

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

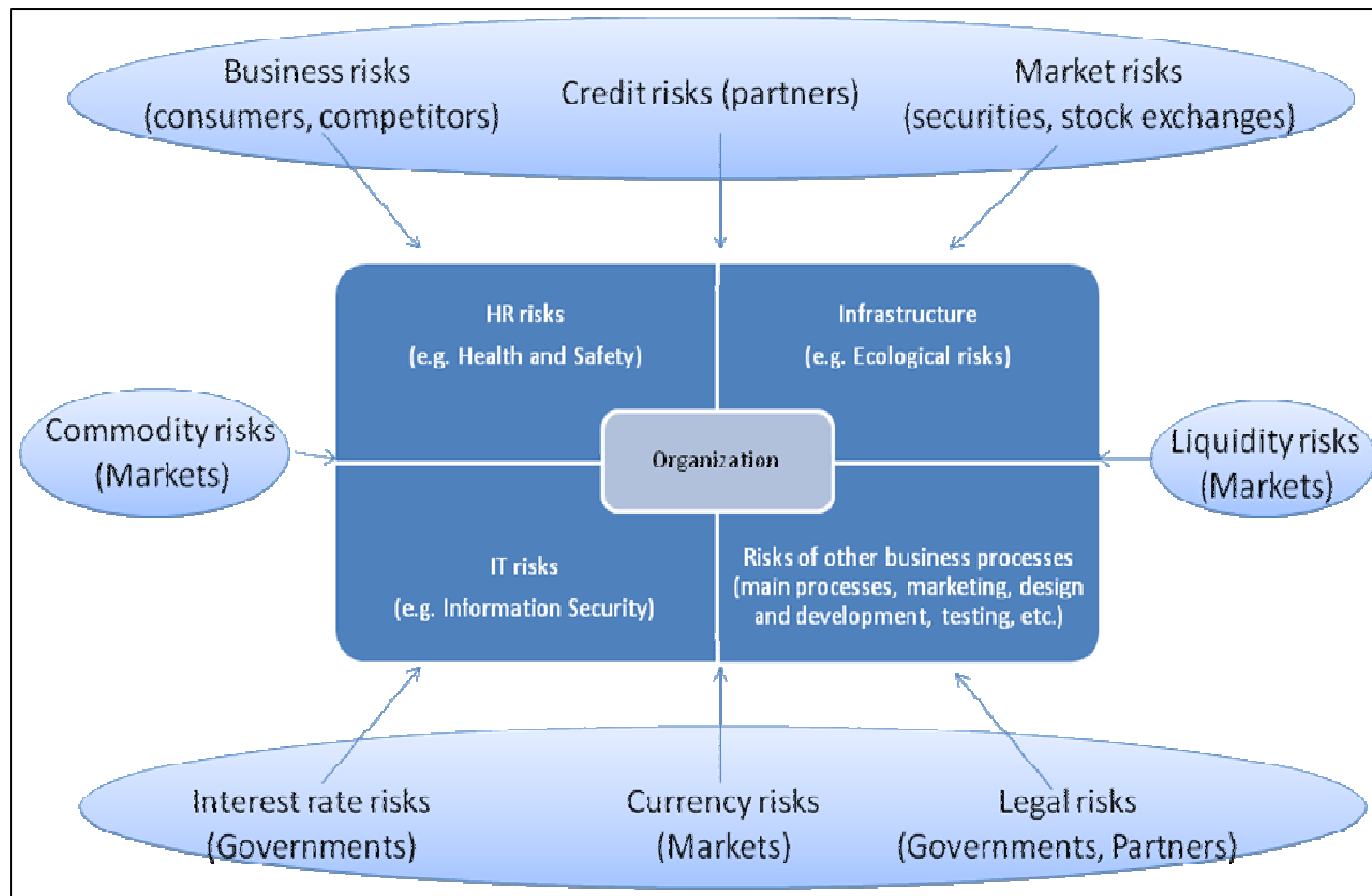
Valentin Nikonov, PhD (Economics), PMP IPMA,  
Director General, Growth Trajectory Consulting  
Company

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.

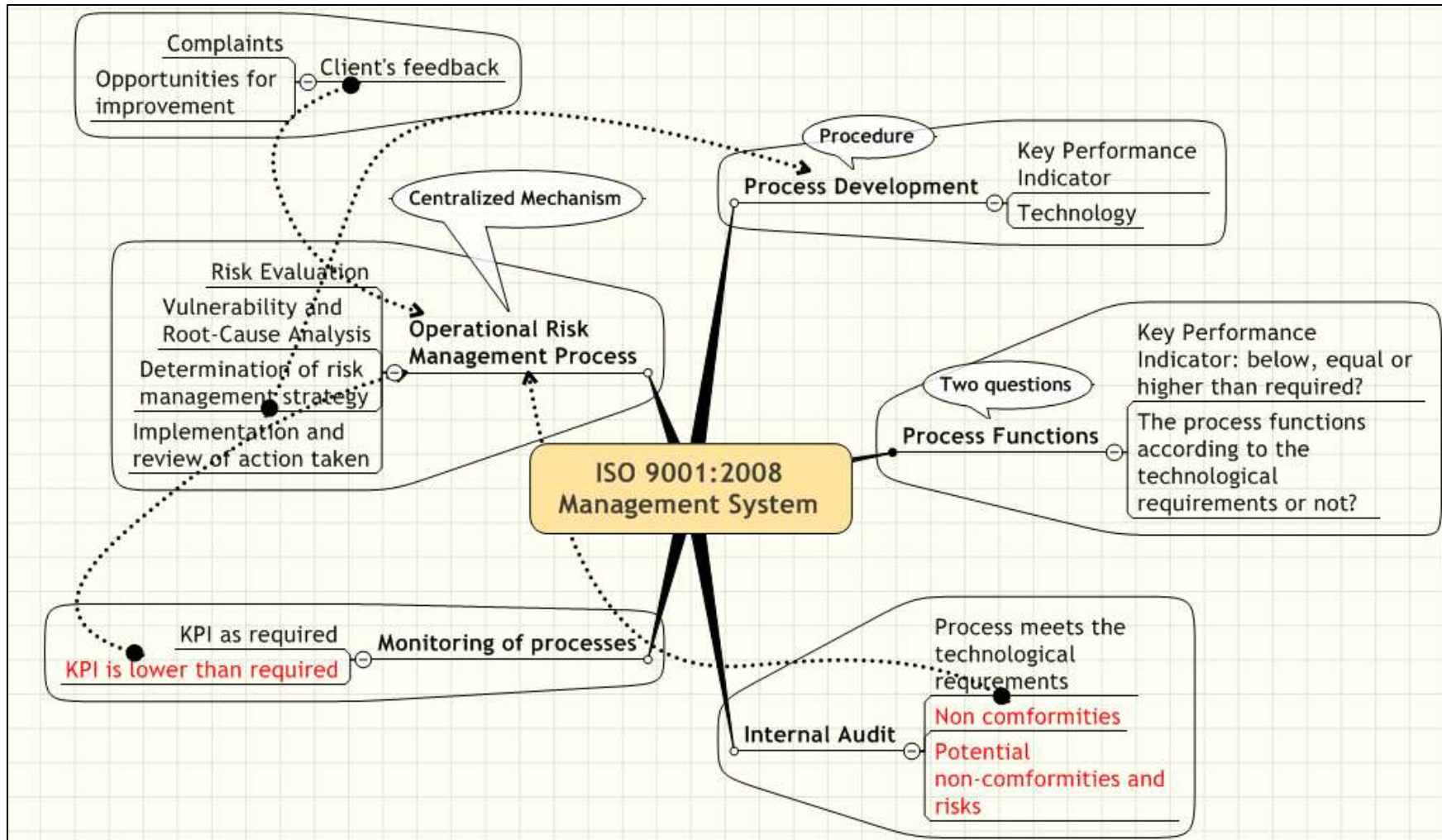
# Too many risks to manage: standards come from different spheres



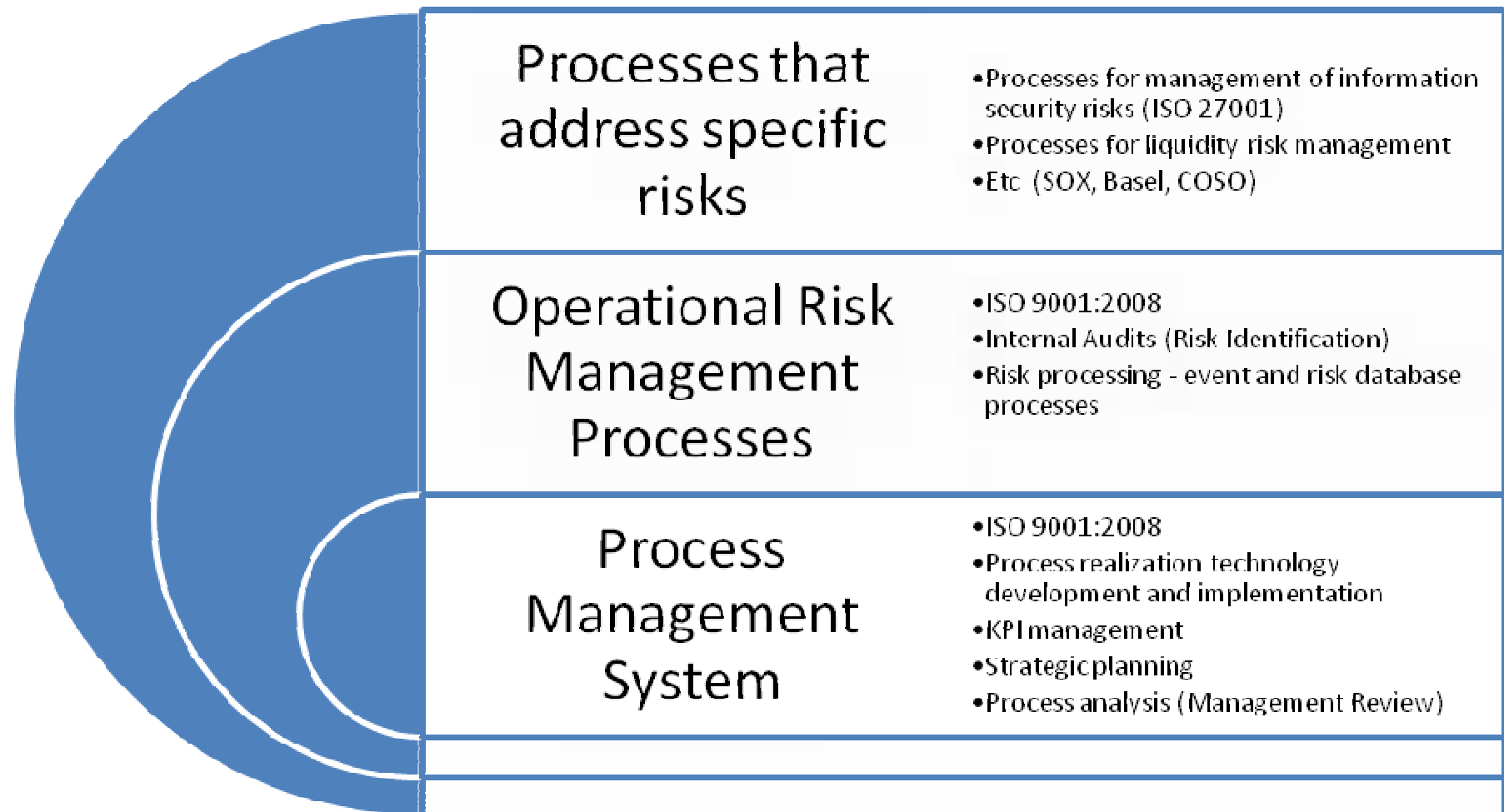
# Necessary conditions to build a RM System

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

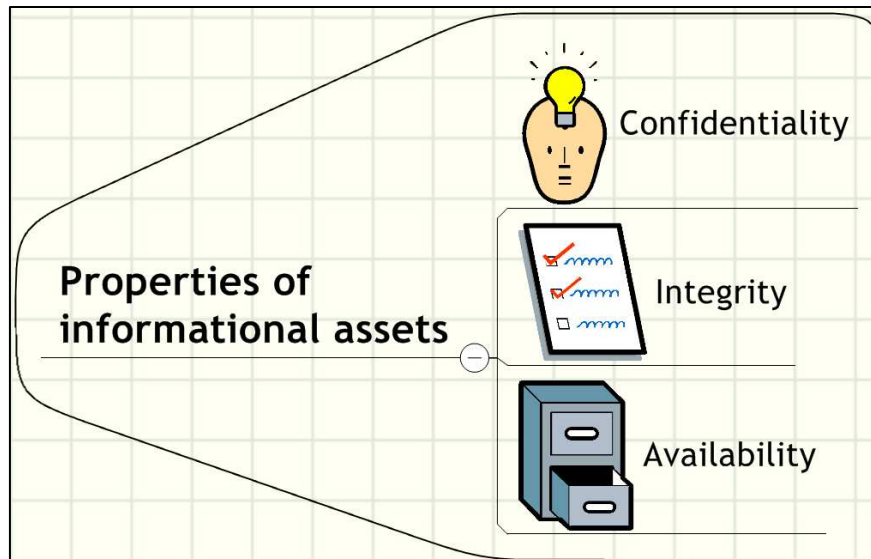


# Three-layer Risk Management System

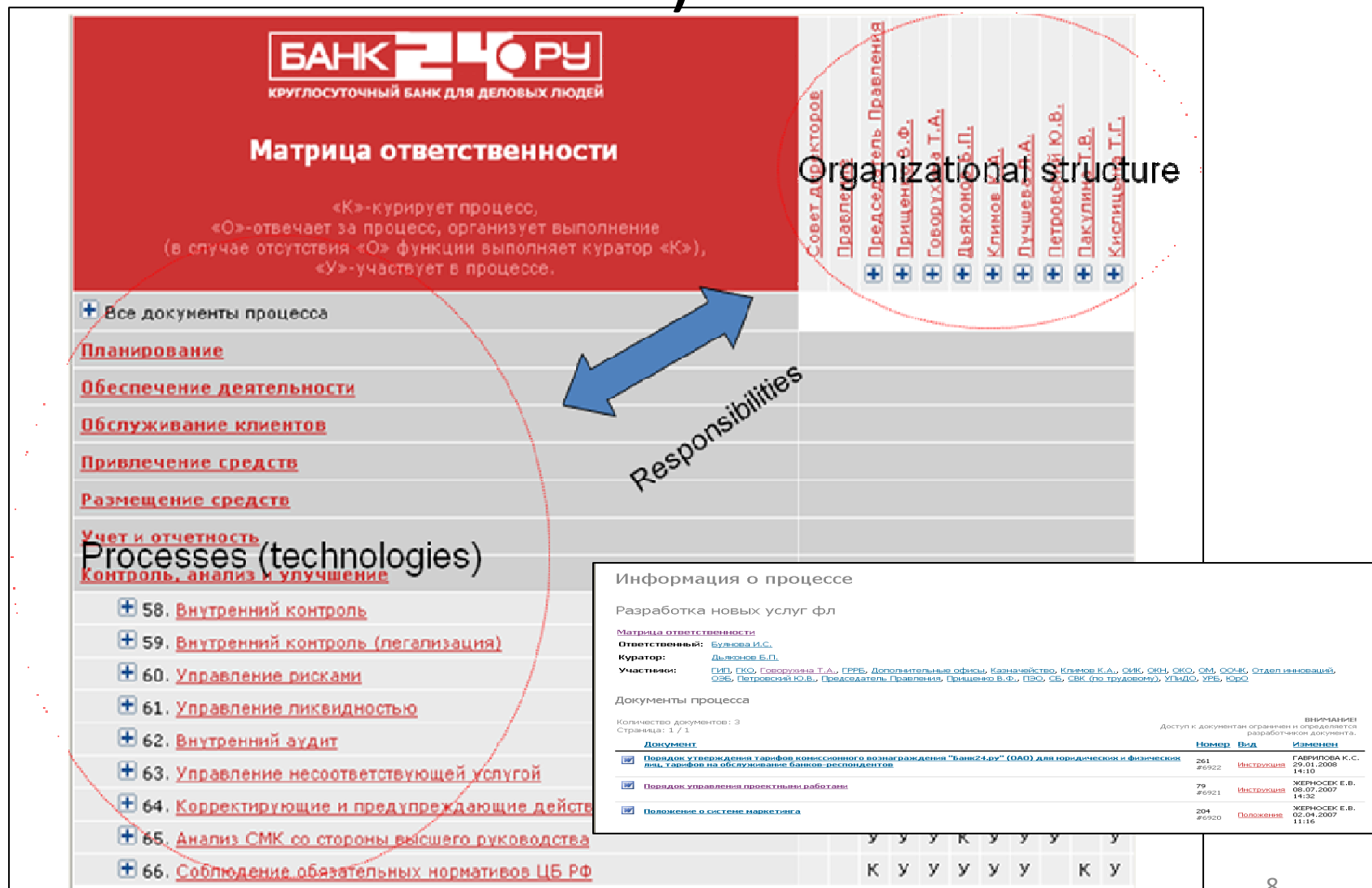


# Case study

- 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)

Добавить наблюдение

Кто заметил:	Никонов Валентин Олегович
Описание ситуации:	

☐ Ограничить доступ к наблюдению

Добавить

**Risk identification**



**Общая информация**

Номер: 2158 от 05.02.2008

Важность: Наблюдение

Состояние: Закрыто

Описание: Возле клиентских компьютеров на К12 и в дополнительных офисах к таблице о том что можно с вопросами обращаться на телефон 9-100 добавить строку: напоминание что бы клиенты не забывали флешки, диски и документы. Были случаи, что данные документы или флешки так и не доходили до специалистов или консультантов, а забирались другими клиентами. В результате клиент вернувшись не найдя своих вещей негатив испытывает к банку.

Подразделение: Отдел маркетинга

Документы:

Инициатор: [Каленский Александр Михайлович](#)

**Состав рабочей группы**

Руководитель: [Кузнецова Светлана Владимировна](#)

Члены группы:

- [Кузнецова Светлана Владимировна](#)
- [Фоминцева Маргарита Александровна](#)

**Работа рабочей группы** (заполняется после заседания рабочей группы)

Дата проведения собрания: 11.02.2008

Причины возникновения несоответствия: возле клиентских компов не размещены объявления

№	Наименование	Ответственный	Дата окончания	Состояние	Действия
1	изготовить и разместить напоминание	<a href="#">Кузнецова С.В.</a>	26.02.2008	Завершена	-

Дата закрытия несоответствия (план): 29.02.2008

Статус: Работа завершена, требуется проведение аудита

**Работа аудитора**

Аудитор: [Кузьменко Светлана Викторовна](#)

Статус: Аудит завершен, работа признана результативной

**Risk  
assessment**

**Risk  
management  
strategy**

Internal Audits (8.2.2  
ISO 9001:2008)

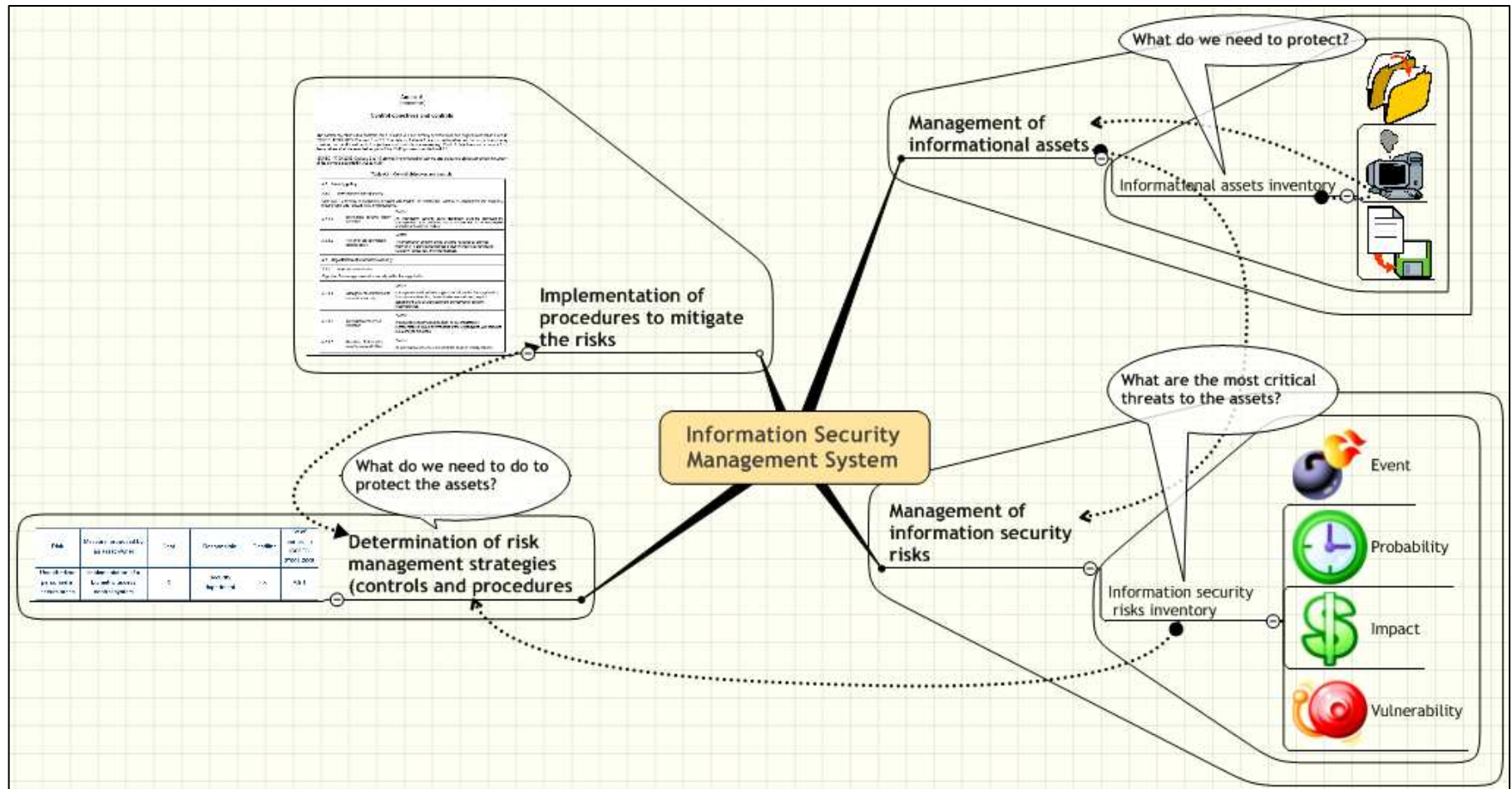
Observations from employees  
(8.5.2,8.5.3 ISO 9001:2008)

Information security risks  
(ISO/IEC 27001)!

Customer feedback  
(8.2.1 ISO 9001:2008)

Operational risk  
management  
process (ISO/IEC  
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	No 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.