CIS® Center for Internet Security®

Guiding Principles for CIS Critical Security Controls

Prioritize

- **Offense Informs Defense**: Critical Security Controls are selected based on specific knowledge of adversarial behavior and how to defend against it.
- **Focus**: Avoid adding “good things to do” unless they can be tied to attacks.

Implement

- **Immediacy**: Action today is more valuable than elegance or completeness tomorrow.
- **Specificity**: Provide **specific**, practical steps on how to implement Critical Security Controls
- **Guide**: Help organizations that are just starting adoption, as well as those that are mature in their adoption.

Sustain

- **Inclusivity**: Create and support a Community of contributors, advocates, adopters, solution vendors, teachers, consultants, auditors, etc.
- **Extensibility**: Create an ecosystem of software, working aides, use cases, tools, references, interest groups, mappings, etc.

Align

- **Integrate**: Create and demonstrate “peaceful co-existence” with existing governance, regulatory, process, management schemes, frameworks, and structures.
- **Understand**: Recognize that the Critical Security Controls exist in a context that is different for each Enterprise. Make value judgments about priority as a Community, but also allow for local, community, or more informed risk judgments.

Simplify

- **Language**: Use specific and understandable terms to help with measurement of Critical Security Controls.
- **Content**: Only include ***Critical*** Security Controls. Where possible, use data to back the selection of a Critical Security Control. Do not be afraid to delete a Critical Security Control if it is no longer relevant.

CIS Controls®

CIS® Center for Internet Security®

Goals for CIS Critical Security Controls Version 8

1. Simplify the language that used for every Critical Security Control, to include Safeguards, and their descriptions so it is easy to understand and consume.
2. Whenever feasible, leverage MITRE ATT&CK, CSAT/tooling and other data to:
    a. Ensure a Critical Security Control mitigates against attack(s)
    b. Ensure a Critical Security Control is prioritized properly
    c. Update Implementation Groups appropriately
3. To the extent practical, provide enough technical detail within a Critical Security Control to enable the measurement of that Critical Security Control.
4. Update the Critical Security Controls to include modern technology (e.g. cloud, mobility) to keep up with the modern systems and software in use by industry.
5. Include Critical Security Controls that are practical and accommodate real-world business/IT scenarios.
6. Write the document with an eye towards measuring costs to organizations.
7. As much as possible, provide backwards compatibility with previous versions of the Critical Security Controls and a migration path for users of prior versions to move to V8.
8. Leverage other best practice guidance (i.e., SW Development, Workforce Development) as appropriate.

CIS Controls®