6clicks

Cyber resilience in 2025:

Your smart guide to NIST CSF

NIST

Contents

Introduction 03

What is NIST CSF 05

What is the difference between NIST CSF and other NIST frameworks? 08

Why implement the NIST CSF? 09

NIST CSF Core 10

Govern 12

Identify 13

Protect 14

Detect 15

Respond 15

Recover 16

NIST CSF Organizational Profiles 17

NIST CSF Tiers 19

How to achieve NIST CSF compliance 23

Streamline NIST CSF implementation with 6clicks 32

Elevate your offerings with AI-powered NIST CSF compliance solutions 34

Learn more about 6clicks 35

01

Introduction

In 2025, cybercrime is projected to cost the global economy $10.5 trillion annually (Cybersecurity Ventures), highlighting the escalating severity of cyber threats. Small businesses are particularly vulnerable, with reports indicating that one in two face the threat of a cyberattack—a significant increase from previous years—often resulting in expenses averaging $500,000. These alarming statistics underscore the critical need for organizations—whether big or small—to adopt robust cybersecurity measures to safeguard their assets and ensure business continuity.

Cybercrime will cost the global economy

$10.5 trillion per year starting 2025

1 in 2 small businesses

face the threat of a cyberattack, with associated costs estimated at $500,000

This is where the NIST Cybersecurity Framework (NIST CSF) comes in. Designed by the National Institute of Standards and Technology, this framework provides a flexible and structured approach to getting ahead of cybersecurity risk. Instead of prescribing specific controls, NIST CSF focuses on high-level outcomes that organizations can tailor to their unique needs, making it a global standard for cybersecurity strategy.

In this guide, we'll explore the core components of NIST CSF, walk through the compliance process, and break down how to streamline implementation—especially with powerful tools like 6clicks, which provides an all-in-one platform for risk management, compliance, and audit readiness.

Let's dive in. →

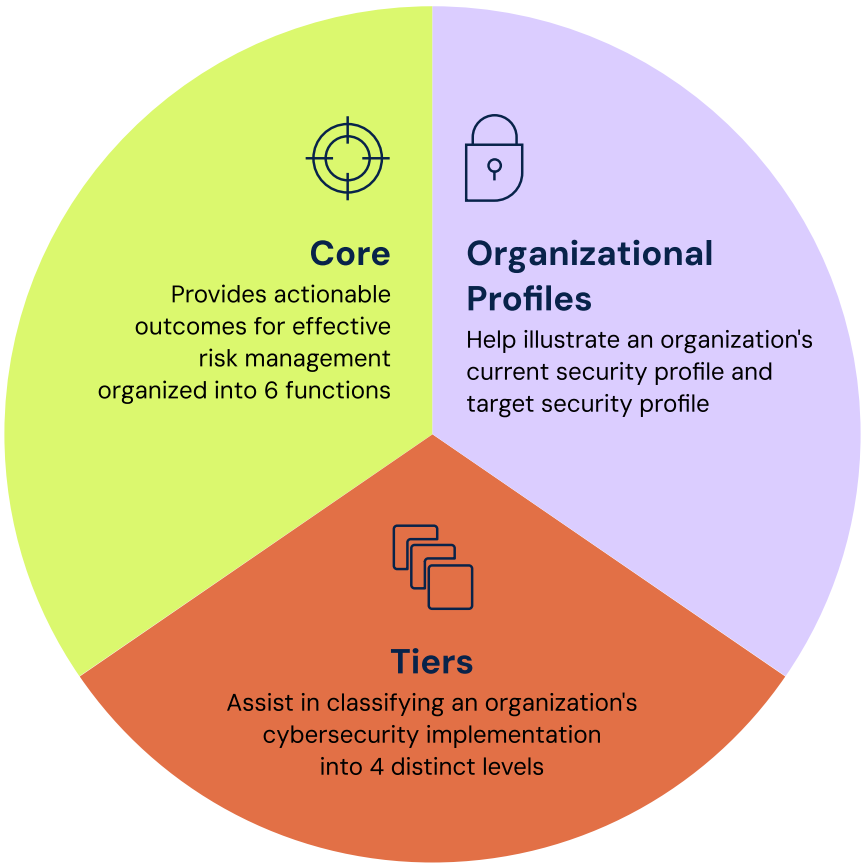
02

What is the NIST CSF

The NIST Cybersecurity Framework provides a flexible structure that organizations can use to build and improve their cybersecurity risk management programs. It helps manage and reduce cybersecurity risk by focusing on outcomes rather than rigid technical requirements. Unlike prescriptive standards, NIST CSF provides a common language and structured approach that can be tailored to organizations of any size, sector, or maturity level.

It consists of three main components:

NIST Cybersecurity Framework



Core

The Core is the heart of the NIST CSF. It organizes cybersecurity outcomes into six key Functions —Govern, Identify, Protect, Detect, Respond, and Recover (NIST CSF 2.0). Each function is further divided into categories and subcategories, which represent specific security outcomes and best practices organizations can adopt. These outcomes are not just high-level principles; they include concrete, actionable guidance covering everything from risk assessment to incident response.

Organizational Profiles

This component outlines two types of profiles that enable organizations to customize the framework to their unique context. The Current Profile describes an organization's present level of security maturity while the Target Profile defines their desired cybersecurity posture based on business needs, regulatory requirements, and risk tolerance.

Implementation Tiers

Lastly, the NIST CSF includes four Implementation Tiers that reflect the maturity and sophistication of an organization's cybersecurity risk management practices: Partial, Risk-Informed, Repeatable, and Adaptive. These tiers do not represent levels of compliance but help organizations evaluate how well risk is managed and communicated across the business.

What is the difference between NIST CSF and other NIST frameworks?

NIST CSF is often compared to other cybersecurity frameworks like NIST RMF, NIST SP 800-53, and ISO 27001—but each serves a different purpose, audience, and implementation approach.

Here's a quick comparison to help you understand how they differ:

Framework	Purpose	Primary Audience	Structure	Certification
NIST CSF	Provides a flexible framework for improving cybersecurity risk management	All organizations	6 core functions, 22 categories, 106 subcategories	Not certifiable
NIST RMF	Guides the process of selecting and implementing controls based on risk	US federal agencies and contractors	7-step risk management process	Not certifiable, but required for FISMA and FedRAMP authorization
NIST SP 800-53	Provides a catalog of security and privacy controls	US government and regulated industries	20 control families	Not certifiable, but required for FISMA, FedRAMP, and CMMC
ISO 27001	Provides a standard for implementing and maintaining an information security management system (ISMS)	All organizations	10 standard clauses and 93 controls	Certifiable via independent audit

Why implement the NIST CSF?

Implementing the framework equips organizations with a comprehensive and scalable risk management strategy. By aligning cybersecurity practices with the framework's outcomes, businesses can strengthen resilience, meet regulatory requirements, and protect their most valuable assets.

Here are the key benefits of adopting the NIST CSF:

Cybersecurity readiness

The NIST CSF outlines specific outcomes across areas like employee training, data protection, and continuous monitoring—helping organizations safeguard systems and data from cyber threats and improve overall security posture.

Regulatory alignment

It supports compliance with major regulations like GDPR, HIPAA, and DORA and shares similarities with standards like ISO 27001 and SOC 2, making it easier for organizations to meet multiple regulatory and industry requirements simultaneously.

Operational resilience

By helping organizations identify, prioritize, and respond to risks effectively, NIST CSF enables smoother handling of and recovery from incidents and reduces the likelihood of significant business disruptions.

Cross-industry applicability

Its flexible, outcome-based approach makes it suitable for all types of organizations—whether public or private, large or small—allowing each to tailor implementation to its specific context.

Risk visibility and governance

The framework promotes executive-level engagement and organization-wide awareness of cybersecurity risks, leading to better governance and more informed decision-making.

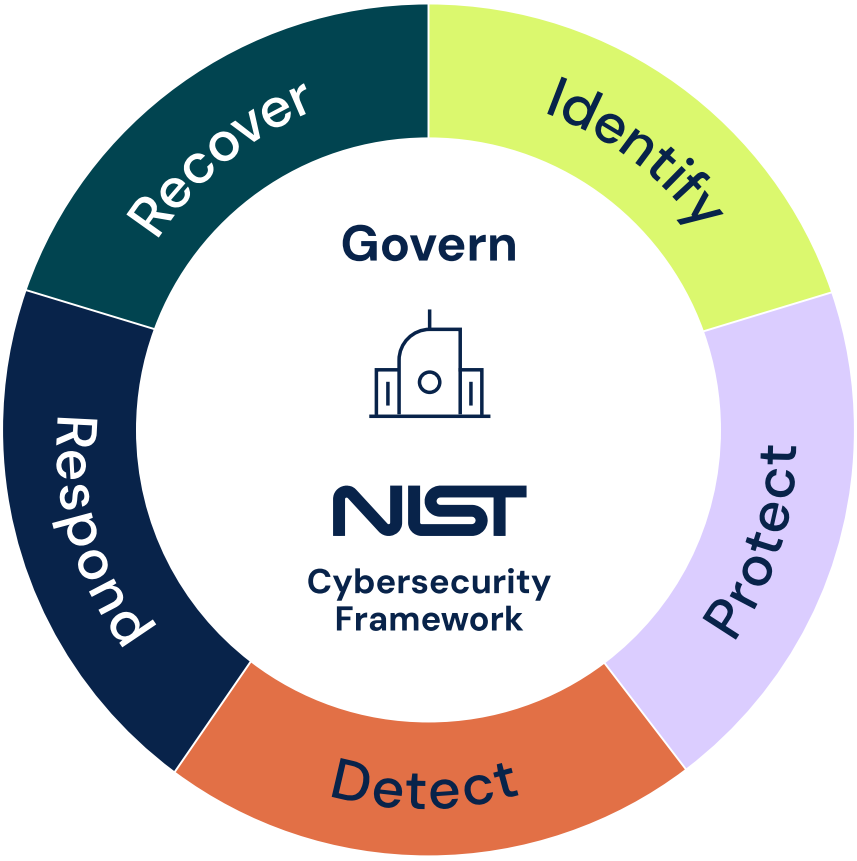
Enhanced trust and credibility

Demonstrating NIST CSF compliance showcases your capacity for robust cybersecurity to customers, regulators, and partners—boosting your organization's credibility and competitiveness.

03

NIST CSF Core

The Core of the NIST CSF is structured around six essential functions. Each function contains categories and subcategories that define specific, actionable outcomes organizations can implement to achieve a strong security posture. In total, the NIST CSF has 22 categories and 106 subcategories which serve as control objectives that can be mapped to your organization's specific controls to assess alignment and support compliance efforts.



Here is an in-depth look at each Core Function: →

Govern

Establish and oversee the organization's cybersecurity risk management strategy.

The Govern function sets the foundation for the entire cybersecurity program. It ensures that cybersecurity risk management is strategically aligned with the organization's objectives, well-resourced, and clearly communicated across all levels. It also covers how cybersecurity roles are defined, how risk policies are enforced, and how oversight is maintained—including across the supply chain.

	Category	Outcome
	Organizational Context	Define the organization's mission objectives, legal, regulatory, and contractual obligations, and stakeholder expectations for the risk management program
	Risk Management Strategy	Establish the organization's risk tolerance and risk appetite and corresponding risk management processes
	Roles, Responsibilities, and Authorities	Assign clear responsibilities and ensure accountability and resource allocation at all levels, from executive leadership to line employees
	Policy	Put in place organization-wide risk management policies
	Oversight	Set up mechanisms for monitoring risk management activities
	Cybersecurity Supply Chain Risk Management	Integrate third-party and supplier risk into the broader cybersecurity risk management strategy

Identify

Understand your environment, assets, and cybersecurity risks.

This function enables organizations to gain a full picture of the resources they need to protect and the risks that could impact them. By identifying assets and assessing vulnerabilities and threats, organizations can prioritize risk mitigation efforts and align them with business needs.

	Category	Outcome
	**Asset Management**	Inventory all assets (hardware, software, facilities, services, data, systems, and human resources) and prioritize based on risk
	**Risk Assessment**	Identify threats and vulnerabilities, evaluate likelihood and impact, and formulate risk response
	**Improvement**	Identify opportunities to enhance risk management processes, procedures, and policies through ongoing evaluation and testing

Protect

Implement safeguards to mitigate the impact of cybersecurity risks.

The Protect function focuses on proactive measures to prevent incidents and minimize exposure. It includes technical, administrative, and physical controls to secure data and systems, as well as training and awareness to ensure that personnel understand their responsibilities.

	Category	Outcome
	Identity Management, Authentication, and Access Control	Ensure only authorized users and devices can access critical data and assets
	Awareness and Training	Educate staff on cybersecurity best practices and their role in protecting the organization
	Data Security	Protect the confidentiality, integrity, and availability of data through encryption, backups, and other measures
	Platform Security	Fortify systems and infrastructure and ensure consistent monitoring for potential weaknesses
	Technology Infrastructure Resilience	Build and maintain a resilient security architecture capable of withstanding attacks

Detect

Identify cybersecurity events quickly and accurately.

This function enables timely detection of threats, anomalies, and potential incidents. With strong detection mechanisms in place, organizations can identify attacks as they occur and take early action to contain or prevent damage.

	Category	Outcome
	Continuous Monitoring	Use real-time surveillance tools and alerting systems to identify suspicious behavior and threat indicators
	Adverse Event Analysis	Investigate anomalies and threat indicators to determine if a cybersecurity incident has occurred, and assess its scope and impact

Respond

Take action to contain the impact of cybersecurity incidents.

Once an incident is detected, the Respond function guides organizations in managing and mitigating its effects. This includes executing response plans, communicating effectively, and conducting thorough analysis to learn from the event.

	Category	Outcome
	Incident Management	Develop and carry out incident response plans to quickly mitigate risks
	Incident Analysis	Investigate root causes to prevent recurrence and improve future responses
	Incident Response Reporting and Communication	Ensure timely and transparent communication with internal stakeholders and, when required, regulatory bodies
	Incident Mitigation	Ensure incident response activities are performed in an adequate and timely manner to contain and eliminate threats

Recover

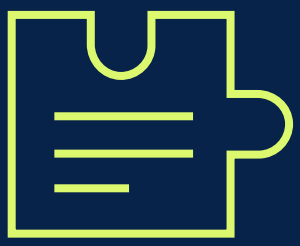
Restore capabilities and operations affected by a cybersecurity incident.

This function focuses on timely recovery to minimize disruption. It involves executing the recovery phase of the incident response plan, restoring normal operations, validating the integrity of recovered systems, and adjusting cybersecurity strategies to prevent future incidents.

	Category	Outcome
	Incident Recovery Plan Execution	Restore affected systems and services through defined recovery activities
	Incident Recovery Communication	Communicate recovery status and updates to internal and external stakeholders

Together, these six functions enable organizations to build, assess, and continuously improve their cybersecurity programs.

04



NIST CSF
Organizational Profiles

One of the most powerful and flexible aspects of the NIST Cybersecurity Framework is its use of Organizational Profiles. These profiles allow organizations to tailor the framework to their specific business context, risk tolerance, and cybersecurity goals—ensuring that implementation is both relevant and actionable.

Current Profile

The organization's current cybersecurity posture. It maps current practices and capabilities to the outcomes in the NIST CSF.

Target Profile

The organization's desired cybersecurity posture. It incorporates business needs, regulatory requirements, and strategic priorities.

By comparing these two profiles, organizations can identify and prioritize the gaps that must be addressed to move from their current state to their desired state. This makes Organizational Profiles an essential tool for aligning cybersecurity efforts with enterprise risk management and driving continuous improvement.

To create your Organizational Profile, follow these five practical steps:

Step 1: Define the scope

Identify what the profile will cover—whether it's the entire organization, a specific business unit, or a targeted threat scenario like ransomware.

Step 2: Collect relevant information

Gather policies, risk priorities, enterprise risk data, BIA findings, compliance requirements, tools, and defined roles that shape your cybersecurity environment.

Step 3: Develop the profile

Map the collected data to NIST CSF outcomes to build your Current Profile. Define your Target Profile by identifying desired outcomes and capabilities.

Step 4: Analyze gaps and plan actions

Compare the Current and Target Profiles, conduct a gap analysis, and create a prioritized action plan (e.g., Plans of Action and Milestones (POA&M) or a risk register) to address gaps.

Execute and evolve

Implement the plan, monitor progress, and update the profile as your environment, risks, or priorities change.

By leveraging Organizational Profiles, organizations can ensure that NIST CSF implementation isn't just a checklist—but a living, strategic component of business resilience and cybersecurity maturity.

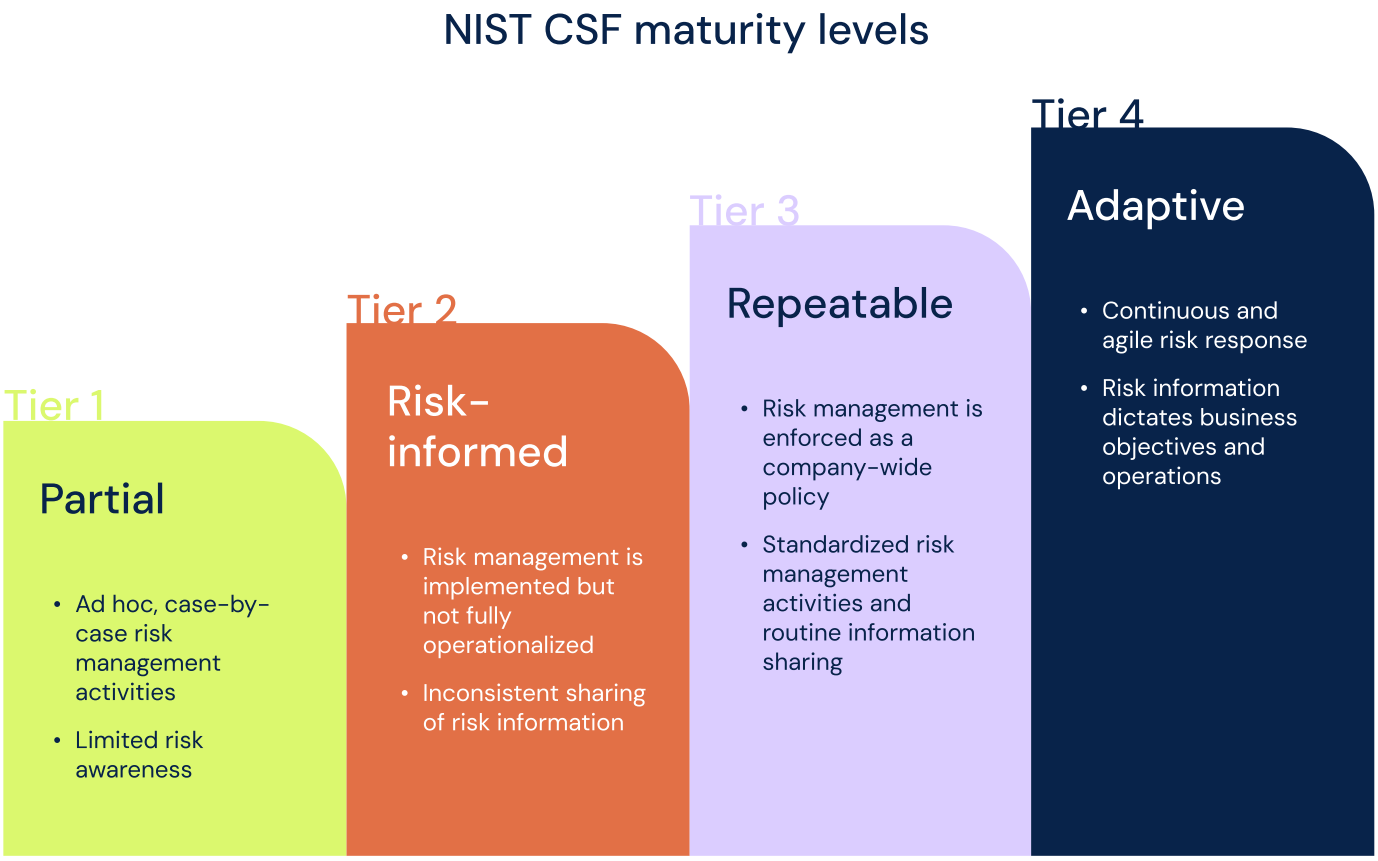
05

NIST CSF Tiers

In addition to its Core Functions and Organizational Profiles, the NIST CSF consists of implementation Tiers that help organizations assess the maturity of their cybersecurity risk management practices and determine how consistently those practices are applied across the organization.

Rather than being a strict measure of compliance, Tiers provide context for how well cybersecurity risk is governed, managed, and integrated into decision-making. They help organizations answer the question: How effectively are we managing our cybersecurity risks today —and how prepared are we to adapt to future ones?

There are 4 Tiers in total, each representing a progression in cybersecurity maturity:



Tier 1: Partial

At the Partial tier, cybersecurity risk management is informal, reactive, and largely uncoordinated. Practices are implemented inconsistently across the organization, often in response to immediate threats or compliance requirements.

- Little to no formal risk management strategy
- Cybersecurity activities are ad hoc and siloed
- Minimal awareness of cybersecurity threats across teams
- Limited understanding of third-party and supply chain risks
- Controls, if any, are undocumented and applied inconsistently

Organizations at this level often struggle to identify, prioritize, or respond to risks effectively. There is an urgent need to establish basic governance, standard policies, and foundational security practices.

Tier 2: Risk-Informed

The Risk-Informed tier reflects an organization that has started to acknowledge cybersecurity risks and apply governance practices—though inconsistently. The approach to cybersecurity is more proactive than Tier 1, but still not fully embedded across the enterprise.

- Some risk management processes are in place, often at the departmental level
- Leadership is aware of cyber risks but may not have full visibility
- Risk information is shared, but not through structured or consistent channels
- Risk assessments are conducted, though not regularly or uniformly
- Third-party risks may be identified but lack continuous oversight

At this level, organizations are transitioning from reactive to proactive risk management, but still need to formalize processes and establish centralized oversight.

Tier 3: Repeatable

At this maturity level, risk management practices are standardized, consistently applied, and enforced across the organization. Cybersecurity is treated as a business priority, with clear policies, regular assessments, and cross-functional collaboration.

- Documented policies and procedures are in place and followed
- Risk assessments are conducted regularly and updated as needed
- Cybersecurity roles and responsibilities are clearly defined and assigned
- Risk information is consistently communicated across teams
- Third-party risks are actively monitored and managed
- Executive leadership is involved in cybersecurity strategy and planning

Tier 3 organizations demonstrate a strong baseline of cybersecurity maturity. They are well-positioned to identify and respond to threats and have the structure in place to continuously improve.

Tier 4: Adaptive

The Adaptive tier represents the highest level of cybersecurity maturity, where risk management is dynamic, data-driven, and fully integrated into the organization's strategic planning and decision-making processes.

- Risk management practices are continuously improved through predictive analysis, threat intelligence, and business context
- Cybersecurity is embedded in organizational culture and embraced by leadership
- Strategic planning, budgeting, and operations are informed by current and anticipated cyber risks
- Business units execute cybersecurity strategies aligned with top-level vision
- The organization can quickly adjust to changes in risk, business goals, or technology

Organizations at this level are not only resilient but agile—able to anticipate threats, adapt rapidly, and lead with cybersecurity as a competitive advantage.

By evaluating your organization against these Tiers, you can assess your current cybersecurity maturity and identify the steps needed to advance. Whether your goal is to move up a tier or solidify your current posture, the Tiers offer a structured path for continuous improvement.

06

How to achieve
NIST CSF compliance

Although the NIST Cybersecurity Framework is voluntary for most organizations, aligning with it demonstrates a strong commitment to cybersecurity, risk management, and operational resilience. Achieving NIST CSF compliance means implementing the framework's practices across your organization and ensuring they're working effectively.

Here's a six-step approach to achieving and maintaining compliance with NIST CSF:

Step 1:
Assess your current cybersecurity posture

Start by evaluating where your organization stands today. This assessment lays the foundation for your Current Profile in the NIST CSF and helps identify gaps in alignment with the framework's Core Functions and Implementation Tiers.

Focus on:

- Reviewing current cybersecurity practices and capabilities
- Identifying risks and controls already in place
- Determining your security maturity (e.g., Partial, Risk-Informed, Repeatable, or Adaptive)
- Gathering inputs from business impact analyses, internal policies, and risk registers

Tip:

Use 6clicks' built-in audit and assessment functionality to run a maturity assessment aligned with NIST CSF Core Functions, then define your Current and Target Profiles accordingly.

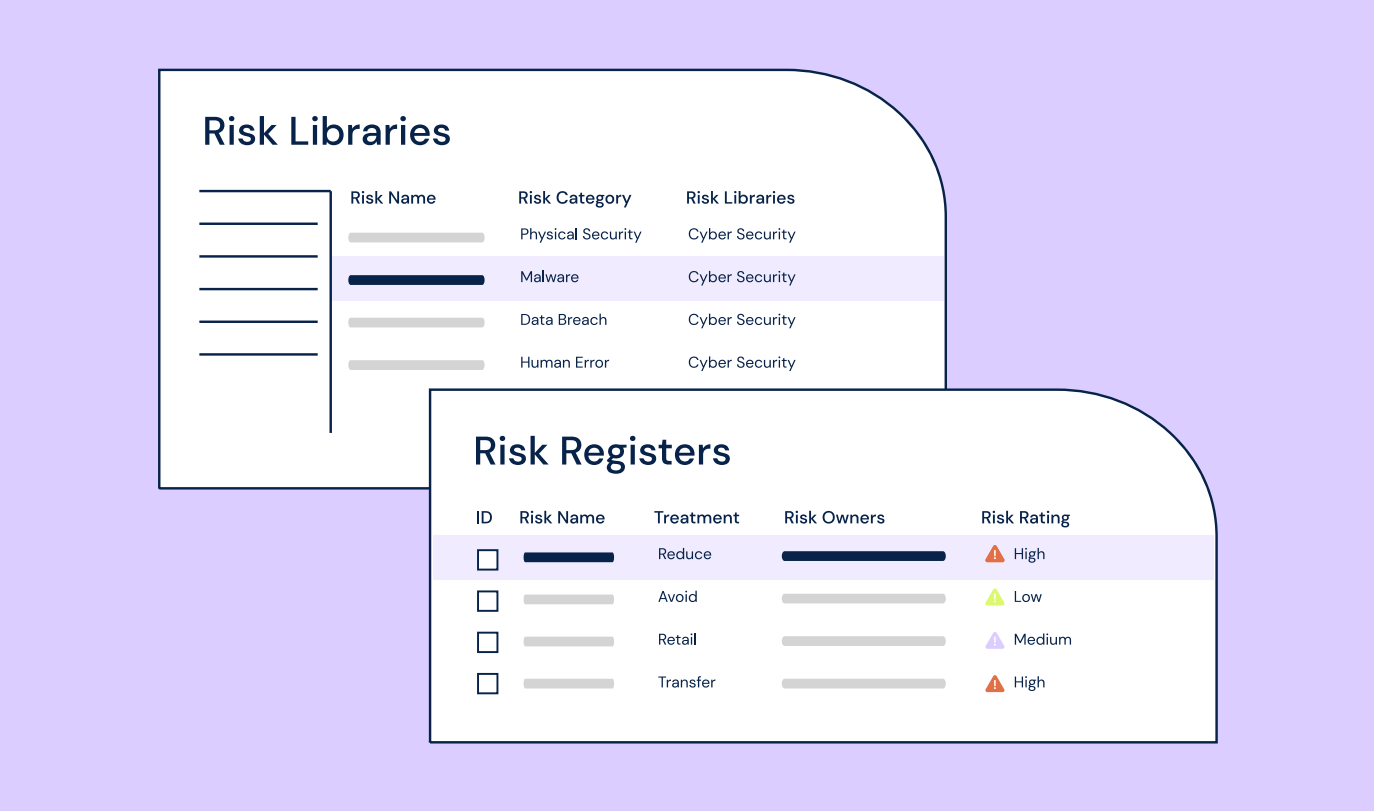
Step 2:
Establish your cybersecurity risk management framework

Next, define how your organization will approach cybersecurity risk management. This step involves developing or updating your risk management policies and procedures to align with NIST CSF outcomes. These should outline how risks are identified, assessed, treated, and monitored across business units and third-party relationships.

Key tasks:

- Establish formal risk management policies
- Define roles, responsibilities, and accountability across the organization
- Determine risk tolerance and ensure the alignment of risk management strategy with business objectives and regulatory obligations

A strong foundation begins with a structured risk management program—something 6clicks makes easy to operationalize. With 6clicks, you can leverage turnkey risk libraries to accelerate risk identification and use a centralized risk register to record, assess, and categorize risks by domain, priority, and more. Create risk treatment plans and assign owners using integrated task management features and easily generate reports to extract detailed insights into your risk posture and track the progress of remediation activities.



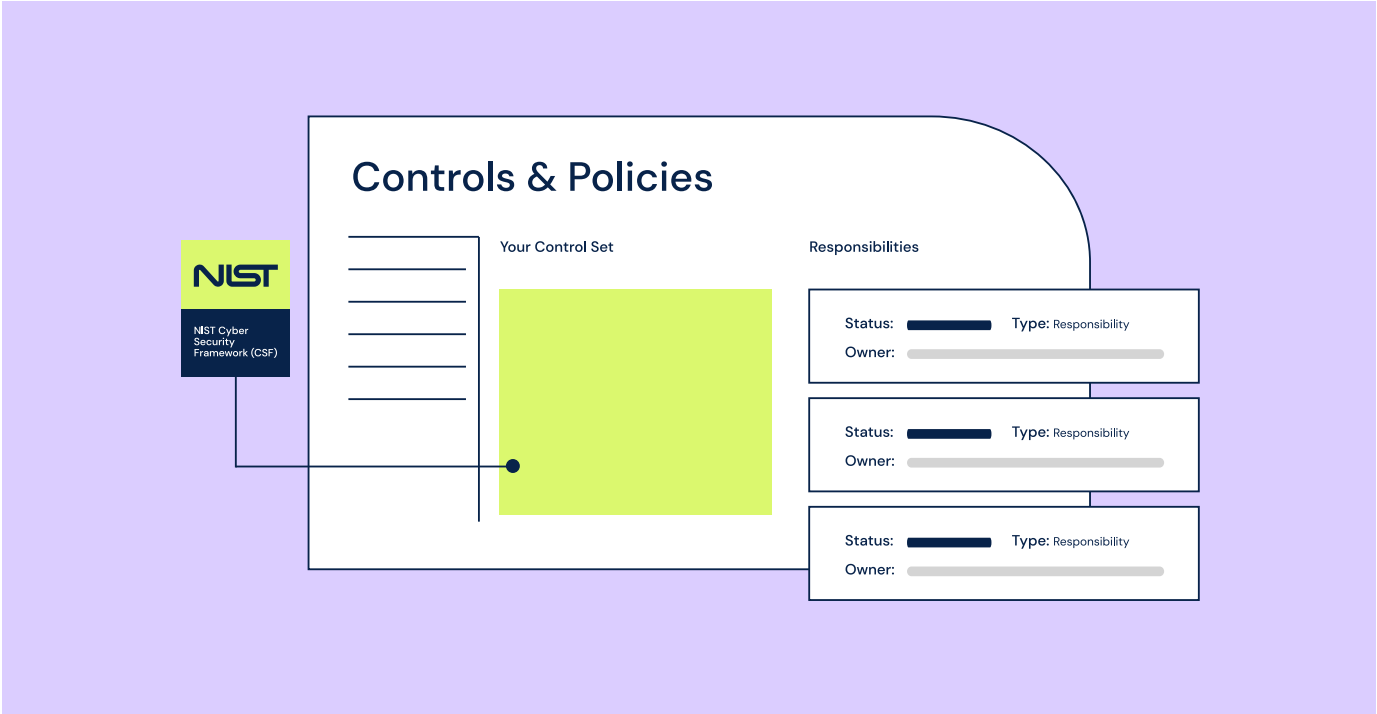
Step 3:
Implement appropriate controls and map them to NIST CSF

Once you've identified your gaps, the next step is implementing or enhancing controls that support the outcomes defined in the NIST CSF. The framework doesn't mandate specific controls—but its 106 subcategories serve as outcome-based control objectives. You can adopt controls that align with these objectives using administrative, operational, and technical safeguards tailored to your organization's environment and risk profile.

Some example controls include:

1. **Multi-factor authentication (MFA)**
   Prevent unauthorized access to critical systems and data.
2. **Encryption of sensitive data**
   Ensure data confidentiality both at rest and in transit.
3. **Regular risk assessments**
   Identify and evaluate potential threats to prioritize mitigation.
4. **Role-based access control (RBAC)**
   Restrict access to systems based on job responsibilities.
5. **Security awareness training**
   Educate employees on identifying and responding to potential threats.
6. **Endpoint protection software**
   Secure devices from malware, ransomware, and unauthorized activity.
7. **Incident response plan**
   Define roles, procedures, and communication channels for managing incidents.
8. **SIEM systems**
   Aggregate and analyze logs to detect anomalies and threats in real time.
9. **Automated backups**
   Enable timely recovery of critical data and systems after an incident.
10. **Patch management process**
    Regularly update systems to address known vulnerabilities.

As a full-stack cyber GRC platform, 6clicks equips you with complete risk and compliance management functionality, enabling you to easily set up and deploy your controls, assign control responsibilities, and even link them to associated risks, assets, issues, and other data.



Our AI engine, Hailey, can also create a complete control catalog for you by analyzing your policy documents. Then, instantly map your controls to provisions within the NIST CSF, allowing you to quickly determine your level of compliance. It's one of the most widely praised features in the 6clicks platform, saving teams hours of manual work and giving instant clarity:

> "And this is where we see the benefit of moving away from a manual GRC process into a GRC tool like 6clicks, which enables you to map each of the different standards to your control set so you only have to do the assessment once."

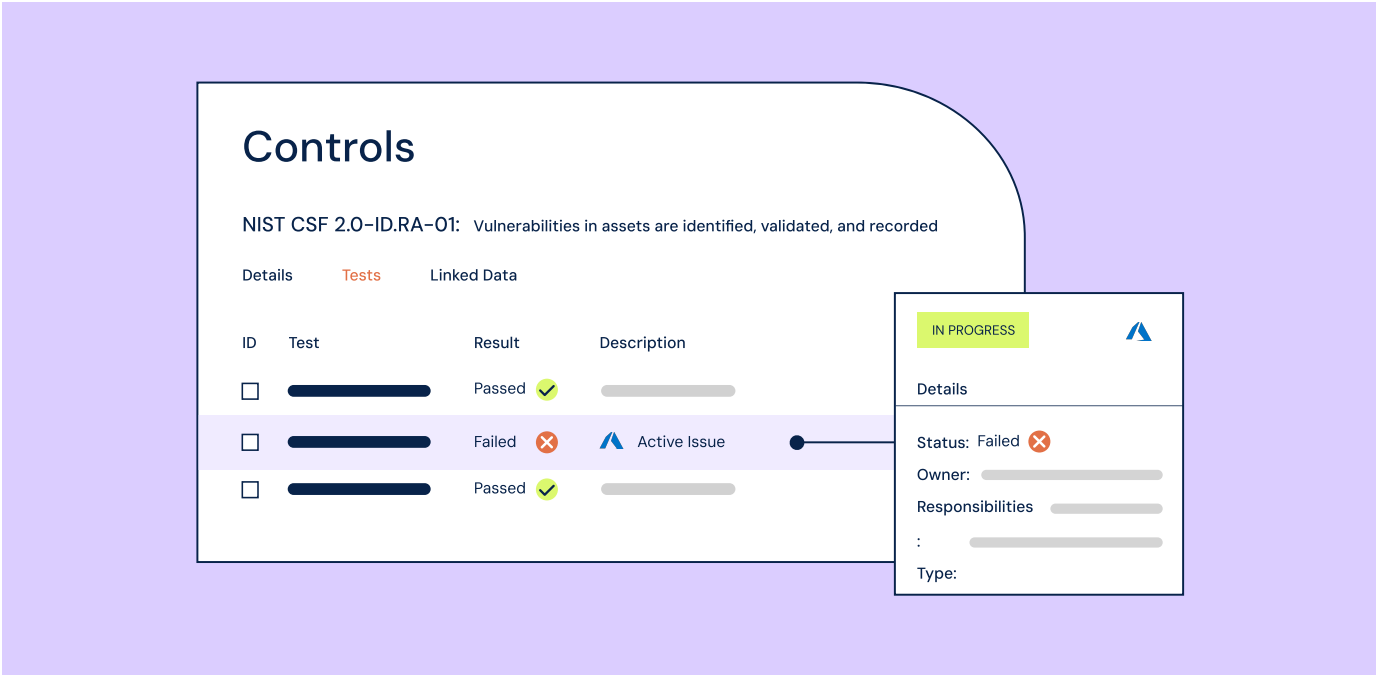
Belinda Edwards
Manager - Governance, Risk and Compliance, CyberCX
CyberCX

Watch the full webinar →

Step 4:
Continuously monitor and test your controls

After implementing controls, it's critical to ensure they're operating effectively over time. Monitoring should include detecting anomalies, identifying control failures, and tracking key risk indicators. Automating this process helps ensure timely detection and response to threats.

6clicks' Continuous Control Monitoring feature helps you with this step by enabling you to conduct automated tests to ensure that controls are operating optimally, providing real-time alerts on control performance and security issues. With automatic evidence collection, you can streamline control validation and support audit readiness with minimal manual overhead.



Its benefits are perfectly captured by one of our users:

> One of the fantastic new features of 6clicks is its ability to integrate with other systems to test technical controls and record whether they pass or fail. This is a huge advantage when it comes to audits—you can easily present evidence through the Trust Portal, showing that your controls are in place and directly linked to your risk management framework."

Belinda Edwards
Manager - Governance, Risk and Compliance, CyberCX
CyberCX

Watch the full webinar →

Step 5:
Perform internal assessments

Internal assessments are essential for validating that your cybersecurity program aligns with the NIST CSF and that your controls are functioning as intended. This step helps you measure progress, verify compliance, and identify areas for continuous improvement.

Fast-track the assessment process with 6clicks' ready-to-use NIST CSF assessment template. Evaluate security implementation across business units or systems and easily generate audit results that provide a clear view of your compliance status.

While NIST CSF does not require formal certification, organizations may choose to engage a third party for a readiness assessment or independent audit to strengthen stakeholder trust and validate their cybersecurity maturity.

Step 6:
Address gaps and maintain ongoing compliance

Cybersecurity isn't one-and-done—it evolves alongside your business, technology, and threat landscape. The final step in NIST CSF compliance is about closing identified gaps and ensuring your program stays aligned over time.

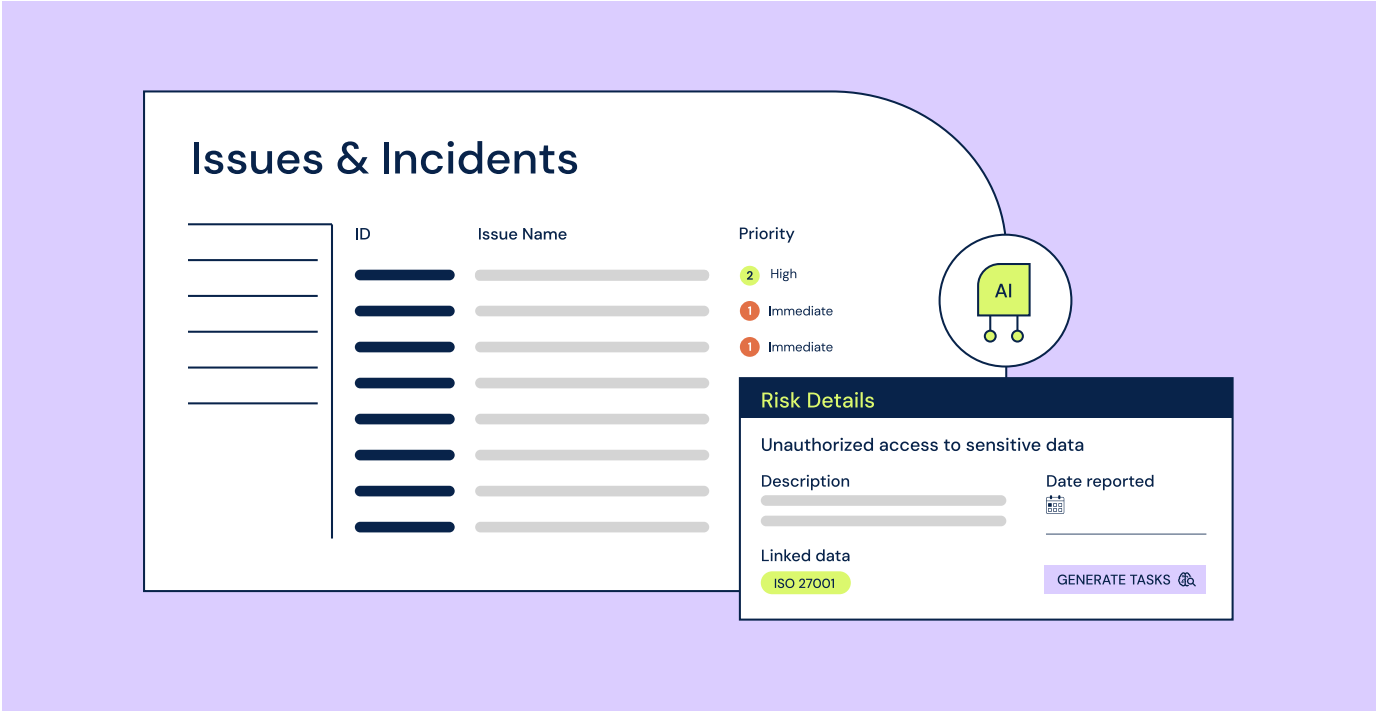
Start by reviewing your assessment results and mapping them to your Target Profile. This helps pinpoint which CSF outcomes are unmet and where controls need improvement. From there, build a prioritized action plan, which may involve:

- Updating or adding controls
- Enhancing documentation or policies
- Assigning responsibilities and training staff
- Improving monitoring and reporting

Maintaining compliance means going beyond remediation. Regularly reassess risks, monitor threats and control performance, and stay informed on regulatory updates.

With 6clicks' integrated issue and incident management feature, you can seamlessly kick off remediation efforts using built-in workflows, create and assign tasks, leverage advanced integrations to automate alerts and monitor resolution in real time, and generate progress reports —all from a centralized platform.

Hailey AI can now also generate tasks directly from issues, reducing manual effort and accelerating remediation.



By treating NIST CSF compliance as a living process, you'll build a program that's not only compliant—but adaptive and resilient.

07

Streamline NIST CSF **implementation with 6clicks**

Power your cybersecurity strategy with next-generation automation and intelligence. 6clicks gives you everything you need to operationalize the NIST Cybersecurity Framework—faster, smarter, and with greater visibility. From AI-driven control mapping to continuous monitoring and audit-ready reporting, it's the platform built to make compliance seamless.

Risk management: Identify, assess, and treat risks with a comprehensive risk register, rich reporting, and risk mapping to assets, controls, and other data across the platform.

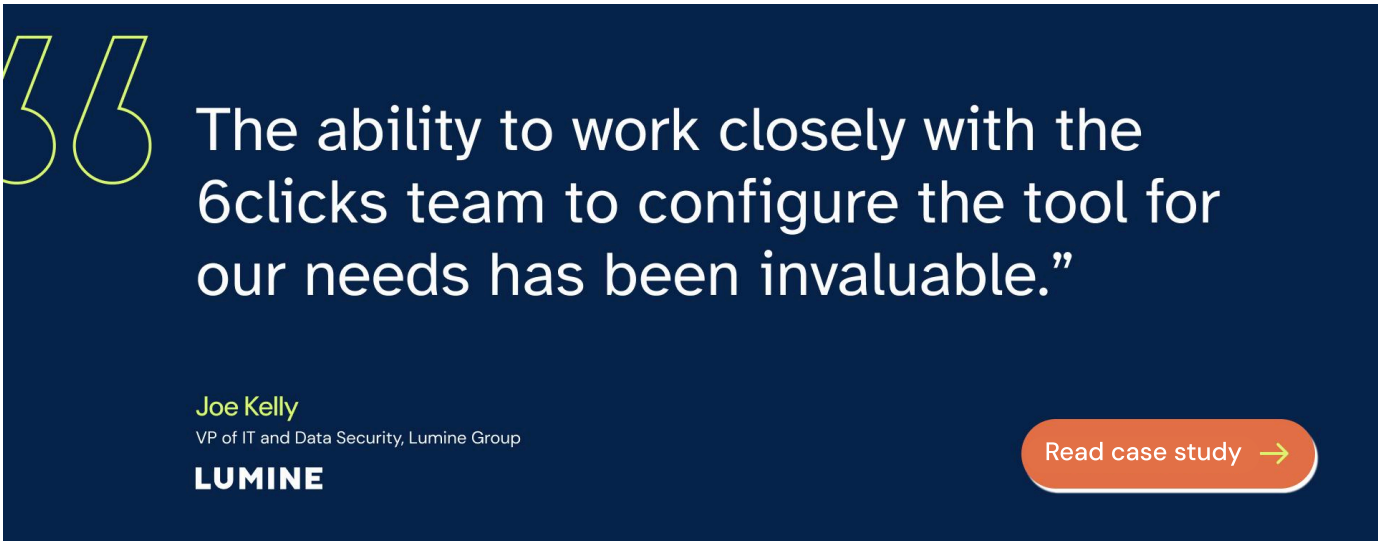
Third-party risk management: Manage all your vendors and suppliers in one place. Fast-track vendor security reviews and stay ahead of third-party threats with automated risk and issue identification.

AI-powered compliance automation: Instantly generate controls from your policies, map them to NIST CSF, and uncover gaps using Hailey AI.

Continuous control monitoring: Automate control testing and evidence collection, trigger real-time alerts, and validate ongoing control effectiveness.

Audit readiness: Use our NIST CSF assessment template to evaluate your controls and verify compliance. Accelerate the process with automated responses powered by Hailey AI.

Let 6clicks help you take control of your cybersecurity program—with a platform that adapts to your needs, backed by a team that's with you every step of the way:



Elevate your offerings with AI-powered NIST CSF compliance solutions

For cybersecurity advisors and managed service providers (MSPs), 6clicks equips you with cutting-edge tools to deliver efficient, scalable, and high-value NIST CSF assessment and compliance services to your clients.

With 6clicks, you can:

- Run NIST CSF assessments at scale using question-based assessment templates and automated workflows
- Manage multiple client environments from a single, multi-tenant interface
- Leverage AI to automate control mapping, gap analysis, and policy creation
- Offer remediation tracking and advisory follow-through from assessment to action
- Deliver branded reports and dashboards that showcase your expertise

Learn more about 6clicks

Book a demo

Ready to build resilient cyber GRC programs powered by AI? Explore the 6clicks platform today.

Book a demo

Join our partner program

Ready to grow your business with cutting-edge technology and expert support? The 6clicks Partner Program is designed to help advisors and MSPs expand their offerings, increase recurring revenue, and deliver world-class cyber GRC solutions at scale.

Unlock partner benefits

Explore helpful resources

Get access to the latest cybersecurity, risk, and compliance news and thought leadership by industry experts.

Read blog

6clicks

6clicks is transforming cyber risk and compliance management with its AI-powered platform, featuring the pioneering Hub & Spoke architecture tailored for federated businesses, advisors, and managed service providers (MSPs). As the first platform to introduce an AI engine specifically designed for GRC, 6clicks delivers a smarter approach to managing cyber risk and compliance. The 6clicks business model is channel-aligned, and SaaS licensing is transparent and straightforward with unlimited user access and access to frameworks. With sales and support operations presence across APAC, EMEA, and NA, and private cloud hosting options on Microsoft Azure, 6clicks equips cyber leaders and professionals to build resilient, trusted, and scalable cyber risk and compliance programs, disrupting traditional GRC solutions and setting a new standard in the industry.

Request a demo