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

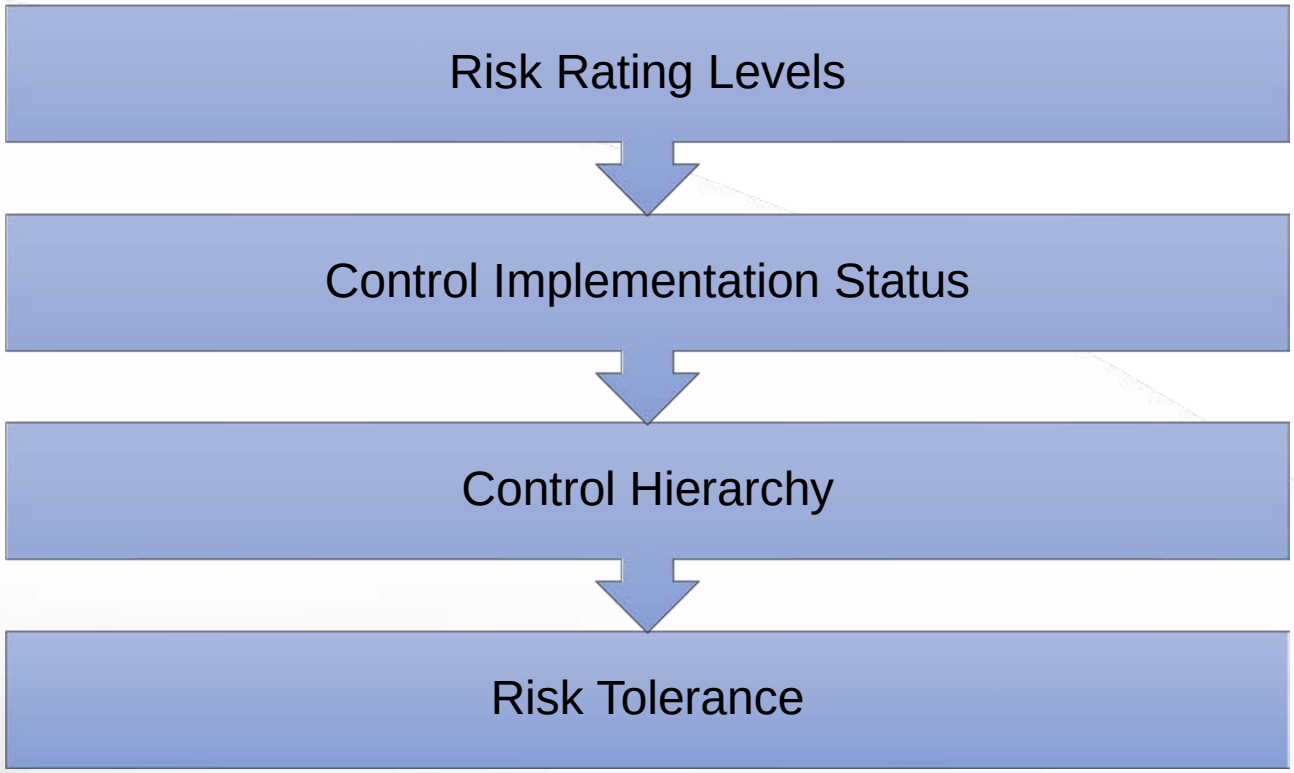
PBGC Pension Benefit Guaranty Corporation

Agenda

- Risk Metrics Strategy
- Calculation of Risk Metrics & Reporting
- Recent Enhancement: Tailored Risk Tolerance
- Questions

Risk Metrics Strategy

The Office of Benefits Administration (OBA) Department uses four key factors to establish risk metrics and measurements strategy.



3

Risk Metrics Strategy

Risk Rating Levels

1. Risk ratings are defined by using three levels (High / Moderate / Low) that were assigned a numerical risk value.

High = 0.64

Moderate = 0.32

Low = 0.16

Control Implementation Status

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

Implemented = 0.00 risk

Planned (POA&M) = full risk value

Risk Accepted (RA) = 0.60 / 0.40 / 0.20

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

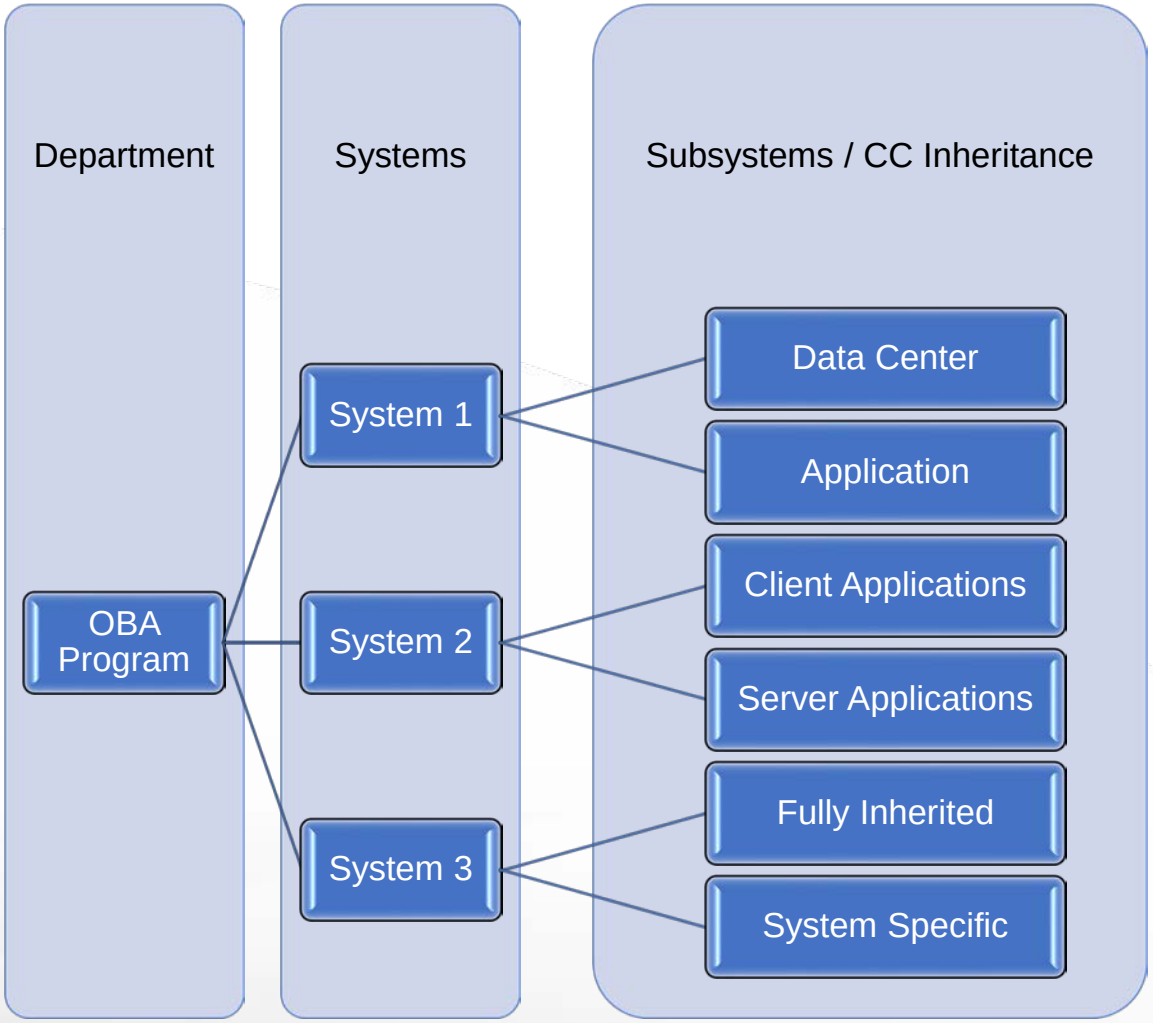
4. The system's overall risk tolerance was established to then show statistically the overall health for each system.

Risk Tolerance = 0.63

Less than 0.63 / 0.63 – 0.815 / more than 0.815

Risk Metrics Strategy

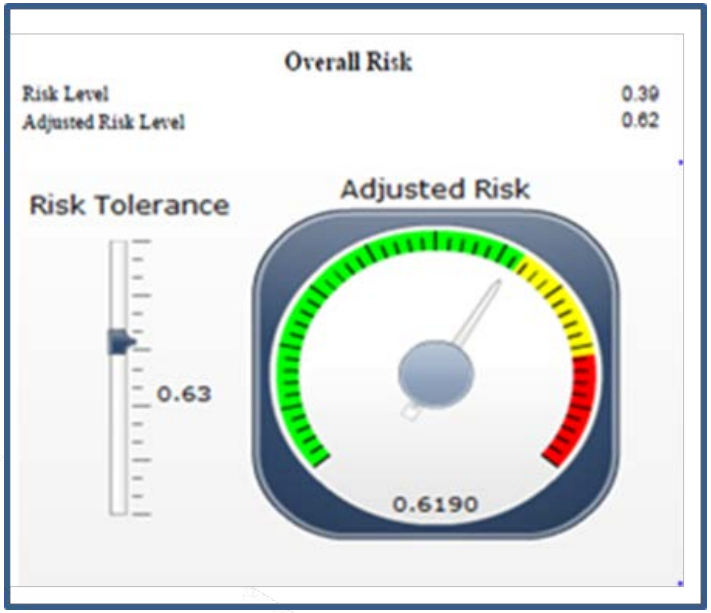
System Control Hierarchy



Pension Benefit Guaranty Corporation

Calculation of Risk Metrics

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.



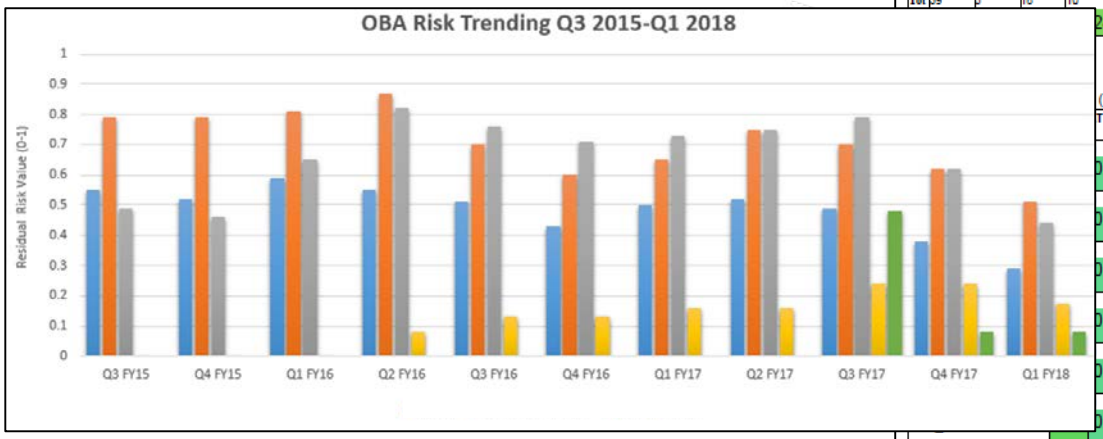
Then the system's **adjusted risk level** is calculated by taking the overall system's risk level and adjusting (dividing) it by the risk tolerance (0.63).

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.



Control	Action Item Short Description	Status	Control Eff	Add Value
AC-6	[illegible]_BIA_RA_010_AC-6 LEAST PRIVILEGE	RBD_Low	0.64	0.20
AC-6(10)	AC-6(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	Implemented	0.32	0.00
AC-11(1)	AC-11(1) SESSION LOCK | PATTERN-HIDING DISPLAYS	Implemented	0.32	0.00
AC-18(1)	AC-18(1) | WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION	NA	0.00	0.00
		Sum	1.28	0.20
Risk Results		Risk Level		0.16
		Adjusted Risk Level		0.25

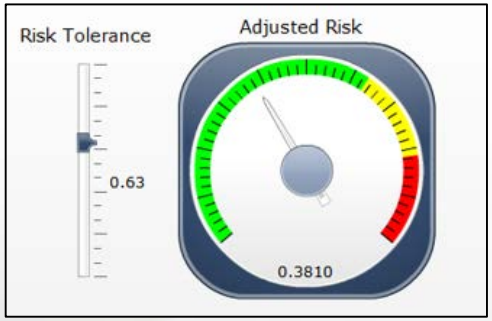
Pension Benefit Guaranty Corporation

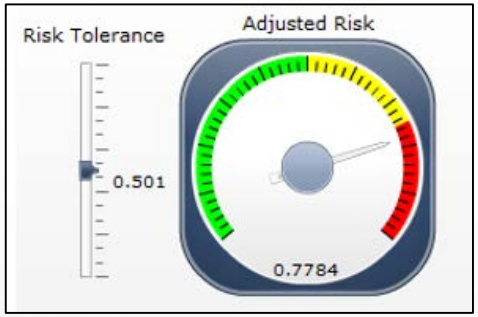
Tailored Risk Tolerance

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)



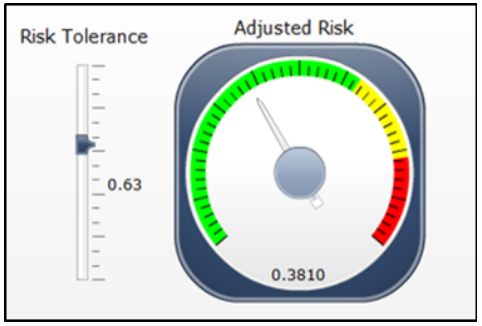


Pension Benefit Guaranty Corporation

Tailored Risk Tolerance

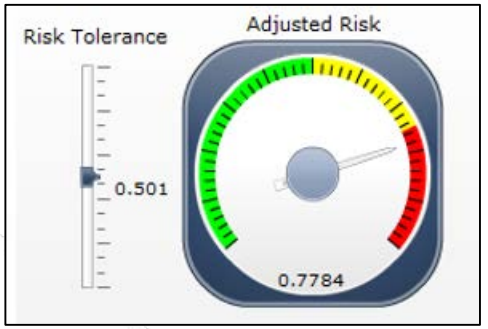
High risk tolerance = 0.63

- 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

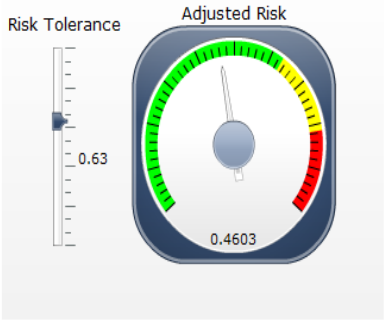
Pension Benefit Guaranty Corporation

Tailored Risk Tolerance

Based upon 0.63 tolerance

Overall Risk

Risk Level	0.29
Adjusted Risk Level	0.46



Overall Adjusted Risk by Family for all systems included in this report

(Each square lists controls evaluated (in white) and the determined residual risk value)

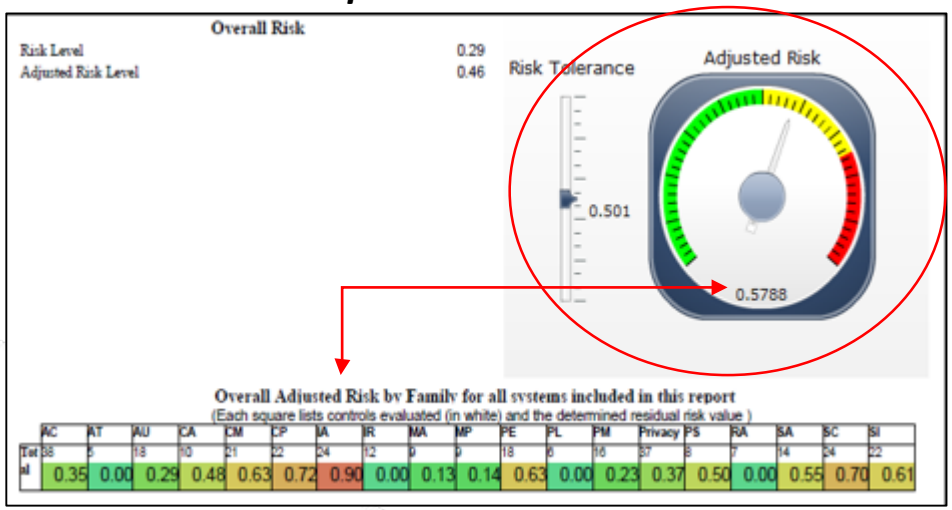
	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PM	Privacy	PS	RA	SA	SC	SI
Total	38	5	18	10	21	22	24	12	9	9	18	8	16	37	8	7	14	24	22
	0.35	0.00	0.29	0.48	0.63	0.72	0.90	0.00	0.13	0.14	0.63	0.00	0.23	0.37	0.50	0.00	0.55	0.70	0.61

Adjusted Risk by Business Object/Family

(Each square lists controls evaluated (in white) and the determined residual risk value)

	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PM	Privacy	PS	RA	SA	SC	SI
ADM_ECD_Fully_Inherited	0	5	0	1	0	1	0	5	0	0	1	3	15	0	0	0	2	0	0
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.23	0.00	0.00	0.00	0.00	0.00	0.00
ADM_ECD_Hybrid_Inherited	1	0	1	2	1	0	1	3	1	1	0	0	0	0	1	1	2	1	1
	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ADM_ITIGSS_Hybrid_Inherited	9	0	1	0	6	0	3	0	0	0	0	0	0	0	0	1	1	0	1
	0.41	0.00	1.00	0.00	0.51	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.99	0.00	0.99
ADM_ITISGSS_Fully_Inherited	14	0	13	1	6	10	3	0	7	8	0	0	0	0	0	3	1	14	16
	0.18	0.00	0.25	0.00	1.00	0.75	1.00	0.00	0.18	0.16	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.86	0.52
ADM_Privacy_Fully_Inherited	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.16	0.00	0.00	0.00	0.00	0.00
ADM_Privacy_Hybrid_Inherited	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	0	0
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.29	0.00	0.00	0.00	0.00	0.00
ADM_WSD_Fully_Inherited	0	0	0	0	0	6	0	0	0	0	17	0	0	0	4	0	0	0	0
	0.00	0.00	0.00	0.00	0.00	0.53	0.00	0.00	0.00	0.00	0.65	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ADM_WSD_Hybrid_Inherited	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0
	0.00	0.00	0.00	0.00	0.00	0.79	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Administar	14	0	3	6	8	3	17	4	1	0	0	3	1	5	3	2	8	9	4
	0.52	0.00	0.00	0.28	0.29	1.00	0.83	0.00	0.00	0.00	0.00	0.00	0.00	0.95	0.95	0.00	0.63	0.00	1.00

Based upon 0.501 tolerance



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

Pension Benefit Guaranty Corporation

Questions/Contact

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