# Introducing the ASIS Executive Protection Standard: A New Era in Organizational Risk Management

### 1. What is the purpose of the ASIS Executive Protection (EP) Standard?

The ASIS draft Executive Protection (EP) Standard provides a comprehensive framework for organizations to develop, implement, and maintain a best-in-class EP program. It is designed to support strategic alignment with enterprise security risk management, leadership commitment, governance, resource allocation, and continuous improvement.

### 2. Who is the standard intended for?

This standard is directed at organizations and their corporate security leaders, risk managers, and senior management who are responsible for establishing and overseeing an EP program. It emphasizes a top-down, management systems approach to EP, rather than individual competency or certification.

### 3. Why is a programmatic approach to EP important?

In today's complex and evolving risk environment, EP must be integrated into the broader security and organizational strategy. A structured program approach ensures consistency, accountability, and continuous improvement. Without a defined program, protective efforts may become fragmented, reactive, or overly reliant on individual capabilities, reducing their effectiveness.

### 4. What is the consensus process and how does it work?

Consensus is a core principle of ASIS Standards development. It does not require unanimity, a specific document page count, or a fixed number of Technical Committee (TC) members. Instead, consensus is the process of ensuring that all viewpoints are considered, that no single interest group dominates, and that there is broad agreement on content. Alternative perspectives are discussed and resolved through open dialogue and collaboration.

### 5. How is the Technical Committee (TC) formed?

ASIS conducts an open outreach to form a balanced and representative Technical Committee (TC). Members are selected taking into consideration expertise, organizational representation, and interest in the subject. The committee includes participants from various sectors, disciplines, and geographies to ensure a diverse range of input and insights. The emphasis is placed on achieving balanced representation across stakeholder groups and subject matter domains rather than committee size, as consensus-building depends on the quality and breadth of perspectives rather than the quantity of participants. Upon completion of the standard, all Technical Committee members and contributing subject matter experts who participated in the development process will receive formal attribution, and recognition for their professional contributions to the final published document.

### 6. What role does ASIS play in the standards development process?

ASIS International is a recognized Standards Developing Organization (SDO), with extensive experience in creating consensus-based security and risk management standards. It serves as a Category-A liaison to ISO/TC 292* (Security and Resilience) and ISO/TC 262**(Risk Management), helping to ensure alignment with global standards and best practices.

** ISO/TC 292 committee has a broad scope of work that covers a variety of security topics including protective security, continuity and organizational resilience, emergency management, and fraud.*

***ISO/TC 262 develops international standards in the field of risk management to support organizations in all their activities including making decisions to manage and minimize the effects of accidents, disasters and faults in technical systems as well as response and recovery from major disruptive risks.*

### 7. Is implementation of the standard mandatory?

No. Like all ASIS standards, implementation is voluntary. However, it provides a backbone for organizations looking to formalize and enhance their EP programs. It offers common language, shared expectations, and a structured path for integration and improvement.

### 8. How does the standard support global application and scalability?

The draft EP Standard is based on a management systems approach and follows the Plan-Do-Check-Act (PDCA) model, similar to other ASIS and ISO standards. This framework ensures the standard is compatible with existing organizational management systems, scalable across enterprise structures of varying complexity, defensible through documented processes and measurable outcomes, and adaptable to diverse operational environments and geographic jurisdictions while maintaining consistency with established international standards development methodologies.

### 9. What does this standard address and what does it not address?

This standard establishes comprehensive organizational frameworks and systematic methodologies for executive protection program management at the enterprise level. It addresses strategic governance, policy development, risk assessment protocols, resource planning, and operational integration within broader corporate security architectures. The standard focuses on institutional capabilities including stakeholder coordination, threat assessment management, performance measurement systems, and alignment with enterprise risk management frameworks.

This standard does not serve as an individual certification mechanism for protection practitioners, nor does it prescribe specific tactical procedures or personal competency requirements. While individual proficiency remains essential to operational success, this standard emphasizes organizational effectiveness through standardized processes, clearly defined governance structures, and sustainable program management practices that ensure executive protection functions operate as integrated, strategic business capabilities rather than disparate operational activities.

### 10. Why is a common standard important for EP programs?

Having a common standard helps organizations benchmark, communicate clearly across departments and partners, and build sustainable, consistent programs. It supports defensible decision-making, improves operational alignment, and fosters resilience in the face of evolving threats. Consistent with ISO 9001 quality management principles and ANSI's emphasis on consensus-driven standards development, this standard provides essential foundational guidance rather than exhaustive procedural documentation.

The focus remains on establishing programmatic approaches, risk assessment frameworks, and performance criteria that enable organizations to develop scalable, risk-based executive protection programs tailored to their specific operational environments. This approach ensures the standard serves as an accessible reference that promotes industry-wide consistency while maintaining the flexibility necessary for diverse organizational contexts and threat landscapes.