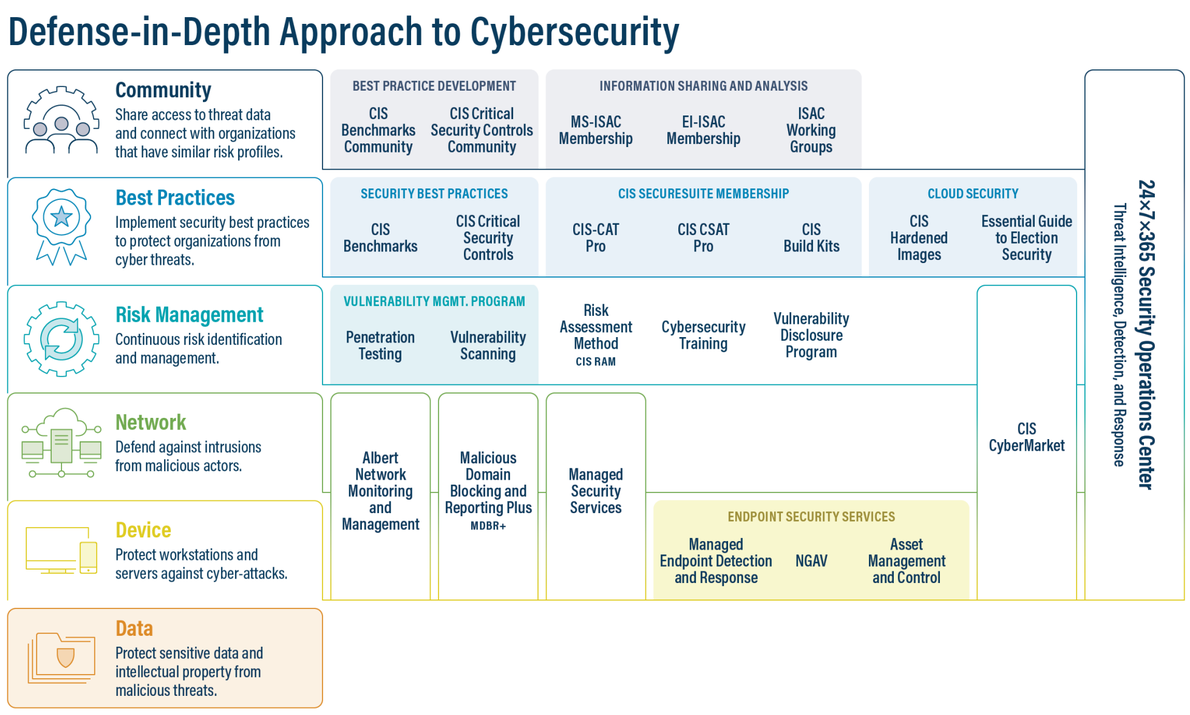
# Defense-in-Depth

Defense-in-Depth is a comprehensive information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout your IT infrastructure to protect the confidentiality, integrity, and availability of that infrastructure and the data within.

No individual action can stop all cyber threats, so we increase security using multiple security mechanisms to mitigate against a wide variety of threats while incorporating redundancy in the event one mechanism fails. When successful, this approach significantly bolsters network security against many attack vectors. An effective defense-in-depth strategy typically includes the security best practices, tools, and policies in the graphic below, and can include many more depending on the maturity of the organization.




## Goals

1. Set a foundation for your defense-in-depth journey by implementing cyber hygiene (Level 1 maturity)
2. Build toward a defense-in-depth posture by implementing baseline election priorities (Level 1 maturity)
3. Continually implement additional defenses by leveraging the Community Defense Model to prioritize your actions (Level 2 maturity)

## Actions

For Defense-in-Depth, the necessary actions vary by maturity as detailed below.

### Level 1 Maturity

Reaching a defense-in-depth cybersecurity posture takes time and resources, but begins with simple actions. For those organizations operating at a Level 1 maturity, this guide is built to help you begin and continually improve your cybersecurity posture.

1. Start a defense-in-depth journey by implementing cyber hygiene through the baseline priority best practices.
2. Continue your journey by implementing this Guide's baseline election priorities.

### Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, also detailed in this guide:

1. Implement additional defenses in a prioritized way by following this Guide's prioritized best practices for your maturity level, based on the real-world, data-driven Community Defense Model.

## Cost-Effective Tools

- The CIS Controls can be a valuable resource for all organizations looking to systematically implement cyber defenses.

## Mapping to CIS Controls and Safeguards

- The CIS Controls, taken together, collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

## Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

Previous
Managing Vendors

Next
Artificial Intelligence in Elections