

Security Metrics > Specific Examples >

Build a Risk Indicator Dashboard

Created by George Campbell, Security Executive Council Emeritus Faculty

Objective: Provide a single display of the key information a manager needs to monitor a set of measures and effectively communicate the status of those measures.

Results Sought: You're busy, and so are those you seek to inform. Immediate comprehension of business information is essential. The data in a risk indicator dashboard is presented in such a way as to maximize understanding with a minimum of explanation. You also reinforce basic security policy with periodic updates like this.

Risk Management Strategy: Your corporate security program can use a traffic light image in dashboard dials to present information to management on risk indicators. The example in the nearby graphic focuses on narrow but important indicators of effective access management.

Access Control Dashboard

Access lists and updated authorizations are reviewed monthly in accordance with policy	
All persons authorized for ongoing physical & logical access are background vetted	
Access spaces are configured and protected in accordance with security policy and standards	
Visitors are escorted and receptionists are trained for applicable access procedures in their spaces	
Periodic security tests confirm resident awareness of access oversight responsibilities	
Cleaning crews are supervised consistent with contract and trash inspected nightly	
The access control system meets the 99.5% uptime reliability standard	

Measurably effective access control—both logical and physical—is a fundamental security requirement. Accomplishing it involves a variety of operational and technology-based countermeasures. This graphic example focuses more on physical than logical access. You will need to decide which dashboard warning lights to include based upon your organization's threat profile, culture and management expectations. The seven examples in this graphic are typical of a basic set of measures.

Where Is the Data? The data you'll need to make these measurements should be readily available. The challenge is in finding ways to communicate your message with a minimum of time and misunderstanding. Your company likely has an executive information system (EIS) managed by the CFO or other administrative unit that may offer examples of executive dashboards that you could employ. Color coding is a way to provide information instantly with little required explanation.

1. Access lists and updated authorizations are reviewed monthly in accordance with policy. This data is typically found in online logging and storage of access authorizations and associated lists. Automated reviews to identify outdated authorizations enable audit and reporting. It's essential to have links to HR and Purchasing to purge access immediately when employees and contractors are terminated.

2. All persons authorized for on-going physical and logical access are background vetted. This data may be easily assembled when completed background investigations are required for granting logical and physical access.

3. Access spaces are configured and protected in accordance with security policy and standards. All spaces are probably not created equal. Periodic security audits will yield data on those more sensitive spaces that fail to meet physical security guidelines.

4. Visitors are escorted and receptionists are trained for applicable access procedures in their spaces. In many organizations, receptionists are the gatekeepers of business sites. Sign-in and badge procedures may be audited for compliance with this basic safeguard.

5. Periodic security tests confirm resident awareness of access oversight responsibilities. Unbadged security personnel can stroll into controlled spaces and collect data on the frequency of challenges by residents. If the unbadged personnel can access more secure areas unchallenged, this should be brought to management's attention immediately.

6. Cleaning crews are supervised consistent with contract and trash inspected nightly. Cleaning crews are often the weak link in physical access management. Service contracts should specify standards of oversight and operations. Daily, random security checks on access and trash collection will provide data on conformance with these requirements.

7. The access control system meets the 99.5% uptime reliability standard. Uptime of critical security systems should be set in vendor specifications and routinely logged and audited for reporting purposes.

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 Metric: 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/>