AXA VENTURE PARTNERS

White Paper

by Ethan Ellinger, Associate

How can software investors turn NIST CSF 2.0 updates into opportunities in cybersecurity and risk management?

New York - London - Paris

www.axavp.com

Ethan Ellinger, Associate

Contextualizing NIST CSF 2.0: How did we get here, and why is it important?

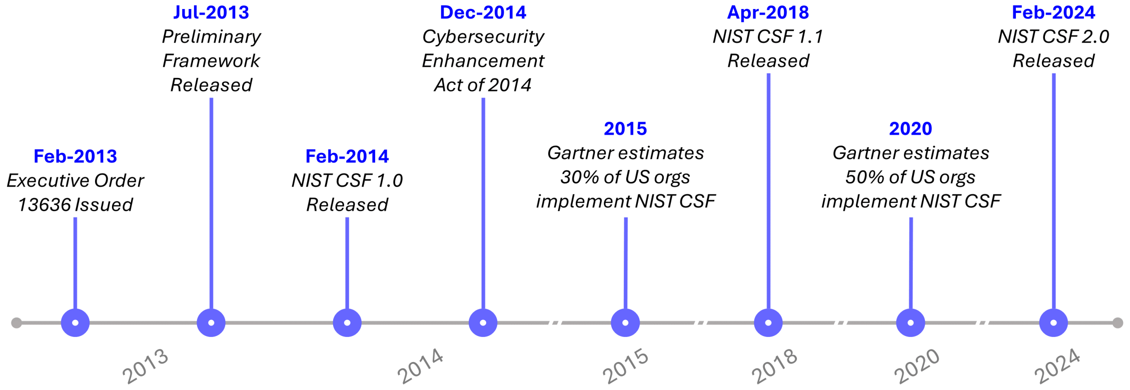
In 2013, an executive order titled "Improving Critical Infrastructure Cybersecurity" was released by President Obama in response to repeated intrusions into the United States' critical infrastructure (chemical plants, water treatment facilities, etc.)[1]. The order tasked the National Institute of Standards and Technology (NIST) to design a framework for both public and private sector organizations to mitigate cybersecurity risks.

NIST, a non-regulatory federal agency, partnered with the private sector, academics, and other government agencies over the next year to develop standards and guidelines that improve the cybersecurity postures of critical infrastructure entities. During development of the Framework, NIST collected and analyzed 15,000+ comments from 270+ organizations and 3,000+ workshop attendees. The NIST Cybersecurity Framework 1.0 was released in early 2014.

Later in 2014, US Congress passed the "Cybersecurity Enhancement Act of 2014". This act encouraged NIST to continue updating the Framework on an ongoing basis. It also encouraged the private sector to actively participate in its development, stating no information shared by a private entity should be used to develop regulating standards for that entity.

The Framework quickly gained popularity. By 2015, Gartner estimated the CSF was used by 30% of all US organizations, growing to 50% by 2020[2]. While initially developed for critical infrastructure sectors, it's now widely adopted by organizations across different industries and sizes.

In early 2024[3], NIST released CSF 2.0, marking the first major update to the Framework since initial release a decade earlier (besides CSF 1.1, which was released in 2018 but mainly refined and clarified language).


Feb-2013
Executive Order 13636 Issued
Jul-2013
Preliminary Framework Released
Feb-2014
NIST CSF 1.0 Released
Dec-2014
Cybersecurity Enhancement Act of 2014
2015
Gartner estimates 30% of US orgs implement NIST CSF
Apr-2018
NIST CSF 1.1 Released
2020
Gartner estimates 50% of US orgs implement NIST CSF
Feb-2024
NIST CSF 2.0 Released
2013
2014
2015
2018
2020
2024

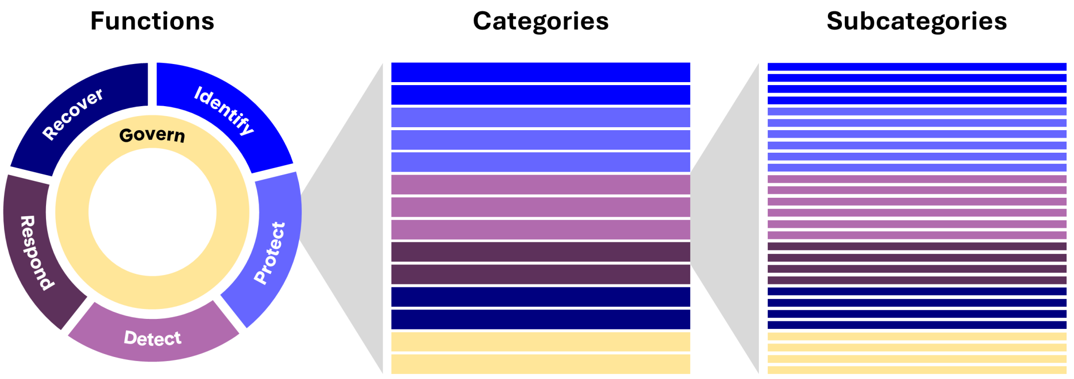
So, why should venture capital and growth equity investors take interest in an opt-in framework created by a non-regulatory government agency? Because NIST CSF 2.0 represents best practices in cybersecurity and risk management, developed with contributions from leading software companies. Further, with a backdrop of growing cybercrime cost and volume, organizations are more incentivized than ever to improve their security posture.

NIST CSF 2.0's expansive reach, the availability of public comments from companies like Amazon and CrowdStrike, and recent codified updates can shed light on the direction of the cybersecurity and risk management industries. **In this paper, I will explore what investors can learn from changes in NIST CSF 2.0, the additions large technology companies requested in the latest version, and pinpoint areas within cybersecurity and risk management that could benefit from these trends.**

Applying NIST CSF 2.0: What is it, and how is it used?

Before discussing changes in NIST CSF's first major update, it's important to understand the Framework's practical application. Here's a rundown:

- **What is NIST CSF?** It's a document and associated resources used to organize best practices, controls, and recommendations for risk management and cybersecurity organizations. The NIST CSF taxonomy includes three structures: **Functions, Categories, and Subcategories** (along with Implementation Examples and References). Organizations looking to implement a comprehensive cybersecurity strategy use the Framework and its underlying standards for guidance.



Example: Protect
Safeguards to manage the organization's risks are used

Example: Identity Management, Authentication and Access Control
Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access

Example: PR.AA-05
Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

- **Are there other cybersecurity frameworks?** Yes, there are several widely used and important cybersecurity frameworks including, but not limited to ISO 27001/2, SOC2, CIS, GDPR, HIPAA. NIST CSF is the focus of this paper because it has been recently updated and its resources are publicly available.

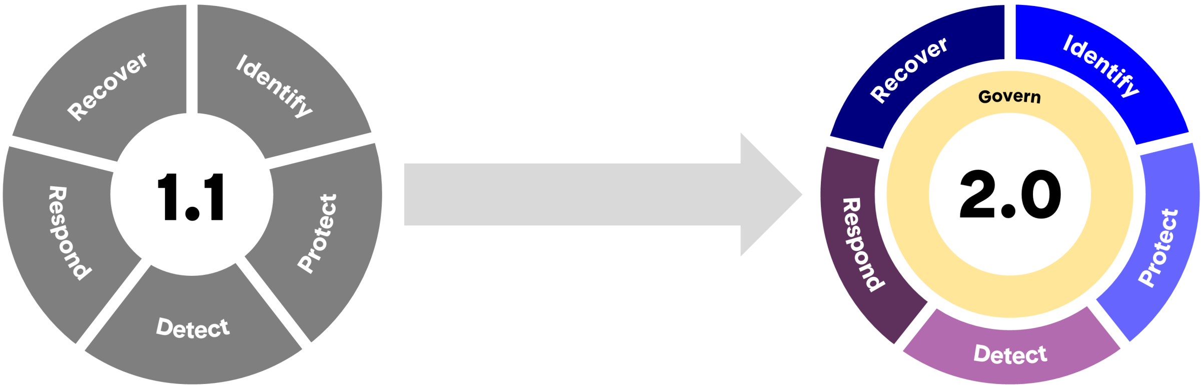
- **Who uses NIST CSF?** The individuals managing the cybersecurity risk program vary by organization. Typically, those responsible for managing cybersecurity standards and compliance will report to the Chief Information Security Officer (CISO), Chief Risk Officer (CRO), or a similar role.

- **How is NIST CSF used?** The Framework serves as a high-level checklist and repository of knowledge for organizations to prepare for, protect against, and respond to cybersecurity threats. Policies and controls are aligned to the NIST CSF subcategories and are maintained within an organization's systems (in spreadsheets, documents, or purpose-fit compliance software). As an outcome-based framework designed for universal applicability, the default recommendations within NIST CSF are quite general. However, the community contributes "Community Profiles" over time, providing more specific advice. For instance, see below from the Cyber Risk Institute's community profile. They have added specificity on how to satisfy the DE.AE-03 Subcategory (i.e. procuring external threat intelligence, and using a SIEM to monitor in-house security):

> **Subcategory from NIST CSF:**
> *"Information is correlated from multiple sources."*
>
> **Response Guidance from Cyber Risk Institute:**
> *"The organization should deploy tools, as appropriate, to collect and aggregate information, including threat intelligence, to provide a holistic view of the organization's security posture. The organization should monitor network traffic in real-time with automated tools in order to detect internal and external cyber threats. For example, a security information and event management (SIEM) tool can be used to collect and log security related documentation for analysis and correlation."*[4]

What changed in NIST CSF 2.0, and what can investors learn from the updates?

Now centered on what NIST CSF 2.0 is used for, and how it's accomplished, let's discuss what has changed and how investors might interpret these updates.



1. New “Govern” function

Perhaps the most obvious change in NIST CSF 2.0 is the new Govern function, which refers to the communication and active monitoring of an organization’s cybersecurity strategies and policies.

As mentioned prior, organizations implementing NIST CSF 2.0 will maintain policies and controls in documents, spreadsheets, or purpose-built compliance software. The addition of the Govern function adds emphasis on an organization’s ability to monitor and improve these policies and controls.

Robust governance, policies, and strategies are crucial for the entire model to function effectively. The Govern function also includes a category for another significant theme in NIST CSF 2.0 - Cybersecurity Supply Chain Risk Management.

2. Emphasis on cybersecurity supply chain risk management

Third-party attack vectors have become more vulnerable in an increasingly interconnected technology landscape. SecurityScorecard found that 98% of organizations have a relationship with a third party who has been breached.

The US government created the FedRAMP compliance program for this reason – because cyber attackers could target third-party providers that hold federal data. Similarly, private entities are custodians of other’s sensitive data.

Consequently, NIST included a full category of controls dedicated to Cybersecurity Supply Chain Risk Management. These controls aim at establishing a supply chain risk program, prioritizing vendors based on criticality, and conducting due diligence on suppliers before entering formal engagements.

3. Acknowledgment of cybersecurity risks from emerging technologies

While not included in the core taxonomy by name, emerging technologies like AI are addressed in the NIST CSF 2.0 document’s discussion section. NIST states “as new technologies and new applications of technology become available, new risks become clear.” The organization also published an AI Risk Management Framework in 2023, which they reference in the document.

NIST advises cybersecurity practitioners to consider AI risks in conjunction with other enterprise risks such as financial, cybersecurity, and privacy. This approach leads to more cohesive and efficient results.

4. What these changes mean to investors

Given the wide adoption of the NIST CSF and its "open source" development process, we can infer that the updates in NIST CSF 2.0 represent both: (1) areas where previous risk management programs have lacked coverage, and (2) current areas of focus for CISOs.

Investors may conclude that cybersecurity software companies addressing these new or updated standards could see increased adoption as potential customers' cybersecurity and risk management programs evolve (specific sub-markets to be addressed later).

What did the mega cap technology companies want to include in NIST CSF 2.0?

Because NIST published the public comments received during its community engagement period, we're able to see what the cybersecurity community wanted to change or add. Over 150 parties submitted comments, from individual contributors to the largest companies in the world. These comments provide unique insights into the focus areas of mega cap technology companies.

> *"The current framework includes credential management, principles of least privilege, network integrity, and user/device authentication. These cybersecurity practices do not represent the current best practices of identity management, authentication nor access control... **We believe more explicit guidance on [Zero Trust Architecture] implementation would yield stronger cybersecurity outcomes. This is no longer a "next step" organizations can take to bolster their security posture, ZTA should be a security baseline."***

CROWDSTRIKE

> *"Although the NIST CSF encompasses various functions that involve metrics and reporting, **it is notable that the newly introduced governance function or the restructured aspects in the identify function have not received similar attention in terms of metrics and measurement guidance...** Therefore, comprehensive guidance on the selection and implementation of appropriate metrics would greatly enhance the usefulness of the CSF in this regard."*

experian

- ***"Highlight the increased adoption of cloud computing since the CSF was originally published through a greater focus on... automation, infrastructure as code, and secure DevOps."***
- *"Enhanced focus on continuous improvement and resilience, through the addition of a new function."*
- *"Provide guidance on [cybersecurity supply chain risk management] and incorporate core concepts into future version[s] of the CSF."*

aws

1. CrowdStrike recommends codifying Zero Trust Architecture as a "security baseline"

Zero Trust Architecture (ZTA) refers to a cybersecurity model that is based on a "never trust, always verify" concept where users and devices are assumed to be harmful until verified as trustworthy. It is an increasingly popular approach to cybersecurity strategy, and CrowdStrike argues that NIST should feature it more prominently in NIST CSF 2.0 because it is now the "security baseline." It's worth noting that NIST also developed and published the preeminent paper on Zero Trust Architecture (NIST 800-207) but does not include ZTA in the core taxonomy of NIST CSF 2.0.

CrowdStrike's comments are indicative that they advocate for increased focus on ZTA's key principles: continuous verification, limiting the "blast radius" of a breach, and automating the context collection and response to cyber threats. Investors may translate these comments to increased focus on ZTA principles among CISOs, and look for alignment to those principles in prospective cybersecurity investment opportunities.

2. Experian seeks guidance on KPIs to monitor

The new Govern function within CSF 2.0 puts more emphasis on reporting and metrics related to cybersecurity. However, Experian recommends that NIST is more prescriptive in the KPIs organizations track, so the efficacy of their cybersecurity program is more easily measured and benchmarked.

Given large cap companies like Experian are turning their attention to tracking cyber risk KPIs, investors may translate these comments to potential market growth among third-party cyber risk scoring companies (like AVP's portfolio company, SecurityScorecard) or real-time security monitoring software.

3. AWS highlights the evolution of cloud computing since 2014

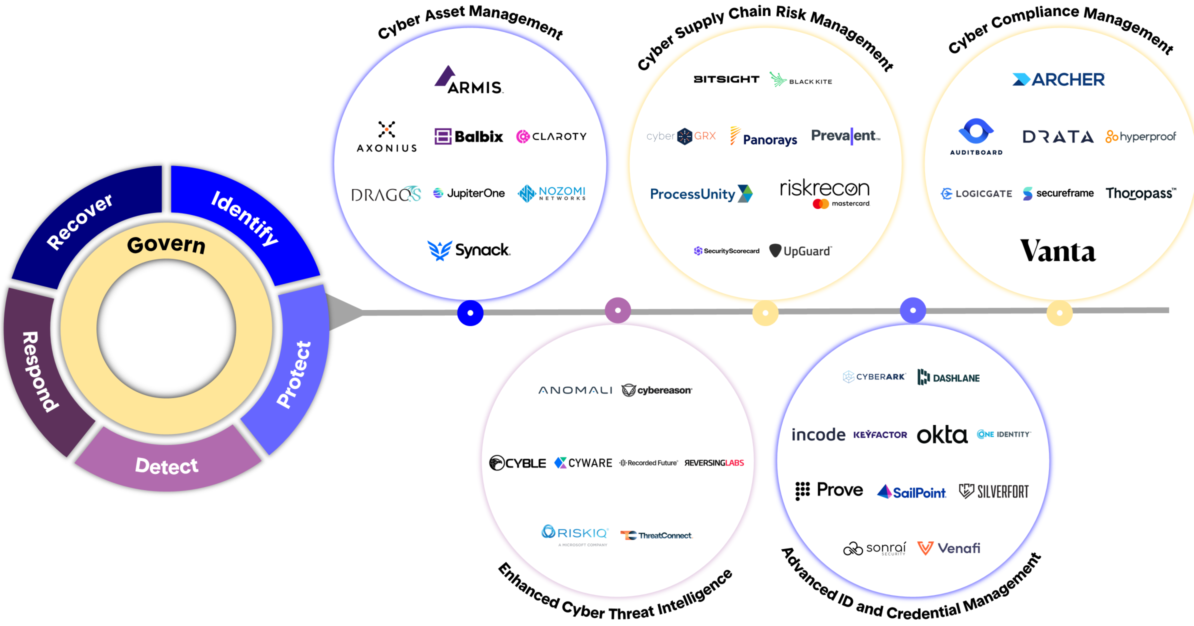
Information technology has changed dramatically since 2014, and the increased adoption of cloud computing has arguably made the largest impact on the scalability, flexibility, and speed of development in modern environments. Cloud computing also comes with different cybersecurity considerations, which Amazon encouraged NIST to discuss in CSF 2.0. As one of the main third-party cloud service providers (CSPs) today, Amazon recommended NIST add language on the "Shared Responsibility Model", where an organization delegates responsibility for a subset of security controls to its third-party CSP.

In their comments, Amazon's posture indicates that they want CSPs to take on *more* responsibility than currently described in the CSF 2.0 draft. For example, they asked that NIST change "external service provider activities and services **are monitored** to find potentially adverse events" to "**maintain awareness** of external service providers activities to identify potentially adverse events."

Investors in cybersecurity software companies may interpret this as a cautionary point. More businesses are migrating their environments to CSPs (namely Google Cloud, Amazon Web Services, Microsoft Azure). If these companies are willing to take on more cybersecurity responsibilities on behalf of their customers, it will be important to understand if or when they will add security features that directly compete with smaller vendors.

Who benefits from the direction of travel in cybersecurity and risk management?

The updates in NIST CSF 2.0 can serve as a guide to the latest best practices in cybersecurity. Reflecting on these changes, I've pinpointed five sub-markets that could experience accelerated growth as CISOs focus more on specific areas of their cybersecurity strategies. Please note that the areas and logos identified below are not comprehensive but represent a selection of concepts the Framework emphasizes more than prior versions.



Logos sorted alphabetically, illustrative and non-exhaustive lists

1. Cyber Asset Management

NIST CSF 2.0 assigns greater scope to asset management than prior versions, with additional subcategories within the Identify function (ID.AM-01 to ID.AM-08). This broader scope may drive growth for software businesses offering IT / OT / IoT Asset Visibility and Attack Surface Management solutions.

2. Cyber Supply Chain Risk Management

NIST CSF 2.0 gives cybersecurity supply chain risk management its own Category (GV.SC). This increased emphasis on processes that identify, develop, and manage supply chain risk management strategies could stimulate market growth. Tools related to cyber supply chain risk management include third-party risk management software, cyber risk scoring platforms, and external attack surface monitoring services.

3. Cyber Compliance Management

NIST CSF 2.0 introduced the Govern function, including several high-level Categories related to oversight, monitoring, and strategic improvement within the risk organization. This new function bridges the gap between the risk organization and the cybersecurity organization's responsibilities within an enterprise. Information Security Compliance software and Risk & Compliance software may see outsized market growth as the CISO and CRO roles are increasingly interconnected.

4. Enhanced Cyber Threat Intelligence

NIST CSF 2.0 further emphasizes the integration of cyber threat intelligence within the risk organization's workflows with the additions of two subcategories in the Detect function (DE.AE-06, DE.AE-07). Threat intelligence is a top priority for IT leaders – according to a 2023 survey from Armis, 70% of decisionmakers called out "keeping up with threat intelligence" as a top three challenge. Procuring threat intelligence into the security organization provides contextual information that informs better decision-making when incidents occur.

5. Advanced Identity and Credential Management

NIST CSF 2.0 provides refined and updated guidance for identity and credential management within the Protect function (PR.AA-01 to PR.AA-06). These updated controls include recommendations for both physical and virtual environments, and the application of identity controls in cybersecurity go much further than physical IDs and multi-factor authentication. Companies that offer ID-based cybersecurity software may benefit from market growth as focus increases, including identity governance and administration software, access management, and certificate lifecycle management.

Final remarks

NIST CSF's update this year provides a snapshot of today's priorities in the cybersecurity ecosystem, which is moving quickly to keep pace with new threats and risks. In this evolving landscape, AVP believes there is a heightened necessity for innovative ideas and technology. We are eager to partner with companies that are developing the next generation of impactful solutions.

If you're an early stage or growth stage company actively building in the cybersecurity or risk management space, we would welcome an opportunity to meet with you.

You can reach out to ethan.ellinger@axavp.com, or connect with the rest of our colleagues at www.axavp.com.

[1] Cybersecurity & Infrastructure Security Agency (CISA) defines all 16 "critical infrastructure" sectors here

[2] Gartner

[3] NIST CSF 1.1 was released in 2018 but mainly refined and clarified language

[4] Cyber Risk Institute

We invest in great entrepreneurs.

We support outstanding companies.

AXA VENTURE PARTNERS

New York - London - Paris

www.axavp.com