Integrating New Services

ELECTION OFFICIAL RISK MANAGEMENT SERIES

> Effectively managing the risks of new services and technologies is crucial when considering service replacement or expansion, be it cyber, physical or operational. *Prioritizing integration is essential.*

Poor integration of new services and technologies can lead to several risks, including:

- New or unexpected vulnerabilities (both physical and cyber)
- Operational inefficiencies or duplicated efforts
- Increased complexity, resulting in longer recovery times during an incident
- Costly rework or abandoned investments
- Fractured continuity and recovery efforts during incidents

Considering new services and technologies through the lens of **integration**—ensuring they work seamlessly with existing systems, support staff and processes, and can adapt to future risks—is one of the best ways to reduce risk, save resources and build trust in the election process. Every new tool or service should enhance your election security, not introduce hidden challenges. When evaluating new services and/or technologies, election officials should consider:

Will this solution work reliably with our existing systems, infrastructure and procedures?

Does it introduce any new risks or potential gaps—cyber, physical or operational?

Can it adapt as threats change and needs grow?

Do we have the staff, training and resources to use and maintain it effectively?

Does it align with our continuity and recovery plans?

Have we talked with our partners—cyber, physical security, continuity, procurement and vendors—about how it will integrate?

Integration ensures that any new tool, service or capability works seamlessly with existing systems, supports your people and processes, and can adapt to evolving risks. This holistic approach is crucial for election jurisdictions to strengthen security and resilience without introducing new vulnerabilities. Effective integration requires careful planning to ensure new solutions fit, work together, and do not create new gaps or conflicts. The following principles highlight the core aspects of effective integration and can help guide evaluation and implementation:

Compatibility. New capabilities should align with your current physical security, cybersecurity, and operational systems—including legacy tools that may have unique requirements.

Data Compatibility. The systems or processes being integrated need to speak the same "language" when it comes to data. For example, both systems should allow an apostrophe or other special characters in a name field.

Interconnectivity. Ensure that information flows securely and reliably across systems, and that new tools can exchange data or alerts as needed.

Staff Readiness. New services must match your staff's ability to operate and maintain them, including training, the user's experience and day-to-day workflows.

Future Adaptability. Choose solutions that can scale or adjust as threats change, technologies advance or your operational needs grow.

Security and Compliance. Integration should strengthen, not weaken, your security posture—paying attention to how systems connect, share data and maintain privacy protections.

Continuous Improvement. Plan for periodic reviews to make sure integrated systems continue to perform as intended, without introducing hidden vulnerabilities over time.

Integration doesn't happen in isolation. It requires coordination across people, processes, and technology and depends on strong partnerships within and outside your office. For election officials, this means collaborating closely with:

- **Cybersecurity teams** to ensure new capabilities fit securely within your networks and systems.
- **Physical security and facilities staff** to confirm tools align with existing site controls.
- **Emergency management and continuity planners** to make sure new capabilities support recovery and resilience.
- **Procurement and policy staff** to build integration requirements into RFPs and contracts from the start.
- **Vendors** who must understand your environment and help ensure their products or services fit and evolve alongside your needs.

When done well, integration helps ensure that every investment—whether it's a physical security upgrade, a new monitoring service, or a technology platform—contributes to a stronger, more resilient election environment.

ELECTION SECURITY RESEARCH PROJECT
A joint effort between
CENTER FOR TECH AND CIVIC LIFE
PLEJ PARTNERSHIP FOR LARGE ELECTION JURISDICTIONS
The Elections Group
and a COHORT OF ELECTION SECURITY EXPERTS