Strategic Planning: Security Program Life Cycle

By the Security Executive Council

The following is an abbreviated portion of the Security Executive Council's strategic planning process. The process represents a compilation of methods we have use successfully with several companies.
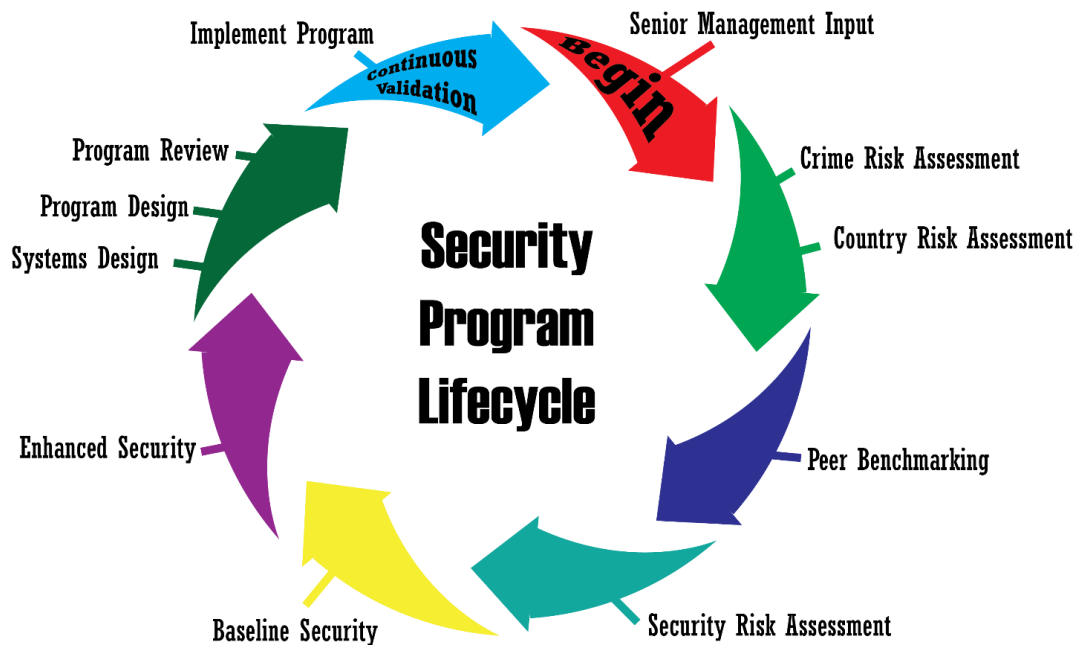
The Security Program Life Cycle is a process whereby security improvements are reviewed on a continuous basis. The cycle includes the following. (Note that some steps may be reordered or removed based on the organization's unique structure and needs.)

- **Senior Management Input.** The cycle begins with a meeting between the security leader, senior executives, and business unit leaders. At this meeting the security leader should focus on listening – gaining insight into the management philosophy, the culture of the business, the long- and short-term objectives, and management's expectation of security needs.
- **Crime Risk Assessment.** In order to understand the physical environment in which business will be conducted, it is imperative that a review of crime statistics in the surrounding area be conducted. This is best accomplished by a direct interface with local, state, and federal public safety officials. Country assessments may also be considered.
- **Peer Company Benchmarking.** Because no one company has all the answers, it is a good idea to benchmark with peer companies to determine the successes and failures they have encountered when identifying and applying security solutions. However, recognize that your organization will be unique to your peers, so benchmarking gives only a portion of the picture.
- **Organizational Security Risk Assessment.** This is designed to assess the security posture at the organization, identify risks that impact both the short- and long-term survivability of the organization, and provide cost-effective solutions to reduce or eliminate identified risks.
- **Baseline Security.** To ensure that all operations maintain an acceptable baseline level of protection, minimum security guidelines should be developed.
- **Enhanced Security.** Solutions to security risks beyond the baseline risks should be measured on a scale. A scoring system is used to measure progress toward the implementation of security solutions identified in the security risk assessment.
- **Security Systems Design.** The results of the baseline security and enhanced security processes provide the foundation for a security plan that is customized for the organization, designed to reduce risks without impeding business operations.
- **Security Program Plan Design.** The security program plan is a living document that will recycle itself through continued risk assessments and benchmarking efforts. Costs and restrictions that impede business operation will determine the degree of risk that management is willing to accept.
- **Continuous Validation.** To achieve operational excellence, regulatory compliance and civil liability reduction, validation or audits must be part of a professionally run security program. Continuous validation of the controls, notification, and response for programs, systems, and mitigations strategies is imperative.

If you would like to learn more about this process, contact us.

Visit the Security Executive Council web site to view more resources in the [Security Program Strategy & Operations : Strategic Planning/Management](#) 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/