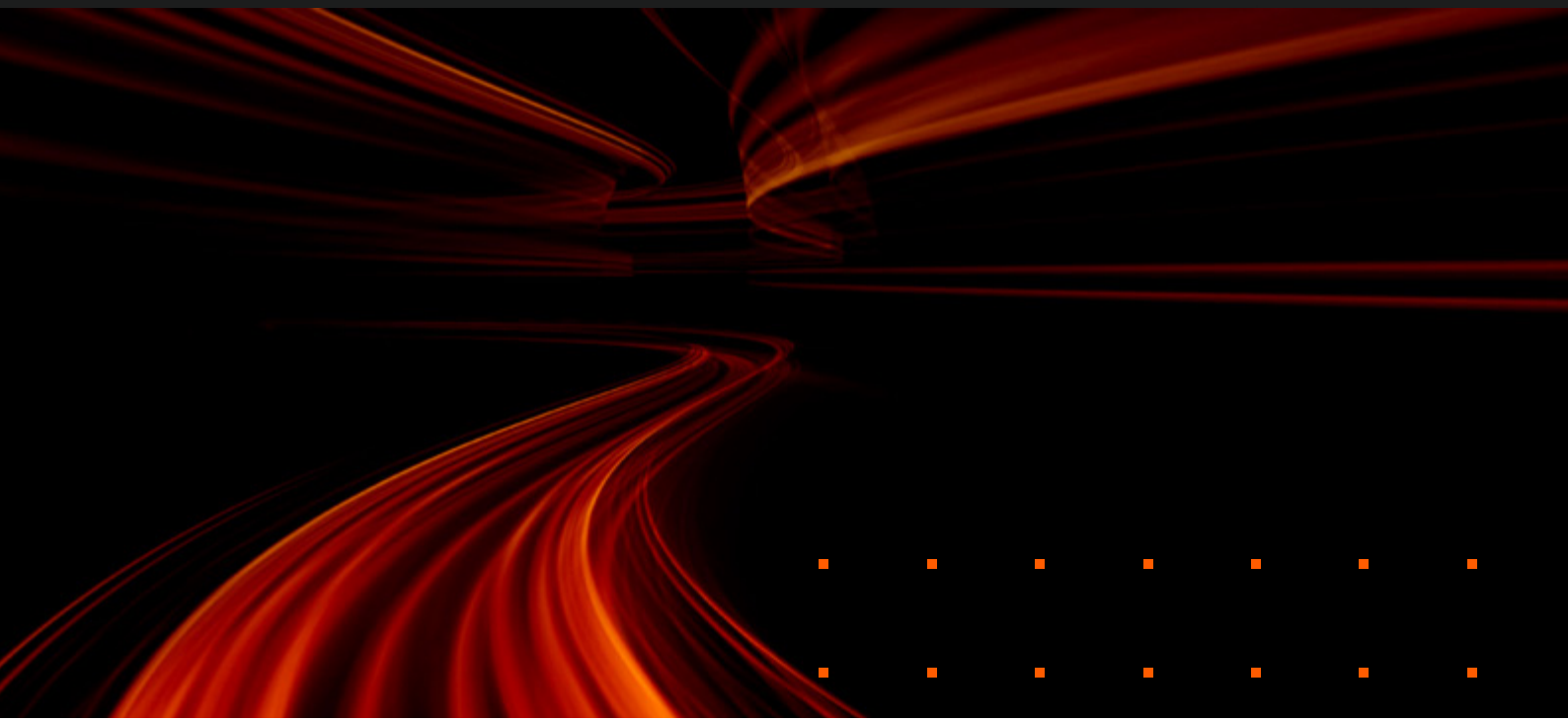
NIST CSF 1.1 Mapped to CIS 8.0

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0



Security frameworks help businesses prioritize the controls needed to protect customer information with federally mandated requirements. Security frameworks also help secure and protect critical infrastructure organizations from cyberattacks.

A security framework defines policies and procedures for establishing and maintaining security controls. Frameworks clarify processes used to protect an organization from security risks. They help information security, and IT security professionals keep their organization compliant and insulated from threats against its information resources and systems.

It can help save time by providing a clear structure for acting. With a framework, it is easier to map where the security journey will begin and help to identify gaps so it will be more precise, actionable conversations with stakeholders at the organization.

Contact Us

truesec.com
hello@truesec.com

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

Preface

Basically, CIS 8.0 security enhancement measures and NIST CSF 1.1 are similar. They are robust, flexible frameworks, providing guidance for creating a comprehensive strategy and finding a level of maturity for an organization's cybersecurity.

	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Identify	Little to no cybersecurity risk identfication.	Process for cybersecurity risk idenification exists, but it is immature.	Risk to IT assets are identified and managed in a standard, well defined process.	Risk to the business environment are identified and proactively monitored on a periodic basis.	Cybersecurity risks are continuosly monitored and icorporated into business decisions.
Protect	Asset protection is reactive and ad hoc.	Data protection mechanisms are implemented acreoss the environment.	Data is formally defined and protected in accordance with its classification.	The environment us proactively monitored via protective technologies.	Protection standards are operationalized through automation and advanced technologies.
Detect	Anomalies or events are not detected or not detected in a timely manner.	Anomaly detection is established through detection tools and monitioring procedures.	A baseline of "normal" activity is established and applied against tools/ procedures to better identify malicious activity.	Continuous monitoring program is established to detect threats in realtime.	Detection and monitoring solutions are continuously learning behaviours and adjusting detection capabilities.
Respond	The process for responding to incidents is reactive or non-existent	Analysis capabilities are applied consistently to incidents by Incident Response (IR) roles.	An IR Plan defines steps for incident preperation, analysis, containment, eradication, and post-incident.	Response times and impact of incidents are monitored and minimized.	The capabilities of all IT personnel, procedures, technologies are regularly tested and updated.
Recover	The process for recovering from incidents is reactive or non-existent	Resiliency and recovery capabilities are applied consistently to incidents impacting business operations.	A Continuity & Disaster Recovery Plan defines steps to continue critical functions and recover to normal operations.	Recovery times and impact of incidents are monitored and minimized.	The capabilities of all IT personnel, procedures, technologies are regularly tested and updated.

Figure 1: Cybersecurity Maturity

CIS tends to be more obligatory; NIST is more flexible, yet they are more alike than different. The benefits of CIS Controls 8.0's relationship to NIST CSF 1.1 occurs in three simple steps:

- Learning the CIS controls and their security measures, inside and out.
- Learning NIST CSF.
- Learning how they relate to each other.

Contact Us

truesec.com
hello@truesec.com

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

By developing a deep understanding of the needs of each system, it's easy to isolate how CIS can be used based on the categories in NIST CSF 1.1. There is a more comprehensive CIS 8.0, and in addition to that, there are specialized CIS, e.g., cloud, IoT, and OT.

What the CIS refers to as measures or safeguards more or less maps to what NIST refers to as categories or subcategories.

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Prodecures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	

A review of the two frameworks should be conducted. First, a review of the CIS is undertaken, followed by a review of NIST CSF.

The CIS provides a detailed account of what an organization should do to defend itself against cyber threats. Here is a brief introduction to the CIS critical security controls.

Keep in mind that this is only a basic introduction to the CIS controls and when there is an interest in implementing a robust cybersecurity architecture.

Contact Us

truesec.com
hello@truesec.com

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

Understanding CIS V.8 Security Enhancement Measures

Whether CIS security enhancement measures or another way is used to guide your cybersecurity security improvement program, you should realize “it’s not about the list.” It’s important to look for the ecosystem that will grow around the list.

- Where can training, supplementary information, and explanations be found?
- How have others implemented and used these recommendations?
- Is there a marketplace for supplier tools and services?
- How should progress or maturity be measured?
- How does this correspond to the countless regulatory and compliance frameworks that apply to the organization?

The true power of CIS security enhancement measures is not about creating the best list; it’s about leveraging a community to actually make a difference and contribute to security improvements. This is done by sharing ideas, tools, teaching, and joint action.

To simplify, CIS security enhancement areas of action will hereafter be described as security controls.

Each control area is then divided into protective measures, specifying methods and techniques to meet the established requirements.

Historically, CIS controls were handled consecutively to focus on cybersecurity activities, with a subset of the first six security checks called ”cyber hygiene.”

However, this turned out to be too simple. Organizations, definitely the smaller ones, may struggle with some of the early security measures and may never be able to implement the latter (e.g., have a backup strategy to help recover from ransomware). Consequently, beginning with Version 7.1, implementation groups (IG) were created, which should currently be seen as the new way to recommend security measures.

Implementation groups are there to help prioritize the implementation of the CIS.

Not all CIS checks are necessary for all organizations. Three different implementation groups have been developed. They specify the controls necessary to ensure that the necessary cybersecurity protection is in place. Another way is to use the implementation groups as a security maturity ladder to introduce the necessary security measures. This is to ensure that the business is not adversely affected.

Contact Us

truesec.com
hello@truesec.com

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

Explanation of Implementation Groups

Implementation Group (IG) 1 – Smaller organizations with modest IT and cybersecurity budgets must meet 56 safeguards, most of which are relatively simple.

Implementation Group (IG) 2 - Smaller organizations with moderate IT budgets must comply with all IG1 safeguards, plus 74 more complex ones. That's a total of 130.

Implementation Group (IG) 3 – Organizations with the most robust IT budgets must comply with all the above safeguards, plus 20 of the most onerous. That's a total of 153.

CIS reports the IG groups in each area in the following manner:

Safeguards Total	5	IG1	2/5	IG1	4/5	IG1	5/5

Contact Us

truesec.com
hello@truesec.com

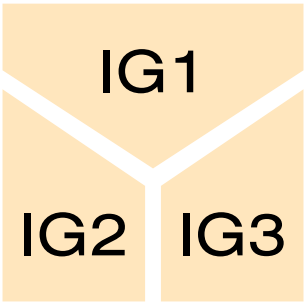
A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

Overall Description of CIS

Each CIS control in the CIS guide describes the following elements:

- Overview - A brief description of the intent of the safeguard and its usefulness as a defensive act.
- Why is this safeguard crucial? - A description of the importance of the safeguard, such as blocking, mitigating, or identifying attacks and explaining how attackers are actively exploiting the absence of this safeguard measure.
- Procedures and Tools - A more technical description of the processes and technologies enabling the implementation and automation of this safeguard.
- Description of Protective Measures. - A table of the specific measures to implement the safeguard.



If the organization meets IG1 safeguards, they meet the requirements for basic hygiene of cybersecurity.

CIS Controls

Basic hygiene for cybersecurity (IG1) consists of 56 safeguards of CIS security controls. In the next level, IG2, there are 130 safeguards, and in the most comprehensive level, IG3, there are 153 safeguards.

Each safeguard has received an add-on, which I call CIS functions. The CIS name is Security Functions and is Identify, Protect, Detect, Respond, and Recover, which can facilitate the strengthening of cybersecurity.

The security measures will be divided into groups of six safeguards to avoid too many impressions in the document.

The division is 1-6, 7-12, and 13-18.

Contact Us

truesec.com
hello@truesec.com

CIS Safeguards 1-6

1. Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all assets within the organization remotely and in cloud environments. This also applies to IoT and OT. It consists of 5 safeguards (2 for IG1; 4 for IG2).

2. Inventory and Control of Software

Actively manage (inventory, track, and correct) all software (OS, systems, and applications) on the network so that only authorized software is installed and can run, and others are prevented. It consists of 7 safeguards (3 for IG1; 6 for IG2).

3. Data Protection

Establish and maintain the data and information management process, inventory, and management throughout its lifecycle. It consists of 14 safeguards (6 for IG1;12 for IG2).

4. Secure Configuration of Enterprise Assets and Software

Establish and maintain a secure configuration process, including both software and hardware. It consists of 12 safeguards (7 for IG1;11 for IG2).

5. Account Management

Establish and maintain account management. It consists of 12 safeguards (4 for IG1; 6 for IG2).

6. Access Control Management

Assign and manage permissions to user account credentials, including administrator accounts and service accounts, to assets and software. It consists of 12 safeguards (4 for IG1; 6 for IG2).

A representative security measure for the basic level is 2.1, ”Establish and Maintain a Software Inventory,” which applies to all three IGs. It requires the organization to keep detailed records of all software approved for use.

To understand how complex and robust IG3 safeguards become, consider 2.7, ”Allowlist Authorized Scripts.”

CIS Safeguards 7-12

7. Continuous Vulnerability Management

Continuously evaluate and track vulnerabilities, using information from public and private sources. It shall be carried out on all assets within the infrastructure. It consists of 7 safeguards (4 for IG1; 7 for IG2).

8. Audit Log Management

Collect, warn, review, and preserve logs of events that can help detect, understand, or recover from an attack. It consists of 7 safeguards (3 for IG1;11 for IG2).

9. Email and Web Browser Protections

Improve the protection and detection of threats from emails and browsers, as these provide great opportunities for attackers to manipulate human behavior through direct engagement. It consists of 7 safeguards (2 for IG1; 6 for IG2).

10. Malware Defenses

Prevent or control the installation, propagation, and use of malicious software, code, or scripts on any asset. It consists of 7 safeguards (3 for IG1; 7 for IG2).

11. Data Recovery

Establish and maintain data recovery practices adequate to restore assets in scope to an earlier time and reliable mode. It consists of 5 safeguards (4 for IG1; 7 for IG2).

12. Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices. It consists of 8 safeguards (1 for IG1; 7 for IG2).

Examples are presented in a similar way to the previous group of safeguards. A representative protective measure for the basic level is the 7.1 ”Establish and Maintain a Vulnerability Management.” This is a process that applies to all three IGs. This requires that the organization can establish and maintain a documented vulnerability management process for the assets and that documentation is reviewed and updated.

To understand how complex and robust IG3 safeguards become, consider 12.8, ”Establish and Maintain Dedicated Computing Resources for All Administrative Work.“ Use dedicated computers, either physically or logically separated, for any administrative tasks or tasks that require administrative access.

CIS Security Controls 13-18

Here are the last safeguards in CIS security measures:

13. Network Monitoring and Defense

Establish and maintain processes and tools to establish and maintain comprehensive network monitoring and defense against security threats in the network infrastructure and users. It consists of 11 safeguards (0 for IG1; 6 for IG2).

14. Security Awareness and Skills Training

Collect, warn, review, and preserve logs of events that can help detect, understand, or recover from an attack. It consists of 7 safeguards (3 for IG1;11 for IG2).

15. Service Provider Management

Develop a process for evaluating service providers that hold sensitive data/information or are responsible for the organization's critical IT platforms or processes to ensure that those providers adequately protect those platforms and data/information. It consists of 11 safeguards (1 for IG1; 4 for IG2).

16. Application and Software Safeguards

Manage (prevent, detect, and remediate) the software security lifecycle, whether proprietary, accountable, or acquired. It consists of 11 safeguards (0 for IG1; 11 for IG2).

17. Incident Response Management

Develop, establish, and maintain an incident management program (e.g., policies, plans, procedures, defined roles, training, and communication). It is to prepare, detect and quickly respond to an attack. It consists of 11 safeguards (3 for IG1; 8 for IG2).

18. Penetration Testing

Test asset efficiency and resilience by identifying and exploiting weaknesses in introduced security controls (people, processes, and technology) and simulating an attacker. It consists of 11 safeguards (0 for IG1; 3 for IG2).

Examples are provided in a similar way to the previous group of safeguards. A representative protection measure for the basic level is 14.2," Train Workforce Members to Recognize Social Engineering Attacks." This process applies to all three IGs. Train employees to recognize "Social Engineering" attacks.

To understand how complex and robust IG3 safeguards become, consider 13.9 "Deploy Port-Level Access Control." Deploy port-level access control, such as 802.1x.

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

Understanding NIST CSF V1.1

The NIST CSF framework provides a common language and a systematic approach to managing cybersecurity risk. The framework is designed to complement, not replace, an organization's cybersecurity program and risk management processes.

The latest update to CSF Version 1.1 was published in April 2018. As with the previous versions, the current CSF is intended to provide general guidelines, complementing an organization's existing cybersecurity infrastructure.

Creating framework profiles allows organizations to identify areas where existing processes can be strengthened or where new processes can be implemented.

This means that, unlike CIS controls, which require methods/techniques, NIST CSF 1.1 does not impose such requirements.

NIST CSF consists of some important components:

- Core functions, CORE (analogous to CIS control levels).
- Implementation levels, TIERS (analogous to CIS implementation groups).
- Institutional profiles, PROFILE to customize an organization's implementation plan.

As with the CIS controls, the subsections below will first describe CSF's codified schedule and then briefly touch on how CIS can be applied to CSF controls.

Contact Us

truesec.com
hello@truesec.com

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

NIST Cybersecurity Framework: Core Functions

The overall component of CSF consists of core functions in which various security measures are organized.

There are five core functions divided into 23 categories of security measures, which are recommended for organizations to implement or map using other architecture methods (CIS, CSA, etc.).

Understanding these features is key to placing CIS controls and other cybersecurity architecture on them.

NIST functions are broken down as follows:

Identify

By understanding the landscape of your company's resources, network, environment, and overall risk profile, you set yourself up to adequately plan and implement protections. Included categories:

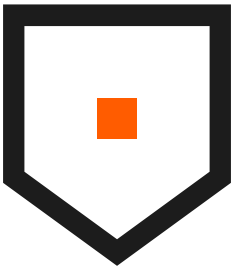
- ID.AM: Identify asset management
- ID.BE: Identify the business environment
- ID.GV: Identify governance methods
- ID.RA: Identify risk assessment measures
- ID.RM: Identify overall risk management
- ID.SC: Identify risk management in the supply chain

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

Protect

Specifies the specific areas that most need to be protected and how they should be protected. This feature is undoubtedly the most important of all. Included categories:



- PR.AC: Protect access with identification
- PR.AT: Strengthen employee awareness through training
- PR.DS: Ensure data security/information security
- PR.IP: Protect sensitive information
- PR.MA: Maintain protection routinely
- PR.PT: Management of protective technology

Detect

Details the different monitoring and evaluation protocols needed for implementation. That's to identify cybersecurity events as they happen and adequately respond to and recover from them. Included categories:

- DE.AE: Detect anomalous cybersecurity events
- DE.CM: Continuous monitoring
- DE.DP: Maintain ongoing detection protocols

Contact Us

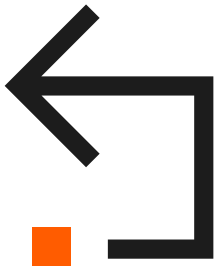
truesec.com
hello@truesec.com

A Truesec guide

NIST CSF 1.1 Mapped to CIS 8.0

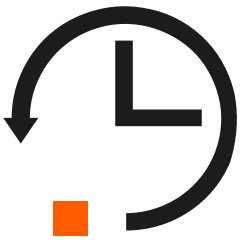
Response

Immediately respond to breaches and other cybersecurity events and limit or eliminate the attacker's access to systems and resources, thus setting the stage for recovery. Included categories:



- RS.RP: Planning and management for response and countermeasures
- RS.CO: Communicate before, during, and after response and countermeasures
- RS.AN: Analyze the effects of events and actions
- RS.MI: Limit the risks and consequences of incidents
- RS.IM: Constantly improve countermeasures

Recover



Restoring control of systems and restoring resources and services to their previous pre-attack conditions. Included categories:

- RC.RP: Recovery practice planning
- RC.IM: Improved recovery plan through evaluation
- RC.CO: Communicates before, during, and after recovery

Contact Us

truesec.com
hello@truesec.com

NIST CSF 1.1 Mapped to CIS 8.0

In this system of functions and categories, there is an additional level: subcategories of individual security measures or methods, of which there are 108.

For example, Subcategory ID.BE-3 indicates that an organization's organizational priorities are communicated.

In the most basic mapping between the different frameworks, it looks something like this:

CIS	NIST
Security functions	Functions
Controls	Categories
Safeguard	Subcategories
Implementing Groups (IG)	Tiers
Asset groups	-

The mapping is as simple as tracking the specific methods managed in the CIS and finding a corresponding subcategory in the NIST schema.

For example, the security measure in CIS Control 14 (Security Awareness and Training) maps more or less directly to subcategories within PR.AT.

Contact Us

truesec.com
hello@truesec.com

NIST CSF 1.1 Mapped to CIS 8.0

NIST Cybersecurity Framework: Implementation Tiers

As mentioned earlier, an additional layer of mapping is dependent on a form of distributed implementation.

NIST CSF 1.1 is grouped into tiers like the CIS implementation groups described above. However, its incremental implementation matrix is less defined than CIS, with three different maturity levels.

In this review, a fifth level is also added, which is more linked to cybersecurity maturity than the other four, which are more execution levels.

Instead of marking subcategories by level, NIST's corresponds to the levels of implementation that an organization seeks based on its overall risk appetite and operational risks.

Each tier presents the level of implementation that needs to be carried out based on the results of selected and desirable security needs.

NIST levels and overall security needs in each:

Tier 1 - Partial

With informal cybersecurity approaches, including ad-hoc and reactive (rather than proactive) risk management, limited integration of cybersecurity practices throughout the organization, and a poor understanding of the IT environment.

Tier 2 - Risk-Informed

With more uniform and formal risk management processes (guidelines and procedures) and a greater organization-wide understanding of and commitment to cybersecurity, both internally and in the larger digital ecosystem.

Tier 3 - Repeatable

Formalized risk management and general cyber defense practices are common throughout the organization, and there is a sense of responsibility and willingness to contribute to the broader cybersecurity environment.

Contact Us

truesec.com
hello@truesec.com

NIST CSF 1.1 Mapped to CIS 8.0

Tier 4 - Adaptive

Robust and proactive risk assessment and management methods that adapt to upcoming threats as they occur; the organization's cyber protection is fully integrated into business practices, and it contributes strongly to the security ecosystem.

Tier 5 - Optimized

There is an integrated risk management program, developed processes (policies, procedures, etc.), resources, and a comprehensive and uniform approach used across the organization. It is based on the changes that the organization is subjected to. Lessons learned (internal and external) from events and information threats, vulnerabilities, etc. Cybersecurity is thus proactively improved.

The organization adapts its cybersecurity methods based on past and present cybersecurity activities. This also applies to the use of predictive (KPI/KRI) indicators.

Note: This is a level that existed before in NIST.

More importantly, unlike CIS, the levels in NIST CSF are not only a measure of maturity but of what security measures must be taken based on the organization's internal and external requirements. Organizations are encouraged to move towards Levels 4 and 5, but it is an optional decision.

Depending on the nature and resources of the organization, it may choose to remain at a lower level if its security needs are met there.

Generally speaking, CIS implementation groups map NIST's implementation levels quite intuitively. For example, controls for CIS Group 1 are relative basic hygiene, which can be loosely mapped against NIS Level 1. As organizations mature in CIS Groups 2 and 3, their infrastructure approaches NIST Levels 3 and 4. Ultimately, one can be mapped against the levels based on how one sees it as appropriate.

Contact Us

truesec.com
hello@truesec.com

Get In Touch

truesec.com/contact

Summary

Insufficient security is no longer just a technical challenge but a business problem. Security must permeate everything that is done in the business.

This document aims to help organizations find a tool to obtain a measurable result and, based on it, develop balanced measures to ensure that the current cybersecurity maturity is improved. This should be an excellent basis for preparing steering documents, routines, and technical security measures.

It also provides an easier way to develop areas that need to be prioritized based on risk value and steps to take for a safer business. Using any of the frameworks that will be reported, what advantages and disadvantages they hold will provide business benefits against organizations that do not build their security on them.

Here are five benefits of using a security framework:

1. It can help save you time by providing a clear structure for acting.
2. Most content in a framework is universally applicable.
3. You can learn from the collective consensus-based guidance and experiences of a community that contributed to the framework.
4. In interpreting security needs across the company.
5. Finally, a framework can be a valuable tool to explain in a common language what you are doing in security to even the non-security-versed people in the organization.

About Truesec

As a global cybersecurity company, we're proud to be at the forefront of protecting organizations and our society against cyber threats. Our purpose has been clear since day one: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact.

Our team consists of cyber specialists covering the full spectrum of cybersecurity, each of us contributing with our unique expertise, willingness to make a difference, and a genuine wish to help. We never cease to challenge and reinvent ourselves to stay ahead of cybercriminals and find the best solution for you.

Contact Us

truesec.com
hello@truesec.com