IMF Case Study: Metrics that Matter

Sanaz Sadoughi
Information Security Officer
International Monetary Fund
Disclaimer

The views expressed herein are those of the speaker and should not be attributed to the IMF, its Executive Board, or its Management.
Who We Are and Why Do We Care?

- 189 member countries
- Lending
- Capacity Development
- Surveillance
Uneasy Questions

Board, CIO, CISO, ERM, Audit

- How secure are we?
- What is our information security posture today compared to last quarter?
- Do we need to invest more in our current capabilities and people?

CIO, CISO, Operational Management, Business Dept.

- How effective are our controls?
- What are our threats and high risk areas?
- Are we protecting the most valuable assets?
- What is the level of compliance to our security policies?

Operational Teams

- Where should we allocate our resources to address high risk areas?
- Are we meeting our SLA’s in addressing incidents and patching?
How to Answer

- Multiple systems of information
- Data collections / cleansing
- Lagging and leading indicators
- Manual processing
- Manual analysis
- Silo reporting

= Relevant

= Impactful

= Actionable

= Different audiences
## Our Goal

### Where we are & How we Progress

- Track & manage risks
- Reduce risk
- Support risk trade-off decision making

### How to Prioritize Decision Making

- Report on outcome of security investments
- Set targets for performance improvement & monitor
- Help with decision making

### How to Answer to Questions

- Provide evidence of risk management & compliance
- Underpin risk appetite discussions
- Satisfy stakeholder expectations
- Make the case for funding
Our Proposed Vision

**Business Value**
- Answers leadership questions
- Transparency
- Context to communicate better
- KRIs

**Operational Value**
- KPIs measured by SLAs
- Provides drill-down capability
- Uses available data in our environment

- Provides self-service platform that enables decision-making.
- Drives cyber hygiene improvements and adds value.
Overview of the Information Security Metrics Program (ISMP)
Where Are We Today

- Metrics on 7 domains
- Using 21 source systems
- Monthly reports
- CIO, CISO, Operational Teams, ERM, Audit
How to Start

Define Requirements
- Identify business objectives
- Questions to be answered

Identify Data Sources
- Assets
- Data owners

Data Collection
- Data validation
- Data cleansing
- Data correlation

Analysis
- Based on agreed approach
- Drill-down
- Consolidated not only silos
- Repeatable

Reports
- Focus on story
- Make it interactive
- Dashboard
- Most important metrics
Objectives of the ISMP

The Implementation of an Information Security Metrics Program (ISMP) allows the organization to:

- Effectively communicate security posture
- Demonstrate the value of the security investment
- Drive performance improvement
- Help prioritize decision making
- Manage risk and compliance
- Provide quantitative measurements
The ISMP Framework

The stakeholder questions can be answered through an ISMP framework below:

1. **Scope of metrics and data collection**
   - Source 1
   - Source 2
   - Source ...
   - Source n

2. **Metrics (Context, KPIs & KRIs)**
   - Domain 1
   - Domain 2
   - Domain ...
   - Domain n

3. **Dashboard & Reports**

4. **Information Security Metrics Program Outcome**
   - Return on Investment
   - Risk & Compliance Management
   - Trending & Set Targets

---

- Data Collection
- Analysis & Metrics
- Dashboard
- Story
The metrics catalog has been designed based on the following hierarchy:

Domain → Outcome → Metric → Raw Data

- **Domain:** Vulnerability Management
- **Outcome:** Understand threat/vulnerability
- **Metric:**
  - % of High vulnerabilities
  - % of Critical vulnerabilities
- **Raw Data:**
  - # of critical vulnerabilities
  - # of vulnerabilities

The hierarchy is structured to reflect the relationship between domains, outcomes, metrics, and raw data, providing a clear and logical flow of information to understand the metrics in the vulnerability management context.
Domains & Reporting

Domains

1. Security Awareness
2. Vulnerability Management
3. Compliance Management
4. Risk Management
5. Identity & Access Management
6. Threat & Incident Management
7. Security Technologies

IMF Mgmt., Board

CIO, CISO, ERM, Audit, Operational Mgmt.

Management (Annual)
Program (Quarterly)
Operational (Monthly)

Operational Teams
Program Level Dashboard

These reports will be reviewed on a monthly basis to take action.

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>DOMAIN SCORE</th>
<th>DOMAIN TARGET RANGE</th>
<th>KPI - KRI</th>
<th>TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Security</td>
<td>3.4</td>
<td>3.5 – 4.0</td>
<td>KRI  (effectiveness of investment)</td>
<td></td>
</tr>
</tbody>
</table>

---

**Top Performing Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of mobile devices managed via MDM</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>% of mobile devices encrypted</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>% of mobile devices with MDM</td>
<td>0.3%</td>
<td></td>
</tr>
</tbody>
</table>

**Bottom Performing Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of mobile devices running iOS</td>
<td>23.4%</td>
<td></td>
</tr>
<tr>
<td>devices not compliant with policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of mobile devices non-compliant</td>
<td>10.8%</td>
<td></td>
</tr>
<tr>
<td>with policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Revised Metrics & KRIIs

Tailored to audience and agreed on what's important - iterative testing of what works.
Case Study

Challenges we faced

- Defining appropriate KRI/KPIs
- Collecting data from different source systems manually
- Defining recommended actions and get buy-in from data owners to act on
- Discrepancy between asset inventory fields and collected information from data owners

Lessons learnt

- Answer Management questions
- Setup a process to receive data from data owners on a monthly basis
- Presenting dashboards with risk level to the management & business sponsors
- Work with data owners to update the asset inventory
Measure Security Posture Using NIST CSF

1. Adopt and customize NIST Cybersecurity Framework (CSF).
2. Define the current and target security maturity postures.
3. Define KRIs, thresholds, reporting frequency.

Drive Action

Desired Information Security Posture
Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

<table>
<thead>
<tr>
<th>Function</th>
<th>Domain/Category</th>
<th>Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect (DE)</td>
<td>Anomalies and Events</td>
<td>2.9</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>2.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Metric</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>KRI Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management (Detection Processes)</td>
<td>% of critical vulnerabilities on most-exposed infrastructure</td>
<td>&lt; 5%</td>
<td>&lt; 10%</td>
<td>&lt; 20%</td>
<td>&gt;= 20%</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>% of critical vulnerabilities on internal infrastructure</td>
<td>&lt; 25%</td>
<td>&lt; 50%</td>
<td>&lt; 75%</td>
<td>&gt;= 75%</td>
<td>3</td>
</tr>
</tbody>
</table>

Risk Statement

Vulnerabilities in the assets can be exploited & led into information disclosure, financial loss, etc.

Proposed Actions

Remediate critical vulnerabilities
Crown Jewels

- Create metrics dashboards for Crown jewels
  - Identify the sensitive information assets
  - Identify the most critical infrastructure and applications
- Prioritize vulnerability assessment and remediation
- Prioritize compliance assessment and remediation
Demo of Metrics & Dashboards
Demo of User Behavior Analysis

EXAMPLE ONLY
IMF Next Steps

- Automation and reduce overhead
- Focus more on context and analysis
- Stakeholder iterative input to refine KRI’s
- Align to NIST CSF (quantitative and qualitative) measures
- Report on actions taken and impact
Next Steps – How you to Apply

Next Month:
- Identify your organizations’ key questions
- Define your requirements and what resonates with your audience

In the first 3 Months:
- List your data sources
- Define potential metrics to start with

Within 6 Months:
- Create sample reports
- Identify quick wins
Takeaways

- Identify your organizations’ key questions
- Identify your crown jewels
- Identify your data sources
- Identify quick wins
- Buy-in from Management
- Be clear if there is a call to action

Start small … But start … Make it relevant … Drive action!
Thank you!

Sanaz Sadoughi
sskhosroshahi@imf.org
International Monetary Fund