ICS

WE SECURE IT

NIST CYBERSECURITY FRAMEWORK

IMPLEMENTATION OVERVIEW

PART OF

datef.lt

MOVE TOGETHER

WE SECURE IT

IMPLEMENTING A CYBERSERCURITY FRAMEWORK

When it comes to cybersecurity, today's businesses are confronted with a perfect storm: the threat landscape has grown in complexity, and people with the skillsets to navigate it are scarce.

Organizations are experiencing greater pressure to be accountable for the data in their care as data security rules throughout the world tighten – and stiffer fines for non-compliance. As a result, with more work than people to perform it, a **cybersecurity framework (CSF)** is no longer a nice-to-have – it's a **need.**

Implementing a cybersecurity framework has two major advantages:

1.) Security procedures have been formalized. Teams can concentrate on **repeatable procedures** to ensure that information is communicated and that individuals are focused on the appropriate topics.

2.) **Scalability** of security activities is possible. Teams may accomplish more when all members buy into the process, especially when resources are limited.

The United States' National Institute of Standards and Technology (NIST) developed the NIST CSF model to assist companies in assessing their security posture and implementing five functions.

ICS INDUSTRIAL CYBER SECURITY S.R.L.
Via Negrelli/Negrellistraße 13/B
I-Bolzano/Bozen 39100

T +39 0471/ 066 500 F +39 0471/ 066 501
M info@industrialcybersec.it
VAT/P.IVA IT02727560217

ICS INDUSTRIAL CYBER SECURITY S.R.L.
Via Negrelli/Negrellistraße 13/B
I-Bolzano/Bozen 39100

T +39 0471/ 066 500 F +39 0471/ 066 501
M info@industrialcybersec.it
VAT/P.IVA IT02727560217

WE SECURE IT

1° IDENTIFY

Cybersecurity was simple in the early days of the internet. IT teams were in charge of a few static assets that accessed data via firewalls, preventing illegal network access. The apps were huge, on-premises, and very uniform. They simply strengthened the network perimeter with access controls to protect data.

As digital work increasingly became web-based, IT lost control and risk shifted toward the end user. The NIST CSF "Identify" function includes a series of sub-categories to help organizations deal with this new world: asset management, business environment, governance, risk assessment, and risk management strategy.

Full visibility into technical & organizational environment and its risks & development of Risk Management

WE SECURE IT

1. ASSET MANAGEMENT

"The data, employees, equipment, and systems that enable companies to fulfill business goals are recognized and managed in accordance with their relative significance to goals and risk."

- NIST (National Institute of Standards and Technology) CSF

Asset management has evolved to include more than just inventorying devices. The National Institute of Standards and Technology (NIST) proposes a more intelligent, holistic approach that takes into account the business function connected with the IT resource. When you contemplate other assets in your company, such as a desk, you don't think of brackets, wood, or other materials. Rather, you create a scenario in which that resource is utilized.

2. BUSINESS ENVIRONMENT

"The organization's mission, objectives, stakeholders and activities are understood and prioritized and used to inform cybersecurity roles, responsibilities and risk management."

– NIST CSF

It's critical to comprehend the larger business environment in order to confidently identify resources. Perhaps you've recently completed a merger or acquisition. Perhaps you offer resources to contractors or your staff work from home. These contextual variations aid in a more in-depth examination of your existing cybersecurity posture.

3. GOVERNANCE

"The policies, procedures and processes to manage and monitor regulatory, legal, risk and operational requirements are understood and inform the management of cybersecurity risk."

– NIST CSF

When all of the controls, measurements, reporting variables, and regulatory requirements are removed, what's left is policy, or what's permitted. You may evaluate your present security measures against your standards if you have a thorough grasp of your organization's policies, processes, and regulatory needs. Some policies may need to be revised, while others may need to be eliminated. In any case, the evidence you need to finish your governance audit resides on your endpoints.

4. RISK ASSESSMENT

"The organization understands the cybersecurity risk to operations, organizational assets and individuals."

- *NIST CSF*

Without detailed understanding of your equipment, it's hard to correctly estimate risk. What are their weak points? On a daily basis, how are they used? What is the likely cost if a risk materializes? Vulnerable resource risks must be thoroughly evaluated, but with a broad view of the potential threats to the resource.

5. STRATEGY FOR RISK MANAGEMENT

"The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions."

– NIST CSF

A risk management plan is more than just a SWOT or roadmap. It all boils down to your objectives and how you intend to attain them using technology. You won't be able to create technological controls that fit with your goals and related risks unless you have a full grasp of your inherent risks and expenses.

WE SECURE IT

2° PROTECT

After establishing the Identify function, the attention may go to safeguarding devices, data, apps, and users. The NIST CSF divides the “Protect” function into four sub-categories: access control, awareness and training, data security, and protective technology.

Development & implementation of appropriate safeguards so as access control, training, policies and protective technology

9. ACCESS CONTROL

"Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions."

– NIST CSF

To protect data, we must be able to regulate how, when, to whom, and under what conditions we allow access. The management of the identities and credentials of individuals who have access to the data is the first step. Authentication approaches rely on trust, which you may earn by providing one or more of the following:

- Something you have (a smart card or token)
- Something you know (a password) (fingerprint or retinal scan)

Managing identities and credentials is critical, but context is also crucial. The NIST CSF mentions two access control contexts:

1. The physical context places the user in the same geographical location as the resource, requiring the 'trust but verify' approach to be used. Physical access restrictions are in place to prevent illegal access to devices, data, and apps.

2. Remote context is similar, only you employ bits and bytes to create a moat around your resources instead of matter.

10. AWARENESS AND TRAINING

"The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements."

– NIST CSF

Simulated phishing schemes can assist identify susceptible personnel, but they don't do much to educate them on cybersecurity concepts. The "Protect" feature requires a higher level of user awareness, which can only be achieved via thorough training. To ensure that each user knows security best practices and the particular security demands of their business, awareness campaigns might include video lessons, signage, policy reviews, and gamification. Training can be a joint effort between IT and HR, and it should be done on a regular basis, not only at employee onboarding.

11. DATA SECURITY

"Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."

– NIST CSF

There are two types of data that need to be safeguarded: data at rest and data in transit. Asset monitoring is a critical technique for safeguarding both. Assets should be managed throughout their entire lifespan, from initial security control installation and activation through ongoing monitoring and proper decommissioning at end-of-life. NIST questions our assumptions about data security, particularly the notion that encryption is sufficient.

12. PROTECTIVE TECHNOLOGY

"Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements."

– NIST CSF

People and processes are important, but they must be complemented by technology. NIST CSF suggests areas where protective technology can help:

Audits serve as a forcing mechanism to push toward greater compliance.

Logs give a clear picture of the current security posture.

Removable Media Security can be detected with asset management and examined for compliance.

Least Privilege policies can be exercised with access controls – role provisions, permissions, exfil restrictions, two-factor authentication, geofencing, and sensitive data discovery.

Gestalt Security – fortifying the network and communications channels – is achieved with WireShark, DPI, UCC, NGFW.

WE SECURE IT

3° DETECT

The NIST CSF Detect function is split into three sub-categories: anomalies and events, information security continuous monitoring, and detection processes.

Development & implementation of appropriate activities to identify a cybersecurity event

13. ANOMALITIES AND EVENTS

WE SECURE IT

"Anomalous activity is detected in a timely manner and the potential impact of events is understood."

– NIST CSF

Asset intelligence plays a critical role once a security event has been detected. What is the location of the device? Is there any other behavior (machine or human) going on at the same time? Is the current occurrence a breach of the security policy? What was going on with the gadget right before the event? What information is at risk? You may fulfill this role with asset intelligence, which is a deep understanding of the device, data, users, apps, and habits.

CONDITIONAL CYBER RISKS:	
• Corporate Network • Physical Environment • Mobile Assets • Endpoints	• User Activity • Business Apps • Corporate Data • Consumer/Customer Data
UNCONDITIONAL CYBER RISKS:	
• Malicious Code • External Service Provider • Out-of-Network Connections • Mobile/Access Point Code	• Unauthorized Hardware & Software • Unauthorized Users • Unauthorized Connections

14. INFORMATION SECURITY CONTINOUS MONITORING

"The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures."

– NIST CSF

Within the sub-goals of the "Detect" function, there are two types of variables:

• Under typical conditions, conditional variables will not cause cybersecurity events. Networks, physical environments, and employees are examples of these elements; they're all part of the organization's fabric and give demonstrable advantages when each has allowed access to data.

• Malicious code, unauthorized software, persons, connections, and devices, external service providers, and vulnerabilities are all threats to digital security, regardless of scenario. Unconditional variables should be systematically pulled out, whereas conditional variables should be subjected to a rigorous cost-benefit analysis.

15. DETECTION PROCESSES

"Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events."

– NIST CSF

Examine each component and analyze the gaps to maintain and test the effectiveness of any detection procedure. This method challenges preconceived notions about what it means to detect dangers. To begin, you must recognize that anomalies require a logical and secure baseline for any device. You can identify departures from what is standard, usual, or anticipated after these endpoints have been brought to a condition of immaculate cleanliness.

WE SECURE IT

4° RESPOND

Despite how rigorously you establish the Identify, Protect, and Detect functions, security breaches are always a risk. NIST CSF's "Respond" function outlines five sub-categories to help you respond in the event of an IT crisis: response planning, communications, analysis, mitigation, and improvements.

Development & implementation of appropriate activities to take action regarding to a detected cybersecurity event.

16. RESPONSE PLANNING

"Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events."

– NIST CSF

NIST assumes your business already has response planning processes in place and suggests evaluating them against five easy questions:

What could happen?

An honest assessment of your existing security posture identifies your vulnerabilities and assists you in determining what may go wrong and the measures you can take to reduce the harm.

What should happen?

Security policy is the foundation of all security, establishing what is and is not authorized.

What would happen?

Security modeling depicts what might occur in a given set of conditions. It isn't necessary for it to take place within sophisticated apps with better visuals. To show counterfactual circumstances and pinpoint significant elements, it might be as simple as brainstorming the impact of suggested policy changes.

What is happening?

To detect abnormal behaviors, security monitoring allows you to evaluate current events in the network, among devices, across IoT, and at the endpoint.

What did happen?

Security investigations give a database of prior incidents that may be used to determine the chance of a repeat occurrence.

Before sending a message in a security situation, there are three crucial questions to ask:

- **Is it correct?** Tell it how it is and speak the facts.
- **Is it beneficial?** Only give information that your stakeholders will find useful.
- **Is it absolutly necessary?** A security incident might be so dangerous that it must be reported to law enforcement.

17. ANALYSIS

"Analysis is conducted to ensure adequate response and support recovery activities."
– NIST CSF

Maintain a goal-oriented mindset when assessing what transpired. Leave the investigation to those with the time to look into the situation. Instead, utilize a reaction scenario with steps that lead to a quick recovery in your security modeling.

18. MITIGATION

"Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident."

– NIST CSF

Stop susceptible resources from spreading. Return to the NIST CSF's first two functions: Identify and safeguard. Isolate infected computers, disable communication, restrict port access, and lock an endpoint with a remote command after the possibility for growth has been identified. Because the attack surface is restricted to only the points of compromise, these steps reduce the negative consequences. Examine the present condition of the compromise and take action once you've been separated.

19. IMPROVEMENTS

"Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities."

– NIST CSF

Introspection helps you to test assumptions and apply factual and verifiable learning. This returns us to the beginning of the response planning process. If your security posture, policy, modeling, monitoring, or forensics are weak, you now have a new input. Operations become more nimble when the procedure is repeated.

WE SECURE IT

5° RECOVER

The last function, "Recover," encourages you to think about what happened and how you can use fresh information to enhance your people, processes, and technology for improved resilience. Plan, better identify, safeguard, detect, respond, and communicate are three sub-goals for the Recover function.

Development & implementation of appropriate activities for maintenance

and/or restoring of capabilities or services affected by a cybersecurity event.

20. PLANNING

"Recovery processes are executed and maintained to ensure restoration."
– NIST CSF

Processes must focus on recovering systems, data, access, applications, and people while planning for a breach. During a security incident, it might be tempting to trust your instincts. The Recover feature allows you to plan ahead of time so you don't have to respond in a panic.

Consider the following questions:
- Does this component of the strategy guarantee restoration?
- Does it increase the chances of a full (and quick) recovery?

As a result, you shift your focus away from prejudice and toward the objective of speedy repair.

21. IMPROVE IDENTIFY, PROTECT, DETECT, RESPOND

"Recovery planning is improved by incorporating lessons learned into future activities."

– NIST CSF

The second part of the Recover function is a call to enhance the other four disciplines – Identify, Protect, Detect, and Respond – by incorporating your new information into your cyber defenses and future incident recovery plans. It's at this moment that you should ask yourself the five key questions once more:

ICS

WE SECURE IT

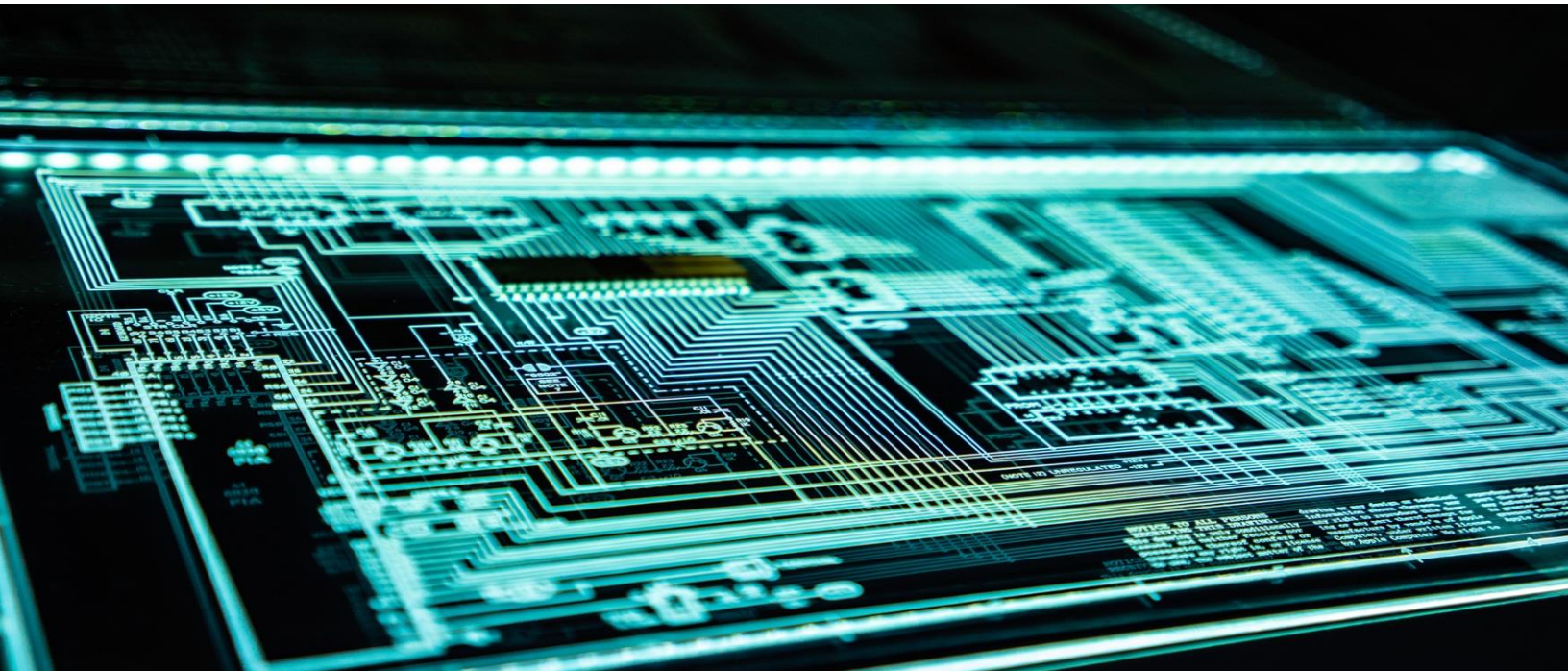
What could happen? -> **Security posture**

What should happen? -> **Security policy**

What would happen? -> **Security modeling**

What is happening? -> **Security monitoring**

What did happen? -> **Security investigations**

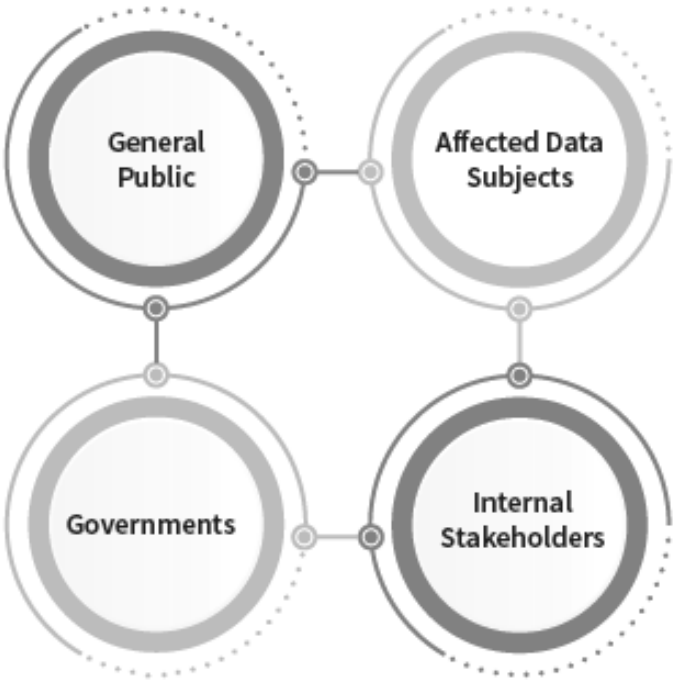


22. COMMUNICATION

"Restoration activities are coordinated with internal and external parties."

– NIST CSF

Finally, look for flaws in your conversations so you can convey information more successfully in the future. Information transmission is the purpose of communication. During your recovery, you must consider four categories of stakeholders: the general public, affected data subjects, governments, and internal stakeholders. Consistent, logically-flowing statements should be used. There's no point in pointing fingers, shifting blame, or competing for compassion. Be open and honest about the actions you're doing to reduce the chances of it happening again.



WE SECURE IT

CONCLUSION

Don't think of the NIST CSF as a major obstacle to overcome. Many of the functions are currently being performed by you and have been for many years. The framework essentially records your functions and procedures in order to codify, sustain, and grow your security practices. With a simple, repeatable approach built on the idea of doing the right things well, it also helps your resource-constrained teams operate more effectively and efficiently. You can provide world-class data protection for your business by building a framework around your team's talents, methods, and technology.

ICS INDUSTRIAL CYBER SECURITY S.R.L.
Via Negrelli/Negrellistraße 13/B
I-Bolzano/Bozen 39100

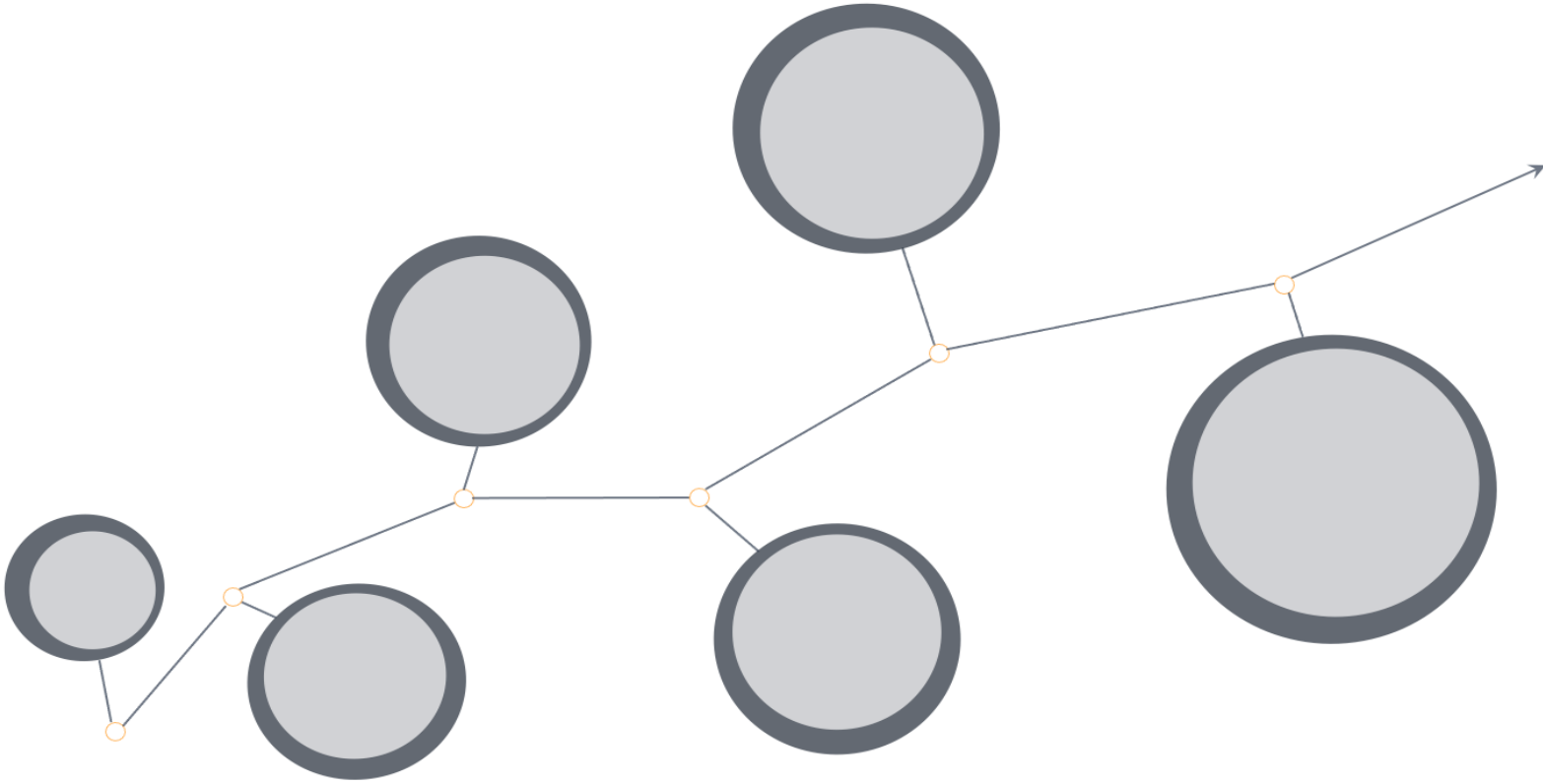
T +39 0471/ 066 500 F +39 0471/ 066 501
M info@industrialcybersec.it
VAT/P.IVA IT02727560217

WE SECURE IT

ABOUT ICS

Industrial Cyber Security is part of Datef Group and provides highly effective cybersecurity solutions that medium and large enterprises rely on. We provide our clients with targeted assessments, as well as technical, organizational, and cultural approaches to mitigate risks and attack surfaces, and optimize our clients' resources.

Our team includes experienced and highly qualified cybersecurity experts who provide our clients with effective cybersecurity strategies with a proven cost-benefit balance.



ICS INDUSTRIAL CYBER SECURITY S.R.L.
Via Negrelli/Negrellistraße 13/B
I-Bolzano/Bozen 39100

T +39 0471/ 066 500 F +39 0471/ 066 501
M info@industrialcybersec.it
VAT/P.IVA IT02727560217

28.07.2021

www.ics-secure.it