Measuring The Value of Information Security

Maninder Bharadwaj
manbharadwaj@deloitte.com
23\textsuperscript{th} July 2011
Current Challenges Organisations are facing

In many service organizations, clients realize that they must have reliable information to address strategic decisions as well as daily operational insights in running the business. However, they do not know how to overcome the challenges to obtaining that critical information.

- Struggle with the perceived magnitude of this effort – where do I start?
- Don’t have the existing data marts to house operational and performance data
- Lack a culture of accountability
- Don’t understand the maturing technology available to enable an information driven culture
- Are overwhelmed with data and are not sure how to use it
- Multiple complex initiatives

Common Mistakes

- Applying ‘band-aid’ and point solutions instead of tackling the challenges in a holistic manner
- Lack a consistent process to translate corporate strategy into operational objectives and then measure whether the strategy was successfully executed
- Rely on the month-end close process, lagging financial indicators, and shadow reporting systems that lack sufficient insight to the business
Information Security Metrics - Defined

Information Security Metrics and Management is an iterative process based approach that improves service operations clients’ ability to measure, monitor, and manage performance.

<table>
<thead>
<tr>
<th>What it IS</th>
<th>What it Is NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• An ongoing process, not an event</td>
<td></td>
</tr>
<tr>
<td>• Increased understanding of information security performance</td>
<td></td>
</tr>
<tr>
<td>• A strong link between measurement and the operational performance</td>
<td></td>
</tr>
<tr>
<td>• Structured reporting on critical and non-critical areas</td>
<td></td>
</tr>
<tr>
<td>• Tailored to a specific risk area</td>
<td></td>
</tr>
<tr>
<td>• Alignment of performance measurement with organizations’ strategy and financial goals</td>
<td></td>
</tr>
<tr>
<td>• An integrated capability leveraging the expertise of resources</td>
<td></td>
</tr>
<tr>
<td>• Just the dashboard for program management of information technology</td>
<td></td>
</tr>
<tr>
<td>• The same for every risk area and business unit</td>
<td></td>
</tr>
<tr>
<td>• Thousands of different metrics</td>
<td></td>
</tr>
<tr>
<td>• A cookie cutter approach</td>
<td></td>
</tr>
</tbody>
</table>

Why Use Metrics?

• To gain insights into operational performance
• To improve decision support
• To align incentives across the organization
• To create a culture of accountability
• To maximize the ROI of information technology & security investments
What are the levers for Information Security Metrics?

The levers help operations improve performance by increasing the effectiveness of performance analytics and the accuracy of security measurement.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Metrics can offer tremendous value by helping calibrate the performance of the security program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Performance Indicator (KPI)</td>
<td>Measure of Information Security performance activity, or an important indicator of a precise health condition of Information Security</td>
</tr>
<tr>
<td>Key Performance Index (KPX)</td>
<td>A summary or correlation of one or more KPIs that provides an indication of the overall performance of a defined area of the Information Security program</td>
</tr>
<tr>
<td>Key Risk Indicator (KRI)</td>
<td>A summary or correlation of one or more KPXs that provides an indication of the state of key risks to the Information Security program as a whole.</td>
</tr>
<tr>
<td>Information Security Dashboard</td>
<td>A virtual reporting mechanism that will provide an indication of the effectiveness of the Information Security Program by reporting on the information security KPIs, KPXs and KRIs</td>
</tr>
</tbody>
</table>
## What are KPIs (Key Performance Indicators)?

### What are Key Performance indicators?
- A key performance indicator is a Measure of Information Security performance activity, or an important indicator of a precise health condition of Information Security.
- Used as an indication of the current state of a component of the business to take the “surprise” out of risk.
- To be effective, the KPI must be defined as precise as possible.
- Can be measured as an “improvement” from a known state or a reference standard.

### How can we define KPIs?
- Must be something that can be measured and continued to be measured.
- Must be precise, meaningful and understandable.
- Must be relevant to the business.
- May be required by legislation and/or Regulations.
- Must have a measurement index that has meaning.
- Must have an appropriate life (Stickiness).
- Should be tied to the organization’s vision and strategy.

### What are the types of KPIs?
- **Threshold** – when an index reaches set targets or falls into set ranges e.g., scores on defined risks.
- **Milestone** – when a specific condition is reached e.g., certification.
- **Quantitative** – measure of value (number, time, $, %, etc.) e.g., number of reported security incidents, lost time due to viruses.
- **Qualitative** – measure of acceptability or health e.g., survey ratings, rating of risks.

### Examples of KPIs
- Awareness
- Risk Assessment
- Risk Management
- Audit
- Benchmarks and Certification
How KPIs can be used to measure effectiveness of investment (EOI)?

A Return on Investment (ROI) for information security is difficult to measure since risk, and especially risk reduction, is challenging to quantify in terms of rupees.

The Effectiveness of Investment (EOI) could be the comparison of the effectiveness of the security measures with the value of the investment.

A collection of KPIs could be used to measure the EOI for information security.
### What are KPXs (Key Performance Index)?

<table>
<thead>
<tr>
<th>What are Key Performance Index?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Key Performance Index (KPX) is a relative summary or correlation of one or more KPIs that provides an indication of the overall performance of a defined area of the security program.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How can we define KPXs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• May prompt the organization to change strategic direction in information security</td>
</tr>
<tr>
<td>• Levels may be triggered by a variety of factors</td>
</tr>
<tr>
<td>• Must be meaningful and understandable</td>
</tr>
<tr>
<td>• Must be relevant to the business</td>
</tr>
<tr>
<td>• Must have a measurement index that has meaning</td>
</tr>
<tr>
<td>• Must have an appropriate life (Stickiness) and</td>
</tr>
<tr>
<td>• Should be tied to the organization’s vision and strategy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What are the types of KPXs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• KPIs are discrete and measurable data points that are integral to the Security Program.</td>
</tr>
<tr>
<td>• Each KPX or in some cases Performance Measure are an aggregate of one or more KPIs.</td>
</tr>
<tr>
<td>• These Performance Measures are used to keep the organization focused on the most important aspects of Information Security</td>
</tr>
<tr>
<td>• Each Performance Measure’s status (as depicted on a speedometer or other graphic) is based on the scores of the underlying KPIs and supporting metrics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples of KPXs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• System Readiness</td>
</tr>
<tr>
<td>• Network Infrastructure</td>
</tr>
<tr>
<td>• Access Management</td>
</tr>
<tr>
<td>• Patch Management</td>
</tr>
</tbody>
</table>

©2011 Deloitte Touche Tohmatsu India Private Limited
## What are KRI (Key Risk Indicators)?

**What are Key Risk Indicators?**

A Key Risk Indicator (KRI) is a relative summary or correlation of one or more KPXs that provides an indication of the overall performance of an information security domain.

**How can we define KRI?**

- Report on the relative state of a significant domain of information security risk to the enterprise
- Relative summary of two or more KPXs
- Used to compare with previous results to indicate trends
- Used to report to executive management on a regular basis
- Basis for justification of action and budget
- Indicates areas of priority

### What are the possible types of KRI?

- Project/Initiative Security Risk Management – measures the adherence to the process and the level of risk that is accepted and implemented by the business
- Information Protection – an overall category which measures the effectiveness of the information protection mechanisms
- Information Security Incident Effectiveness – measures the effectiveness of the security incident management process

### Examples of KRI

- Threats and Vulnerabilities
- Information Protection
- Governance
- Awareness
- Access Control
How do KRIs, KPXs, KPIs and Measurements interact?

**KRIs**
- Overall state of Risk

**KPRs**
- Correlation of assessments

**KPIs**
- Assessment of Current State
- Efficiency of Patching
  - Average number of days between the time the patch was made available and the time it was applied to 99% servers and 90% desktops
- Up to date anti-virus definitions
  - Percentage of systems with need of AV updates and with inadequate file definitions
- Security Alerts and Actions
  - Number of critical security alerts from external sources reviewed and addressed each month

**Measurements**
- Number of critical MS Patches
- Number of Service Disruptions due to patching
- Number of MS Patches Applied
- Time recorded for patches to be applied on 99% servers
- Time recorded for patches to be applied on 90% desktops
- Number of systems needing AV updates
- Number of systems with inadequate AV file definitions
- Number of critical security alerts per month
- Number of security alerts addressed within time

**Deloitte Touche Tohmatsu India Private Limited**
©2011
The Solution!

**Presentation**

- Key Risk
- Benchmarked

**Process & Modules**

- Key Risk Planning
- Key Risk Collection
- Key Risk Analysis
- Key Risk Reporting

**Security Infrastructure**

- Dashboard
- Access Control
- Audience specific views

- Workflow & Scheduling
- Analysis Engine with Business Rules
- Analytics & Trending

- Questionnaires & Automated Data Collection
- SIM/SEM Integration
- Extract, Transform, Load (ETL)
- Data Quality
- Master Data Management

**Storage**

- Database
- Data warehouse
- Document Management

©2011 Deloitte Touche Tohmatsu India Private Limited
The Result

The dashboard aims to transform data from operations to actionable information for decision makers.

Example Security Dashboard

<table>
<thead>
<tr>
<th>Key Risk Indicators</th>
<th>Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>3.17</td>
<td>18%</td>
<td>0.57</td>
<td></td>
</tr>
<tr>
<td>Project/Initiative Security Risk Management</td>
<td>4.3</td>
<td>16%</td>
<td>0.69</td>
<td></td>
</tr>
<tr>
<td>Information Protection</td>
<td>2.12</td>
<td>20%</td>
<td>0.42</td>
<td></td>
</tr>
<tr>
<td>Information Security Incident Management Effectiveness</td>
<td>4.5</td>
<td>6%</td>
<td>0.27</td>
<td></td>
</tr>
<tr>
<td>Security Awareness</td>
<td>4.6</td>
<td>10%</td>
<td>0.46</td>
<td></td>
</tr>
<tr>
<td>Security Governance</td>
<td>3.0</td>
<td>14%</td>
<td>0.42</td>
<td></td>
</tr>
<tr>
<td>Threat Mitigation Effectiveness</td>
<td>3.2</td>
<td>16%</td>
<td>0.51</td>
<td></td>
</tr>
</tbody>
</table>

Overall Score: 100% 3.34
## Value Delivered

Using the correct information security measurement techniques result in increased value to the organization

<table>
<thead>
<tr>
<th>Increased Insight</th>
<th>Improved Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What services make money? Lose money? Why?</td>
<td>• Time spent on getting information</td>
</tr>
<tr>
<td>• What is the EOI / ROI for investment in information security areas?</td>
<td>• Extrapolate or guess at missing data</td>
</tr>
<tr>
<td>• What is my profitability across service lines? customers?</td>
<td>• Inconsistent Extraction processes</td>
</tr>
<tr>
<td>• Where should I focus my cost reduction initiatives? How do I track success?</td>
<td>• Resolve numbers that don’t “tie out”</td>
</tr>
<tr>
<td>• How can I optimize services? Should I consolidate technology or services?</td>
<td>• Filtering of data done at many levels</td>
</tr>
<tr>
<td>• How do I measure success? What is the optimal performance level?</td>
<td>• Limited time for analysis</td>
</tr>
<tr>
<td></td>
<td>• Overhead to consolidate data for business decisions</td>
</tr>
<tr>
<td></td>
<td><strong>Analytics</strong></td>
</tr>
<tr>
<td></td>
<td>• Information is consistent</td>
</tr>
<tr>
<td></td>
<td>• Extraction is planned, organized, structured, automated</td>
</tr>
<tr>
<td></td>
<td>• View data from many angles - slice and dice</td>
</tr>
<tr>
<td></td>
<td>• Drill down to pinpoint problems/opportunities</td>
</tr>
<tr>
<td></td>
<td>• Create multiple “what if” scenarios and validate</td>
</tr>
<tr>
<td></td>
<td>• Fact based business decisions validated by analysis</td>
</tr>
</tbody>
</table>

## Value Proposition

<table>
<thead>
<tr>
<th>Revenue</th>
<th>Direct Cost Savings</th>
<th>Intangible Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enhanced receivables management</td>
<td>• Savings through position control, productivity dashboard, improved scheduling, and continuous tracking</td>
<td>• Speed to Decision Making</td>
</tr>
<tr>
<td>• Impact of Investments – program expansions and new services</td>
<td>• Capital savings through improved asset management</td>
<td>• Reliability of Information</td>
</tr>
<tr>
<td>• Improved security management techniques</td>
<td>• Improved understanding and management of cost drivers and high cost areas</td>
<td>• Standardized taxonomy</td>
</tr>
<tr>
<td>• Improved decision making capability on investments</td>
<td></td>
<td>• Increased organizational accountability</td>
</tr>
</tbody>
</table>

©2011 Deloitte Touche Tohmatsu India Private Limited
Information Security Metrics – The Iterative Cycle

The Information Security Metrics provide a single point of reference for concise, executive-level information for business and technology owners.

Define the objectives & requirements for measuring and reporting on statistics & health of the information security program

Identify metrics that need to be captured or provide indications of the current status or health of the information security program

Report the current information security dashboard for executive review and actions

Maintain the measurements to ensure that accurate information is being captured

Analyze the metrics and produce the information security dashboard applying the appropriate threshold and weighting factors

Take actions on indicated scores

Review the dashboard indications that indicate a score

Report the current information security dashboard for executive review and actions

The Information Security Metrics provide a single point of reference for concise, executive-level information for business and technology owners.
Case Study
## The Business Case

### Background:
- Deloitte’s ability to design and implement a performance reporting solution to capture and disseminate service and operational performance measurements.
- Deloitte’s ability to identify key performance indicators for service operations and implement data marts to capture and report those KPI’s.

### Business Problem/Objective
- Little to no consistency in the information security operations data reported
- Disparate reporting processes and tools
- Current reporting capabilities could not support the new technological advancements
- Difficulty in timely tracking of overall information security performance

### Deloitte’s Role
- Define key management metrics to track on a daily, weekly and monthly basis. Develop metric definitions. Define data collection procedures (including data sources). Assign reporting roles and accountabilities.
- Develop a user-friendly process and toolset to accommodate service operations data collection and report production.
- Develop detailed business and technical user guide to facilitate ongoing support of the reporting tool.
- Conduct preliminary end-user training to select individuals. Pilot/test the reporting toolset and process with initial reorganized team.
- Refine tool and process based on feedback received from the pilot. Conduct site-wide end-user training to all relevant reporting resources. Roll-out the reporting process and toolset to the entire user base.

### Outcome/Earnings
- Consistent and transferable reporting process that supports the new organizational design, provides rigor, and promotes timeliness in reporting
- Consistent reporting process and toolset used for tracking daily, weekly and monthly key performance metrics
- Formal business and technical end-user manual to provide ongoing support the reporting process and toolset
The Dashboard consisted of 4 major KRI\textsc{s}.

<table>
<thead>
<tr>
<th>KRI Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>KRI</td>
</tr>
<tr>
<td>#1</td>
</tr>
<tr>
<td>#2</td>
</tr>
<tr>
<td>#3</td>
</tr>
<tr>
<td>#4</td>
</tr>
<tr>
<td>Y</td>
</tr>
</tbody>
</table>
### Dashboard Description

**Information Security Dashboard**

<table>
<thead>
<tr>
<th>KRI</th>
<th>Current Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>Information Protection</td>
<td>1</td>
<td>25%</td>
<td>.25</td>
</tr>
<tr>
<td>#2</td>
<td>Inappropriate Use</td>
<td>3</td>
<td>25%</td>
<td>.75</td>
</tr>
<tr>
<td>#3</td>
<td>Threat Management</td>
<td>4.73</td>
<td>25%</td>
<td>1.18</td>
</tr>
<tr>
<td>#4</td>
<td>Access Control</td>
<td>3.66</td>
<td>25%</td>
<td>.92</td>
</tr>
</tbody>
</table>

**Overall Score**

- The score that is the sum of all of the weighted scores for the KPXs making up this KRI
- Illustrates the current KRI score for this topic in relation to the score for the last reporting period. The color indicates the score level and the arrow direction indicates this score in relation to the last one for this topic
- The weighting factor that is applied to reflect the level of importance this KRI has on the overall score for Information Security
- The overall Information Security score that is the sum of all of the weighted KRI scores

©2011 Deloitte Touche Tohmatsu India Private Limited
# The Dashboard is supported by the KPXs

<table>
<thead>
<tr>
<th>KRI: Information Protection</th>
<th>Comments</th>
<th>Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>R KPX 1: Information Protection Incident</td>
<td></td>
<td>1</td>
<td>50%</td>
<td>0.5</td>
</tr>
<tr>
<td>R KPX 2: Vulnerabilities in Information Protection</td>
<td></td>
<td>1</td>
<td>50%</td>
<td>0.5</td>
</tr>
<tr>
<td>Y KPX 3: Information Protection Incident</td>
<td>Reported by Privacy</td>
<td>3</td>
<td>100%</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KRI: Inappropriate Use</th>
<th>Comments</th>
<th>Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y KPX 3: Information Protection Incident</td>
<td></td>
<td>3</td>
<td>100%</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KRI: Threat Management</th>
<th>Comments</th>
<th>Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>G KPX 4: Operational Countermeasures vs. Malicious Code</td>
<td></td>
<td>5</td>
<td>24%</td>
<td>1.2</td>
</tr>
<tr>
<td>G KPX 5: Malicious Software Impact</td>
<td></td>
<td>4.8</td>
<td>18%</td>
<td>.86</td>
</tr>
<tr>
<td>G KPX 6: Intrusion Detection Systems</td>
<td>Not available yet</td>
<td></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>G KPX 7: Patching</td>
<td></td>
<td>4.4</td>
<td>18%</td>
<td>.79</td>
</tr>
<tr>
<td>G KPX 8: Internal Vulnerabilities</td>
<td></td>
<td>5</td>
<td>20%</td>
<td>1.0</td>
</tr>
<tr>
<td>G KPX 9: System Security Readiness</td>
<td></td>
<td>4.44</td>
<td>20%</td>
<td>.89</td>
</tr>
<tr>
<td>100%</td>
<td>4.73</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KRI: Access Control</th>
<th>Comments</th>
<th>Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>R KPX 10: Administering Unauthorized User Accounts</td>
<td></td>
<td>3.66</td>
<td>100%</td>
<td>3.66</td>
</tr>
</tbody>
</table>
The Dashboard is supported by the KPXs

<table>
<thead>
<tr>
<th>The Key Risk Indicator Topic</th>
<th>Comments</th>
<th>Score</th>
<th>Weighting</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>R KRI: Information Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R KPX 1: Information Protection Incident</td>
<td>The name of the KPX carried forward from the KPX detailed Dashboard</td>
<td>1</td>
<td>50%</td>
<td>0.5</td>
</tr>
<tr>
<td>R KPX 2: Vulnerabilities in Information Protection</td>
<td></td>
<td>1</td>
<td>50%</td>
<td>0.5</td>
</tr>
<tr>
<td>Y KRI: Inappropriate Use</td>
<td>Comments</td>
<td>Score</td>
<td>Weighting</td>
<td>Weighted Score</td>
</tr>
<tr>
<td>Y KPX 3: Information Protection Incident</td>
<td>Reported by Privacy</td>
<td>3</td>
<td>100%</td>
<td>3</td>
</tr>
<tr>
<td>G KRI: Threat Management</td>
<td>Comments</td>
<td>Score</td>
<td>Weighting</td>
<td>Weighted Score</td>
</tr>
<tr>
<td>G KPX 4: Operational Countermeasures vs. Malicious Code</td>
<td>The KPX scores carried forward from the KPX Detailed Dashboard</td>
<td>5</td>
<td>24%</td>
<td>1.2</td>
</tr>
<tr>
<td>G KPX 5: Malicious Software Impact</td>
<td></td>
<td>4.8</td>
<td>18%</td>
<td>.86</td>
</tr>
<tr>
<td>G KPX 6: Intrusion Detection</td>
<td>Not available yet</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>G KPX 7: Patching</td>
<td></td>
<td>4.4</td>
<td>18%</td>
<td>.79</td>
</tr>
<tr>
<td>G KPX 8: Internal Vulnerabilities</td>
<td>The KPX Weighting factor to reflect the relative importance of one KPX of the others</td>
<td>5</td>
<td>20%</td>
<td>1.0</td>
</tr>
<tr>
<td>G KPX 9: System Security Readiness</td>
<td></td>
<td>4.44</td>
<td>20%</td>
<td>.89</td>
</tr>
<tr>
<td>R KRI: Access Control</td>
<td>Comments</td>
<td>Score</td>
<td>Weighting</td>
<td>Weighted Score</td>
</tr>
<tr>
<td>R KPX 10: Administering Unauthorized User Accounts</td>
<td>The total score for the KRI by adding the sum of the weighted KPX scores</td>
<td>3</td>
<td>100%</td>
<td>3.66</td>
</tr>
</tbody>
</table>
# KPX Detailed Report

## KPX #1 – Information Protection

### KPX 1 – Information Protection Incident

<table>
<thead>
<tr>
<th>Underlying KPIs</th>
<th>Baseline</th>
<th>Wt %</th>
<th>Comment or Measurement</th>
<th>Score</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>KPI 1-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of lost or stolen devices that may result in the leakage of confidential information</td>
<td>&lt; 20%</td>
<td>5 (G)</td>
<td>50</td>
<td>90%</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>60-20%</td>
<td>3 (Y)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt; 60%</td>
<td>1 (R)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1.1.1 - Number of devices reported lost or stolen</td>
<td>3 - 7</td>
<td>0 - 2</td>
<td>N/A</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>&gt; 7</td>
<td>3 (Y)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1.1.2 - Number of devices with information privacy protection</td>
<td>&gt; 90%</td>
<td>5 (G)</td>
<td>N/A</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>90-65%</td>
<td>3 (Y)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
<tr>
<td></td>
<td>&lt;65%</td>
<td>1 (R)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>KPI 1-2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of incidents where emailing results in leakage of confidential information</td>
<td>&lt; 5%</td>
<td>5 (G)</td>
<td>50</td>
<td>20%</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>5-15%</td>
<td>3 (Y)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt; 15%</td>
<td>1 (R)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1.2.1 - Number of reported Email security incidents this month</td>
<td>0 - 2</td>
<td>5 (G)</td>
<td>N/A</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>3 - 5</td>
<td>3 (Y)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
<tr>
<td></td>
<td>&gt; 5</td>
<td>1 (R)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1.2.2 - Number of incidents where email resulted in leakage of confidential information this month</td>
<td>0</td>
<td>5 (G)</td>
<td>N/A</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1-2</td>
<td>3 (Y)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
<tr>
<td></td>
<td>&gt; 2</td>
<td>1 (R)</td>
<td></td>
<td></td>
<td>1 (R)</td>
</tr>
</tbody>
</table>
# KPI Definition

## KPI 1.1 - Percentage of lost or stolen devices that may result in leakage of confidential information

<table>
<thead>
<tr>
<th>Objective</th>
<th>Comments</th>
<th>Baseline</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>To measure the potential for leakage of confidential information due to the loss of devices that do not have privacy protection mechanisms in place.</td>
<td>The measurement for the number of devices that has essential privacy protection installed is not yet available. Measurement M1.1.1 is for information only and does not contribute to the KPI.</td>
<td>Weighting - 50%</td>
<td>100 - M1.1.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric Objective &amp; Goal</th>
<th>Baseline</th>
<th>ICBC Contributing Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>M1.1.1 - Number of devices reported lost or stolen</strong></td>
<td><strong>Objective:</strong> To assess the potential for risk to information due to lost or stolen devices. <strong>Goal:</strong> To have zero lost or stolen devices.</td>
<td><strong>Baseline</strong></td>
</tr>
<tr>
<td><strong>Information Risk Management</strong></td>
<td><strong>Corporate Security</strong></td>
<td><strong>Weighting - N/A</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Score</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>0 - 2</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>3 - 7</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>&gt; 7</strong></td>
</tr>
</tbody>
</table>

| **M1.1.2 - Percentage of devices with information privacy protection** | **Objective:** To determine if lost or stolen devices may result in leakage of confidential information. **Goal:** To have all devices installed with information privacy protection. | **Baseline** | **ICBC Contributing Measurements** |
| **IT Support** | | **Weighting - N/A** | **DSUP.19 - Number of devices that have essential information privacy protection installed** |
| | | **%** | **SRS.3 - Number of laptops** |
| | | | **SRS.4 - Number of PDAs** |
| | | | **SRS.5 - Number of Blackberries** |
| | | | **SRS.6 - Number of Smartphones** |
| | | | **M1.1.2 = DSUP.19 / (SRS.3 + SRS.4 + SRS.5 + SRS.6) * 100** |

| | | | **Score** |
| | | | **> 90** | **5 (G)** |
| | | | **90-65** | **3 (Y)** |
| | | | **< 65** | **1 (R)** |
Overview of the structure supporting the KRI

KRI – Information Protection

KPX 1 – Information Protection Incident

KPI 1.1 – Percentage of lost or stolen devices that may result in leakage of confidential information
- M1.1.1 - Number of IT components with up-to-date antivirus definitions this month
- M1.1.2 - Number of IT Components at a point in time

KPI 1.2 – Percentage of incidents where email results in leakage of confidential information
- M1.2.1 - Number of reported security incidents this month
- M1.2.2 - Number of incidents where email resulted in leakage of confidential information

KPI 2.1 - Percentage of mobile devices with essential security protection
- M2.1.1 - Number of mobile devices at a point in time
- M1.1.2 - Number of mobile devices with essential security protection at a point in time

KPX 2 – Vulnerabilities in Information Protection

KRI – Information Protection

Metric

KPI

Measurements

- DSUP.19 Number of devices that have essential information privacy protection installed
- SRS.3 – Number of laptops
- SRS.4 – Number of PDAs
- SRS.5 – Number of Blackberrys
- SRS.6 – Number of Smartphones
- IR.6 – Number of devices reported stolen or missing

- IR.1 – Total number of information security incidents
- EMAL.10 – Number of security incidents where email resulted in the leakage of confidential information
- DSUP.17 – Number of devices that have essential security protection installed
An *example KPX for Threat Management Malicious Software

KPI – Malicious Software Impact
Impact of malicious software to the organization in terms of productivity losses (Hrs lost to clean and recover systems).

Measurement - 2
Number of virus/worm incidents impacting the organization.

Measurement - 3
Number of incidents at other organizations that may stem from a virus/worm attacks.

KPI – Malicious Software Events
The number of Malicious Software events caught and prevented by the malicious software program within a set time period.

Measurement - 1
Number of instances of malicious software impact avoidance.

Measurement - 4
The extent or impact of virus/worm incidents (hours of lost productivity).

Measurement - 5
Time since the last malicious code Signature update.

KPI – Malicious Software Program Failures
Number of malicious software program failures (failures of the program to detect malicious code or incidents where the program was circumvented.

Measurement - 6
Number of systems with active monitoring capabilities.

* More Intuitive examples follow