Cybersecurity 101: Securing Your Digital Environment Glossary

Center for Internet Security (CIS) - A non-profit organization focused on enhancing cybersecurity across the public and private sectors. They are well-known for their development of security best practices, tools, and resources that help organizations protect their IT systems and data.

- **Implementation Groups (IG)** - A way to prioritize the implementation of the CIS Controls based on an organization's resources, risk profile, and cybersecurity maturity. IG1 focuses on basic cyber hygiene. IG2 Includes all IG1 controls plus additional controls that address a broader range of threats and vulnerabilities.

- **Domain** - A high-level category within the CIS framework that addresses a specific area of cybersecurity. CIS Controls are a set of prioritized actions designed to mitigate the most common and significant cyber threats. Each control focuses on a particular aspect of cybersecurity, such as asset management, access control, or data protection.

- **Safeguards** - The individual actions or technical solutions that organizations implement to fulfill the broader goal of a domain.

Cybersecurity Program - The collective effort your organization puts into protecting your information assets from cyber threats.

Control - A security measure or action taken that is implemented to manage risk by reducing the impact and likelihood of security threats and vulnerabilities. Controls are designed to protect the confidentiality, integrity, and availability of information and information systems. They can be technical (e.g., firewalls, encryption), administrative (e.g., policies, procedures), or physical (e.g., locks, surveillance) in nature.

Guidelines - Recommendations rather than a mandatory requirement.

Information Security Framework - A structured approach to managing and mitigating risks, ensuring comprehensive coverage of all essential security domains.

Information Security Policy - The formal document, authored by senior leadership, legal, and compliance, that outlines an organization's approach to managing and protecting its information assets.

Policy - A set of statements that identifies the principles and rules that govern an organization’s protection of information systems and data.
- Typically written to be broad enough to be applicable and relevant for many years.
- Should survive long-term and are less-likely to change than other documents.
- Should be periodically reviewed and updated, as necessary.

Procedures - A detailed step-by-step guide to achieve a particular goal or requirement.
- Procedures tell you how to implement your policies and how to meet your standards and baselines.

Standard - Specific and granular requirements that give direction to support broader, higher-level policies.
- Establish specific behavior and actions that must be followed and enforced to satisfy policies.
- May be mandatory for a given organization by contract or law.