INTRODUCTION

The Essential Guide to Election Security

MATURITY

Maturities

Determining Your Maturity Level

Prioritizing Best Practices for the Level 1 maturity

Prioritizing Best Practices for the Level 2 and Level 3 maturities

BEST PRACTICES

Index of Best Practices

Addressing Physical Threats

Join the EI-ISAC

Asset Management

Encrypt Data at Rest

Encrypt Data in Transit

Managing Infrastructure with Secure Configurations

User Management

Backups

Incident Response Planning

Building and Managing Staff

Patching and Vulnerability Management

Remediate Penetration Test Findings

Perform Internal Penetration Test

Exercising Plans

Exercising a plan before it is needed is almost as important as having the plan in the first place. Virtually any type of plan can be exercised, including normal operations and in the face of network disruptions, physical threats, disinformation, power outages, and many other types of incidents.

Generally, you can either take part in exercises offered by others – such as a state election office or CISA – or run your own exercises internally. Both are important. Internal exercises will test your own plans and your ability to execute on them. External exercises will further test those plans and introduce ideas you may not have considered.

ON THIS PAGE

Goals

Actions

Level 1 Maturity

Level 2 and Level 3 Maturities

Cost-Effective Tools

Mapping to CIS Controls and Safeguards

Mapping to CIS Handbook Best Practices

Goals

1. Learn the types of exercises that make sense for your organization (Level 1 maturity)
2. Participate in exercises or create your own (Level 1 maturity)

Actions

For Exercising Plans, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Participate in CISA's annual Tabletop the Vote exercise through your state leadership.
2. Your state may have other exercises. Contact your state election director and consider participating in these as well.
3. Have plans for other incidents and exercise them at least annually. While facilitated exercises are preferred, an internal tabletop-style walkthrough is better than nothing.

Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Consider participating in other exercises or creating your own with the CISA critical infrastructure exercise guides.
2. Have a regular schedule for exercises. Stick to it.

Cost-Effective Tools

- CISA's critical infrastructure exercise resources: Downloadable exercise planning and comprehensive exercise packages.
- MS-ISAC's tabletop exercise resources: SLTT focused tips, tricks, reviews, and exercise packages for download.

Mapping to CIS Controls and Safeguards

- 17.1: Designate Personnel to Manage Incident Handling
- 17.2: Establish and Maintain Contact Information for Reporting Security Incidents
- 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
- 17.4: Establish and Maintain an Incident Response Process
- 17.5: Assign Key Roles and Responsibilities
- 17.6: Define Mechanisms for Communicating During Incident Response
- 17.7: Conduct Routine Incident Response Exercises
- 17.8: Conduct Post-Incident Reviews
- 17.9: Establish and Maintain Security Incident Thresholds

Mapping to CIS Handbook Best Practices

- 33, 72

Previous
Managing Removable Media

Next
Formal Cybersecurity Assessments