

K12 Cybersecurity Tool Kit

SELECTING A CYBERSECURITY FRAMEWORK

What is a Cybersecurity Framework?

Similar to education curriculum frameworks, a cybersecurity framework is a conceptual structure that describes tools and approaches to articulate the practices a school, district or service district will use to implement and manage cybersecurity ongoing. The framework provides prioritization, guidance and structure and helps the organization to align with best practices and to meet the legal and compliance requirements for their jurisdiction.

Why do I need a Framework?

The simple reason to select and adopt a cybersecurity framework is to avoid reinventing the wheel. Multiple organizations, non-profit, government, and for-profit, have developed reputable cybersecurity frameworks that provide effective guidance and organization for cybersecurity programs. There is no need to invent a new framework for your organization, there are many to choose from.

Selecting a cybersecurity framework provides several key benefits:

- Provides a standard against which to assess risks and gaps in existing security controls
- Helps prioritize where to expend resources
- Lends authority and legitimacy to cybersecurity program efforts. Demonstrates that the program is consistent with operational standards and norms.
- Supports continuous process improvement efforts

Common Cybersecurity Frameworks

There are several well-known frameworks utilized for cybersecurity programs including CIS Top 18, COBIT, ISO 27001 & 27002, and NIST 800-53. Many of the standard frameworks and their related controls are designed and scaled for full size organizations that have fully staffed and dedicated risk teams. For K12 Institutions, the CIS Top 18 is a viable entry level approach for schools and

districts. The other frameworks listed here are described to provide a basic background and overview for the K12 practitioner, however, do not represent an optimal or realistic starting point for most districts.

Center for Internet Security (CIS) Top 18

The CIS Top 18 Controls are a prioritized list of actions recommended by the Center for Internet Security to protect organizations and their data from known vectors of cyber-attacks. These controls are clearly defined into three categories: basic, foundational, and organizational controls. Each control area is clearly defined and explained. The advantage of the CIS Top 18 controls is that they simplify and prioritize recommended security actions and they align well with all the other frameworks in the industry, but are easier to understand and use. Additionally, these are available free of charge to all organizations at <https://www.cisecurity.org/controls/cis-controls-list/>.

CIS also provides prioritized implementation groups to help organizations move sequentially through cybersecurity process improvement activities. These implementation groups build the bridge between where districts are now, and what steps they need to take next.

Here's an example of the implementation groups - here is group 1, 2 and 3 for CIS control 1:

01 Inventory and Control of Enterprise Assets		
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	  
1.2	Address Unauthorized Assets	  
1.3	Utilize an Active Discovery Tool	 
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	 
1.5	Use a Passive Asset Discovery Tool	

For more information on how to get started using the CIS Top 18, see the CIS Implementation Groups guidance at: <https://www.cisecurity.org/controls/v8/>

National Institute for Standards and Technology (NIST) Publication 800-53

NIST Publication 800-53 is a comprehensive set of well documented controls for organizations to use to protect their information systems, operations and assets from security risks including, “hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.”(NIST 800-53) The advantages of the NIST Publication 800-53 controls is they are

free and available to the public and they are comprehensive and complete. Spanning over 400 pages, they represent a veritable catalog of controls. This is also the disadvantage; it can take time and experience to sift through NIST's flexible and customizable controls and determine which ones to implement as part of a district cybersecurity program.

Control Objectives for Information and Related Technology (COBIT)

COBIT is a framework that was developed by ISACA (the Information Systems Audit and Control Association®). The COBIT framework identifies key IT processes and the elements that make up each process. COBIT is not specifically a cybersecurity framework, but it does include controls for systems development, deployment, and management. Typically utilized by auditors, COBIT is highly detailed and can be overwhelming for first time users of a framework. Another disadvantage of COBIT is that it is not free and must be purchased from ISACA. Many of the elements of COBIT are incorporated into NIST 800-53 and the CIS Top 20.

International Organization for Standardization (ISO) 27001 & 27002

The ISO 27001 standard is an international standard that describes how to manage information security. ISO 27002 is a companion document that provides a series of best practices for implementing information security in an organization. The ISO framework is presented at a higher level than COBIT and is easier to understand. This framework focuses on domains including: information security policies; organization of information security; human resource security; asset management; access control; cryptography; physical and environmental security; operation security; communications security; systems acquisition, development, and maintenance; supplier relationships; information security incident management; business continuity management and compliance.

While higher level and easier to work with than COBIT, the ISO standards are also not free and must be purchased from the International Organization for Standardization.

Conclusion

The choice of cybersecurity framework is somewhat dependent on the experience, maturity and complexity of the organization. However, for K12 school districts the CIS Top 20 is generally more effective than other frameworks because it provides a digestible and actionable framework with supporting directions and prioritization.

All the frameworks here are reputable and can be the foundation of a strong cybersecurity program. It is recommended that personnel responsible for leading a cybersecurity program be aware of these frameworks and pick one that works best for their organization. Because simplicity can be a virtue in developing a cybersecurity program, districts may find the CIS Top 20 the easiest framework to use initially.

About CoSN:

CoSN, the national association of school system technology leaders, believes that technology is an essential component of learning today, and is deeply committed to the use and distribution of technology in school systems. However, all technologies must be properly assessed for design and appropriateness in the modern classroom. Educators and companies alike must recognize and uphold their responsibilities to protect the privacy of student data.

Working together, educators and the private sector serve millions of students by providing them with the rich digital learning experiences and access needed to succeed in college, work and life. That partnership is critical to ensuring that students will have the tools necessary for success in the 21st century.

Consortium for School Networking 1325 G St, NW, Suite 420, Washington, DC 20005



Permission is granted under a Creative Commons Attribution + Non-commercial License to replicate, copy, distribute, and transmit this report for non-commercial purposes with attribution given to CoSN.