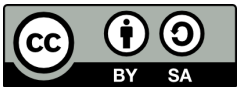
# UC2 Risk Ruler for CVSS 4.0: Visualizing Precision, Maturity, and Confidence

March 24, 2025

V1.3

Rob Arnold - Acorn Pass, LLC
AcornPass.com





## Abstract

The UC2 Risk Ruler enhances the Common Vulnerability Scoring System (CVSS) version 4.0 by adding a visual representation of maturity, confidence, and precision to vulnerability scores. CVSS 4.0 provides a standardized set of qualitative severity labels — None, Low, Medium, High, and Critical — which map to numeric scores for assessing the potential severity of vulnerabilities. However, CVSS alone does not account for the difference between the exact numerical score (precision), the expert judgment regarding the assessment's reliability (confidence), and the completeness of the available metric groups (maturity). The UC2 Risk Ruler bridges this gap, allowing stakeholders to see not only how a CVSS numeric score aligns with bins that reflect uncertainty, but also explicitly distinguishes between the score's numerical exactness and the completeness of its underlying metric groups. This added dimension supports more transparent and defensible cybersecurity decision-making.

**Keywords:** Common Vulnerability Scoring System (CVSS), Vulnerability severity, Data confidence, UC2 Risk Ruler, Vulnerability management, Qualitative and quantitative scores, Cybersecurity decision-making, Model sensitivity, Data transparency.

# Table of Contents

**Table 1** - CVSS Risk Ruler v1.2

| 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 | | | | | | | | | | |

**Description:** CVSS 4.0 and earlier produce a precise score (e.g. 4.2) for a given vulnerability even when optional elements of the vector string are missing. This diagram illustrates translation of numeric scores into less-precise bins with ranges that depict uncertainty introduced by lower CVSS maturity (missing vector elements) or when confidence in the metrics is uncertain. Translating scores to labeled bins avoids communicating false-precision. Adding ranges to precise scores improves compatibility with advanced analysis techniques such as stochastic models of risk.

# Introduction

The **UC2 Risk Ruler**[1] enhances the **Common Vulnerability Scoring System (CVSS)** version 4.0 by adding a visual representation of maturity and confidence levels to vulnerability scores. CVSS 4.0 provides a standardized set of qualitative severity labels — None, Low, Medium, High, and Critical — which map to numeric scores for assessing the potential severity of vulnerabilities. However, CVSS alone does not account for the confidence in the underlying data and assumptions from which scores are calculated, which can vary based on the amount and quality of available information. The UC2 Risk Ruler bridges this gap, allowing stakeholders to see not only how a CVSS numeric score aligns with bins that reflect uncertainty. This added dimension supports more transparent and defensible cybersecurity decision-making.

# Overview of CVSS 4.0

**CVSS 4.0** is a globally recognized framework for quantifying vulnerability severity through numeric scores that map to qualitative labels. It calculates scores using four metric groups:

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

Together, they form a CVSS Maturity Model that is explained in detail in the forthcoming CVSS User Guide[2]. In summary, higher levels of maturity include additional metric groups that can cause CVSS scores to differ – sometimes substantially – as metric groups are implemented. Table 2 illustrates the normal progression of maturity, which also increases certainty in the scores. Once all four metric groups are represented in a CVSS vector string, the resulting numeric score is considered as precise as it can be under the current CVSS standard.

[1] https://www.acornpass.com/uc2/risk-ruler
[2] At the time of this writing the CVSS User Guide is in draft status and the maturity model is stable, but still subject to change before final release.

**Table 2** - CVSS Maturity Model (source: CVSS User Guide Q1 2025 DRAFT)

| 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 (and optionally Supplemental) |
| 4 | CVSS-BTES | X | X | X | X | Consumer | CVSS-Base ***fully*** augmented with Threat, Environmental ***and*** Supplemental in a complete, systematic manner. |

Regardless of maturity, the final CVSS score is always expressed as a single numeric score between 0.0 to 10.0. Since CVSS does not intrinsically consider the confidence or maturity level of these scores, the CVSS Risk Ruler provides a bridge between those concepts and the numeric scores to visualize the relationship between precision, confidence, and CVSS Maturity.

This approach maintains backward compatibility for vulnerability management systems that were designed to ingest a single numeric score for each vulnerability. Additionally it provides a uniform method for more complex analysis. Stochastic models that expect probability distributions, rather than point estimates, can ingest bin ranges *and* the numeric score to provide a more nuanced analysis.

# Mapping Confidence Levels to CVSS Scores

The **UC2 Risk Ruler** aligns with the CVSS Specification[3] by incorporating a structured differentiation of three key concepts: precision (the exactness of the numeric score), confidence (the expert's judgment regarding data reliability), and maturity (the completeness of the underlying metric groups). Further alignment includes the qualitative labels: None, Low, Medium, High, Critical as defined in the CVSS Specification. This framework helps stakeholders interpret severity, clarify the distinction between the score's numerical value (precision) and its underlying reliability (confidence), and assess the robustness of the metric groups (maturity), which enables more transparent prioritization of vulnerabilities. The UC2 Risk Ruler applies confidence levels as follows:

- **Precise Confidence**: At this level the raw CVSS score, complete with its decimal, is considered the ultimate level of maturity and confidence in a CVSS score. The CVSS Maturity Model assumes that all metric groups are fully defined, which include: Base, Threat, Environmental, and Supplemental metrics; CVSS Maturity Level Four or CVSS-BTES.
- **High Confidence**: At this level, the raw CVSS score is rounded to one decimal place (e.g., 4.2 becomes 4). This represents the first step down, in terms of confidence and certainty, from the precise scores CVSS is capable of producing when the inputs are extremely reliable. These integer-rounded values are suitable when data quality is imperfect, but still quite high[4]. The CVSS Maturity Model assumes that the three primary metric groups are fully defined, which include: Base, Threat, and Environmental metrics; CVSS Maturity Level Three or CVSS-BTE.
- **Medium Confidence**: This level aligns with the CVSS-defined qualitative labels (None, Low, Medium, High, Critical) and ranges are introduced to define each bin. These ranges are taken directly from the CVSS Specification. This level also assumes the Base and Threat metric groups are defined; CVSS Maturity Level Two or CVSS-BT.
- **Low Confidence**: Low confidence applies the UC2 methodology by mapping scores to three broader, overlapping segments—Low, Medium, and High. This means that a score may fall within a range that aligns with more than one severity label or numeric range, which is compatible with UC2 analysis methodology[5]. As with the high and medium levels of confidence, these overlapping segments help avoid communicating "false precision" that could arise from uncertain data, providing a more realistic visual of potential severity when CVSS maturity is defined with only the Base metric group; CVSS Maturity Level one or CVSS-B[ase].
- **Unknown Confidence**: This broadest range signifies the lowest data confidence, presenting a wide, indeterminate span of possible severity outcomes. It signals that more/better data or analysis is needed before the score can reliably inform decisions.

[3] https://www.first.org/cvss/v4-0/specification-document
[4] Ranges are not explicitly given for this level, but ±0.5 would make sense.
[5] https://www.acornpass.com/uc2

Unscored vulnerabilities should be treated as *unknown* because they could take on any severity value once scored. This also corresponds to the lowest level of CVSS Maturity Model, which is defined as not using CVSS at all, but rather relying on purely subjective labels that have no numeric definition; CVSS Maturity Level Zero.

Using confidence levels, the UC2 Risk Ruler for CVSS 4.0 enables teams to interpret CVSS scores in a way that minimizes overconfidence in low-certainty data and promotes transparency and facilitates better communication with decision-makers.

## Benefits of the UC2 Risk Ruler

The UC2 Risk Ruler provides several key benefits that strengthen vulnerability management programs and processes:

1. **Precision in Decision-Making**: By viewing both severity and confidence, security teams can prioritize vulnerabilities while being transparent as to the decision making and the outcomes of those decisions.
2. **Unified Interpretation of Quantitative and Qualitative Data**: The tool harmonizes CVSS numeric scores with qualitative severity labels and confidence levels, allowing process and models to ingest CVSS scores in quantitative or qualitative form.
3. **Enhanced Stakeholder Communication**: The visual confidence levels make it easier to communicate transparently across teams and with non-technical stakeholders, fostering trust in security decisions.

## Practical Application Scenarios

In practice, the UC2 Risk Ruler for CVSS 4.0 is valuable in situations where vulnerability data confidence varies or where a bridge between quantitative and qualitative scores is needed.

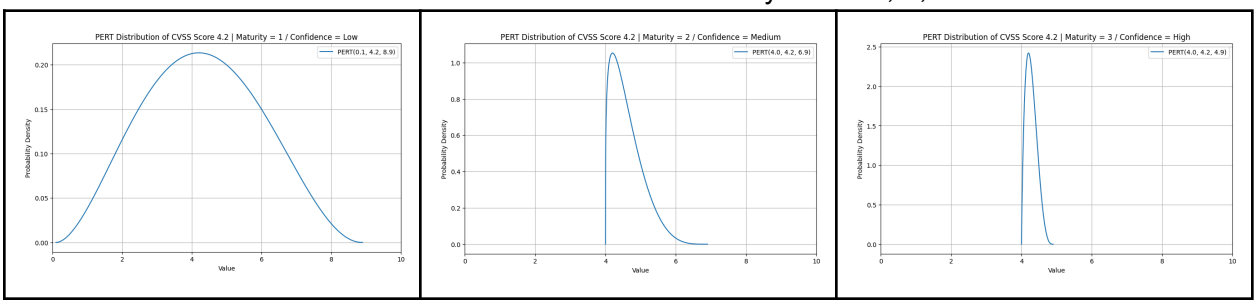
## Use Case - Decision Makers

The tool visualizes confidence, allowing leadership to select an appropriate level of certainty to inform decision-making. It illustrates what happens as confidence in CVSS scoring data increases or decreases. For a given set of vulnerabilities, start at the bottom 'Unknown' row, assuming no knowledge. Move up one row and ask, 'Is this level of information sufficient to make a defensible decision?' If not, continue moving up until an adequate level of certainty is identified. Then, discuss what data sources are necessary to achieve this level of confidence. Alternatively, start with a row that reflects the current level of confidence, then ask:  'Is decision making improved by moving up or degraded by moving down?'

# Use Case - Quantitative Model Sensitivity

Understanding how confidence impacts your vulnerability management program is crucial. To test this, use the chart to lower a batch of scores from precise CVSS Base scores to those with wider ranges reflecting reduced confidence. For example, begin with a full precision score such as 4.2. The first reduction in confidence, to CVSS maturity level 3, yields a range between 4.0 and 4.9. At level 2, the range becomes 4.0 to 6.9, and a range between 0.1 and 8.9 represents CVSS maturity level 1. Use these adjusted ranges as inputs to evaluate your program's sensitivity to score variability and make more robust decisions. Here are examples of CVSS 4.2 at levels 1, 2 and 3 of maturity/confidence using a PERT distribution.

**Table 3** - PERT Distributions for CVSS score 4.2 at maturity levels 1, 2, and 3.




Run the vulnerability management process or model once with the low range and again with the high range, asking: 'Did the process/model outcome change for one vs. another?' If the answer is yes, it is sensitive to that level of confidence. Otherwise, it is not sensitive to that level of confidence, which means increasing confidence will not provide additional benefit.

# Future Iterations

Looking forward, the CVSS Risk Ruler will need to evolve alongside other elements of the CVSS specification. In particular, the CVSS Maturity Model is still in draft as of this writing and any changes made to it should be reflected in future versions of this framework. Similarly, the Uniform Confidence/Certainty Estimation methodology (UC2) – from which the CVSS Risk Ruler originated – is evolving at the same time. Since the CVSS Risk Ruler is a UC2 derivative, it too should influence future iterations of this paper and the framework it contains. In fact, there is a discrepancy between UC2's philosophical view of scale segmentation that does not align with the CVSS 4.0 Specification that assigns unequal bin ranges to qualitative labels. Resolving this and keeping pace with future revisions of relevant standards and methodologies will be the subject of future iterations.

# Conclusion

The UC2 Risk Ruler for CVSS 4.0 improves CVSS-based vulnerability management by adding transparency and a bridge between quantitative and qualitative scores, among other benefits. By showing both the score and confidence of CVSS outputs, the tool equips organizations to make better-informed, transparent decisions. It also provides a framework for testing

process/model sensitivity to determine the optimal level of confidence needed to make rational and defensible decisions.

---

# Glossary of Terms

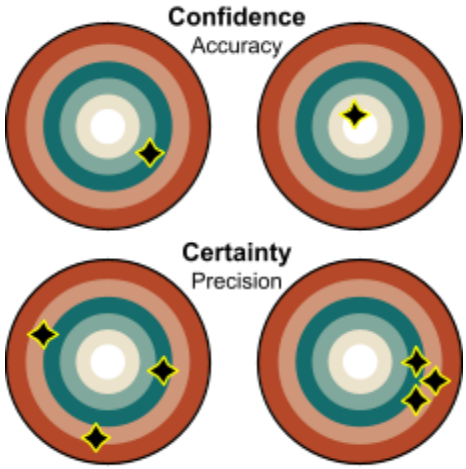
## CVSS Specific Maturity and Precision

**Maturity:** The completeness or robustness of the underlying metric groups used in CVSS. Higher maturity indicates that more components (Base, Threat, Environmental, Supplemental) are fully defined.

**Precision:** The degree of exactness of the CVSS numeric score. A precise score reflects a high level of numerical specificity.

## Confidence and Certainty

**Confidence** refers to the ability of an expert to make subjective, accurate predictions that align with the objective truth. If truth is the bullseye of a target, confidence represents how close estimations are to the center. Confidence is the expected proximity to truth.




**Certainty** is the agreement between multiple estimates from many sources. Tightly grouped estimates indicate more certainty; more dispersion means less. Certainty is a measure of precision and consistency, not closeness to truth.

## Data Types

**Quantitative:** An expression of quantity using numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

**Qualitative:** An expression of the nature of something based on non-numerical categories, levels or narrative description.

## Data Origin

Objectivity and subjectivity are independent concepts from quantitative or qualitative data types. In particular, a harmful idea lies in thinking that quantitative data is always objective

**Objective:** An unbiased, impersonal observation of something.

**Subjective:** An interpretation or estimate based on the state of knowledge and available evidence. Often reflects a personal belief, but also applies to proxy measures.

Objective data from actual observations has a very high degree of confidence. The certainty may be all over the board, but the observations are about as faithful to truth as one could hope. Data derived from experts that spent a lifetime observing relevant scenarios, can be just as confident and highly certain in some cases.

Quantitative data is often favored because it has a very measurable certainty which makes it appealing. Certainty masquerading as confidence has dire consequences for unsuspecting stakeholders because closeness to truth far outweighs data consistency when making critical decisions. Presenting certainty as confidence exacerbates this issue, which is what UC2 and the UC2 Risk Ruler were designed to address.