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

Diagram:
- Business risks (consumers, competitors)
- Credit risks (partners)
- Market risks (securities, stock exchanges)
- Commodity risks (Markets)
- HR risks (e.g. Health and Safety)
- Infrastructure (e.g. Ecological risks)
- IT risks (e.g. Information Security)
- Organization
- Risks of other business processes (main processes, marketing, design and development, testing, etc.)
- Interest rate risks (Governments)
- Currency risks (Markets)
- Legal risks (Governments, Partners)
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

| Processes that address specific risks | • Processes for management of information security risks (ISO 27001)  
• Processes for liquidity risk management  
• Etc (SOX, Basel, COSO) |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Operational Risk Management Processes | • ISO 9001:2008  
• Internal Audits (Risk Identification)  
• Risk processing - event and risk database processes |
• Process realization technology development and implementation  
• KPI management  
• Strategic planning  
• Process analysis (Management Review) |
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)

Organizational structure

Processes (technologies)
Operational Risk Management System (ISO 9001)

Risk identification

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)
ISO 27001:2005 Information Security Management System

Management of informational assets

<table>
<thead>
<tr>
<th>Name</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Criticality</th>
<th>Owner</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients database</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>The head of sales division</td>
<td>Sales division</td>
</tr>
</tbody>
</table>

Management of informational risks

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

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.