How to Assess Your Executive Protection Program Readiness

Executive protection at a crossroads

Executive protection (EP) programs are at a critical inflection point. Often undervalued and underfunded, executive security teams suffer from a perception as reactive, costly, or misaligned with broader corporate priorities. However, the rapidly escalating threat landscape means organizations can no longer afford to take a reactive approach to protecting their most critical assets — their people.

Historic challenges: Why EP programs have struggled

- × **Executive reluctance:** Concerns about privacy, image, and intrusiveness have limited buy-in for protective measures.
- × **Reactive posture:** Traditional programs often wait for threats to escalate instead of proactively preventing them.
- × **Disconnected systems:** Silos between physical, digital, and corporate teams have created blind spots in threat visibility.
- × **Perceived extravagance:** Viewed as a "perk," EP costs face shareholder scrutiny, further complicating investments.
- × **Lack of ROI metrics:** EP programs have historically struggled to connect their value to measurable outcomes.

A turning point: Intelligence-driven protection

Recent high-profile events underscore the urgent need to modernize. Proactive EP programs have become a business imperative — not just a safety measure but a strategic asset for organizational resilience.

Key drivers for change

- **Growing complexity of threats:** Executives face an evolving threat landscape, from physical risks to cyber harassment and reputational attacks.
- **Demand for proactive measures:** Boards and executives increasingly demand programs combining intelligence and prevention.
- **Technology as an enabler:** Modern tools enable seamless integration of threat monitoring, analysis, and response.
- **Protecting organizational stability:** Proactive EP programs shield not just people, but also company reputation, shareholder trust, and operational continuity.

Reframing the conversation: Leading with intelligence

- **The opportunity:** Mature protective efforts are intelligence-driven. By leveraging data to anticipate threats, they ensure that those charged with securing protectees can make smart decisions at the right time.
- **Strategic alignment:** EP is no longer about visible bodyguards; it's about integrating intelligence, technology, and human expertise to create a seamless, discreet, and proactive protection strategy.
- **What's at stake:** Failure to act exposes organizations to significant risks, from reputational fallout to disruptions in leadership continuity.

This checklist will help you assess your organization's readiness to implement a modern EP program. Each section outlines key capabilities critical for success, combining **proactive and reactive measures** for a comprehensive approach. The checklist highlights the importance of integrating **technology-driven capabilities** for intelligence and monitoring with **human expertise** for effective response and threat management. Use it to identify gaps and prioritize areas for improvement.

Key capabilities to assess

Risk assessment and intelligence gathering

Proactively identify and assess threats using intelligence and risk analysis tools.

Vulnerability assessments: Conduct vulnerability assessments across physical, digital, and public domains, including residences, office buildings, routes, social media, fringe sites, and the dark web	□
24/7 threat intelligence: Monitor threat landscapes through location-based threat intelligence	□
Open-source intelligence (OSINT): Utilize OSINT to track mentions of executives and risks on the public and dark web	□
Incident pattern analysis: Analyze historical incident data to forecast future risks	□

Principal management

Ensure targeted protection by profiling and prioritizing executives and critical locations.

Principal profiling: Maintain profiles of executives, including routines, vulnerabilities, and preferences	□
Risk-based prioritization: Identify high-risk individuals and locations based on roles and visibility	□
Custom security plans: Develop tailored security measures for executives and locations	□

Continued on next page

TIP: As you work through this checklist, you may notice some elements that you don't currently have in place or that you could improve. We recommend making note of those and creating an action plan on how to address them.

Threat actor / POI management

Track and manage threat actors to mitigate potential risks proactively.

POI database: Maintain an updated database of threat actors and behaviors	□
Continuous monitoring: Monitor POIs and priority risks in real time to anticipate threats	□
Link and pattern analysis: Analyze POI activities and patterns to assess risk escalation	□

Threat investigation

Streamline investigations to address and neutralize threats efficiently.

Threat triage: Establish processes for assessing the credibility and severity of reported threats	□
Investigation tools: Leverage technology to aggregate evidence from various sources (digital footprints, background checks, watchlists, etc.)	□
Real-time collaboration: Between protection teams and key operational partners, like HR, Operations, Events, and Facilities	□
Threat escalation protocols: Clear guidelines for when and how to take additional protective measures or involve external partners, such as law enforcement	□

Operational planning and logistics

Plan and execute security measures for high-risk situations.

Travel security protocols: Develop travel security protocols for domestic and international trips	□
Crisis response plans: Establish emergency playbooks for crisis response	□
Redundant communication systems: Ensure 24/7 secured communication channels have been established and contingency planning has been done	□
Event security management: Plan security for appearances at high-profile events and ensure threat monitoring is in place prior to and during them	□

Physical security measures

Implement robust physical security protocols to protect executives.

Close protection teams: Deploy trained personnel for close protection	□
Residence security: Audit and upgrade residential security	□
Secure transportation: Use appropriate vehicle types and trained drivers for secure transport	□
Access control measures: Implement robust access control measures at workplaces and ensure seamless connectivity with monitoring systems and incident response teams	□

Continued on next page

Digital and cybersecurity integration

Safeguard executives in the digital realm.

Executive cyber protection: Monitor data breaches and cyber threats targeting executives	□
Phishing and fraud detection: Implement real-time phishing and fraud detection alerts	□
Personal device security: Enhance personal device security for executives	□

Training and awareness

Ensure all stakeholders are prepared to handle crises effectively.

Executive training: Train executives on situational awareness and emergency protocols	□
Family security awareness: Extend security awareness training to family members	□
Simulated drills: Conduct tabletop and field exercises for crisis scenarios	□

Collaboration and stakeholder management

Foster alignment across teams and external partners.

Cross-functional collaboration: Integrate data sharing and workflows between EP, Corporate Security, IT, HR, and legal teams	□
Internal stakeholders: Establish regular check-ins with Executive Assistants, Chiefs of Staff, and other planning teams to synchronize and align on logistics, threats, and other key operational needs	□
Local law enforcement liaison: Build pre-established relationships and protocols with local law enforcement and emergency responders	□

Policy and compliance framework

Ensure the program aligns with legal and cultural expectations.

Executive protection policy: Establish documented protocols and responsibilities for EP	□
Legal compliance: Maintain compliance with privacy, security, and regulatory requirements	□
Cultural sensitivity: Adapt protocols to align with regional and cultural sensitivities	□

Learn how Ontic enables corporate security and executive protection teams to move beyond reactive security measures with a holistic, technology-driven protective intelligence solution.

Learn More