Medicon Engineering Themes
Volume 2 Issue 3 March 2022
Review Article

Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security

Erfan Koza*

University of Applied Sciences Niederrhein, Moenchengladbach, Germany

***Corresponding Author:** Erfan Koza, University of Applied Sciences Niederrhein, Moenchengladbach, Germany.

Received: January 31, 2022; **Published:** February 28, 2022

Abstract

Assessing risks and vulnerabilities in the multilayered context of a critical infrastructure is a challenge. A wealth of methods, standards, and frameworks can be used to tackle this task. However, to achieve successful results in incident response management, to apply only theoretically and technically rigorous methods is far from sufficient. Critical to achieving the desired results is how a method, framework, or standard is implemented in practice. This paper compares two independent international standards (ISO/IEC 27 K family, especially ISO/IEC 27001 and NIST Cyber Security Framework) in a semantic analysis aimed at achieving general information security objectives in critical infrastructure. The methods and structures specified in the two processes are analyzed so that it can be determined what common as well as specific challenges exist in performing strategic and operational tasks to identify and address vulnerabilities.

Keywords: ISO 27001; Critical Infrastructure; NIST CSF; Information Security Management System

Introduction

According to the interpretation of its holistic approach, information security consists of three interactive and coherent elements: IT security, organizational security, and human factors, whose interplay is propagated in a variety of differentiated models. The interplay of these three features trivially leads to the interpretation that an appropriate level of information security can only be achieved if all three factors are planned and executed in a complementary manner [1]. The recent growth of cyber-crime and the associated risks are forcing most companies and especially critical infrastructure to pay more attention to information security. A breach of the basic values of information security (availability, integrity, and confidentiality) can, especially for critical infrastructure, sometimes lead to an interruption in the security of supply in the sense of the provision of necessities and ensure that, for example, the energy supply, water supply or stationary supply of the population is no longer guaranteed. In addition to economic and monetary damage, such attacks can lead to reputational damage and, much worse, danger to life and limbs. The damage can also have an intersectoral impact on downstream processes or industries. Such influences, the so-called domino effect or cascade effect, occur when, for example, a critical technical infrastructure such as energy supply is affected, whose intersectoral dependencies or interdependencies can be related to the downstream processes in health care, telecommunications, water supply, sanitation, and finance, which ultimately to a widespread collapse of many parts of society can lead [2].

The work presented in this paper is based on an ontological review of existing international information security practices and standards using semantic analysis. The paper presents a summary of two complementary and holistic practices, as well as the presentation of their technical similarities and differences.

The essential goal of this paper is to compare two practices commonly used in practice to identify commonalities and distinctions, so that a statement can be made about what challenges may exist in the operational and strategic implementation of these standards in practice and how these can be efficiently addressed. These practice-oriented suggestions for combining these two standards are consolidated as a professional conclusion from the analysis.

Methodology

The results of the present work are based on two independent security engineering procedures in the field of information security developed and published by two different international institutes, ISO/IEC (based on the earlier results of British Standards) and the National Institute of Standards and Technology (NIST). In this context, semantic content analysis follows a predefined scheme. The definition of the scheme should also serve in the further course to make the results from the two security-related procedures comparable with each other. For this purpose, the history, structure (main framework with the content requirements), quantification of the requirements, referencing scheme, implementation methodology, focused approach, and the conceived target group are recorded and executed individually.

Based on the crystallized results from the content analysis, the commonalities (common intersection of the methods as consistency of the two methods) as well as their differences (ambiguity) are defined and determined. From this, possible conclusions can ultimately be derived about the common as well as specific challenges exist in performing strategic and operational tasks to identify and address vulnerabilities (Fig. 1).

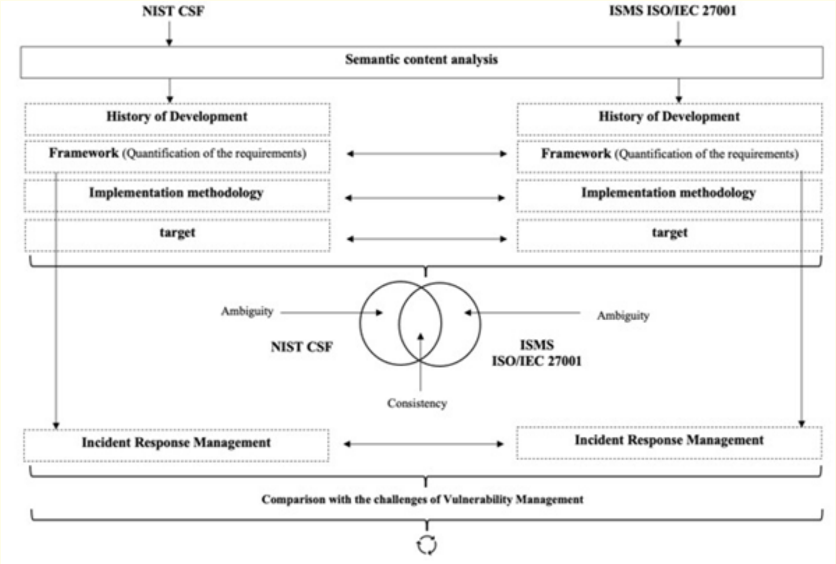
NIST CSF
ISMS ISO/IEC 27001
Semantic content analysis
History of Development
Framework (Quantification of the requirements)
Implementation methodology
target
History of Development
Framework (Quantification of the requirements)
Implementation methodology
target
Ambiguity
Ambiguity
NIST CSF
ISMS
ISO/IEC 27001
Consistency
Incident Response Management
Incident Response Management
Comparison with the challenges of Vulnerability Management

Figure 1: Method Construction.

Results and Discussion

This holistic approach is declared and set up worldwide with differentiated methodological approaches. These include, for example, the implementation and auditing of an ISMS based on ISO/IEC 27001 [3] and implementation based on the Cybersecurity Framework (NIST CSF) [4] to declare the requirements arising from the triangulation of information security and to underpin these with the associated code of practice. The listed security engineering procedures use differentiated frameworks to ensure procedural continuity and procedural dynamics. In the following sections, the results of the content analysis are presented.

The ISMS based on ISO/IEC 27001 draws on the idea of continuous improvement from ISO/IEC 9000 [5] and implements the Plan-Do-Check-Act-Cycle (PDCA-Cycle) (Deming quality assurance model). ISO/IEC 27001 is an integral part of the ISO/IEC 27000 series of standards and defines the requirements for an ISMS and is used in this context as the normative basis for the implementation and certification processes. The 27000 series of standards [6] have been published in a collaborative effort between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The core content of ISO/IEC 27001 is based on the previous work of British Standard 7799 by British Standards Institution (BS 7799 Part2). The defined phases with the associated clauses in ISO/IEC 27001 interact in a framework, that is provided based on ISO 9000 in all norms of the ISO standard as an idea for continuous improvement. In relation to aspects of information security the implementation and ongoing operation of the ISMS are understood as an iterative and incremental process in analogous to digitization. As a result, ISMS must be implemented with the ability to monitor and optimize itself on an ongoing basis. In this context, the conceptual approach from project management is applied to aspects of an ISMS. One of the most important aspects in this consideration is the PDCA-Cycle. Planning is primarily about the mental anticipation of upcoming processes.

In this process, success-oriented options and organization and communication structure for action are defined (defining the ISMS) based on the defined goals (what is the goal of the management system? Guaranteeing and maintaining an appropriate level of information security), which are implemented in a subsequent process? (Implementing and executing the ISMS), monitored (monitoring and auditing the ISMS) and, in the event of deviations, corrected with control measures (maintain and improve the ISMS), so that the defined target state can be achieved in the intended quality and quantity.

The overarching management structure is defined by the common structure of the ISO/IEC standards as the high-level structure of the ISO standards (ISO 9001, ISO 14000, ISO 45001, ISO/IEC 2000-1, ISO 22000, ISO 22301, ISO 28000) and is defined in terms of Integrated Management System (IMS).

As organizations increasingly manage multiple compliance frameworks simultaneously, it makes sense to implement an integrated management system due to increased efficiency (avoiding redundancy and duplication of effort). An IMS is a management system that integrates all components of an enterprise into a unified system to enable the achievement of defined objectives in a resource-efficient manner. Before going into more detail on the content structure of ISO/IEC 27001, reference is made to the 27 K family for a better understanding. The 27 K family can be structurally divided into four sections.

The first section of structural organization of the 27 K series of standards begins with ISO/IEC 27000 [6], in which relevant terminology and definitions are described in the form of a glossary. This is used as a terminological basis, for example, to enable uniform language among system users. The main advantage of ISO/IEC 27000 is its simplified form of the terminology, which can be used for a better understanding among users. The second section includes the (implementation instructions) guides (ISO/IEC 27002 to ISO/IEC 27005) used to operationalize the ISMS. The third section contains the generally applicable and industry-independent standards and main frameworks, which thematize the requirements for both ISMS implementation and for ISMS auditing. The third section contains the sub-standards (ISO/IEC 27010 to ISO/IEC 27019, except for ISO/IEC 27799)), which are essentially defined as sector-specific security standards. The fourth section includes the series of standards ISO/IEC 27030 to ISO/IEC 27044, which deal as sub-standards with security-related areas of information security (Fig. 2).

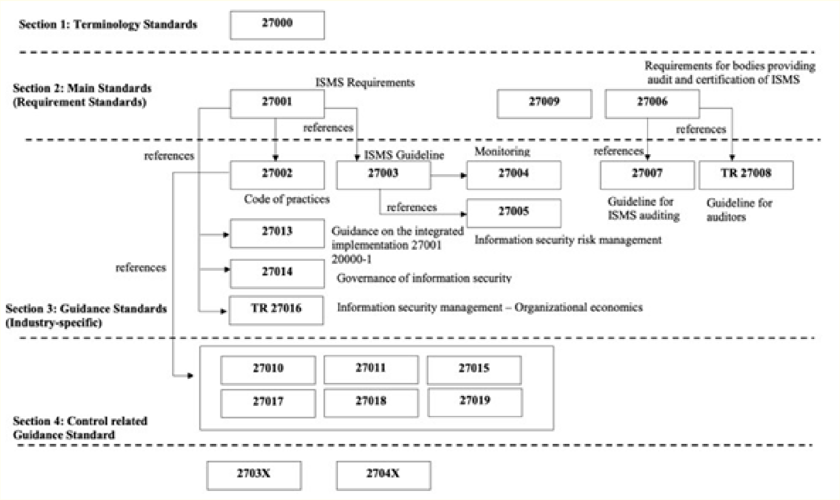
Section 1: Terminology Standards
27000
Section 2: Main Standards (Requirement Standards)
ISMS Requirements
27001
27009
Requirements for bodies providing audit and certification of ISMS
27006
references
references
references
ISMS Guideline
Monitoring
references
27002
27003
27004
27007
TR 27008
Code of practices
references
27005
Guideline for ISMS auditing
Guideline for auditors
27013
Guidance on the integrated implementation 27001 20000-1
Information security risk management
references
27014
Governance of information security
Section 3: Guidance Standards (Industry-specific)
TR 27016
Information security management – Organizational economics
27010
27011
27015
27017
27018
27019
Section 4: Control related Guidance Standard
2703X
2704X

Figure 2: Interrelationship of 27 K family.

In conclusion, the four sections can be described as follows [3]:

Section 1: Conceptual standard

Section 2: Standards that specify requirements, Section

3: Standards describing general guidelines,

Section 4: Standards describing sector-specific guidelines.

The content structure of ISO/IEC 27001 as a normative standard consists of two parts, with the first part covering the overarching requirements of a management system with the main clause (Table 1).

PDCA-Cycle Assignment	*Clause (Sub clause)*
Plan	Clause 4: Context of the Organization (4.1 / 4.2 / 4.3 / 4.4)
Plan	Clause 5: Leadership and Commitment (5.1 / 5.2 / 5.3
Plan	Clause 6: Planning (6.1 / 6.2)
Plan	Clause 7: Support (7.1 / 7.2 / 7.3 / 7.4 / 7.5)
DO	Clause 8: Operation (8.1 / 8.2 / 8.3)
Check	Clause 9: Performance Evaluation (9.1 / 9.2 / 9.3)
Act	Clause10: Improvement (10.1 / 10.2)

Table 1: ISO/IEC 27001 Structure.

In detail, clause 4 to 10 define 23 requirements for the ISMS. Table 1 lists the assignment of the ISO/IEC structure to the individual phases of the PDCA cycle [3]. In clause 4 "Context of the Organization" following a top-down methodology, the relevant internal and external topics are analyzed and included in the ISMS scope. The intention of the scope is to define and delimit company values that are to be protected with the help of the management system. The scope describes the area of application of the ISMS. An established procedure is to first identify the critical business processes to be protected using a top-down approach. The individual information objects that are processed in these business processes can then be derived from this. Once the information is known, the applications, systems, media, infrastructure, and buildings used to process this information can be inferred. Figure 3 shows the relationship between individual corporate assets. The insights gained here also form the basis for the conception of asset management. As a rule, all persons and associated organizational units that are necessary to enable information processing also lie within this scope. In addition, there may be external services that are used, and interfaces to areas outside the scope that also need to be identified.

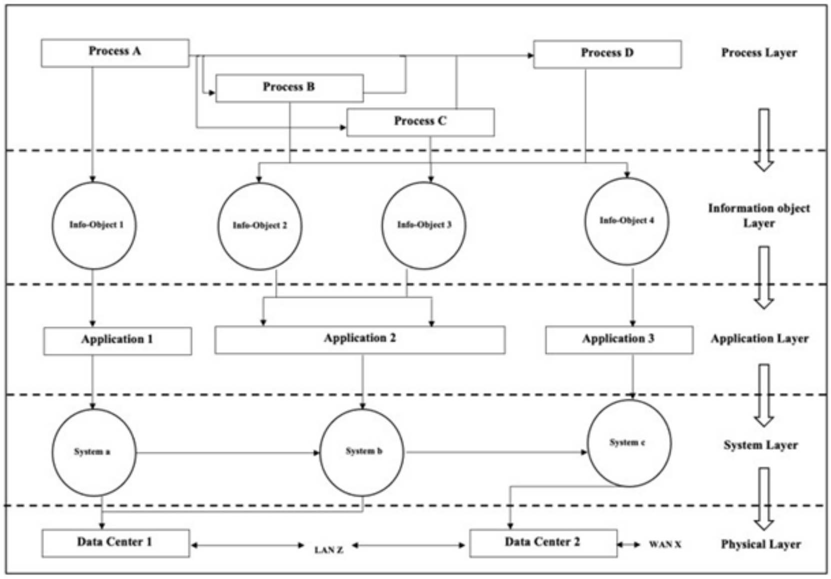

Figure 3: Scoping process.

The inventory of assets is conducted within asset management. Ensuring and maintaining information security is an interactive and incremental task, the successful achievement of which depends on the human and financial resources required. The embedding of management as the responsible authority reflects this characteristic and should consequently serve as a stimulus for achieving an adequate security culture. In addition to the announcement of an overall information security strategy, goals, objectives, roles and responsibilities, methods for the continuous improvement and for support the other strategic decision-makers must also be defined. These units are addressed and outlined in clause 5. This next step of the implementation process in clause 6 focuses on risk management. To this end, the scope defined in clause 4 must be integrated into the risk management process and analyzed in terms of hazards specific to the company. This process is divided into three sub-steps: Information security risk assessment, information security risk treatment and information security monitoring (ongoing monitoring and risk communication) - For the development of a relevant risk management strategy with its operationalization, ISO/IEC 27001 refers to ISO/IEC 27005. ISO/IEC 27005 [7] provides guidance for information security risk management.

The approach described supports the general concepts defined in ISO/IEC 27001. It provides guidance for implementing a risk management approach that supports the implementation of and complies with the information security risk management requirements of ISO/IEC 27001. The measures to be derived from the risk management procedure must be supplemented by the controls in Annex A.

Annex A of ISO/IEC 27001 defines the technical, organizational, and individual requirements, which are declared with 114 controls in 13 separate sections. The requirements from Annex A can ultimately be operationalized and implemented by the guideline standard ISO/IEC 27002 "Code of practices".

Therefore ISO/IEC 27002 [8] provides a list of generally accepted measurement objectives and proven measures as guidance for selecting and implementing measures to achieve information security. The purpose of ISO/IEC 27002 is to provide guidance for the implementation of information security measures. Clauses 5 to 18 provide specific advice and guidance on best practices for implementing the measures set out in ISO/IEC 27001, controls A.5 to A.18 (Table 2).

Annex A	***Description***
A.5	Information Security Policies
A.6	Organization of Security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operation security
A.13	Communication security
A.14	System acquisition, development, and maintenance
A.15	Supplier relationship
A.16	Information security incident management
A.17	Information security aspects of business continuity management.
A.18	Compliance

Table 2: Annex A of ISO/IEC 27001 [3].

Based on the overall information security strategy defined in control A. 5 and the defined ISMS objectives, the necessary resources in the form of competencies must be procured in control A.7. This usually involves the integration of a chief information security officer as the central strategic and operational authority for the ISMS, who is responsible not only for the initial implementation but also for the ongoing operation of the ISMS. In addition, the overall strategy is known to all employees through the publication of the information security policy. In this way, every employee is committed to maintaining information security and is made aware that the information security is a collective task in the sense of the holistic approach.

In addition, procedures for managing documents and records are integrated and regular communication structures are defined and established. In control A. 8, the defined plans from control A. 6 are operationalized, repeated, and executed at regular intervals. Many guidelines, procedural instructions, and work instructions must be defined as a documentary and made available to employees for the purpose of knowledge management and as a source of information [3]. In addition, existing security gaps must be closed or optimized in terms of processes. Furthermore, the employees must also be trained and sensitized in the individual general and dedicated areas. The objective of this phase is to ensure that the defined strategic and operational guidelines are passed on to employees in the First Line of Defense so that they can behave in a manner that is compliant with information security. In control 9, individual monitoring units must determine both the individual correct implementation of the defined policy and measures and the effectiveness of the overall ISMS.

The operational review of compliance with the individual policies can be carried out on a random basis by the CIO (e.g., office tour to check compliance with the clean desk policy). However, the effectiveness of ISMS must be analyzed using analytical procedures such as the generation of KPIs. For this purpose, ISO/IEC 27001 refers to ISO/IEC 27004 to enable meaningful methods for integrating and generating KPIs. ISO/IEC 27004 [9] provides guidance and direction for developing and applying measures to evaluate the effectiveness of ISMS, measure objectives, and measures for implementing and manage information security in accordance with ISO/IEC 27001. The purpose of ISO/IEC 27004 is to provide a framework for measurement that enables the effectiveness of ISMS to be assessed in accordance with ISO/IEC 27001. In addition, clause 9 (Table 1) specifies the requirements for internal audits. The internal audit must be carried out by a third party, impartially and independently (e.g., via externally commissioned auditors or internal auditors, provided they are not part of the ISMS project) to ensure the objectivity and validity of the audit.

From the internal audit, the own findings are defined (recommendations and deviations), which must be eliminated and optimized during the continuous improvement processes. The internal audit thus serves as a quality assurance instrument that is used to achieve the defined objectives from control A. 5. These findings are integrated into the management review. The final decision on how to deal with the findings is made by management.

The deviations from the internal audit must be analyzed by root cause analysis for their origins and reasons why these deviations occurred. The idea here is to find common deficits from the analysis results as an intersection, which can possibly be regarded as a single point of failure about the ISMS. Thus, not all deviations have to be revised, but possibly the origin. In this way, an efficient procedure can ultimately be developed, which saves resources and time. If the deviations can be traced back to different sources and causes, these must be eliminated and optimized individually and one by one. This phase reflects the idea of continuous improvement and represents the self-improving capability of a management system, which must constantly be able to adapt to the modified internal and external environment in a flexible, dynamic, and efficient manner.

For adequate implementation, ISO/IEC 27001 refers to other series of standards, such as ISO/IEC 27002 for implementation guidance and ISO/IEC 27005 for risk management. While the requirements in clauses 4 to 10 in the first part must be met in full, the controls of ISO/IEC 27001 as state of the art must first be projected onto the ISMS-Scope and restrictive ones must be proactively excluded in a separate procedural step, in the Statement of Applicability (SoA). This gives companies the opportunity to define an individual scope of controls (if not specified by the legislator) and to project the requirements of ISO/IEC 27001 onto their core processes with high criticality. This also allows companies to select a dedicated scope, e.g., the OT network for power supply. ISO/IEC27001 also can be used to determine information security topics by any organization. This provides the option of identifying and integrating the topics according to the holistic approach and to extend them with industry-specific standards (e.g., ISO/IEC TR 27019 "power supply control systems," ISO/IEC 27799 "Health informatics and ISO/IEC 27011 telecommunication organizations") or according to topic-specific requirements (e.g. ISO/IEC 27031 "Business continuity," ISO/IEC 27033 "Network security," ISO/IEC 27032 "Cyber security," ISO/IEC 27034 "Application security", ISO/IEC 27035 "Security incident management", ISO/IEC 27036 "Outsourcing" and ISO/IEC 27037 "Digital forensics"). The section structure allows the individual specific topics and target groups of the ISO/IEC 27 K series of standards to be separated. Thus, ISO/IEC 27001 can address industry-independent target groups and develop a universal set of requirements that can be implemented and used by both the critical infrastructure and regular enterprises.

NIST Cybersecurity Framework

The National Institute of Standards and Technology's (NIST) mission has been modified in recent years by Cybersecurity Enhancement Act of 20141 (CEA). As a result of this modification, NIST is engaged in the identification and development of cybersecurity risk frameworks that are applied to the voluntary use of Critical Infrastructure Operators. The CEA, therefore, tasked NIST with developing a flexible, cost-effective, and performance- based approach, measures, and control mechanisms that can be used to identify, assess, and manage risks. The NIST CSF is a risk-based approach that, as an integral part of the risk management process, focuses on the use of business drivers to identify, assess, and control cybersecurity activities.

NIST CSF is divided into three coordinated modules: The Framework Core, the Implementation Tiers, and the Framework Profiles (Fig. 4), [4].

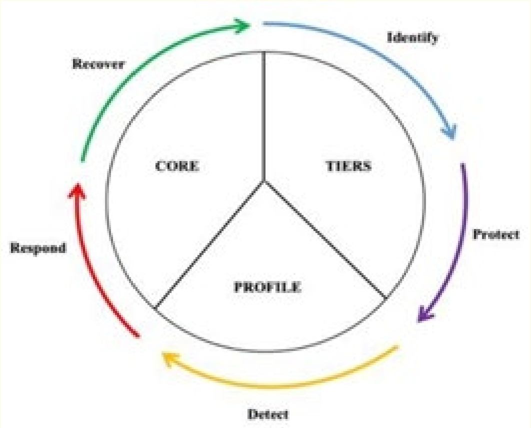

Figure 4: NIST CSF Components [4].

The interactivity of the individual frameworks can basically be described as follows: The Framework Core defines an intersectoral method to describe the main topics to be considered within a risk-based approach, dependent of the application area. In this way, the Framework Core provides a topic-specific, step-by-step guide for identifying and defining the security-related focal points. It defines in detail "what needs to be done" to achieve an adequate and sustainable information security level. In detail the Framework Core consists of cyber activities and can be participate as a translation layer to build a meta level that can be used as a simplistic and non-technical common language to communicate between multi-disciplinary teams.

The Framework Core are concretized into four parts [4]:

- Functions,
- Categories,
- Subcategory, and
- Informative References.

To deepen the granularity as well as the precision of the functions, the functions use a four-fold referencing layer. Each function refers to a set of categories, which are then broken down into subcategories. The categories determine the individual topic areas as well as the 5 functions as the specific breadth of cybersecurity. In this way, the categories reflect a holistic view of information security and cover the cybersecurity goals of an organization, while not being overly detailed. The subcategories are the deepest levels of abstraction of the core. The defined clauses at the subcategories level represent outcome- based statements that can be tailored to the needs of the organization in terms of risk- based implementation [4].

Thus, five functions refer to 23 categories, which in turn are distributed to 108 further subcategories. Below is the table that depicts these categories and functions (Table 3), [4].

Function	***Framework Core***		
	Category	***ID***	***Subcategory***
Identify	Asset Management	ID. AM	ID-AM 1 – 6
	Business Environment	ID. BE	ID.BE-1 – 5
	Governance	ID. GV	ID. GV-1 – 4
	Risk Assessment	ID. RA	ID.RA-1 – 6
	Risk Management Strategy	ID. RM	ID.RM-1 – 3
	Supply chain Risk Management	ID. SC	ID.SC-1 – 5
Protect	Identity Management &Access control	PR. AC	PR.AC-1– 7
	Awareness and Training	PR. AT	PR.AT-1– 5
	Data security	PR. DS	PR.DS-1– 8
	Information Protection Processes & Procedures	PR. IP	PR-IP-1– 12
	Maintenance	PR.MA	PR.MA-1– 2
	Protective Technology	PR.PT	PR.PT-1– 5
Detect	Anomalies and Events	DE.AE	DE.AE-1– 5
	Security Continuous Monitoring	DE.CM	DE.CM-1– 8
	Detection Processes	DE. DP	DE. DP-1– 5
Respond	Response Planning	RS.RP	RS.RP-1
	Communication	RS.CO	RS.CO-1 – 5
	Analysis	RS.AN	RS.AN-1 – 5
	Mitigating	RS.MI	RS.MI-1 – 3
	Improvements	RS.IM	RS.IM-1 – 2
Recover	Recovery Planning	RC.RP	RC.RP-1
	Improvements	RC.IM	RC.IM-1 – 2
	Communication	RC.CO	RC.CO-1 – 3
	∑ = 23	∑ = 108	

Table 3: NIST - Framework Core.

For further guidance, the Framework Core provides examples of informative references to the categories and subcategories, but organizations should determine for themselves which standards, policies, and practices, including industry-specific ones, are most appropriate for their needs.

The informative references also form the final level of the referencing layer and include a total of 6 technical reference works as compendiums, including

- NIST SP 800-53 Rev. 4,
- ISO/IEC 27001:2013,
- COBIT 5,
- CIS CSC,
- ISA 62443-2-1:2009 and
- ISA 62443-3-3:2013.

The overall, the functions represent he highest level of abstraction of the Framework Core. These functions include identify, protect, detect, respond, and recover, which relate to cybersecurity risk management as well as general risk management.

Citation: Erfan Koza. “Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security". Medicon Engineering Themes 2.3 (2022): 26-39.

The identify function provides the basis for developing an organizational understanding to design and implement key aspects of cybersecurity risk management. This understanding allows users to focus on and prioritize their business-specific efforts, depending on their business context, resources, and threat situation, in accordance with their risk management strategy and business requirements. The protect function primarily comprises preventive protection mechanisms that are used to ensure the business continuity of the critical services and the defined business processes in the intended quality and quantity [4].

The detect function defines the activities that are used as warning and early detection systems to identify vulnerabilities and incidents in a timely manner. In detail, this summarizes the activities that are used for anomaly detection, vulnerability detection, and ongoing monitoring of cybersecurity events and to verify the effectiveness of protective measures, including network and physical activities. The Response Function includes corrective activities that are used as part of incident response management to contain the impact of a potential cybersecurity incident (e.g., sandboxing). Specifically, it summarizes activities that define the response planning process that occurs during and after an incident. These processes are ultimately both of organizational nature (e.g., definition of a response team consisting of emergency managers, external stakeholder, compliance officers, etc. and their communication structure) and a technical nature (e.g., digital forensic analysis), [4].

In addition to this, the knowledge gained can be considered as lessons learned from current and previous detection/response measures as a preventive measure to avoid recurrence of the event and implemented in the previous organizational and technical processes in the sense of ongoing improvement. The Recover Function identifies the reactive activities used in crisis, emergency management and disaster recovery management to maintain resiliency plans and restore capabilities or services that have been impacted by a cybersecurity incident. As a result, these recovery activities are mission-critical activities and are used to restore normal operations in a timely manner.

Therefore, these activities are divided into emergency preparedness (e.g., creating recovery plans, conducting emergency exercises to increase response speed, and validating and optimizing defined recovery plans and procedures) and coordinating internal and external communications during and after a cybersecurity incident recovery. Based on the Framework Core as the Backbone, the *Implementation Tiers* define the four higher-level Tiers that provide insight into how the organization sees cybersecurity risk and the processes for managing that risk. The defined four tiers are as follows [4]:

Tier 1: Partial
Tier 2: Risk Informed
Tier 3: Repeatable
Level 4: Adaptive

These describe an increasing level of rigor and sophistication of the functions and categories defined as cybersecurity activities within the Framework Core. By selecting the level, organizations gain the ability to define their desired level, ensuring that the selected level meets the organization's objectives, is achievable, and reduces cybersecurity risk to critical assets and resources to an acceptable level to the organization. The tier does not represent the maturity levels, which represent the level of effectiveness and efficiency of activities. The tiers allow organizations to weigh their decision making with respect to addressing cybersecurity activities, which areas of the organization are a higher priority and could receive additional resources. In this context, the framework tier can be understood as a quantitative-qualitative tool that can be used to classify activities in terms of actionability and comparability. Now, how can the Framework Core and the Framework Tier be operationalized? For this, the business/process level managers determine the desired level to be achieved in individual activities, which ultimately need to be approved by the Senior Executive Level [4].

This sets the overall benchmark for how the cybersecurity risks will be managed within the organization and represents the prioritization and weighting of individual activities within a Target Profile that will influence the assessment of progress in addressing gaps. Successful implementation of the NIST CSF is based on achieving the outcomes described in the organization's Target Profile not on setting the tiers. To achieve individual weightings in the Target Profile, an analysis of the progress achieved must now be initialized in a Current Profile. In this context the Framework Profiles represent the operationalization level, which can be individually managed on the part of the organizations. In this phase, organizations can assign their individual characteristics, guidelines, legal and contractual requirements to the individual areas of the Framework Core and evaluate and compare them using the tier methodology [4].

The "Target" Profile can now be compared with the "Current" Profile, i.e., with the current implementation or maturity level, to identify the possible security-related and security- organizational gaps. This allows the organization to make an individual decision depending on its resources and capacities and to prioritize its identified focus areas individually and optimize them on an ongoing basis with the help of a treatment plan. To operationalize the NIST CSF, NIST defines a 7 - step guide that can be used to systematically implement each of the defined frameworks into organizations' existing security activities. In the first step, "Prioritize and Scope," the priorities and scope are defined to define the desired business requirements and the associated risk tolerances (e.g., as the target implementation level in Target Profile). For this, the. Business and mission objectives and overall organizational priorities are established. The second step, "orientation," after determining the scope of the cybersecurity program, lists components (systems and assets), regulatory requirements, and the risk approach. Threats and vulnerabilities are identified for these systems and assets based on sources. In the third step, "Establishing a Current Profile," the organization establishes a current profile by defining the outcomes of the framework's core categories and subcategories in practical terms. Within the subsequent step, "Conduct a Risk Assessment," the organization conducts a risk assessment of the operating environment. Here, the probability of an event and its potential impact on the organization is identified [4].

In the fifth step, "Create a Target Profile," the organization creates a Target Profile together that concentrates on assessing the categories and subcategories of the framework that illustrate the organization's desired cybersecurity results. Therefore, it is necessary to consider influences and requirements of external stakeholders (customers, service partners) when creating a Target Profile. The next step in the process is to compare or contrast the two "Current Profile and Target Profile" portfolios [4].

In this step, "Determine, Analyze, and Prioritize Gaps," after analyzing and identifying the gaps, a prioritized action plan is defined to close the gaps. Prioritization is done by considering benefits, costs, risks, and the results of the target profile. Within the treatment plan, measures are formed with associated financial, professional, and human resources. Profiles are used here to enable informed and cost-effective decisions. In the final procedural step, "Implement Action Plan," measures are defined to close the gaps. It also adapts current cybersecurity practices to achieve the target profile. This is where a continuous thought process plays an essential role. The steps are repeated in regular cycles that the process of cybersecurity is improved. For example, more frequent repetition of the orientation step leads to improved quality of risk assessments [4].

In addition, organizations can monitor progress through iterative updates to the current profile, and then compare the current profile to the target profile. Organizations can also use this process to align their cybersecurity programmes with the intended implementation level of the framework.

Consistency of ISO/IEC 27001 and NIST CSF

The following common intersections can be defined from the content coherence analysis: both standards place the holistic approach of information security with the triangulation of information security in the foreground of consideration. For this purpose, both standards and procedures consider aspects of IT security, organizational security, and human factor, which can be addressed in the form of individual security practices through awareness and training programs.

The modular structure of the two international methods and the associated separation of the individual security-related topics makes it possible to operationalize the individual topics separately, depending on the company's individual resource allocations and financial strength. This flexibility and reduction in complexity allows small and medium- sized companies, which are not classified as CRITIS but nevertheless use digitalized processes and networked computer technology to fulfill their operational processes, to select subject areas and introduce them accordingly.

For example, with the increase in attack vectors in social engineering, phishing attacks, such companies can implement information security awareness requirements and train their workforce with targeted, proven, and efficient steps to sustainably and efficiently activate the human firewall to defend against such attacks. Another example of the simplicity and efficiency of the two processes can be declared in the form of so-called quick wins. Thus, even such companies can already contribute to optimizing their security simply by applying a password policy, introducing strong passwords (e.g., passwords with a length of 15, upper and lower case, special characters, and digits) and by introducing two-factor authentication for remote access. If companies outsource their IT services, they can, for example, use the requirements from A. 14 (System Acquisition, Development & Maintenance) and A. 15 (Supplier Relationships) and A. 18 (Compliance) of ISO/IEC 27001 to address security in outsourcing processes, outsourced development processes, and compliance requirements, thus making a significant contribution to increasing supplier security. This provides companies with effective declarations in the sense of State of the Art (doing the right thing) and efficient implementation instructions (doing the right thing right).

In the logical conclusion, both procedures include the relative strategic and operational roles and entities that address both the internal organization and external service providers, suppliers, and authorities (ISO/IEC 27001 with 114 controls in A. 5 to A. 18 in Annex A and NIST CSF with Framework Core with 108 subcategories as result-oriented activities). Both processes can be instantiated intersectoral and thus represent a generalizable procedure for increasing the organization's information security level sustainably and cost-effectively with the aid of a systematic and predefined catalog of requirements. This meta-concept of the two procedures enables both critical infrastructures and other organizations to operationalize the procedures and adapt them flexibly to their respective structures. Owing to the predominant complexity and diversity of information security, both procedures use a referencing model to define individual subject areas, which, in turn, are differentiated into further integral components.

Consistency	***Description***
Holistic view of IS	Triangulation of Information Security with IT security, organizational security, and human factors of security
Generalizability	Intersectoral implementation, as the requirements are defined at meta level (ISO/IEC 27001 with 114 Controls in Annex A and NIST CSF with Framework Core with 5 Function, 23 categories and 108 Ssubcategories)
Flexibility	Adaptability, since the topics are considered individually depending on the organization.
Simplicity	Complexity reduction through the referencing model
Efficiency	Complexity reduction, as the topics are separated and defined in a referencing model (ISO/IEC 27 K family and Framework Core, Tier and Profile in NIST CSF)
Methodology	Top-Down Methodic (Clause 4 – 10 in ISO/IEC 27001 and 5 functions in NIST CSF)

Table 4: Consistency of ISO/IEC 27001 and NIST CSF.

In this way, the individual topics or topic areas can be executed incrementally (ISO/IEC 27001 with reference to ISO/IEC 27002 and ISO/IEC 27 K - structure and NIST CSF with Framework Core). A further advantage lies in the specification of the topics, which can also be achieved by separating them. For example, the security aspects of inventory, personnel security, procurement security, compliance, auditing, etc. can be separated from each other through the separate declarations and thus addressed in a targeted manner to the respective responsible areas. This makes it possible to operationalize the individual topics in parallel, despite sequential declarations, to accelerate project duration. Both procedures choose, even if this is not immediately visible, a top-down methodology to define the relevant topics and address them if necessary. In essence, this approach is defined in ISO/IEC 27001 by clauses 4 to 10 and the 15 subject areas in Annex A from A. 5 to A. 18, and in NIST CSF by the Framework Core with five functions and 23 categories.

Differences of ISO/IEC 27001 and NIST CSF

The fundamental difference between these two procedures lies in their main methodology of operationalizing the holistic approach. ISO/IEC 27001 adopts a process- oriented approach in which information security aspects are used as controls for internal process implementation. In other words, ISO/IEC 27001 defines the requirements for an information security management system with the objective of implementation, maintenance, and continuous development of preventive, reactive, and detective measures. However, the NIST CSF is a risk-oriented approach, which is used to identify and prioritize security gaps and is to be considered as an integral instrument or as a useful instrumental extension, whose objective is the cost-efficient and targeted optimization of the security level of an organization. The fundamental difference between these two procedures lies in their main methodology for operationalizing the holistic approach. ISO/IEC 27001 adopts a process-oriented approach using aspects of information security as controls for implementing internal processes. In other words: ISO/IEC 27001 defines the requirements for an information security management system whose goal is to implement, maintain, and continuously evolving preventive, reactive, and detective measures. NIST CSF, on the other hand, is a risk-oriented approach that serves to identify and prioritize security gaps and is to be regarded as an integral tool or a useful instrumental extension whose goal is the cost-effective and targeted optimization of an organization's security level. In a further consideration, it is even possible to assign the controls of ISO/IEC 27001 directly to the individual levels of the Framework Core, to the function via informative references.

Thus, for example, the 15 topics of ISO/IEC 27001 can be weighted in a Target Profile and evaluated based on the Current Profile to identify the gaps that exist, for example, strategically or operationally in ISMS, to eliminate them based on an Action Plan. This example makes it clear that despite the methodological approaches, both procedures can be operated and run in a compatible manner. However, despite the interoperability and compatibility, both procedures use different approaches to integrate the idea of continuous improvement. NIST CSF does not define an explicit life cycle and only refers to the iterative character of CSF: the higher the frequency of iterations, the faster the organization reaches the desired level. In contrast to NIST CSF, ISO/IEC 27001 defines a fixed procedure with the PDCA cycle, which also addresses the life cycle of the ISMS. Furthermore, as previously mentioned, the two procedures share the ability to reduce complexity by using a referencing model. However, while ISO/IEC 27001 refers to its own 27 K family, NIST CSF refers to a spectrum of relevant standards.

Conclusion

Both methods have a good international reputation due to their proven, empirically based, and robust approach, and can be operationalized sequentially and in parallel due to their modular design. Additionally, both methods can be implemented and operated independently of the sector. Due to the close relationship between the two procedures, as well as the direct reference of the NIST CSF to ISO/IEC 27001, the two procedures can be implemented and operated together, i.e., in combination. In this context, the process-oriented methodology of ISO/IEC 27001 and the associated 114 controls (A. 5 to A. 18 of ISO/IEC 27001) can be seamlessly integrated into the 5 functions of NIST CSF. This integration is particularly important when organizations have certain resource constraints, both human and financial, and therefore, need to prioritize their security processes (using the two profiles). Thus, companies can classify and operationalize their security-related activities according to current time criticality and resource capacity. Through this, process-oriented and risk-based views can be linked to create the possibility to transform the process-oriented holistic solution approach into a kind of necessary project plan and to plan and execute security-related activities depending on individual characteristics and to obtain a certain planning security. Furthermore, with the help of the combination of the two methods, synergies can be defined that will benefit successive optimization or continuous improvement processes.

References

1. J Jeong, J Mihelcic, G Oliver and C Rudolph. "Towards an Improved Understanding of Human Factors in Cybersecurity". IEEE 2019: Proceedings of the 1st International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS) and the 5th International Conference on Collaboration and Internet Computing (CIC), IEEE, Piscataway, N. J (2019): 338-345.
2. W Hurst, N Shone and Q Monnet. "Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures". IEEE 2015: Proceedings of the International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK (2015).

3. DIN EN ISO/IEC 27001:2017-06. "Information technology- Security techniques-Information security management systems- Requirements". Beuth Verlag, Berlin, Germany (2017): 1-35.
4. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurit". (2021).
5. DIN EN ISO/IEC 9000:2015-11. "Quality management systems- Fundamentals and vocabulary". Beuth Verlag, Berlin, Germany (2015): 1-104.
6. DIN EN ISO/IEC 27000:2017-10. "Information technology-Security techniques-Information security management systems-Overview and vocabulary". Beuth Verlag, Berlin, Germany (2017): 1-49.
7. DIN EN ISO/IEC 27005:2018-07. "Information technology- Security techniques-Information security risk management". VDE Verlag, Berlin, Germany (2018): 1-56.
8. DIN EN ISO/IEC 27002:2017-06. "Information technology- Security techniques- Code of practice for information security controls". Beuth Verlag, Berlin, Germany (2017): 1-112.
9. DIN EN ISO/IEC 27004:2016-12. "Information technology- Security techniques-Information security management – Monitoring, measurement, analysis and evaluation". Beuth Verlag, Berlin, Germany (2016): 1-58.

Volume 2 Issue 3 March 2022