Beyond the Checkbox

Using Cybersecurity Frameworks to Drive Real Risk Reduction

by Mark Kirkendall

PERCEPTIVE
— CYBER —

January 2026

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

Executive Summary

Cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF) and the CIS Critical Security Controls are foundational to modern security programs. They provide proven structure, shared language, and vetted safeguards based on real-world threats.

Yet many organizations struggle to translate framework assessments into meaningful action. Too often, results are reduced to compliant / compliant, with remediation efforts driven by checklist order rather than actual risk.

This paper argues that frameworks are not the problem—they are the starting point. Real risk reduction occurs when framework findings are evaluated alongside additional context, including maturity, likelihood, impact, and criticality.

For small and mid-sized organizations that lack the resources for deep-dive, asset-level risk modeling, this approach offers a practical and defensible way to prioritize security improvements.

Looking past compliance status to consider both the relative importance of controls and the maturity of their implementation allows organizations to prioritize improvements that meaningfully reduce risk.

The Checkbox Critique — Revisited

Criticism of framework-based security often centers on a perceived disconnect between compliance and security outcomes. This criticism usually emerges when assessments:

- Treat all gaps as equally urgent
- Prioritize findings based solely on framework sequence
- Emphasize documented compliance over operational effectiveness

In these cases, organizations may invest time and money addressing low-risk gaps while leaving high-risk weaknesses exposed.

> ***Frameworks Were Never Meant to Be Checklists***
>
> *"The Framework is not a one-size-fits-all approach… Organizations should prioritize actions that reduce cybersecurity risk in a cost-effective way."*
> — **NIST Cybersecurity Framework**

It is important to recognize that frameworks were never designed to be prioritized remediation plans. NIST CSF, for example, explicitly describes itself as a risk management framework, not a compliance checklist. The gap lies not in the frameworks themselves, but in whether assessment results are viewed strictly through a compliance lens or evaluated more holistically in the context of current implementation, effectiveness, and organizational risk.

Why Frameworks Still Matter

Cybersecurity frameworks remain among the most practical and effective tools available—particularly for organizations with limited resources or developing security programs.

Frameworks:

- Reflect decades of incident response and threat analysis
- Provide a common language across technical and executive audiences
- Align naturally with regulatory and oversight expectations
- Scale as organizations mature

> ***Why Federal Agencies Still Recommend Frameworks***
>
> *"The NIST Cybersecurity Framework helps organizations understand, manage, and reduce their cybersecurity risk."*
> *— **Cybersecurity and Infrastructure Security Agency (CISA)***

Agencies such as CISA and MS-ISAC consistently recommend cybersecurity frameworks as the foundation of cyber hygiene programs for state, local, tribal, and territorial (SLTT) organizations, as well as utilities and small to medium-sized businesses. Their guidance emphasizes using frameworks to *organize, align, and prioritize* cybersecurity activities—not merely to document compliance.

When used with appropriate context, cybersecurity frameworks give organizations clear guidance on what to focus on, helping them avoid rushed, inconsistent, or reactive security decisions.

Adding Context: Criticality, Maturity, Likelihood, and Impact

Framework alignment answers an important question: *What safeguards should exist?*
Risk management answers a different one: *Which weaknesses matter most right now?*

Bridging that gap requires contextual evaluation.

Criticality

Some controls are inherently more important than others. For example, controls related to identity, access, vulnerability management, and backups consistently appear in analyses of major incidents. Models such as **CIS Implementation Groups** acknowledge this reality by distinguishing baseline safeguards from more advanced ones.

Maturity

Maturity reflects how consistently and effectively a control operates in practice. A control that exists only on paper, is applied inconsistently, or is implemented for only part of the organization may provide a false sense of security. Conversely, a well-implemented control—one that is deployed as intended to

meaningfully reduce risk—may warrant lower priority even if further improvement is possible, particularly when less mature controls present greater risk exposure.

Likelihood

Likelihood represents how probable exploitation or failure is in the organization's environment. This can be estimated using observable factors such as exposure, known attack trends, and threat intelligence from sources like CISA, MS-ISAC, and vendor advisories.

Using a simple graduated scale allows organizations to make consistent judgments without requiring advanced threat modeling.

Impact

Impact reflects real-world consequences if a control fails: operational disruption, data exposure, regulatory consequences, and reputational harm. Impact is highly contextual—what is catastrophic for one organization may be manageable for another.

Together, likelihood and impact allow organizations to move beyond abstract severity labels and toward defensible prioritization.

Using Real-World Threat Data to Assess Likelihood

"Known Exploited Vulnerabilities are vulnerabilities that have been actively exploited in the wild and pose significant risk to federal enterprises."

— CISA Known Exploited Vulnerabilities (KEV) Catalog

Impact Goes Beyond Technical Severity

"Cyber risk includes operational disruption, financial loss, reputational damage, and legal or regulatory consequences."

— NIST Risk Management Guidance

— CISA Known Exploited Vulnerabilities (KEV) Catalog

Not All Controls Reduce Risk the Same Way

A key reason checklist-based approaches fall short is that they often treat controls as if they reduce risk equally, even when frameworks provide some built-in prioritization, such as the CIS Implementation Groups. In reality, controls influence risk in fundamentally different ways.

Preventive controls primarily reduce likelihood. Detective controls reduce time to detection and therefore impact. Recovery controls limit severity and duration. Governance controls enable sustainability but rarely stop attacks directly.

This distinction matters.

An organization with immature preventive controls may face constant compromise risk, regardless of how well documented its policies are. Conversely, strong detection and recovery capabilities can mean the difference between a minor incident and a major breach.

Frameworks intentionally include all control types, but binary scoring masks these differences. A risk-informed approach recognizes that improving a weak preventive control often reduces more risk than marginally improving an already mature governance process.

> ***Different Controls Reduce Risk in Different Ways***
>
> Security controls reduce risk by **lowering the likelihood of compromise**, **reducing time to detection**, or **limiting the impact of an incident**. Mature programs balance all three.
>
> *— Derived from NIST CSF Functions (Protect, Detect, Respond, Recover)*

Myths vs. Reality

Myth: Frameworks are just compliance checklists
Reality: Frameworks define expected safeguards; risk context determines priority.

Myth: Frameworks ignore real-world threats
Reality: Frameworks are built from real incidents; interpretation determines effectiveness.

Myth: Small organizations can't use frameworks meaningfully
Reality: Frameworks are often most valuable to smaller organizations where resources are limited.

Myth: Compliance equals security
Reality: Security depends on maturity, likelihood, and impact—not checkmarks.

> ***Frameworks Scale Down as Well as Up***
>
> "The NIST Cybersecurity Framework is designed to be flexible and usable by organizations of all sizes and sectors."
>
> *— NIST CSF Guidance*

From Assessment to Action

Organizations do not need perfect data or enterprise tooling to make better decisions. They need structure, context, and consistency.

By combining framework assessments with maturity-aware, risk-informed prioritization, organizations can:

- Focus limited resources where they reduce the most risk
- Clearly explain and defend security decisions to leadership, auditors, and financial stakeholders
- Demonstrate due diligence grounded in real-world risk rather than theory

Frameworks become most powerful **after the checkbox**, when assessment results inform action rather than simply documentation.

In Closing

Frameworks do not fail organizations. They succeed when used as intended: as a foundation for understanding, prioritizing, and reducing cybersecurity risk. The moment organizations move beyond binary compliance and apply real-world context, frameworks transform from static checklists into strategic tools for meaningful risk reduction.

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

> ***Frameworks Succeed When Context Is Applied***
>
> Frameworks provide structure. Context provides clarity. Together, they enable meaningful and measurable risk reduction.

priorities match your reality.

About the Author

Mark Kirkendall is an IT Security Manager for a county government with over 25 years of experience in information technology, including more than 14 years focused on cybersecurity and local government environments. He holds a Master's degree in Cybersecurity from California State University San Marcos.

Perceptive Cyber

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