Mariam Mostafa Amin Mostafa
2205084

Security standards and guides help organizations in the implementation of systems hardening in a structured manner. Some of the well-known standards and guides are listed as under:

1. CIS Benchmarks (Center for Internet Security)
Overview: The Center for Internet Security, also known as CIS, provides a set of extensive configuration guidelines for securing different systems, software, and hardware. The benchmark of the CIS contains best practices to harden specific operating systems, such as Windows and Linux, network devices, and cloud services.
How it helps: Benchmarks provide a comprehensive step-by-step guideline on how to secure the systems. An organization may follow this benchmark in ensuring the configuration settings by a system, which will reduce its vulnerability adding to the general security posture. The guidelines undergo continuous updating to catch up with the emerging threats and vulnerabilities.

2. NIST Guidelines - National Institute of Standards and Technology
Overview: NIST publishes several cybersecurity frameworks, among them the NIST Cybersecurity Framework CSF and NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Documents present best practices for securing IT environments and can be used to create comprehensive hardening strategies.
How it helps: The NIST guidelines put great emphasis on the security of all aspects of an organization's IT infrastructure, from network design to access controls. Because the basis of NIST's approach is risk management, organizations easily adapt hardening efforts based on their specific needs but in a way that aligns with regulatory requirements.

3. ISO/IEC 27001 (Information Security Management Systems)
Overview: The ISO/IEC 27001 standard applies to designing, implementing, maintaining, and continual improvement of an ISMS. It gives requirements for how sensitive company information is supposed to be handled, staying secure.
How it helps: ISO/IEC 27001 helps with the implementation of an all-encompassing approach to cybersecurity through the establishment of processes such as risk assessments, technical controls, and continuous monitoring and improvement. It helps organizations in hardening systems across an entire infrastructure by aligning security practices to global standards.

How These Standards Help in Implementing Hardening Strategies:
Structured Guidance: Standards provide operational steps to harden systems, hence making complete security implementation quite easy for organizations. Risk Management: It provides priority-based hardening of resources in the organization based on the risks it faces, hence ensuring that critical systems are first. Compliance and Auditing: The guidelines being followed will enable organizations to be in compliance with numerous industry regulations; besides, they also establish measurable benchmarks by which auditing and improvement of security can be ensured.
Continuous Improvement: Because the standards are updated and revised from time to time, new threats and vulnerabilities are catered for, which acts as a stimulating factor to update their hardening strategy at all instances continuously.