Risk Metrics: A Practical Approach to Implementation

NIST Federal Computer Security Managers Forum

Debra Graul, Information Systems Security Manager (ISSM)
Baan Alsinawi, Information Security Program Manager

February 28, 2019
• Risk Metrics Strategy
• Calculation of Risk Metrics & Reporting
• Recent Enhancement: Tailored Risk Tolerance
• Questions
The Office of Benefits Administration (OBA) Department uses four key factors to establish risk metrics and measurements strategy.

1. Risk Rating Levels
2. Control Implementation Status
3. Control Hierarchy
4. Risk Tolerance
Risk Rating Levels
1. Risk ratings are defined by using three levels (High / Moderate / Low) that were assigned a numerical risk value.

Control Implementation Status
2. The risk rating for a control also includes consideration for the effectiveness of the control (Implemented / Planned / Risk Accepted).

System Control Hierarchy
3. Overlays are used so the full effect of the control risk can be applied within the context of the overall system.

Risk Tolerance
4. The system’s overall risk tolerance was established to then show statistically the overall health for each system.

Risk Tolerance = 0.63
Less than 0.63 / 0.63 – 0.815 / more than 0.815

High = 0.64
Moderate = 0.32
Low = 0.16

Implemented = 0.00 risk
Planned (POA&M) = full risk value
Risk Accepted (RA) = 0.60 / 0.40 / 0.20
Risk Metrics Strategy

System Control Hierarchy

Department

Systems

Subsystems / CC Inheritance

OBA Program

System 1

System 2

System 3

Data Center

Application

Client Applications

Server Applications

Fully Inherited

System Specific
The system’s risk level is calculated using an additive type formula that takes into consideration each control’s: risk rating; implementation status & value; and hierarchical placement in the system’s overlay.

Then the system’s adjusted risk level is calculated by taking the overall system’s risk level and adjusting (dividing) it by the risk tolerance (0.63).

The adjusted risk level is visually displayed in a dial to the risk tolerance baseline (0.63)

- Within 0.63 tolerance = green (adjusted risk less than 0.63)
- Close to 0.63 tolerance = yellow (adjusted risk between 0.63 – 0.815)
- Outside of 0.63 tolerance = red (adjusted risk more than 0.815)
Risk Reporting

- Detailed comprehensive reports are prepared quarterly to capture the statistics, analysis, impact, and trending of the various systems risks.
- From these analyses, the team presents a variety of visual diagrams representing the risk metrics and measures at different levels to management on an on-going basis.
How can we include consideration for the unique characteristics and features of our systems, such as:

- High Value Assets (HVA)
- Type of data
- Complexity & breadth of system
- Hosting Characteristics

**Tailor the risk tolerance measure** from one metric (0.63) to a range (three levels) could achieve better analysis: High (0.63), Moderate (0.501), or Low (0.331)
Tailored Risk Tolerance

**High risk tolerance = 0.63**
- Says “we are more comfortable with a higher level of non-compliance”
- Key system characteristics: Not mission critical, limited use, fairly simple features (i.e. not overly complex)
- Tolerance range = less 0.63, between 0.63 – 0.815, more than 0.815

**Moderate risk tolerance = 0.501**
- Says “we are comfortable with a moderate level of non-compliance”
- System characteristics: Internally hosted, PII, mission critical, HVA
- Tolerance range = less 0.501, between 0.501 – 0.75, more than 0.75

**Low risk tolerance = 0.331**
- Says “we are not comfortable with non-compliance”
- System characteristics: Externally hosted, PII, mission critical, HVA
- Tolerance range = less 0.331, between 0.331 – 0.67, more than 0.67
**Tailored Risk Tolerance**

**Based upon 0.63 tolerance**

- Overall Risk: 0.29
- Risk Tolerance: 0.63
- Adjusted Risk: 0.46

**Based upon 0.501 tolerance**

- Overall Risk: 0.29
- Risk Tolerance: 0.501
- Adjusted Risk: 0.46

This risk tolerance seems more relevant to the current state of system when referencing summary row.
Contact:

Debra Graul, Information Systems Security Manager (ISSM), PBGC
Graul.Debra@pbgc.gov, (202) 355-2904

Baan Alsinawi, Information Security Program Manager, TalaTek
Alsinawi.Baan@pbgc.gov, (703) 828-1132, ext. 711