Metrics for Risk Management
versus
Metrics for Security Attribution

Jennifer L. Bayuk
jennifer@bayuk.com
www.bayuk.com
## Compare: Risk vs Security

<table>
<thead>
<tr>
<th>Measures:</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflects:</td>
<td>Organizational Structure</td>
</tr>
<tr>
<td>Favors:</td>
<td>Automation</td>
</tr>
<tr>
<td>Demonstrates:</td>
<td>Trends</td>
</tr>
</tbody>
</table>
Compare: Compliance

Often based on self-assessment reporting.
Compare: Organization

Facilitates comparison between different sets of management.
Compare: Automation

Facilitates comparison between different types of technology, often used for audit remediation.

Total patched or otherwise automatically verified to be secured via specific tools.

Machine population

Identity Map to Identified Users

OS Config Verified

100%

0%

Laptop

Desktop

UNIX

OS/390

Windows 2003

Z/OS
Compare: Trends

Often used to depict activity beyond control of management

Facilitates demonstration of staff activity requirements

Note: blank lines indicate no incidents were reported, mostly weekends.
## Contrast: Risk vs Security

<table>
<thead>
<tr>
<th>Focus is:</th>
<th>Coverage</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based On:</td>
<td>Policy</td>
<td>Process</td>
</tr>
<tr>
<td>Relies On:</td>
<td>Explanations</td>
<td>Accountability</td>
</tr>
<tr>
<td>Reflects:</td>
<td>Assessment</td>
<td>Implementation</td>
</tr>
</tbody>
</table>
Contrast: Focus

Risk Coverage vs Security Quality

Focus on quality of security results in this type of report.

Confidence in totals comes with aggregation rather than collection.

Total Number of applications
Total applications scanned for code vulnerabilities

Jennifer L. Bayuk, LLC
Contrast: Basis

**Risk Policy** vs **Security Process**

- Population in compliance
- Population not in compliance
- Population with authorized exceptions to compliance

Security managers look for correlation.

Control points from process directly correlated to measured activity.
Contrast: Reliance

Risk

Security

Explanations vs Accountability

Where there is a process in place designed to maintain the metrics, there should be accountability for poor results.

Risk manager hears proximate cause, e.g.: “server down”

Security manager should ask: “What was root cause?”
Contrast: Reflects

Risk Assessment vs Implementation

Risk manager sees no dramatic changes

Security manager sees systemic issue

Detail behind OS Comparison from "Automation" example
Prevalent versus Necessary Metrics

What makes security an attribute?
How to find it?
What objectives are met using only risk metrics?
Should overlap be pursued or avoided?

Questions? Discussion…

jennifer@bayuk.com
www.bayuk.com