SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues

Excerpt: Corporate Security Maturity Assessment Peer Comparison

Maturity frameworks were originally conceived as a process to aid in the development of computer software. However, since its arrival, the idea of the capability maturity model (CMM) process has been promoted as a tool to help improve other business areas as well, for example, for supply chain, HR and project management processes. However, there is no widely accepted standard maturity model for the physical / corporate security world. The Security Executive Council (SEC) recognizes the benefits that can be achieved by understanding the idea behind the maturity model frameworks and applying those processes to corporate security programs.

To help security practitioners, the SEC has established, as an initial draft, a set of corporate security maturity assessments for five different security programs. These assessments were then condensed for initial testing purposes. The goal is to provide corporate security practitioners a tool that can be applied relatively quickly, but also to retain enough of the core of the maturity model process to provide actionable results.

While we are able to compare scores across the current pool of participants, it needs to be made clear that maturity models are not designed to use to compare one security program or one organization to another. They are not a ranking tool. They can measure improvement towards a goal over time. However, an organization that gets a lower score on a maturity model assessment is not necessarily providing less effective security to their organization; this is very dependent on industry, corporate culture, risk appetite, to name a few elements that influence the level of security desired.

The SEC's Corporate Security Maturity Assessment

Common maturity frameworks strive to classify programs into categories or levels. Each level builds on the last. For example, to be classified at level "2" the program being assessed must exceed all the requirements that define level "1".

Different frameworks may use a differing number of maturity levels as well as nomenclature, but most follow the pattern set up by the original software based CMM. For this initial assessment work, the SEC chose to simplify the framework using four levels:

Informal => Managed => Measured and Effective => Optimized

To progress to higher levels of maturity a security program must engage processes that are repeatable and not dependent on a single point of failure (documented and managed); they must measure results to ensure that they are meeting objectives and facilitating improvement (measured and optimized).

The programs/services selected for the initial assessments were ones common to many security organizations:

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

The SEC developed assessment questions to cover five initial domains of a security program:

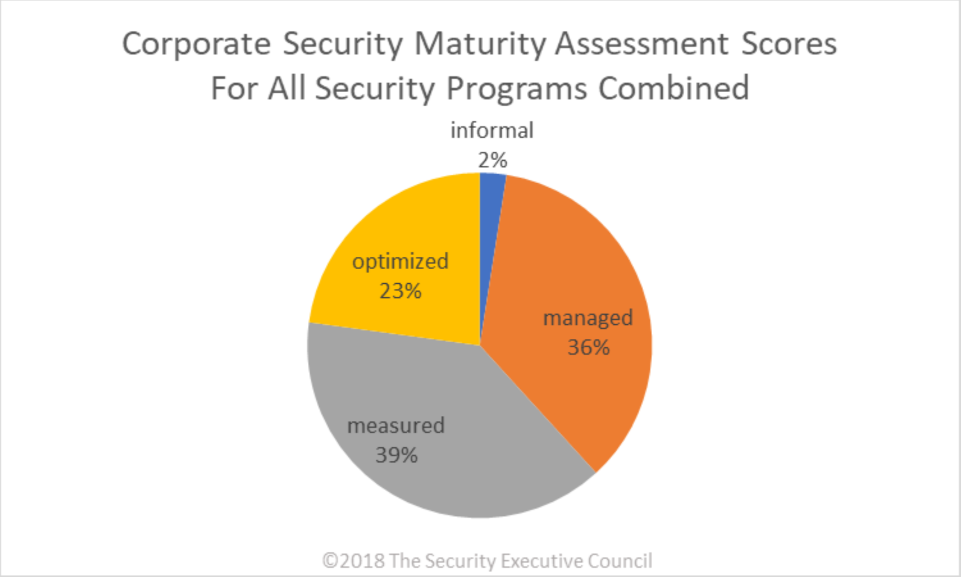
- Governance, Policy and Procedures
- Senior Management Engagement in the Mission
- Risk Reporting, Tracking and Assessment
- Standards of Competence and Staffing
- Performance Measurement and Quality Assurance

Questions were developed for each of the domains specifically to draw out the significant factors identifying each of the levels of maturity. In this way the length of time required to complete the assessment was kept to a minimum.

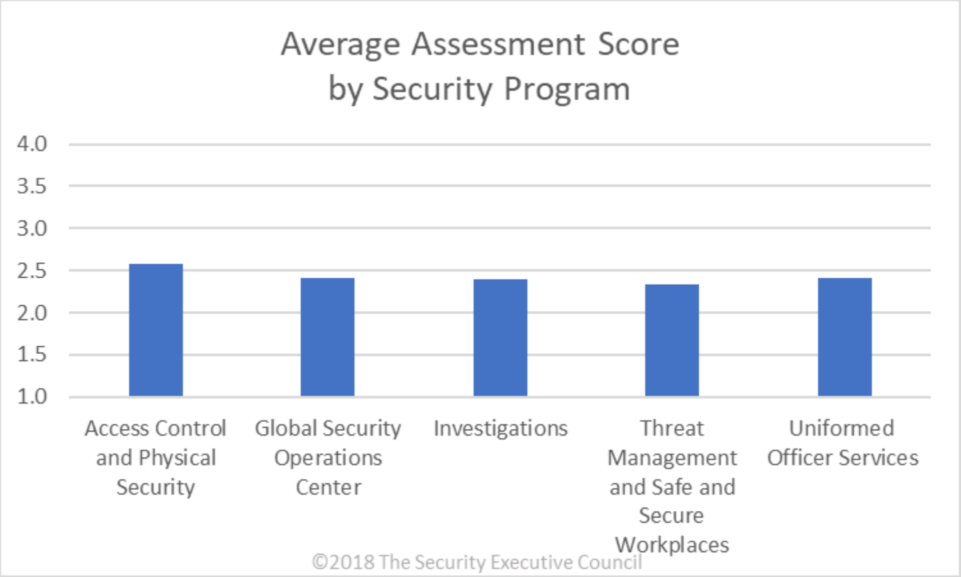
Excerpt of Comparisons

For the five programs offered, over 280 maturity assessments were completed. Most of the participants reported annual revenues exceeding $1 billion, spanning a multitude of industries.

The average maturity assessment score was 2.4 (the possible score ranged from 1 to 4).

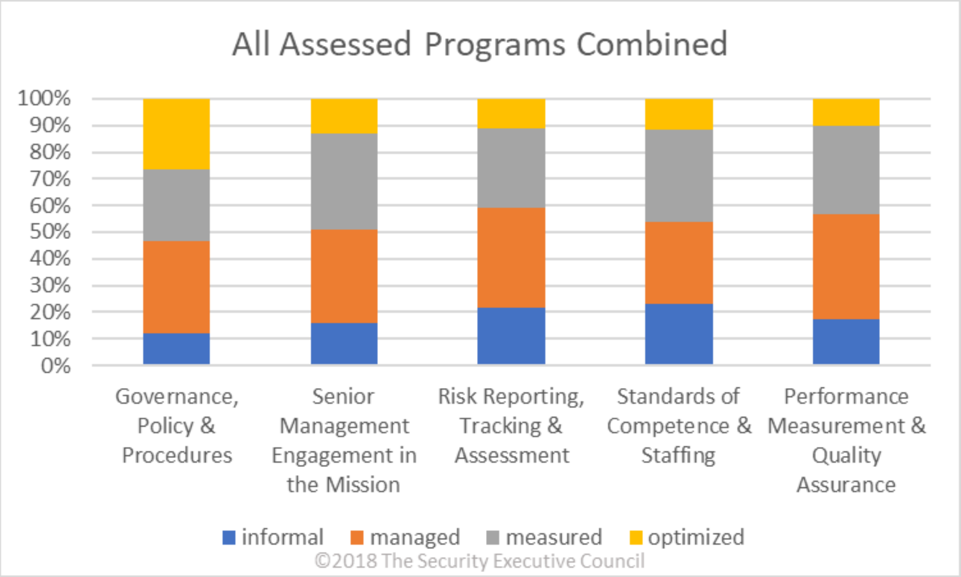


Assessment Scores by Security Programs:



All Programs Combined by Domains

Average Score: 2.4 out of 4



To Participate

Each maturity survey is a self-assessment tool and not an audit. It can be used to close gaps to achieve the desired maturity level. It can also be used as a team exercise to check where team members think the security organization is related to maturity (note – in early testing often scores varied amongst team members).

Visit this page to assess any of the five initial programs in your organization.

Data collected in these assessments will be kept confidential and will not be shared with third parties. If research based on this information is published it will only be done in an aggregate form that preserves the privacy of the participants and the organizations they represent.

Click here for more information on Capability Maturity Models for corporate security.

Visit the Security Executive Council web site to read other articles 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/