Why Most Cyber Risk Scores Get Priorities Wrong — and How to Fix It

A modern prioritization approach for SLTT, School Districts, and SMB Organizations

PERCEPTIVE
— CYBER —

August 2025

Phone: (209) 214-9541
Email: contact@perceptivecyber.com
Website: www.perceptivecyber.com
Address: PO Box 361, Vallecito, CA 95251

Executive Summary

Many small-to-medium public sector agencies and businesses — from cities and counties to school districts and private enterprises — base their cybersecurity assessments on respected frameworks such as the **NIST Cybersecurity Framework (CSF)** and the **CIS Critical Security Controls**. These frameworks are invaluable for identifying gaps and organizing improvements. However, in many organizations, the way assessment results are prioritized leaves room for improvement — not because of the frameworks themselves, but because of how the findings are interpreted and acted upon.

Traditional risk assessments often follow a detailed process of cataloging assets, modeling threats, and calculating likelihood and impact through extensive analysis. These approaches are invaluable for organizations with mature cybersecurity programs, but they can be complex and time-consuming for smaller agencies and businesses with limited staff.

Perceptive Cyber's methodology is designed to complement, not replace, those deeper approaches by providing a streamlined, **framework-driven foundation** that helps organizations quickly identify their most urgent priorities. As maturity grows, this foundation can expand into more advanced risk management practices.

Too often, risks are ranked solely by severity labels like *High, Medium, Low,* without fully considering:

- **Maturity** – How well is the safeguard implemented today?
- **Likelihood** – How probable is exploitation in your environment?
- **Impact** – What would the real-world damage be?
- **Criticality** – How critical is the control or safeguard to protecting against common attacks?

This can lead to investing time and resources into areas that are already well-defended while leaving truly vulnerable systems exposed.

Perceptive Cyber's methodology addresses this challenge by weighing **Maturity, Likelihood, Impact, and Criticality** to produce a **Risk Priority Score** that reflects the *true* priority of action — not just what appears severe at first glance. This enables leaders to clearly identify and communicate their highest-priority risks, justify investments to upper management, and direct limited resources where they will have the greatest impact.

The Risk Prioritization Gap

Framework-based assessments have become a cornerstone for SLTT organizations, schools, and SMBs alike:

- **NIST CSF** provides a flexible, outcome-based model for identifying, protecting, detecting, responding, and recovering from cyber threats.
- **CIS Controls** offer actionable, prescriptive safeguards that translate best practices into clear implementation steps.

Both approaches are valuable — and we encourage organizations to adopt them — but neither dictates how to *prioritize* your fixes beyond general guidance or, in the case of the CIS Controls, implementation groups to help identify which controls are most important.

While in-depth risk modeling remains the gold standard for large enterprises, many organizations are not yet advanced in their cyber maturity journey and lack the resources to conduct a traditional risk assessment that fully maps asset inventories to detailed threat catalogs.

Our approach bridges that gap by leveraging existing frameworks (like NIST CSF and CIS Controls) as a proxy for expected safeguards, focusing on the organization's current posture to drive quick, practical risk prioritization.

When using security frameworks, most organizations still take the results, look at the implementation groups or severity, and address the "High" items first.

The flaw in that approach:

- **Severity is only part of the picture.**
- A "High" severity finding in an already mature area may pose less immediate risk than a "Medium" severity gap in a critical, vulnerable process.

When maturity, likelihood, impact, and criticality aren't factored in, you can end up working on the wrong problem first — and leaving your real weaknesses exposed.

Example: Vulnerability Management vs Asset Inventory

Both NIST CSF and CIS Controls include these two well-known safeguards:

NIST CSF	CIS Controls
DE.CM-8 – Vulnerability scans are performed	**CIS Control 7** – Perform automated vulnerability scans of internal assets
ID.AM-1 – Physical devices and systems are inventoried	**CIS Control 1** – Establish and maintain a detailed enterprise asset inventory

Current State in Our Example Scenario

Vulnerability Management (DE.CM-8 / CIS 7)

- **Maturity:** 2/10 – Scans are irregular, patch validation is manual, and remediation tracking is inconsistent.
- **Likelihood:** 5/5 – Exploitation of known vulnerabilities is common and often automated.
- **Impact:** 5/5 – Could disrupt multiple systems and lead to data compromise.
- **Criticality:** 3/3 – Directly protects every connected asset.

Asset Inventory (ID.AM-1 / CIS 1)

- **Maturity:** 7/10 – Inventory is current, tied to procurement/disposal, and 90%+ accurate.
- **Likelihood:** 3/5 – Moderate risk from unknown or rogue devices.
- **Impact:** 4/5 – Missing assets hinder incident response but are less likely to enable immediate compromise.
- **Criticality:** 3/3 – Foundational to both security and compliance.

EXAMPLE VALUES

Maturity (0-10)

0 - No Implementation
1 – Basic Implementation
2 – Basic Implementation
3 – Basic Implementation
4 – Intermediate Implementation
5 – Intermediate Implementation
6 – Intermediate Implementation
7 – Advanced Implementation
8 – Advanced Implementation
9 – Advanced Implementation
10 – Full Implementation

Likelihood (1-5)

1 - Not Foreseeable.
2 - Foreseeable.
3 - Expected.
4 - Common.
5 - Current.

Impact (1-5)

1 – Negligible
2 – Acceptable
3 – Unacceptable
4 – High
5 - Catastrophic

Criticality (1-3)

1 – Moderate
2 – Significant
3 - Critical

Why Traditional Ranking Fails Here

Compliance-driven scoring — whether tied to NIST CSF or CIS Controls — often puts **Asset Inventory** ahead of **Vulnerability Management** because:

- Asset Inventory is “foundational” in the framework sequence.
- Vulnerability Management is sometimes seen as a follow-on activity.

However, this prioritization approach overlooks a critical reality in our scenario: Vulnerability Management remains dangerously underdeveloped, with threats that are both highly likely and potentially severe. In contrast, Asset Management demonstrates a far higher level of maturity. While continued improvements in Asset Management are important, they should not displace the more urgent need to strengthen Vulnerability Management.

Perceptive Cyber’s Prioritization

Control	**Maturity (0–10)**	**Likelihood (1–5)**	**Impact (1–5)**	**Criticality (1–3)**	**Traditional Priority**	**Real Priority**
Vulnerability Management	2	5	5	3	2	1
Asset Inventory	7	3	4	3	1	2

Result:

- Vulnerability Management jumps to the top because low maturity + high likelihood + high impact + high criticality = *urgent*.
- Asset Inventory remains important but can be improved after closing the immediate vulnerability gap.

Why This Matters in 2025

The cyber landscape has shifted:

- **AI-driven attacks** drastically shorten the time between vulnerability disclosure and active exploitation.
- **Supply chain compromises** mean even trusted partners can introduce risk.
- **Expanding regulations** require better evidence of prioritization decisions.

For SLTT, School, and SMB leaders managing tight budgets and limited staff, fixing the *right* things first is essential. Misaligned priorities don’t just waste resources — they can lead directly to ineffective responses to incidents.

Our methodology integrates the structure of frameworks like NIST CSF and CIS Controls with a weighted scoring approach that considers:

- **Maturity** – Are you strong here or dangerously weak?
- **Likelihood** – How probable is an incident in this area?
- **Impact** – How damaging would it be if it happened?
- **Criticality** – How essential is the control or safeguard to basic cyber defense?

The output is a **Risk Priority Score** that aligns security improvements with *actual* risk — ensuring compliance efforts strengthen your defenses instead of just filling checkboxes.

Our methodology provides a **starting point for organizations building cyber maturity**. It aligns directly with frameworks and regulatory requirements while laying the groundwork for deeper, traditional risk management efforts in the future.

As organizations grow, Perceptive Cyber’s tools and services will evolve to support more advanced processes — from asset-level risk modeling to sophisticated threat simulations — but the key is to **start now** with actionable insights that reduce real-world risk.

How Our Methodology Complements Leading Frameworks

Perceptive Cyber does not replace traditional risk assessments — instead, it provides a scalable foundation for agencies and businesses to begin their journey.

Think of it like the CIS Controls: while they don’t capture every detail of cybersecurity, they offer a practical roadmap for getting the basics right. Our methodology does the same for risk prioritization, ensuring every step toward compliance also strengthens true security outcomes.

Perceptive Cyber’s Risk Prioritization Methodology is designed to work hand-in-hand with respected standards such as the **NIST Cybersecurity Framework (CSF)** and the **CIS Critical Security Controls**. While these frameworks provide proven structure and guidance, they don’t always prescribe how to prioritize remediation activities. Our approach bridges that gap.

By weighing **Maturity, Likelihood, Impact, and Criticality**, we enable organizations to focus on the controls that matter most — not just those labeled “High Severity.” This ensures that investments in compliance also strengthen real-world security outcomes.

In addition, Perceptive Cyber has developed an **Assessment Framework** that incorporates the strengths of NIST CSF and CIS Controls while aligning with IT security elements of key regulatory requirements, including:

- HIPAA Security Rule (45 CFR Part 164, Subpart C)
- CJIS Security Policy 6.0
- PCI-DSS v4.0
- FERPA IT security expectations

This unified approach provides a comprehensive way to assess IT security posture across multiple obligations, streamlining compliance efforts while ensuring risk-based prioritization.

Regulatory Alignment

HIPAA Security Rule

The HIPAA Security Rule requires covered entities and business associates to implement technical safeguards that protect electronic Protected Health Information (ePHI).

- The Perceptive Cyber Assessment Framework maps directly to these technical safeguards, helping organizations evaluate their encryption, access controls, audit logging, and transmission security.
- By prioritizing based on risk, organizations can focus first on safeguards with the greatest likelihood of preventing ePHI compromise.
- While this does not guarantee HIPAA compliance — since administrative and physical requirements are also critical — it provides a strong foundation for the IT security portion of HIPAA obligations.

CJIS Security Policy 6⍰0

The CJIS Security Policy establishes baseline requirements for protecting criminal justice information.

- Our framework incorporates CJIS-mandated IT security expectations such as access controls, advanced authentication, audit capabilities, and incident response.
- The Risk Prioritization Methodology helps agencies address high-likelihood threats such as unauthorized access or weak authentication first, ensuring CJIS-related gaps are not just identified but also addressed in the right order.

- As with other regulations, full compliance also depends on policy, training, and procedural measures outside the scope of IT security — but our framework strengthens the technical backbone of CJIS adherence.

PCI-DSS v4⍰0

Payment Card Industry Data Security Standard (PCI-DSS) v4.0 sets requirements for protecting cardholder data.

- The Perceptive Cyber methodology helps organizations assess safeguards such as vulnerability management, network segmentation, secure authentication, and encryption — all critical PCI-DSS components.
- By applying risk-based prioritization, organizations can ensure that the controls most vital to protecting cardholder data receive attention first.
- Our approach supports PCI-DSS compliance efforts but must be paired with administrative, contractual, and process-level measures for full certification.

FERPA

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. While FERPA does not prescribe detailed IT security standards, it requires institutions to take “reasonable methods” to safeguard data.

- The Perceptive Cyber Assessment Framework, aligned with trusted NIST CSF and CIS Controls, provides that “reasonable” structure, helping schools and districts demonstrate due diligence in securing student information.
- Risk-based prioritization ensures that safeguards protecting the confidentiality and integrity of education records are not just implemented, but implemented in the areas of greatest vulnerability.
- As with other regulations, FERPA compliance includes administrative and policy obligations; our methodology addresses the IT security side that supports those obligations.

What’s Coming Next

In the coming weeks, we’ll release the **Perceptive Cyber Risk Prioritization Workbook** — a practical tool for applying this methodology to your own organization.

In the near future, our SecPosture360 platform will integrate this prioritization model into a complete, framework-aware assessment and reporting system.

Follow **Perceptive Cyber** on LinkedIn for updates, free resources, and practical guidance to ensure your priorities match your reality.

📞 **Phone:** (209) 214-9541
✉ **Email:** contact@perceptivecyber.com
🌐 **Website:** www.perceptivecyber.com
📍 **Address:** PO Box 361, Vallecito, CA 95251