

# Measure Influence by Tracking Recommendations

By George Campbell

All non-revenue-producing organizations like Corporate Security are in the influence business. Influence is a measure of effectiveness, and we need to apply various processes to evaluate security's effectiveness. There are a variety of ways Security can do this, but the method described here may yield the most informative results.

**Objective:** To track the recommendations Security makes to other business units and determine what percentage are accepted.

**Results Sought:** To better assess our ability to influence change and effectuate risk management improvements in our clients' security practices.

**Risk Management Strategy:** The chart to the right displays the status of security risk assessment recommendations to four different business units in a year. The percent of recommendations accepted or implemented,

compared with the percent not accepted, should indicate the degree of influence Security holds over the recipient business executive. Recommendations awaiting action are merely in a queue for eventual analysis. The real ringier here is the percent of the total recommendations that are deemed Audit Committee Notable (ACN), a status typically warranting very high levels of resolution priority.

Let's take a look at Business Unit A, which received 37 security improvement recommendations during the year. Fourteen of those were deemed ACN and 22 were satisfactorily resolved. Looking behind these numbers, we would find that none of the four unaccepted recommendations were in the Notable category. This is significant because it may mean that the influence of the Audit Committee is stronger than that of Corporate Security. But it is very important to note that this escalation option open to security indicates a high degree of confidence by Audit and the Board of Directors in the integrity of the process employed by security in performing its risk assessments and analyses and framing a resolution strategy with the business units. Other points of interest might be the aging of unresolved recommendations, especially if they fall within the ACN category.

The remaining business unit examples follow the same pattern, with the exception of Unit B, which has rejected 60 percent of security's recommendations, claiming that only internal or external audit has the competence to evaluate their business controls. Security's recommendations in this unit are under external review for final findings.

This chart displays the work of a highly proactive security executive who has obtained the confidence of senior management. This example is about more than being influential. If we are to be a legitimate and full partner of the corporate governance process, our role clearly involves setting expectations on business unit stewardship of security policy. If your responsibilities only extend to or physical security operations, your programs still fall within this process. Physical security is the front line of protection for all corporate assets and is clearly accepted as a key element in information security and business continuity as well.

**Where Is the Data?** The data that form the conclusions and substance of the recommendations made by Security are embedded in the risk assessment process. **ST&D**



George Campbell is emeritus faculty of the Security Executive Council and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the Security Executive Council Web site, [www.securityexecutivecouncil.com/?sourceCode=std](http://www.securityexecutivecouncil.com/?sourceCode=std). The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.

