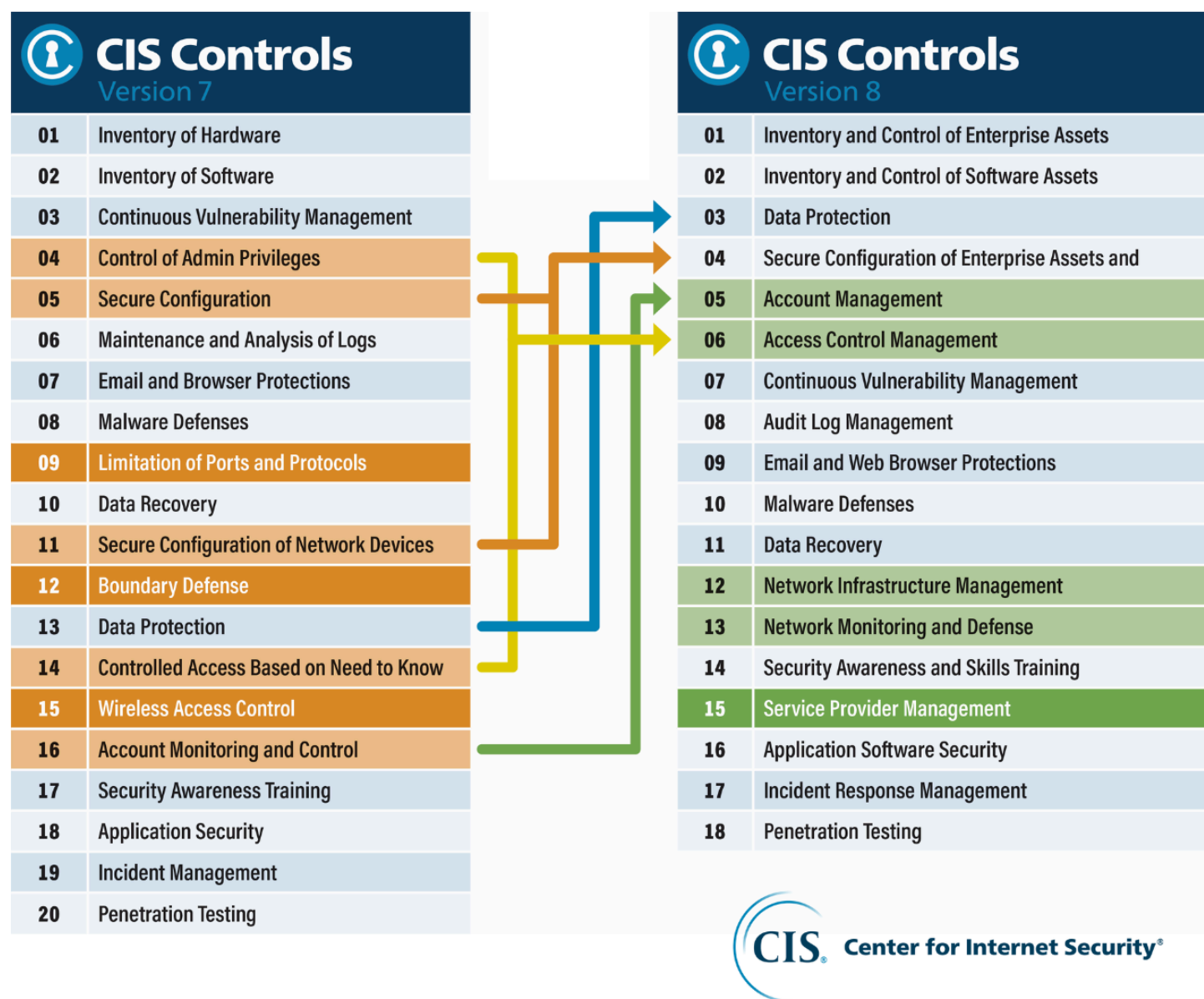


CIS Controls Overview

Document Owner: M Civello

Version	Document/Change Log	Date
v8.0	CIS Released an Update to CIS Controls: Introduced Governance to align with CSF	18 May 2021
v8.1	CIS Release an Update: Emphasis on Policies, Procedures and Processes	6 January 2025

Table 1: Outlines the Major Changes between version v7 and v8:



Governance

CIS Adds Governance Security function to align to NIST Cybersecurity Framework (CSF) 2.0, the recent update emphasizes the importance of policies, procedures and processes within an organized CS program.

Standards Alignment

CIS updated v8.1 aligns with CSF 2.0 to drive consistency, improved usability, reporting and benchmarking,

Asset Classifications

Asset classifications were revised to make them more consistent in documentation. It includes “asset type” labels to include Device, User, Applications, Data, Networks, Software and now will include Documentation as a category to account for plans, policies, procedures, and workflows.

Definitions

Detailed definitions have been added for terminology of "sensitive data", plan" and "process" to glossary. In addition, it includes types. Physical or Digital Data - [stored, processed or managed] by the organization that must be kept private, accurate, reliable, current and available at all times.

Change to Evolving Cyber Controls Ecosystem

CIS Controls v8 addresses modern threats to systems and software, Cloud-based computing, virtualization, mobility, outsourcing, remote work, changes in attack tactics, and security safeguards for most enterprise organizations.

Simplified

Each safeguard provides a single focused task (or grouped tasks) details, actions and defined metrics. The role-based focus is no longer the method, v8.1 unifies the CIS Controls by tasks and activity rather than who manages it. The approach is to implement, track, measure and assess controls; then prioritize controls based upon evolving threats and use metrics to justify investment in implementing controls.

With v8 the CIS Controls work in alignment with existing independent standards and best practice security recommendations and industry frameworks such as SOC 2, HIPPA, MITRE ATT&CK, NIST, and PCI-DSS.