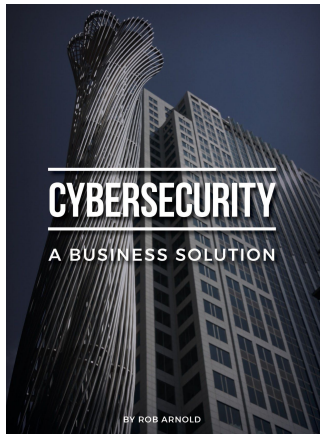
UC2 Risk Ruler for CVSS 4.0: Visualizing Precision, Maturity, and Confidence

Rob Arnold

April 8, 2025

Rob Arnold - (semi) Retired Cyber Risk

CEO Round Table



Author
and
Thought
Leader

Congressional
Testimony

NIST - Cybersecurity and
Data Privacy Frameworks

Senior Advisor NRMC
ICT SCRM Task Force - Executive Council

FIRST - SIG Member

What is UC2; What is a Risk Ruler?

UC2 is short for Uniform Confidence/Certainty estimation. It is an approach and set of tools that address several issues that are common in risk estimation techniques. Deployed between analysis and modeling, UC2 brings uniformity and interoperability that improve risk model results and improve stakeholder engagement.

The UC2 Risk Ruler offers a simplified, UC2 based scale that adjusts and captures confidence levels in risk predictions, helping subject matter experts express estimates that vary in certainty. By aligning data-driven and expert-derived risk estimates in a unified manner, the tool addresses challenges such as false accuracy, overconfidence, and the difficulty of aggregating disparate data types.

`UC2 ➔ UC2 Risk Ruler + CVSS = UC2 Risk Ruler for CVSS`

Learn more: https://www.AcornPass.com/uc2 - https://www.AcornPass.com/uc2/risk-ruler

Introducing the UC2 Risk Ruler for CVSS

Purpose: Augment CVSS 4.0 with a visual framework that conveys severity along with the underlying precision, confidence, and maturity of the score.

Challenge: CVSS scores offer a single numeric value that lacks mechanisms to convey maturity and completeness of the metrics that lie behind the score.

Objective: Enable more transparent and defensible cybersecurity decisions.

Key Benefits

- **Enhanced Prioritization:** Clarify insights and rank vulnerabilities effectively by augmenting numeric scores with context to mitigate false precision.
- **Improved Communication:** Translates numeric severity score into actionable intelligence for diverse stakeholders.

CVSS 4.0 and Metric Groups

CVSS is a globally recognized framework for quantifying vulnerability severity through numeric scores. Version 4.0 calculates scores using four metric groups:

1. **Base Metrics** (required) - Capture intrinsic attributes of a vulnerability.
2. **Threat Metrics** (optional) - Reflect how exploitability changes over time.
3. **Environmental Metrics** (optional) - Tailor scores to specific user environments, considering factors like mitigations and criticality.
4. **Supplemental Metrics** (optional) - Provide additional, non-scoring insights.

CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:L/SA:N/E:P/CR:M/IR:L/AR:H/MAV:X/MAC:X/MAT:P/MPR:L/MUI:N/MVC:L/MVI:N/MVA:H/MSC:X/MSI:N/MSA:N/S:N/AU:N/R:A/V:X/RE:L/U:Red

Base (11 metrics)	Threat	Environmental (14 metrics)	Supplemental (6)
AV:P/AC:H/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:L/SA:N	E:P	CR:M/IR:L/AR:H/MAV:X/MAC:X/MAT:P/MPR:L/MUI:N/MVC:L/MVI:N/MVA:H/MSC:X/MSI:N/MSA:N	S:N/AU:N/R:A/V:X/RE:L/U:Red

CVSS Maturity Model (draft)

- Maturity increases as additional metric groups are added to the vector string.
- Greater maturity provides more confidence.

Level	Label	Metrics				Provider	Description
		Base	Threat	Env	Supp		
0	N/A					N/A	No CVSS
1	CVSS-B *or* CVSS-Base	X				Vendor	CVSS-Base which reflects only vendor-specific information
2	CVSS-BT	X	X			Threat Intelligence	CVSS-Base with Threat intelligence
3	CVSS-BTE	X	X	X		Consumer	CVSS-Base, Threat, and Environmental
4	CVSS-BTES	X	X	X	X	Consumer	CVSS-Base ***fully*** augmented with Threat, Environmental ***and*** Supplemental in a complete, systematic manner.

→ More Maturity / Confidence →

This model also aligns to the "Analyze/Prioritize" row of the SANs Vulnerability Management Maturity Model

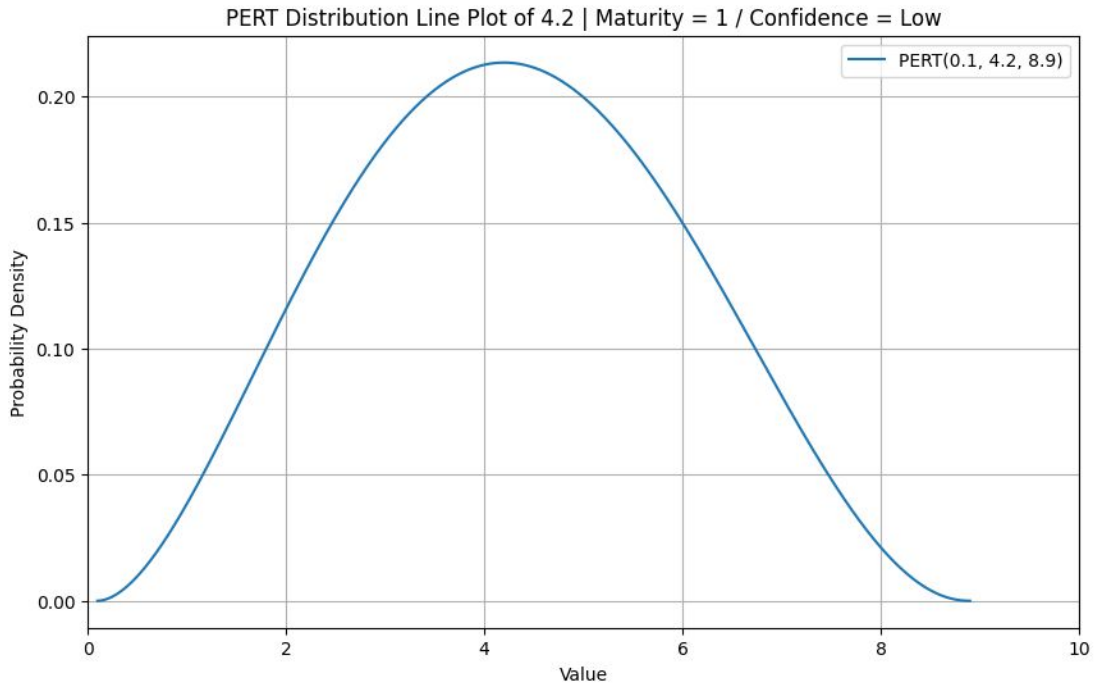
UC2 Risk Ruler for CVSS

Maturity / Confidence	Local Environment + Threat + Supplemental										
CVSS-BTES (4) Precise	0.0 - 10.0										
	Local Environment + Threat										
CVSS-BTE (3) High	0	1	2	3	4	5	6	7	8	9	10
	Threat Enhanced (also Qualitative Severity)										
CVSS-BT (2) Medium	None	Low			Medium			High		Critical	
	0 - 0.09	0.1 - 3.9			4.0 - 6.9			7.0 - 8.9		9.0 - 10	
	Unaugmented, Vendor Expertise Only										
CVSS-Base (1) Low		Medium									
		0.1 - 8.9									
	Low							High			
	0 - 3.9							7.0 - 10			
	Unknown										
No CVSS (0) Unknown	High - N/A										
	Medium										
	0 - 10										
	Low - N/A										

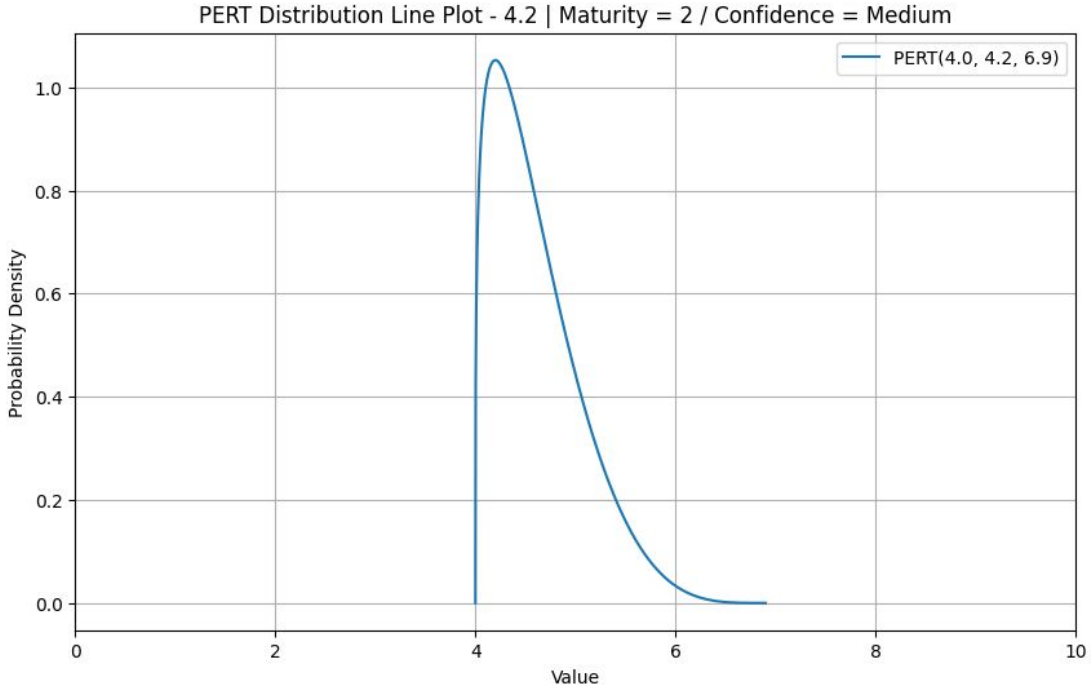
➔ More Maturity / Confidence ➔

PERT Distribution Examples (for Quants)

CVSS-Base 4.2
Maturity Level 1 (Low)
Range: 0.1 - 8.9



CVSS-BT 4.2 -
Maturity Level 2 (Medium)
Range: 4.0 – 6.9



UC2 Risk Ruler for CVSS - Example

Vulnerability XYZ has a high Base score as set by the vendor: **CVSS-Base:** 8.6

Maturing that with additional metrics that leads to a lower score: **CVSS-BTE:** 4.2

How can we think about these two numbers that point to the same vulnerability?

How can we present these scores *and the context* to leadership?

The UC2 Risk Ruler for CVSS is designed to solve these issues through visual representation of three aspects that lurk behind the numeric scores:

- **Precision:** Exactness of the numeric score
- **Maturity:** Completeness of underlying metric groups
- **Confidence:** Expert judgment on data reliability

UC2 Risk Ruler for CVSS

Start here

CVSS-BTE: 4.2 CVSS-Base: 8.6

Maturity / Confidence											
	Local Environment + Threat + Supplemental										
CVSS-BTES (4) Precise	0.0 - 10.0										
	Local Environment + Threat										
CVSS-BTE (3) High	0	1	2	3	4	5	6	7	8	9	10
	Threat Enhanced (also Qualitative Severity)										
CVSS-BT (2) Medium	None	Low			Medium			High		Critical	
	0 - 0.09	0.1 - 3.9			4.0 - 6.9			7.0 - 8.9		9.0 - 10	
	Unaugmented, Vendor Expertise Only										
CVSS-Base (1) Low		Medium									
		0.1 - 8.9									
	Low							High			
	0 - 3.9							7.0 - 10			
	Unknown										
No CVSS (0) Unknown	High - N/A										
	Medium										
	0 - 10										
	Low - N/A										

Summary

The UC2 Risk Ruler adds a critical layer of *context* to CVSS scores by visualizing precision, confidence, and maturity.

- Enhances both decision-making and model sensitivity analyses.
- Supports more transparent and defensible cybersecurity decisions.

Final Thought

The UC2 Risk Ruler for CVSS is a bridge between precise quantitative scores and qualitative, actionable risk insights.

Thank You

Rob Arnold
https://AcornPass.com

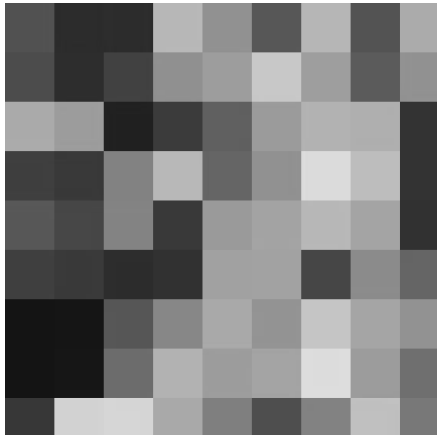
FIRST™
Improving Security Together

Precision/Maturity as Resolution

Precision/Maturity/Confidence as Image Resolution

- CVSS Metrics ⇒ Pixel Count
- Maturity ⇒ Increased Confidence

CVSS Base



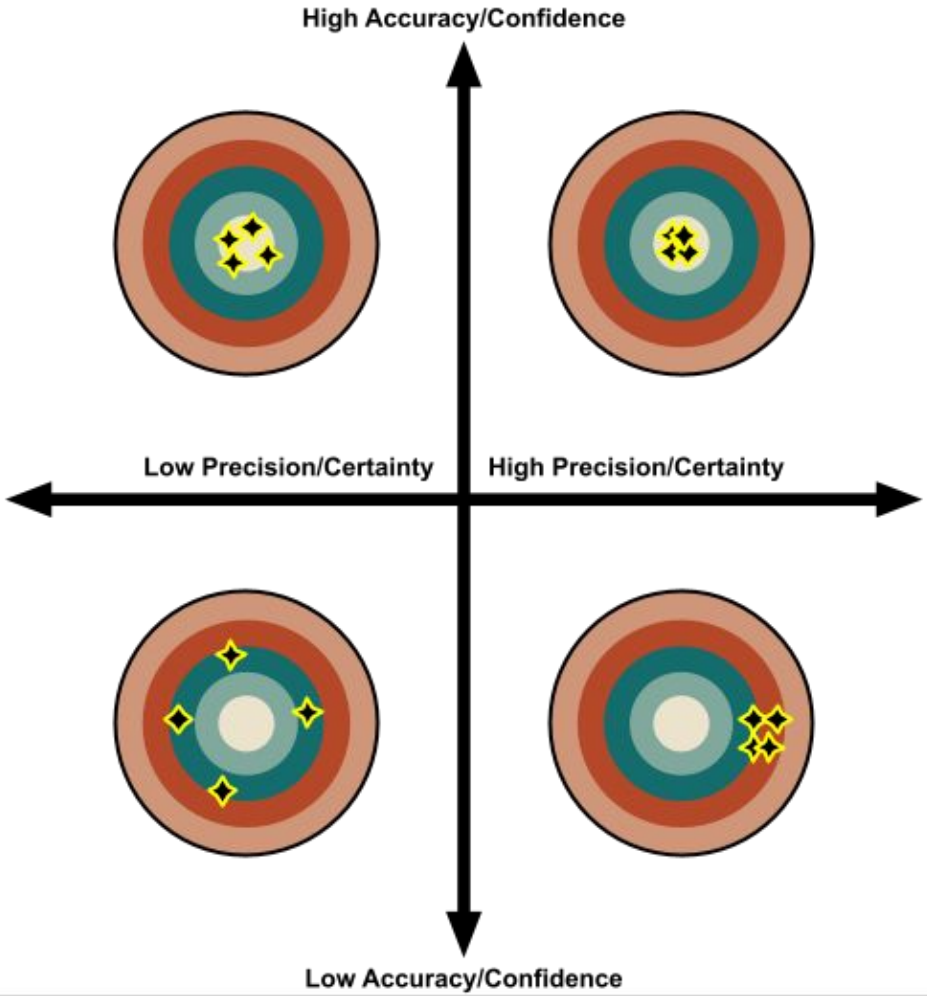
CVSS-BT

CVSS-BTES

Confidence and Certainty | Accuracy and Precision

Confidence / Accuracy: the ability to make predictions that are near the objective truth. The distance of a shot from the bullseye is a visual example.

Certainty / Precision: is the agreement between multiple estimates. Tight grouping of shots on a target is a visual example.



“Imperfect” Scales Are Still Useful

A quant walks into a kitchen and sees a chef using °F or °C. He argues that unless she precisely measures the molar movement of molecules on a proper scale, all her food is inedible.

Temp	Celsius (°C)	Fahrenheit (°F)	Kelvin (K)
Freezing Water	0°C	32°F	273.15K
Room Temp	25°C	77°F	298.15K
Boiling Water	100°C	212°F	373.15K