SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues >

Ranking Security Performance

Created by the Security Executive Council

At some point, the corporate leadership team will ask how your security program ranks. *They'll want to know whether their security is poor, fair, good, better, or best in both performance and value;* and to know that, they'll need to compare it to something. They may ask you to perform the assessment, or they may ask a third party.

If you *assess and rank your performance proactively* rather than waiting to be asked, you may be exempt from management requirements to perform ranking assessments their way later. The SEC has seen multiple clients experience exactly that.

But what – or whom – to rank Security against? And how?

Here are four of the most often-used ranking methodologies we've seen.

Peer Benchmarking Usually done via survey with a select group of peers on tangible aspects of a program or function (budget, number of staff, responsibilities). *Best use:* • Researching startup security programs or taking over a new security department. • Understanding industry risk and mitigation strategies • Situations that require immediate decisions on specific operations *Pros:* • Potentially fast • Low cost *Cons:* • Results dependent on who participates • Hard to get direct comparisons	**M&A and Divestiture Processes** Usually involves measuring service levels, costs, customers, business value and capacity, with a goal to rationalize the organizations. *Best use:* • Deciding or evaluating best-value program • Understanding cultural requirements • Identifying criticality of costs, services • Determining staffing to maintain service levels • Determining workload and staff capacity • Defining customer expectations and support requirements *Pros:* • Can create common language and organizational understanding of what Security does *Cons:* • Costly • Takes time
Top 25% / Quartile Analysis Analyzes competitors to identify the programs performing at the top 25% and ranks your programs by comparison. *Best use:* • Quality and competitive improvement initiatives • Analyzing cost-versus-results equations • Branding and re-setting security expectations and image *Pros:* • Rank could help secure funding/resources to achieve higher performance *Cons:* • Can be expensive • Low scores may pose risk to the program or security leader position	**Corporate Security Maturity Assessment** Defines where your program falls on a spectrum, from reactive to optimized and value-adding. It measures quality, consistency, sustainability, and organizational alignment in relationship to a growth/evolved state. *Best use:* • Tracking program development progress against a timeline and expectations • Determining progress milestones and results for funding and resources investment • Setting strategy and goals for security department and teams • Aligning with other staff function maturity levels *Pros:* • Comprehensive • Measures progression *Cons:* • Can take time/resources to achieve desired level

Peer industry benchmarking is the most frequently requested of these methodologies. Here are a couple of tips for using it well.

Benchmark to Learn, Not to Win

If your goal in this process is to make yourself look good, you can benchmark against a company without a formal security program and come out smelling like a rose. But you'd be doing a horrible job. You goal should be to become the best, not to be the best.

To safeguard the process against bias, have the benchmarking team document their dimensions of measurement before they engage internal or peer benchmarking partners. This helps avoid unintentional manipulation of questions or measures that might skew the results in your favor.

Choose Wisely

Finding apples to apples comparisons in peer organizations will be difficult, because security program structures and services vary widely among and across industries and companies. Keep the focus of your benchmarks broad enough to provide the best possible comparables.

Choose Wisely

Finding apples to apples comparisons in peer organizations will be difficult, because security program structures and services vary widely among and across industries and companies. Keep the focus of your benchmarks broad enough to provide the best possible comparables.

The SEC currently offers five brief program-level maturity self-assessments that provide instant results. These can be used proactively to assess performance before being asked by senior management. They can also be used as a team exercise, comparing scores among team members and discussing where you are and where you want to be. Participants remain anonymous and will receive a future peer score comparison report.

- Uniformed Officer Services assessment
- Access Control and Physical Security assessment
- Investigations assessment
- Global Security Operations Center assessment
- Threat Management and Safe and Secure Workplaces assessment

While benchmarking is the most-requested method, the corporate maturity assessment may be among the most familiar to senior management. Maturity models are commonly used in many industries and corporate functions, including IT, supply chain, HR, and marketing. Here's what's unique about corporate security maturity assessments:

- **Management of Expectations.** Maturity models compare against a standard rather than another entity. This means they can be used as a way to compare company expectation to company reality. They are a way to determine the function's ability for continuous improvement.

- **Objectivity = Defensibility.** Independent maturity model assessments are made against accepted standards of maturity. The SEC's comprehensive and program service maturity level assessments rank maturity based on years of research with

hundreds of security practitioners. *This objectivity helps security programs define their place in a continuum and identify a roadmap to the next level.* It also lends credibility to your arguments for investments and resources.

Next Steps

Don't wait to be asked to rank your performance. If you want to discuss the options and alternatives with peers, contact the knowledgeable leaders of security programs that make up the Security Executive Council. Our successful team has the experience assessing the performance of their security programs that you can tap into for guidance.

Visit the Security Executive Council website for other resources in the Security Program Strategy & Operations: Emerging Issues 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/

