Finding your Privacy Pulse: How to Use KRI to Measure Your Privacy Risk

Franchesca Sanabria, Principal National Privacy Practice
Eric Dieterich, GM of Advisors & National Privacy Practice Lead
IIA Miami Chapter Conference
January 25, 2019
Focal Point Data Risk

Our Integrated Risk Management Portfolio

Technology Risk Consulting
Solve pressing IT and business challenges with expert consulting services, with a focus on cyber security, data privacy, and advanced data management.

Cyber Workforce Development
Build your cyber security workforce development program, evolving your security capabilities through prescriptive learning programs and lab-intensive courses.

Technology Integration
Delivers system implementations and managed services for the leading Identity Governance and Access Management (IAM) and eGRC systems.

Audit and Compliance
Offers assessments, co-sourcing, and managed support to solve internal audit and compliance challenges, including SOX, HIPAA, and GDPR.
Our Holistic Approach

Core Service Areas

- Cyber Security
- Identity Governance
- Cyber Workforce Development
- Data Privacy
- Technology Integration
- Data Analytics
- Internal and IT Audit
What are KRIs?

• Key Risk Indicators (KRIs) can be used across an organizational to measure how risky an activity is.

  1. **Leading Indicators:** Emerging risk trends for events that might happen in the future and need to be addressed.
     • *An increased amount of personal information being collected due to change in operations.*
     • *An increase in social engineering and phishing attacks.*

  2. **Current Indicators:** Where you currently sit with your risk exposure.
     • *The number of staff that have yet to completed a new privacy regulation training.*
     • *The number of systems without encryption of data-at rest.*

  3. **Lagging Indicators:** Events that took place in the past that have the possibility of taking place again.
     • *A breach of personal information.*
     • *A natural disaster impacting continuity of operations.*
## Attributes of a KRI

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantifiable</td>
<td>Numbers, percentages</td>
</tr>
<tr>
<td>Predictable</td>
<td>Show early warning signs</td>
</tr>
<tr>
<td>Auditable</td>
<td>Measure the status of risk and control</td>
</tr>
<tr>
<td>Comparable</td>
<td>Tracks trends over a period time</td>
</tr>
<tr>
<td>Thresholds</td>
<td>A pre-defined level that will trigger an action</td>
</tr>
</tbody>
</table>

- Thresholds can be based on industry tolerance or internal acceptance
- Senior Management should be aware / approve thresholds
- Should coincide with risk appetite of the organization
Case Study: Wimbledon Investments

- Wimbledon has established an Executive Management Risk Committee and framework as part of their Enterprise Risk Management (ERM) program to assess risks.
- Wimbledon used analytical data to identify and monitor their major risks.
- KRIs have been most helpful for the company when they are used to manage uncontrollable risks.

**Success Story:**
- Wimbledon has a concentration of mortgage borrowers employed by China’s mining industry.
- They recognized that the health of mining companies was necessary for continued employment of borrowers.
- So a KRI they needed to consider was *how can we predict when mining companies will experience a downturn?*
- In response Wimbledon's ERM began monitoring China’s economy including the employment rate of mining companies, factors that could contribute to or affect the organization’s investments.
# The Difference between a KRI and KPI

<table>
<thead>
<tr>
<th>Indicator Metric</th>
<th>What does it measure?</th>
<th>What is its purpose?</th>
<th>Who is the audience?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Risk Indicator (KRI)</strong></td>
<td>Quantify risk</td>
<td>Non-operational and focuses on risk identification</td>
<td>Executive Management and the Board</td>
</tr>
<tr>
<td></td>
<td>A snapshot of an organization’s current risk posture and risk mitigation techniques</td>
<td>Helps organizations understand the risks involved and the likelihood of not having a positive result</td>
<td></td>
</tr>
<tr>
<td><strong>Key Performance Indicator (KPI)</strong></td>
<td>Measure performance (i.e., how effectively something is operating)</td>
<td>Provide metrics for operational performance</td>
<td>Operations and Middle Management</td>
</tr>
<tr>
<td></td>
<td>Measures how well individuals, business units, projects are performing according to their goals</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Challenges of Understanding Privacy Risks

• Complex ecosystem of data sharing models, internally and externally.
• Limited awareness of what data is most important to the organization and the life cycle of the data (i.e., defining your crown jewels).
• Legacy storage terms and uses of data conflicting with privacy-by-design concepts (i.e., minimum necessary).
• Potential alignment with a broad range of regulatory and industry standards.
• Shared responsibilities for privacy across the enterprise, no single point of ownership.
Benefits of Measuring Privacy Risks

In response to growing challenges, many organizations have begun focusing on key risk indicators in addition to compliance assessments.

- Enables and enhances continuous risk monitoring/reporting
- Aids in decision making
- Identifies privacy risks that may inhibit an organization’s ability to achieve specific objectives
- Enhances the risk management posture of the organization
What is a Privacy KRI?

- Privacy KRI s measure control effectiveness across a defined privacy risk framework.
- The goal of privacy KRI s are to identify actionable and measurable metrics for key controls supporting an organization’s privacy program.
- Privacy KRI s also help an organization better understand their risk appetite.

**KRI s** measure *both the cause and the consequences of a possible risk*:

- What is a Privacy KRI?
- What would cause this event to happen?
- What are we doing to prevent it?
- What plans are in place to minimize the damage?
- What would be the consequences if it occurs?
How to Build the Privacy KRI Framework

1. Identify Privacy and regulatory requirements of the organization
2. Review the data classification and privacy policy
3. Identify existing privacy processes and practices
4. Define privacy risks
5. Define privacy controls
6. Define KRIIs

Key Contributors:
- Legal
- Privacy
- Audit
- Information Security
- Compliance
- Marketing
- Human Resources
## Privacy KRI - Examples

<table>
<thead>
<tr>
<th>Privacy Domain</th>
<th>Risk</th>
<th>Control</th>
<th>KRI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Risk Management</td>
<td>Unauthorized access that results when a third party exceeds or misuses access</td>
<td>Third parties security due diligence is performed over third parties upon onboarding and throughout the duration of the relationship</td>
<td>% of vendors with access control issues identified as “high risk”</td>
</tr>
<tr>
<td>Privacy Policies and Frameworks</td>
<td>The act of not following policies, standards or procedures</td>
<td>Exceptions to the Privacy Policies are reviewed and approved through a formal risk acceptance process and revisited periodically</td>
<td># of approved exceptions to the policy not revisited within a defined period of time</td>
</tr>
<tr>
<td>Privacy-by-Design</td>
<td>New types of data collected on website not understood</td>
<td>Privacy Impact Assessments (PIA) are performed during the design of new features on website, including adding/modifying data collected from customers</td>
<td>% of PIAs with a moderate or above risk ranking</td>
</tr>
</tbody>
</table>
Privacy KRI - Examples

Key privacy areas for which KRI can be defined:

- Privacy Notice
- Consent Management
- Privacy Complaints
- Data Retention
How to Monitor the KRI Program

• Track and report on KRIIs
• Leverage tools and dashboard reporting
• Establish risk mitigation plans to address KRI limits
• Reassess KRI inventory on a regular basis
Franchesca Sanabria
Principal, National Privacy Practice
fsanabria@focal-point.com
917-903-4890

Eric Dieterich
GM of Advisors & National Privacy Practice Lead
edieterich@focal-point.com
786-390-1490