Understanding Cybersecurity Frameworks

**frame • work (cybersecurity governance)**

1. a compilation of state-mandated and international cybersecurity policies and processes to protect critical infrastructure.

2. precise instructions for companies to handle personal information stored in systems to ensure their decreased vulnerability to security-related risks.

**Apples & Oranges.** That’s an idiom many people use when comparing two like-items that aren’t supposed to be *like* each other at all. But ironically, apples and oranges are more similar than not, and like apples and oranges so are *Cybersecurity Frameworks*.

**Simply stated**, a Cybersecurity Framework is a collection of mandates, policies and processes assembled and (when applied in an infrastructure) reduce and manage “Risk” to an organization.

These frameworks include the requirements that an organization’s security program should be designed around and measured against.

Numerous frameworks cover 16 different infrastructure sectors in the U.S. and Canada, which adds a level of complexity for organizations to know which framework(s) to adopt.

In a February 2021 report released by the Gartner Group, more than 20 percent of their clients had still not selected a security framework as a baseline by the end of 2020. The most common factor (for 95 percent of those organizations), was the level of confusion, complexity and uncertainties associated with how to effectively implement a cybersecurity framework.

Moreover, when applied properly, a cybersecurity framework enables IT security leaders to manage risks with a greater degree of confidence and closure. An organization can adapt an existing cybersecurity framework or develop a hybrid version that will suit specific business objectives.
According to a study recently conducted by Accenture, cyber attacks are expected to exceed $5.2 trillion by 2024. Much of the problem, as reported by Accenture, is the increase in the amount of sensitive data and proprietary information and processes that organizations are being held accountable to protect and manage.

Ensuring appropriate security controls and processes continue to increase the operational budgets of companies of any size, while several obstacles still impede operational success. To implement a security framework means the organization is relying on a combination of tools, processes, and resources. This translates into spending money and investing time and talent in hopes of preventing security “events.”

Cybersecurity frameworks are the fundamental building blocks that we use as IT security professionals to create comprehensive baselines to measure the effectiveness of a security initiative.

Framework adoption helps organizations align with guidelines relevant to their industry and/or area of operation, while helping achieve specific business goals.

For example, the Health Information Portability and Accountability Act (HIPAA) remains an essential component of healthcare organizations. Let’s assume those same firms also need to protect personally identifiable information (PII) or electronic protected health information (ePHI). In this case, those firms may also want to consider basing their frameworks around the National Institute of Standards and Technology (NIST) cybersecurity framework and focus their attention on data privacy.
Yet, choosing the right cybersecurity framework is no small task. Cybersecurity frameworks help organizations compartmentalize and manage security processes and threats, providing scalable, repeatable and relevant procedures on which to build a comprehensive security solution.

As a starting point, your management team should gain a fundamental understanding of the frameworks implemented most frequently among the 16 infrastructure sectors.

These fall into three categories, including Control, Program and Risk Frameworks.

The Center for Internet Security (CIS) is the most widely used framework by U.S. agencies and focuses on the top 20 security controls relating to common issues trending. The CIS v7 Framework also adapts well for small and midsize organizations.

1. Control frameworks

Organizations often implement a security control framework as a baseline to assist in their efforts to meet a specific set of regulatory requirements or mandates.

Control frameworks concentrate on the security controls that are either deployed or missing within an operational infrastructure. In the case of the latter, revealing potential holes in the defenses of a system’s security infrastructure.

A comprehensive cybersecurity control framework helps get a solid security infrastructure off the ground by:

- Identifying the foundation or baseline of controls that need to be implemented in an organization.
- Assessing the current technical state of the operation.
- Developing a base-level set of priorities for the security team.
- Determining the order in which security controls need to be implemented into the system.

The most widely implemented cybersecurity control framework is the Center for Internet Security’s CIS v7 framework.
The CIS is constantly reviewing business and operational trends, modifying their “top 20 lists” to reflect prominent security trends.

These high-level controls include 20 separate control groups, divided into basic, foundational, and organizational categories.

As a baseline, research from third-party analysts has suggested that implementing CIS Controls can reduce the risk of a successful cyberattack in a company by as much as 85 percent.

II. Program Frameworks

Program Frameworks include an assortment of governance and oversight, along with technical, practical, and applied controls that should be aligned to the values, vision, mission, and purpose of the organization.

Program frameworks provide comprehensive, segmented guidelines and processes that help senior leadership (including boards of directors) answer four fundamental questions:

- What are we doing right now to secure our operations?
- How do we measure the results and success from our efforts and investment?
- What do we want to do to advance our security posture?
- When do we want to achieve an improve state?

The two most recognized program frameworks are the NIST Cybersecurity Framework (CSF), and what is arguably the most comprehensive framework, ISO 27001.

Created as a response to the Cybersecurity Enhancement Act of 2014, the NIST CSF aligns with federal guidelines for instituting a “voluntary framework that organizations could follow to establish a prioritized, flexible, repeatable, performance-based and cost-effective approach to managing cyber threats.”

NIST is a general use framework that spans five sections and covers everything from identification to recovery. It is a suitable framework for any size organization.

Like CIS, the NIST CSF divides its control processes into three subclassifications, including Core, Profiles, and Implementation. The NIST framework helps organizations both identify their current state of “cyber-maturity” and establish benchmarks to help mature their cybersecurity posture.
NIST uses easy-to-understand language to describe each process. And although NIST was designed with a focus on the federal government, its principles also apply well to the private sector.

Rounding out the top three major cybersecurity frameworks, ISO 27001 (referred to as ISO27K) is perhaps the most comprehensive. It was established by the International Standardization Organization (ISO) and the International Electrotechnical Commission (IEC).

ISO27K serves as an international standard that outlines how organizations should manage their respective information security processes and procedures.

The ISO 27K framework is one of the most popular security frameworks that organizations implement worldwide.

Large enterprises frequently use the framework to design their Information Security Management System (ISMS).

### III. Risk Frameworks

This third framework category is often viewed as a subset of the other two. Risk Frameworks provide a tactical roadmap for cybersecurity professionals to ensure programs align with stated regulations or mandated requirements.

Key factors are of risk frameworks include:

- How the organization identifies, classifies and quantifies risk.
- How an organization structures its risk management program and controls.
- How the organization prioritizes responses to an “event of a compromise.”

---

**ISO 27001 Framework (high-level components)**

<table>
<thead>
<tr>
<th>Plan</th>
<th>Do</th>
<th>Check</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Context</td>
<td>Leadership</td>
<td>Planning</td>
<td>Support</td>
</tr>
</tbody>
</table>

---

“Understanding Cybersecurity Frameworks” © 2021 Guidacent
Risk frameworks can also overlap into federal, state, international, and sector-specific mandates, such as the Payment Card Industry (PCI) and the General Data Protection Regulation (GDPR).

**Getting Started**

Choosing an appropriate framework may be difficult because so many of them overlap. To avoid falling into an “analysis-paralysis loop,” begin with a cybersecurity framework and implementation strategy that aligns with your business goals.

Each of the frameworks mentioned has their pros and cons.

Cybersecurity frameworks provide a basis for establishing a strong security posture and reducing the risk of a compromise, and adopting a framework requires a decision to commit time and resources to the project. In the end, however, your organization will be far better positioned to manage risk while enabling your business.

Want to lean more about frameworks, including NIST800, ISO27K, HITRUST, and CIS'7?

**Contact Guidacent today** for a free consultation. Our team of experienced, certified Information Security Professionals can help any sized organization, regardless of where you might find yourself on the “Cybersecurity Maturity” scale.

---

**What Every Organization can do NOW!**

- Security Awareness Training
- Adopt a Mandatory Security Framework
- Review Supply Chain SLAs
- How is Your MSP Managing Your Data?
- Perform a Security Assessment
- Adopt Principles of Least Privilege
- Insist on a “Zero-trust” Security Posture!

Ready to learn how Guidacent can help your business **establish** a strong cybersecurity **framework**?

Email us at [cybersecurity@Guidacent.com](mailto:cybersecurity@Guidacent.com) to schedule a free consultation.