

ISO 27001 - NIST - CoBIT - Integrated Framework Model

Executive summary

The increase in concern among businesses and customers about protecting their information has led to more complex security requirements, many times involving the integration of multiple approaches.

In turn, modern information security implementation projects have become even more challenging, especially information technology processes.

And, when we talk about integrating approaches, it is not a question of simply creating a single list of what each approach requires and implementing them, but rather to coordinate these requirements, through trade-offs between conflicting objectives and alternatives, and by reinforcing the common ones, so that the implemented requirements can meet the expected overall outcomes.

Therefore, before ensuring compliance with requirements, it is paramount to consider a process of integrating security practices into business activities, but strange as it may seem, there are not many readily available materials regarding integrating practices.

Our approach embraces the three areas, namely ISO 27001, the leading ISO standard for Information Security Management; COBIT, an IT management and Governance Framework; and NIST SP 800 series, a set of documents published by the United States government iro IT Technology Security, to which ISO 62443 (IoT) will be added

We will present their similarities and differences, and how they can be used together during an information security implementation project to improve information protection.

Introduction

One key point when considering any business process implementation is meeting existing and planned needs and expectations, which can be translated in terms of compliance with Senior Management decisions namely;

- a) Business objectives
- b) Requirements of Interested Parties
- c) Legal requirements (e.g., Laws, Regulations and EUGDPR)
- d) Policies, Processes and activities (e.g., operational objectives).

And, if ensuring simultaneous compliance with so many different requirements was not challenging enough, even in similar processes we may have different approaches for handling their implementation, which also must be addressed, for example, in terms of legal requirements, each Framework may have different objectives and demand different actions to protect information, hence we need to be absolutely clear of planned actions based upon the Assessment, findings and what are the desired Objectives to be achieved,

In terms of information technology processes, frameworks like COBIT and ITIL also have different approaches toward Information Security.

The purpose NOW is to present how ISO 27001 Standard can be integrated with IoT, SOC and SIEM requirements, including if required the COBIT framework and the NIST SP 800 series of documents in

the same ISMS implementation/remediation project, to achieve information protection and enhance information security.

By adopting the aforementioned Frameworks/Standards we will focus on a Single project that integrates information security practices with information technology management and governance practices, an organization will not only reduce project risks and speed up the implementation process, whilst adding value to the business by reducing the post-implementation administrative effort, optimizing resource allocation, and ensuring a proper alignment between organizational objectives and the goals supported by information security and information technology.

For those unfamiliar with the identified Frameworks/Standard, the following provides a brief overview;

ISO 27001:2022 Revision

ISO 27001 describes and provides guidance as to how to Manage Information Security (Data Protection).

It consists of 10 Domains and 97 Security Controls grouped into 4 sections (the Annex A), with the purpose of helping organizations to define, implement, operate, control, and improve Information Security based on a Risk Management approach.

ISO 27001 Annex A covers controls related to organizational structure (physical and logical), human resources, information technology, and supplier management, among others.

Its adoption is recommended for organizations to which information represents one of the most critical business assets, or those whose main business deliverables are related directly to information (e.g., research and development organizations, credit card processors, banks, content providers, social networks, etc.).

Like other ISO management standards (e.g., ISO 9001 for quality management, and ISO 14001 for environmental management), ISO 27001 was designed to be applicable to organizations of any size and industry.

Likewise, ISO 27001 also does not offer details about how it should be implemented, only the requirements to be fulfilled.

To assist with implementation, ISO has released several standards in the ISO 27k series, like ISO 27002:2022 (guidelines for all controls), ISO 27017 (guidelines for information security in cloud environments), and ISO 27031 (guidelines for information technology readiness for business continuity). These will be integrated in THIS ENGAGEMENT to optimise where they are applicable during the course of the engagement.

By implementing ISO 27001, an organization can reduce risks related to confidentiality, availability, and integrity of information;

1. achieve compliance with laws, regulations, and contracts demanding protection of sensitive information;
2. reduce business costs due to fewer incidents;
3. and improve public image because of the publicity that can be gained with the standard.

NIST SP 800 Series

The NIST SP 800 series provides guidelines for the implementation of computer security policies, procedures, and configurations, such as:

SP 800-39 - Managing Information Security Risk: provides specific guidance for integrating information security risk management with organizational operations

SP 800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories: provides specific guidance for prioritization of information systems based on impact assessment

SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations; provides controls to be used (256 controls grouped into 18 categories) based on the impact assessment and baselines

Its approach allows an organization to directly implement specific security-related practices in computer environments, as well as general risk management and operational process.

The NIST SP 800 series is recommended **for organizations that are highly dependent on computer environments**, and for those required to provide a stable and trustworthy computer environment.

These documents provide both nonspecific and non-technology-oriented practices, as well as recommendations for specific technologies, and like COBIT and ISO 27001, can be used by organizations of all sizes, from both the private and public sectors.

The main disadvantages of the NIST SP 800 series are related to the lack of centralized documents to help beginners to have a systemic overview of the material, and the fact that the documents do not cover integration with management practices or with other organizational processes.

CoBIT

COBIT (Control Objectives for Information and Related Technologies) is an IT management and governance framework managed by ISACA (Information Systems Audit and Control Association).

It provides implementable controls over information technology governance and management, organized in IT-related processes, which support the fulfilment of several business requirements (e.g., resource allocation, information use and protection, etc.).

Its approach allows us to identify optimal benefits realization with acceptable risk levels and resource use, providing a holistic view of the IT processes and the interests of internal and external stakeholders.

COBIT is recommended for organizations that depend on technology for relevant and reliable information, and for those that provide information and information technologies that require specified levels of quality, reliability, and control.

This framework is nonspecific and can be used by organizations/entities of all sizes, from both the private (either for commercial or not-for-profit purposes) and **public sectors**.

COBIT's main disadvantages are related to its implementation costs, the need for highly specialized knowledge, and the details about the interconnections and interdependencies between its

processes and other organizational processes (hence the need for specialized and experienced personnel).

The COBIT framework, currently in its fifth version, is divided into four domains:

1. Plan and organize identifies the utilization of IT to help the organization to achieve its objectives.
2. Acquire and implement includes the acquisition of IT solutions, their integration into business processes, and their required maintenance to keep fulfilling business needs.
3. Deliver and support requires a focus on the execution of applications and their results in an effective and efficient way.

It also covers security and training needs.

4. Monitor and evaluate providing assurance that IT solutions are achieving their goals and are compliant with legal issues.

Similarities and differences

The key to successfully integrating these practices is understanding how they are similar and how they are different, in order to better understand what to put together and what to break apart.

So, let's first take a look at the commonality between ISO 27001, COBIT and NIST SP 800 documents:

Availability of methodologies for implementation

COBIT and some NIST SP 800 process-related documents provide methodologies for how to implement the frameworks in practice, while ISO 27001 already has a proven implementation methodology.

Although their steps are not 100% aligned, minor adaptations can easily narrow the gaps (see next section for detailed information).

Process-oriented

ISO 27001, COBIT and NIST SP 800 process-related documents make use of a process approach to organize the activities, and this can be used to form a systemic view of how they can interact.

Security implementation based on Risk Management

ISO 27001:2022 adopts a Risk Management approach to identify which Security Controls are applicable.

Technology neutrality on processes

Considering processes, all three approaches rely on general concepts, in both information technology and information security, which gives organizations the freedom to adopt the technologies most suitable for their environments.

Cross-industry applicability

ISO 27001 is certifiable.

There are many benefits to be gained with a system in which a third-party that is trusted by your clients, partners, and regulators can vouch for your efforts to keep information safe.

Such certification pays for itself through cost savings from consolidating specific audits for each interested party into one single audit accepted by all of them, better public image, and increased competitiveness.

NIST SP 800 also provides some sort of certification process, but they are used only internally by U.S. government agencies for release of information systems into production.

ISO 27001 and COBIT are internationally recognized.

ISO 27001 is the world-leading standard for managing information security, and COBIT is the *de facto* framework adopted by organizations around the world when we talk about information technology governance and management.

ISO 27001 goes beyond IT.

IT environments are only one aspect that needs to be considered when we want to protect information.

Paper-based information, as well as information flowing through conversations and meetings, also needs to be protected, and ISO 27001 is better prepared to manage these situations.

Although NIST SP 800 is provided for U.S. organizations, and COBIT is not an official world-wide framework, all of them can be applicable to any type and size of organization, like ISO 27001.

Now that we have seen the similarities among these three approaches, let's take a look at their differences.

Please note that these points do not necessarily work against or exclude each other; on the contrary, they can be used to cover each other's gaps.

ISO 27001 requires Information Security objectives to be defined according to organizational context in terms of Confidentiality, Integrity, and Availability (CIA).

The same need for security objectives applies to the NIST SP 800 series, so an organization can define which documents it will use.

Controls coverage

ISO 27001 has controls to cover the protection of information, regardless of where it is found.

COBIT focuses its controls on information technologies, covering not only information security controls, but also controls related to IT operations (e.g., acquisition process).

As for the NIST SP 800 series, its documentation focuses on computer security, having many controls also described in ISO 27001 and ISO 27002, but with a greater level of detail, as well as controls not covered by ISO 27001, like "Network of Things."

Additionally, some NIST documents are technology-specific, like guidelines for the security of Apple's and Microsoft's operation systems.

COBIT has a well-defined governance structure.

A critical point in the maintenance of a management system, the governance structure provided by COBIT can help establish and maintain the alignment of information technology and information security with business objectives.

Integration of ISO 27001, COBIT, and the NIST SP 800 series

As mentioned in the previous section, COBIT, ISO 27001, and the NIST SP 800 process-related documents provide methodologies for how to implement their practices.

The following table gives one suggestion for how a project manager might consider these three frameworks in a single implementation project:

Table 1 - Comparison between COBIT, ISO 27001, and NIST SP 800 implementation approaches

#	ISO 27001 Steps	CoBIT Steps	NIST CSF	Rationale
1	Obtain Management Support	Initiate Program		Involves the recognition and agreement on the need to implement information technology and information security practices to handle sensitive issues
2	Define project methodology and documentation			By adopting a project management approach, you can minimize risks of not concluding the implementation or of running over budget or deadlines
3	Define the scope	Define problems and opportunities Define roadmap	Identify business environment and assets	Involves the understanding of business environment and definition of the implementation scope and priorities
4	Write an ISMS policy			Involves the definition of high-level guidelines regarding what is to be achieved and how control is to be performed
5	Define the risk assessment methodology	Plan program	Identify governance	Involves the development of practical solutions (policies, procedures, and processes) for the identification, analysis, evaluation, and treatment of risks

6	Perform the risk assessment & risk treatment	Execute plan	Identify risks and risk management strategies	Involves the execution of defined risk assessment methodology, so the risks considered unacceptable can be managed
7	Write the Statement of Applicability		Identify risks and risk management strategies	Involves the documentation of the proposed security environment, involving risks to be treated, which controls are and aren't to be applied, as well as their respective justifications
8	Write the Risk Treatment Plan	Plan program	Identify risks and risk management strategies	Involves the details about actions to be performed for implementation of controls, their measurement, responsible parties, resources, and deadlines
9	Define how to measure the effectiveness of controls	Plan program	Identify risks and risk management strategies	
10	Implement the controls & mandatory procedures	Execute plan	Protect	Involves the effective implementation of controls (e.g., access control, awareness and training, etc.), and their sustainable operation, considering not only technologies and processes, but also people's competencies
11	Implement training and awareness program	Execute plan	Protect	
12	Operate the ISMS	Realize benefits Review effectiveness	Detect Respond Recover	Involves the operation of controls, and detection and response to events and abnormalities, including recovering to normal conditions
13	Monitor the ISMS	Review effectiveness	Detect Respond	Involves the measurement and analysis of results for evaluation of success,
14	Perform the internal audit	Review effectiveness	Detect	

				and the respective actions needed to handle unsatisfactory results and opportunities for improvement
15	Conduct the management review	Review effectiveness	Respond	
16	Take corrective and preventive actions	Review effectiveness	Respond	