

Demonstrating Value > Alignment >

Thirteen Fundamentals for a Successful Security Program

The SEC has identified 24 programs that can fall under the security function's purview, each with its own required activities and skillsets. It's tempting to assume that developing or formalizing one program – travel security, for example – would entail entirely different steps than would others, such as access control, resilience or investigations. However, we have found there are a handful of fundamentals that apply to the implementation of any type of security program.

This list below includes 13 fundamental considerations for a successful corporate security program. It can be used to structure a new program and/or assess an existing one. It may also provide some assurance to management that your program is in step with other successful security organizations.

These proven practices will set any security program on a strong footing, helping to ensure that it is organizationally aligned, professionally operated, appropriately resourced, and defensible.

24 Programs that Can Fall Under the Security Function's Purview

- Business Continuity
- Contingency Planning
- Crisis Management
- Data Science & Business
- Value Metrics
- Disaster Recovery
- Emergency Response
- Event Security
- Executive Protection
- GSOC
- Incident Response
- Information Security
- Insider Threat
- Intelligence and Analysis
- Investigations
- Pre-employment Screening
- Product Protection
- Regional Security Program
- Resilience
- Risk Management
- Security Technology
- Supply Chain Security
- Travel Security
- Uniform Security
- Workplace Violence

✓	Corporate Security Program Fundamentals (in no particular order)
	A risk assessment is conducted and revisited. Mitigation plans are based on risk assessment results.
	All stakeholders concur on the service delivery model to be used for the program.
	There are formal, documented policies and procedures.
	Services provided by the program correspond with risks of concern to senior management/board of directors and the culture of the company.
	The program has defined costs and resource requirements that may be tracked to specific risk management and service-level objectives.
	The program follows a security strategic plan that coordinates with the strategic plan of the organization.
	There is executive management agreement that organizational stakeholders are the risk owners and that residual risk remains even after program mitigations controls.
	The security leader consults with stakeholders on the program's risk mitigation plans.
	The program is audited for compliance and checked against standards.
	The program maintains situational awareness and monitors for emerging issues that may impact the organization and risk management strategy.
	Staff and program continuity are maintained through training, strategic recruitment, career development and succession planning.
	Measures and metrics are created to assess proficient performance and/or are used to adjust gaps in the program.
	The program engages with employees across the organization to bolster awareness of security requirements and expectations.

The SEC has a number of resources that can help security leaders meet these foundational objectives:

[When Your Security Proposals Keep Hitting a Wall, Try Looking at Your Security Service Delivery Model](#)

[Aligning Security Services with Business Objectives](#)

[Considering Conditions, Circumstances, Culture and Resources](#)

[Influential Strategies for Corporate Security](#)

[Six Steps of Risk Assessment](#)

[Key Performance Indicators in Security](#)

[Corporate Security Policy Template](#)

[Are You Thinking Strategically?](#)

[Emerging Issue Awareness](#)

Visit the Security Executive Council web site to view more resources in the [Demonstrating Value : Alignment](#) series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our [3-minute video](#) to learn more.

Contact us at: contact@secleader.com

Website: <https://www.securityexecutivecouncil.com/>