Information Security Governance Framework

Andrej Volchkov
www.stramizos.com
avolchkov@stramizos.com
Objective

- Information security is on the board of director’s agenda, the management is accountable, but their understanding of security issues is lagging.
- The universe of security controls and activities must be modeled by hierarchy to facilitates understanding by senior management.

Presentation of a simple framework to facilitate understanding of information security governance activities.
Information security is important

- Contributes to the business development by assuring reliable operations and enabling new business opportunities in the digital economy.
- Facilitates service level differentiation (secure connections, reliable data transfers, secure outsourcing, etc.).
- Protects client data and secure transactions. Should be perceived as a competitive advantage.
- Contributes to enterprise compliance with legal and regulatory frameworks.
- Protects a company’s reputation.
- Reduces operational (financial) risks.
...and must be addressed at the highest level in the company

- Security must be overseen by decision-makers having the necessary authority.

  but,

- Are they knowledgeable?
- Do they understand security issues?
- Do they have the necessary tools?
- Do they know what questions to ask?

...and must be addressed at the highest level in the company
Ask yourself the following questions...

- Are the board and management involved in strategic information security decisions?
- Who defines the security strategy and policies?
- Who is legally responsible for the security posture and data protection?
- Do you know which business processes are at risk?
- Who owns sensitive data?
- Is your security adapted to meet real business needs?
- Do the business lines participate in security committees making decisions about securing their business processes?
- Do you know if your security expenditures are justified? What is the return on security investment (ROSI)?
What's there for me (senior executive)?

- What are my main responsibilities in managing the security program?
- What questions should I ask security specialists to assess our situation?
- How can I understand the jungle of security controls? What's there for me?
- Is there any simple framework for security governance?
- Where are my key responsibilities in IS?
- Etc.
What are the main areas (activities), related to security, which management should pay attention to?

or

As InfoSec governing body, what should we care about?

(please mention one or two)
The response may be: **Three-Level Control Framework (TLCF)**

**Strategic:**
Global orientation for the Security Program (Strategy, Policies, Organization)

**Tactical:**
Management of the Security Program (Risk, Program, Reporting and Oversight, Compliance, Asset, Metrics)

**Operational:**
Operational security controls
Building blocks of a TLCF

- Policies
- Risk management
- Assets management
- Security Operations
- Strategy
- Program management
- Compliance
- Reporting, Oversight
- Organization
- Metrics

Strategic (Governance)  
Tactical (Management)  
Operational
Building blocks of a TLCF

Standards can be mapped to the blocks of the framework

- Policies
- Risk management
- Assets management
- Strategy
- Program management
- Compliance
- Organization
- Reporting, Monitoring
- Metrics / KPI
- Security Operations
Each security-linked domain has controls in all three levels
Each security-linked domain has controls in all three levels

- ISMS
  - Solution or technology (Cloud, Mobility)
  - Domain (Cybersecurity, Continuity, DP)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Strategy</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks</td>
<td>Program</td>
<td>Reporting</td>
</tr>
<tr>
<td>Asset mgmt</td>
<td>Compliance</td>
<td>Metrics</td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each security-linked domain has controls in all three levels.
How can this framework be used?

Use case 1: IS Governance self-assessment

Use case 2: Impact on governance - proactive approach
Use case 1. IS Governance self-assessment

1. Chose a subject of the self-assessment: ISMS, cybersecurity, data privacy, specific technology, etc.

2. Establish a questionnaire based on standards, best practices, maturity models, etc. for each of the building blocks of the model.

3. Have a brainstorming session with management based on the questionnaire.

4. Consolidate the findings for each block.
Do we have a written security **Policy** and internal regulatory framework?

Have our security **risks** been identified? What measures are being taken to mitigate them?

How should we manage our **Assets**? Do we have an **Inventory** of sensitive data? Who is responsible?

Is our security **Strategy** defined? How should we proceed to develop a security strategy aligned with business needs?

How is our security **Program** managed? How should we prioritize investments?

Are we **Compliant** with security-related regulations? What is our compliance roadmap?

Do we have a security **Reporting** system? How should we design dashboards for better decision-making?

Are we **Compliant** with security-related regulations? What is our compliance roadmap?

Do we have **Metrics** or KPIs for security and related domains? How can we establish effective metrics?

Is our **Organization** optimal? Who are our security governing (decision-making) and management bodies?
Process

Brainstorming based on questions

Consolidate findings

It's a quick win, does not replace the audit!
Use case 2: Impacts on governance - proactive approach

• Analyze a specific domain from the viewpoint of all the building blocks.
• Aim to establish good governance practices in anticipation of the major change.

Examples:
1. How do data privacy regulations impact IS governance?
2. How does the outsourcing impact IS governance?
## Impacts of Data Privacy regulations on GRC (excerpt)

<table>
<thead>
<tr>
<th>Policies</th>
<th>Strategy</th>
<th>Organization</th>
<th>Reporting</th>
<th>Asset mgmt</th>
<th>Compliance</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a Data Privacy policy or adapt existing Data Protection or security policy.</td>
<td>Review security strategy to encompass Data Privacy principles.</td>
<td>Responsibilities in Data Privacy protection (Data Processors, Data Controllers, Data Owners)</td>
<td>Adapt reports to include DP risks and the effectiveness of associated controls.</td>
<td>Classification of personal data. Data flows of personal data.</td>
<td>Make a gap analysis with DP regulations. Review the liability of third parties.</td>
<td>Put in place special metrics for Data Privacy (e.g. access rights to sensitive data).</td>
</tr>
</tbody>
</table>
Does operational changes impact IS governance?

Examples

1. Encryption techniques.
2. Audit findings and recommendations.

<table>
<thead>
<tr>
<th>Policies</th>
<th>Strategy</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Program</td>
<td>Reporting, Oversight</td>
</tr>
<tr>
<td>Assets</td>
<td>Compliance</td>
<td>Metrics / KPI</td>
</tr>
</tbody>
</table>
### Policies
- Build a framework for internal regulation.
- Establish policies and guidelines structure.

### Strategy
- Security initiatives should support business issues.
- Visualize on 1 page.

### Organization
- Involve business units (data owners, etc.).
- CISO must move towards GRC.

### Risks
- Design security risk management concept.
- Evaluate risks based on external events.

### Program
- Build a control catalog.
- Establish a program review process.

### Reporting
- Risks reports,
- Posture & Maturity
- Strategic initiatives.
- Balanced scorecard.

### Asset management
- Classification of data.
- Data, application and flow inventory.

### Compliance
- Readiness map.
- Gap analysis based on questionnaires.

### Metrics
- Maturity.
- Modeling for ROSI.
- Cost analysis.

---

Some tools and tips
Thank you for your attention!

Andrej Volchkov

www.stramizos.com
avolchkov@stramizos.com