

ASSET RISK SCORING.



An asset risk score ranks what to fix first by combining what the asset is worth, how exposed it is, and how likely a threat is to reach it. **The arithmetic is easy; the inventory, the criticality labels and the exposure facts behind it are the hard part.**

- INVENTORY FIRST
- CRITICALITY × EXPOSURE × THREAT
- CONTEXT BEATS SEVERITY
- RE-SCORE CONTINUOUSLY

01 THE MECHANISM

Start From a Complete Inventory

CIS Control 1 makes the enterprise asset inventory the first safeguard: every end-user, network, IoT and server asset — physical, virtual, remote or cloud — with owner and department, so unmanaged assets are found and removed. **You cannot score what you have not listed.** [04]

Score Impact Before Threat

FIPS 199 rates the loss of confidentiality, integrity or availability as low, moderate or high and takes the high-water mark across the information a system holds. **Criticality is a property of the asset, set before any CVE arrives.** [02]

Then Weigh Likelihood

NIST SP 800-30 defines risk as a function of adverse impact and likelihood, where likelihood combines whether a threat event is initiated with whether it causes harm. **Exposure and exploit activity feed likelihood; criticality feeds impact.** [01]

02 THE FLOW

Build the Score DESIGN

- Inventory:** enumerate assets with owner, function, data held and network position. CSF 2.0 ID.AM-01 and ID.AM-02 keep hardware, software, service and system inventories; ID.AM-05 prioritizes them by classification, criticality, resources and mission impact. [03]
- Classify:** assign criticality from what the asset does and holds — domain controllers, sensitive databases, privileged identity groups — then have owners confirm; automated classifications can miss the crown jewels only the business knows. [10]
- Expose:** record reachability facts: internet-facing, authentication required, path to critical assets. CISA treats an asset reachable by unauthenticated or untrusted entities over a public network as publicly exposed, wherever it sits. [07]

Run the Score OPERATE

- Tailor:** adjust vulnerability severity to the asset. CVSS v4.0 Environmental metrics set confidentiality, integrity and availability requirements per system; the specification says Base metrics should be enriched with Threat and Environmental values. [05]
- Decide:** turn the score into an action tier. SSVC combines exploitation status, automatable, technical impact, mission prevalence and public well-being into Track, Track*, Attend or Act. [06]
- Re-score:** recompute as inventory, exposure and exploitation change. A per-device exposure score that combines every relevant CVE with internet-facing status and criticality recalculates daily. [09]

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Criticality (Impact)	What the asset does and holds. FIPS 199 low/moderate/high per security objective with the high-water mark; product classifiers rank devices, identities and cloud resources by cyber-role.
Exposure (Reachability)	Whether an attacker can get to it: public-network reachability without authentication, position on attack paths to critical assets, and the compensating controls in the way.
Threat (Likelihood)	Whether anyone is trying: confirmed exploitation (KEV), forecast probability (EPSS), automatable exploit code, and adversary intent, capability and targeting per SP 800-30.
Ownership (Accountability)	A named owner and department per asset (CIS 1.1), so a score becomes a work item someone can accept, fix or formally except.

04 SCORING INPUTS COMPARED

INPUT	SUFFICIENT ALONE?	WHAT IT MISSES
CVSS Base Score Only	No	Intrinsic severity, constant across environments by definition; says nothing about your asset, its exposure or whether exploitation is happening.
Business Criticality Only	No	Knows what matters but not what is reachable or attacked; ranks every weakness on a crown jewel equally.
Exposure / Internet-Facing Only	No	Finds the front door but ignores what is behind it; an exposed brochure site outranks an internal domain controller.
Exploitation Status Only (KEV, EPSS)	No	Population-level evidence and forecast; blind to presence, reachability and consequence in your own estate.
Composite Asset Risk Score	No	Combines all four, yet is only as good as the inventory and labels beneath it; needs owners, exceptions and re-scoring to mean anything.

ASSET RISK SCORING.

INVENTORY · WEIGH · RANK

05

PROGRAM OPERATIONS

Treat the inventory as a control, not a spreadsheet. CIS 1.1 records address, hardware address, name, owner, department and connection approval; 1.2 handles unauthorized assets weekly (remove, deny, quarantine). Report coverage as assets scored over assets discovered. [04]

Publish the formula and the tiers. Whether you use FIPS-style impact levels, SSVC decisions or a 0–100 exposure score, owners must see why an asset ranks where it does; SP 800-30 allows quantitative, qualitative and semi-quantitative approaches, so pick one and document it. [01] [06]

Let evidence override the score. A KEV listing or a confirmed compromise moves the asset to the top regardless of composite value; BOD 26-04 ties its shortest timeline to public exposure, KEV status, automatable exploitation and total control. [07] [08]

Measure movement, not the number. Track score reduction per remediation and per asset–CVE pair; expect new vulnerabilities to offset fixes within a cycle, and re-review criticality when systems change roles. [09] [03]

06

CONTROL MAPPING

FRAMEWORK BASIS

NIST CSF 2.0 ID.AM-05 prioritizes assets by classification, criticality, resources and mission impact; ID.RA-01 records validated vulnerabilities in assets; ID.RA-05 uses threats, vulnerabilities, likelihoods and impacts to prioritize risk response. [03]

IMPACT LEVELS

FIPS 199 expresses a system's security category as SC = {(confidentiality, impact), (integrity, impact), (availability, impact)} with values low, moderate or high, taking the highest value across the information types the system holds. [02]

VULNERABILITY TAILORING

CVSS v4.0 CVSS-BTE adds Threat and Environmental metrics to the Base score; SSVC maps exploitation, automatable, technical impact and mission or well-being to Track, Track*, Attend and Act. [05] [06]

PRODUCT SCORING

Defender Vulnerability Management scores each CVE from CVSS and EPSS, each device from all its vulnerabilities plus internet-facing status and criticality, and the organization as the average of assets; Exposure Management flags critical assets via predefined and custom classifications. [09] [10]

07

WHAT THIS DOES NOT SOLVE

Unknown Assets Score Zero

Shadow IT, forgotten cloud accounts and unmanaged devices never make the list. **Discovery gaps are the largest scoring error.** [04]

Criticality Drifts

A test box becomes production; a service account gains admin. **Labels decay unless owners re-confirm them.** [10]

Scores Are Not Risk Appetite

A ranked list says what is riskiest, not how much risk leadership accepts. **Thresholds and exceptions are governance calls.** [01]

Averages Hide Outliers

An organization-wide average can look healthy while one exposed critical system tops the list. **Always read the tail.** [09]

08

MYTHS VS. REALITY

MYTH

“A CVSS 9.8 means fix it first, everywhere.”

REALITY

Base metrics are constant across environments; **the spec expects Threat and Environmental enrichment** first. [05]

MYTH

“Criticality is the security team’s call.”

REALITY

Impact levels describe harm to operations, assets and individuals: **a business judgment security records.** [02]

MYTH

“If it is behind the firewall it is not exposed.”

REALITY

Reachable by untrusted entities over a public network means exposed, **regardless of physical or logical location.** [07]

MYTH

“One score serves every decision.”

REALITY

SP 800-30 separates threat-, asset- and vulnerability-oriented analyses; **each answers a different question.** [01]

MYTH

“The number is the risk.”

REALITY

A composite ranks; **presence, reachability and consequence still get checked** before acting. [08]

09

SPEAK THE PROGRAM — KEY TERMS

ASSET CRITICALITY

How much the organization depends on an asset: **the impact if it is lost**, set before any threat.

HIGH-WATER MARK

The **highest impact level** across the information types a system holds, per security objective.

EXPOSURE

Whether and how an attacker can **reach** the asset; public reachability without authentication is the strongest signal.

CVSS-BTE

A CVSS v4.0 score with **Threat and Environmental** metrics applied on top of the Base.

SSVC

A decision tree that turns exploitation, automatability, impact and mission into **Track, Attend or Act.**

ATTACK PATH

A chain of exposures leading to a critical asset; **choke points** are where one fix cuts many paths.