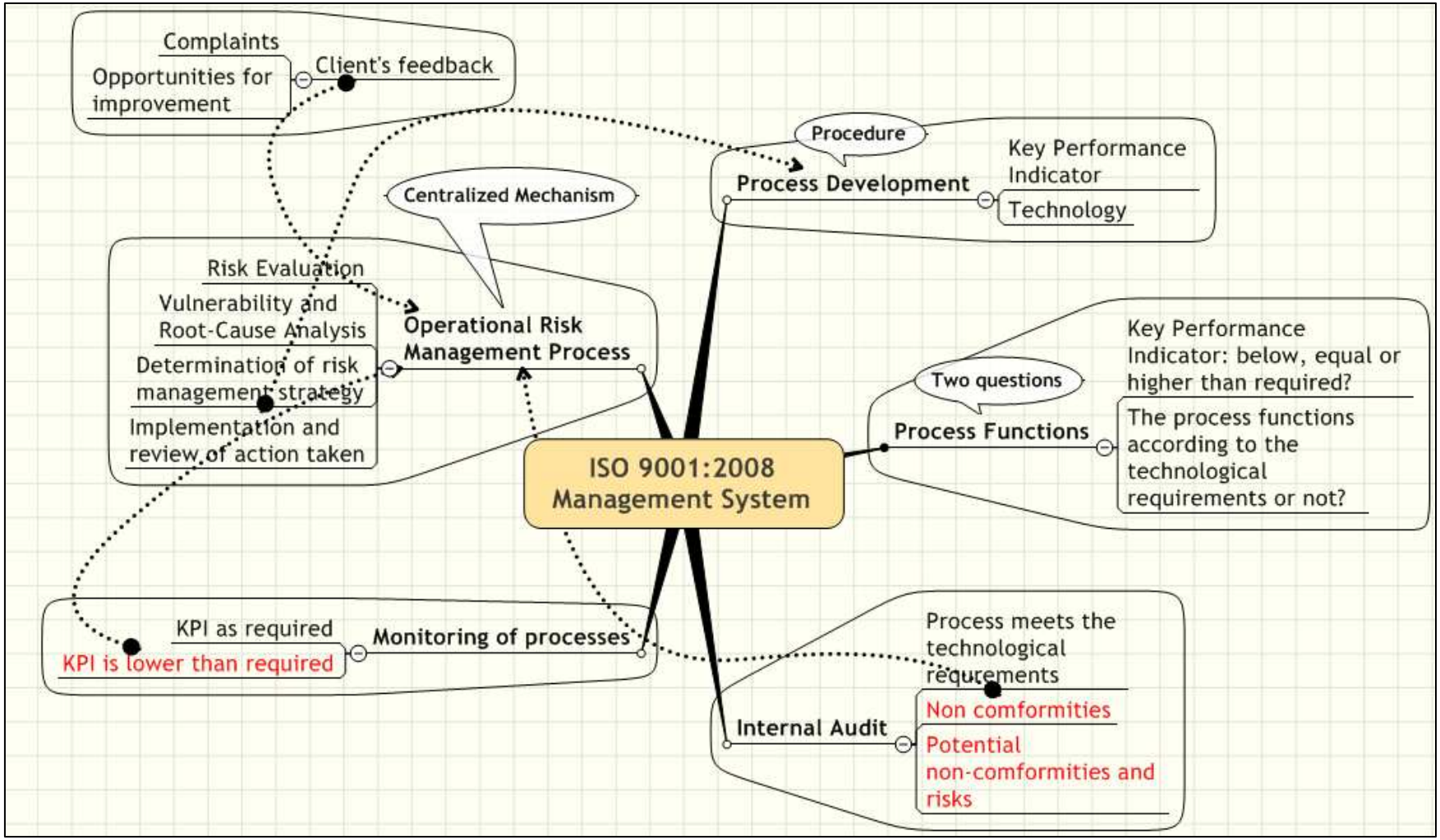


Necessary conditions to build a RM System

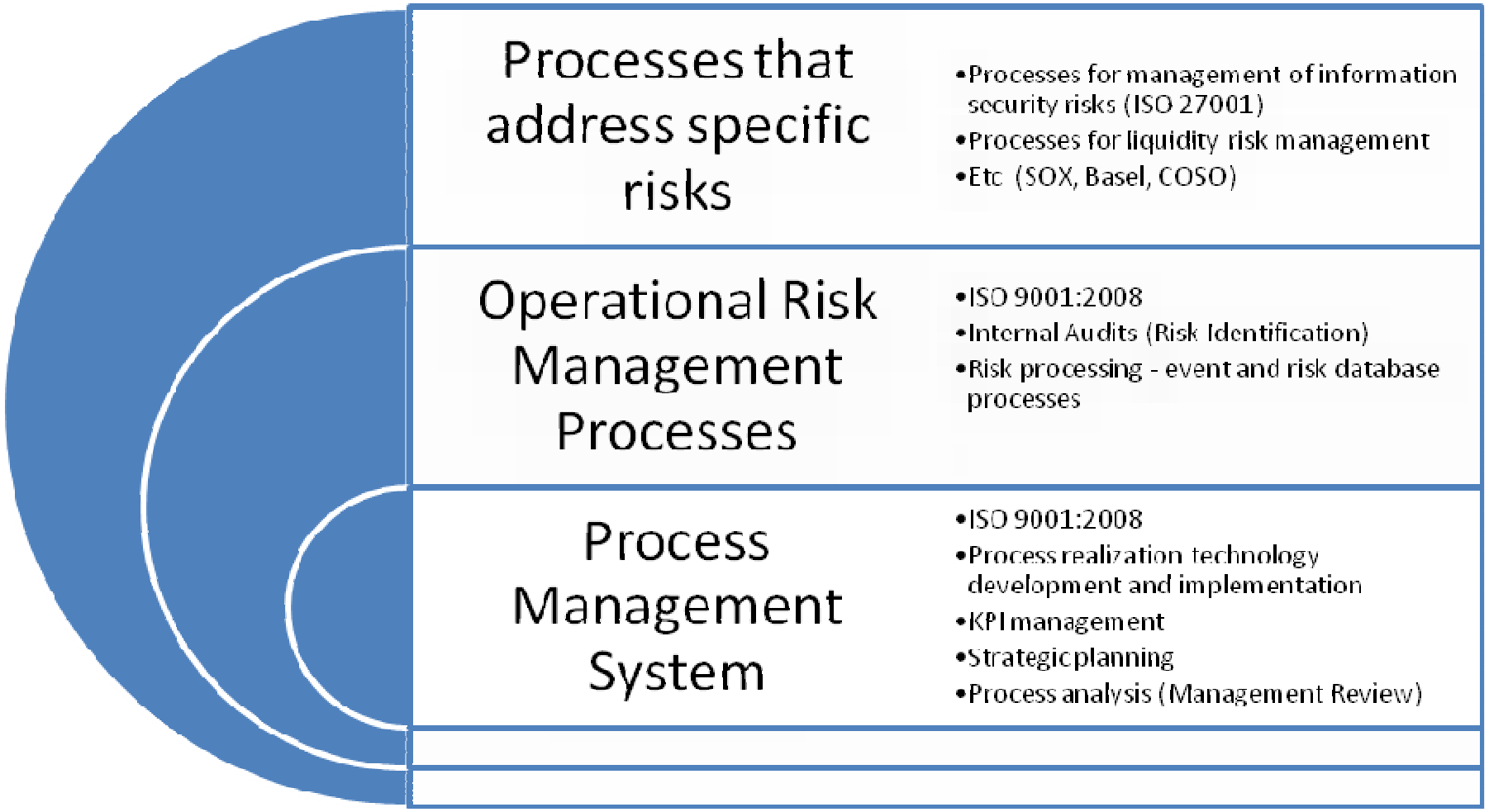
1. Process management framework
   – Risks are managed by business processes
2. Operational risk management system
   – Risks ‘reside’ in the business processes

- ISO Management System Standards are very helpful – risk management system is already there

Business process and operational risk management system

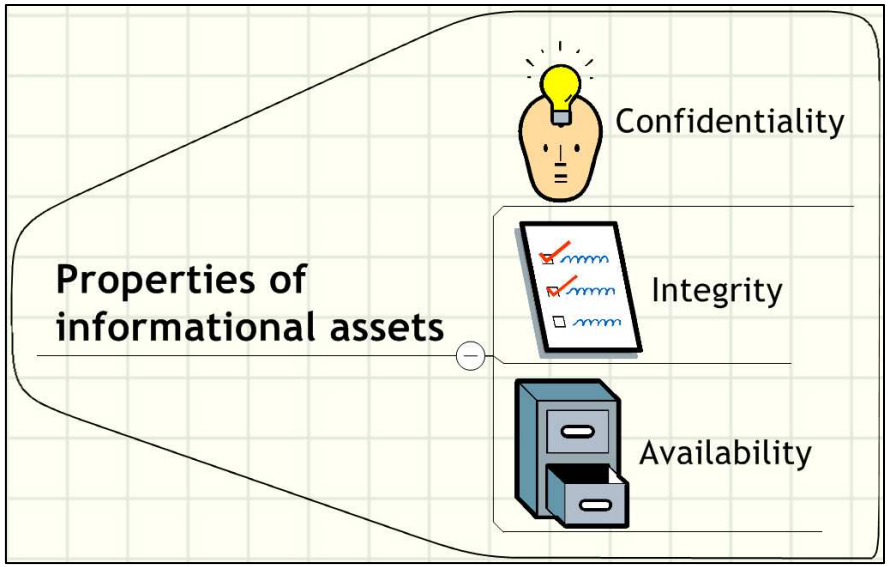


Three-layer Risk Management System

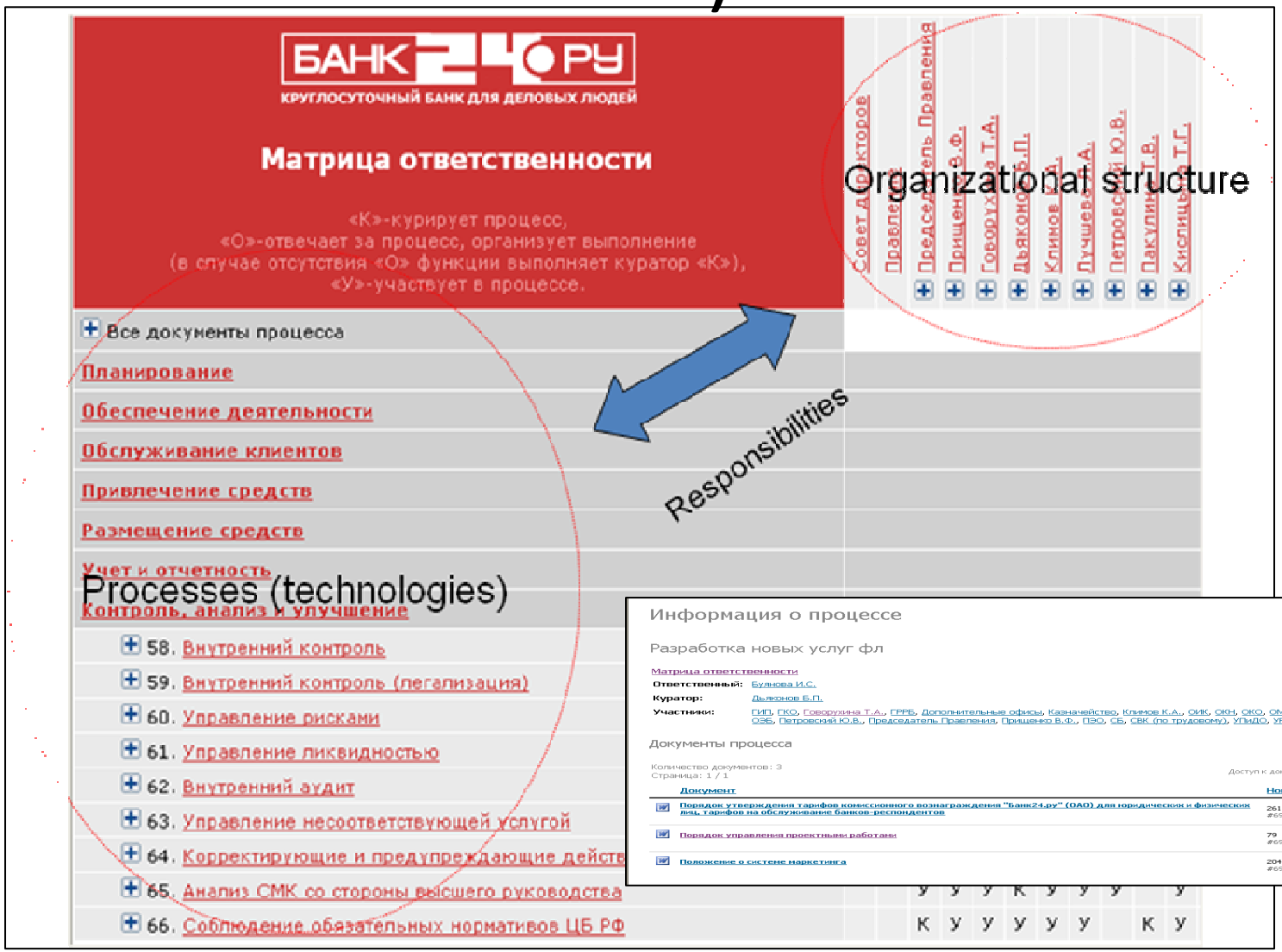


Case study

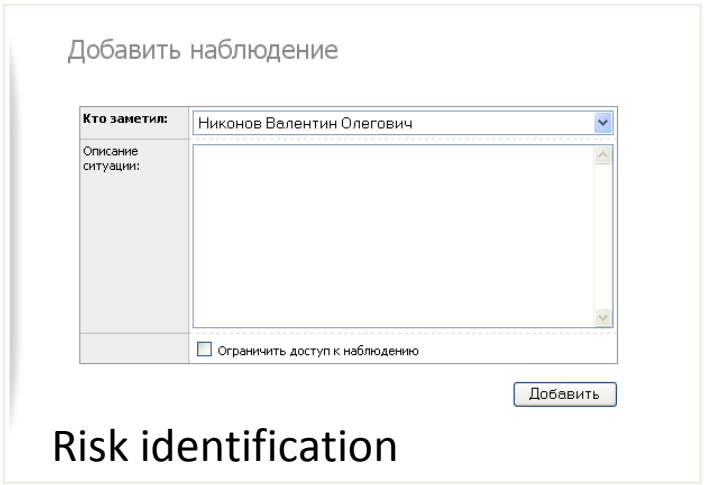
- Operational risk management on the basis of ISO 9001:2008
- Integrating Information Security Risk management processes (based on ISO 27001:2005)



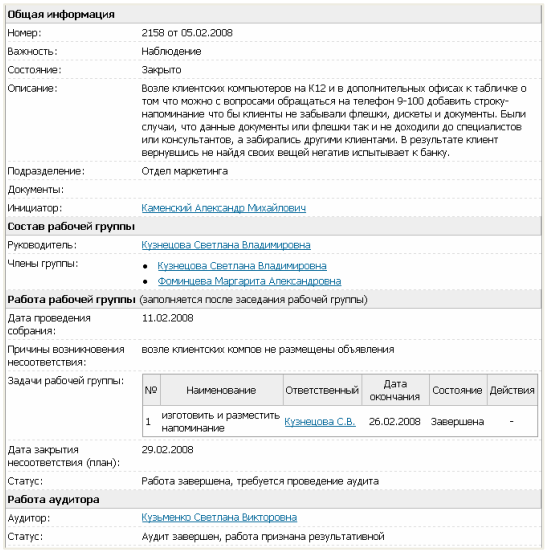
Business Process Management (ISO 9001)



Operational Risk Management System (ISO 9001)



Risk identification



Risk assessment

Risk management strategy

Internal Audits (8.2.2 ISO 9001:2008)

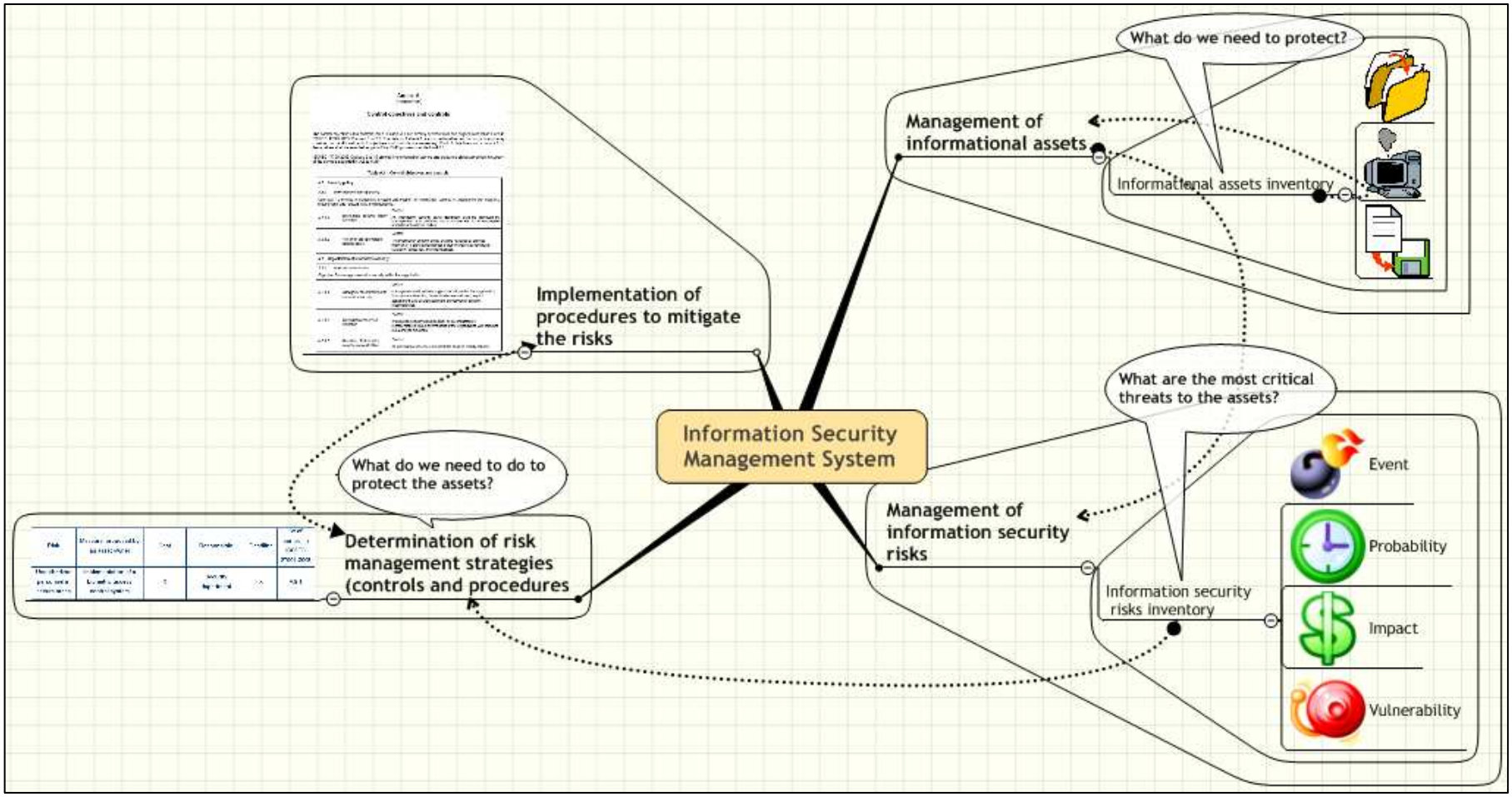
Observations from employees (8.5.2,8.5.3 ISO 9001:2008)

Operational risk management process (ISO/IEC 9001:2008)

Information security risks (ISO/IEC 27001)!

Customer feedback (8.2.1 ISO 9001:2008)

Adding processes for specific risks - Information Security (ISO 27001:2005)



ISO 27001:2005 Information Security Management System

Management of informational assets

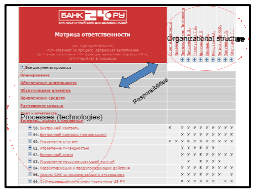
Name	Confidentiality	Integrity	Availability	Criticality	Owner	Users
Clients database	*High*	*High*	*High*	*High*	*The head of sales division*	*Sales division*

Management of informational risks

Risk	Measure, proposed by an asset owner	Cost	Responsible	Deadline	№ of control in ISO/IEC 27001:2005
Unauthorized personnel in secure areas	Implementation of a biometric access control system	X	Security department	X	A.9.1

Annex A

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance



'New lines' in the process table – raising business efficiency

Conclusion

- ISO MS Standards application forms a ground for implementation of a three layer enterprise-wide risk management system, which provides effective and consistent management of risks;
- Though different organizations manage different risks, the structure of a Risk Management System is the same for organizations of all types;
- Further development of risk management tools and methods on the basis of existing ISO standards would be beneficial for risk management promotion and application at all levels.