

Security Metrics > Specific Examples >

Create a Business Unit Scorecard

Created by George Campbell, Security Executive Council Emeritus Faculty

Objective: To assess the security of various business units and effectively communicate our findings and recommendations to business leaders.

Results Sought: We are using metrics to engage in positive change. We want local management to be more focused on their responsibilities for reducing risk, rather than leaving it to us as the inspector of last resort.

Risk Management Strategy: There are two ways to deal with business units' security trouble spots. One way is to bring them directly to the attention of the CEO and the audit committee. If we go this route, we may gain points for a “gotcha” that makes the security department look good in the eyes of upper management, but we will probably gain an enemy in the ranks who may remain a powerful thorn in the side of our objectives. A second way is to proactively work with the business unit to assess and report on several key areas of risk exposure and collaborate on solutions.

The scorecard process is risky from an internal business-relations perspective. No line manager wants headlines highlighting his or her failure to protect the enterprise. This process must be a pre-advertised, coordinated and accepted part of the corporate risk management strategy. When appropriately planned, incorporated as a consolidated part of the periodic metrics reporting process, and sold to participating line managers, the process will be a powerful tool for addressing business units' perceived shortfalls in attention to specific areas of vulnerability.

We are not the corporate cops who get our headlines from nailing idiots who should know better. We are resident experts who have a unique perspective on operational risk and need to see ourselves as change agents intelligently using this unique knowledge. By informing the manager of this proposed assessment process and working with designated individuals in the business unit, we can create and present an honest report of past performance while still achieving a positive response from the manager.

This is not unlike the process employed by Internal Audit: We are coming; here is the focus; we will work with you to identify deficiencies and help you correct them, all on the record. If you don't want to play, we will do our job and let the chips fall where they may. Few intelligent managers will refuse to participate when it's put to them that way.

Annual Business Unit Security Scorecard

Business Unit: Administrative Services Risk Manager: Charles Brown
Accountable Executive: Paul A Jones Scope: Corporate-Wide

Maintaining an Ethical Environment	Excellent awareness & support for business conduct policy throughout the management team.
Protecting Private Information	Repeated notable audit findings. Frequent source of network virus. Poor laptop controls. Management insufficiently engaged in risk.
Maintaining Safe & Secure Workplaces	Propped doors & disabled access controls. Improvement in timely notification of emerging issues with workplace violence potential.
Plan/Prepare for Business Continuity	65% compliance with full plan testing for critical business processes needs improvement.
Vetting Third-Party Relationships	80% of all engagements in the past two years failed to conduct adequate risk-based due diligence.
Employee Vetting	No hires of candidates or vendors with notable adverse backgrounds in the last year.
Response to Security Incidents	Management's response to multiple incidents has been collaborative with good follow-up to address noted vulnerabilities.

Issue Resolution: All issues identified within this review have been addressed within a Risk Mitigation Plan scheduled for completion by the end of Q2.

Where Is the Data? Look at the categories of review of a fictional Administrative Services unit in the nearby chart. Each one can point to a record to support the conclusions.

- *Maintaining an Ethical Environment:* In the example in the chart, there have been internal investigations that provide evidence that management has a low tolerance for misconduct and supports doing the right thing. Administrative Services has been proactive in working with the security department as allegations have emerged, and they have supported sanctions where evidence supported them.

- *Protecting Private Information:* Periodic inspections and audits have shown poor controls in this area, according to Security's and Internal Audit's records.
- *Maintaining Safe and Secure Workplaces:* Security has advised Administrative Services of propped doors and disabled controls and the potential for workplace violence this vulnerable position creates. They are getting the point, so the scorecard acknowledges improvement with a yellow.
- *Plan/Prepare for Business Continuity:* Security can find no record of contingency plan testing for one third of this unit's critical business operations, and this raises concerns.
- *Employee Vetting:* Security gives Administrative Services the results of background investigation findings, and hiring records show they are not hiring the bad guys the security department has identified.
- *Vetting Third-Party Business Relationships:* Security can find no record that more than one in five third-party relationships has been vetted for security or business risk.
- *Response to Security Incidents:* Where incidents have occurred, the business unit has responded well.

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](#). The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.

Originally published in Security Technology & Design

Visit the Security Executive Council website for other resources on the [Security Metrics: Specific Examples](#) 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 here: <https://www.securityexecutivecouncil.com/>