Determining Your Maturity Level

This section provides some general characteristics for each of the three maturities. Read through them, determine your current maturity, and use that maturity throughout the Guide to choose your implementation strategy.

If you're unsure of what maturity properly represents your jurisdiction, begin at the Level 1 maturity and move upward as appropriate.

If you've already implemented the guidance in a best practice for your overall maturity, consider leveling up to the next maturity for that best practice. It's all part of the process of continual improvement.

Level 1 Maturity

An organization is likely at a Level 1 maturity if most of the following statements apply:

1. You have no dedicated cybersecurity staff, though you may contract for IT staff or share an IT security resource with other governmental functions, such as a county recorder.
2. While cybersecurity matters to you, you most often consider it in terms of keeping systems operational and not about detailed threats.
3. You have not undergone a formal cybersecurity assessment, like the National Cybersecurity Review (NCSR). This is more than just automated scanning, but a full expert assessment.
4. You do not have current continuity of operations or disaster recovery plans or have rarely tested them.
5. You receive cybersecurity guidance and alerts from external sources, but have difficulty understanding or knowing how to apply them within your organization.
6. You don't have a thorough incident response plan, don't exercise it regularly, or don't feel confident in what to do when an incident occurs.

Now go implement the Level 1 best practice priorities!

Level 2 Maturity

Your organization is likely at a Level 2 maturity if most of the following statements apply:

1. You have dedicated resources to manage and protect IT infrastructure.
2. You have already implemented basic cybersecurity measures, like Implementation Group 1 from the CIS Controls, the appropriate cybersecurity profile from the NIST CSF, or equivalent control sets.
3. When you receive cybersecurity alerts and directives, you generally know how to mitigate the risk.
4. You actively seek formal guidance for improving your cybersecurity posture.
5. You understand the threats facing your organization and other organizations similar to yours.
6. You track assets and conduct regular backups with at least one copy stored offline.
7. You respond to threat and risk assessments by developing and executing on plans of action and milestones (POAMs).

Now go implement the Level 2 and Level 3 best practice priorities!

Level 3 Maturity

Your organization is likely at a Level 3 maturity if most of the following statements apply:

1. You have dedicated personnel with expertise in specific cybersecurity domains.
2. You have resources that specialize in different aspects of cybersecurity, such as penetration testing or application security.
3. You conduct regular cybersecurity assessments, have after-action plans, and track progress against those plans.
4. You conduct vulnerability management, including scanning for vulnerabilities, paying attention to threat intelligence, and creating prioritized lists for tackling vulnerabilities.
5. You have the ability to detect minor events and anomalous behavior, preventing major disruptions.
6. You leverage technology to help defend against nation-state threat actors and zero-day attacks.
7. You deploy tools to address major areas of cybersecurity defense, such as network monitoring, endpoint protection, and application firewalls.

What to do with your maturity?

Based on your maturity, you can begin implementation based on the guidance for that maturity within each best practice. If you find that guidance isn't what you expected, consider moving up or down in maturity. If you are at the Level 2 or Level 3 maturity, take the time to review best practices and recommendations from the earlier maturity(ies) to make sure that you've covered everything that makes sense for you.

All organizations are different with unique combinations of skills and resources. Election offices should tailor these implementation programs to make sense in the context of their respective capabilities and responsibilities, keeping in mind that the ultimate goal is not to fill in checkboxes but to develop effective and continually improving risk mitigation strategies.

Now go implement the Level 1 best practice priorities or the Level 2 and Level 3 best practice priorities!