SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

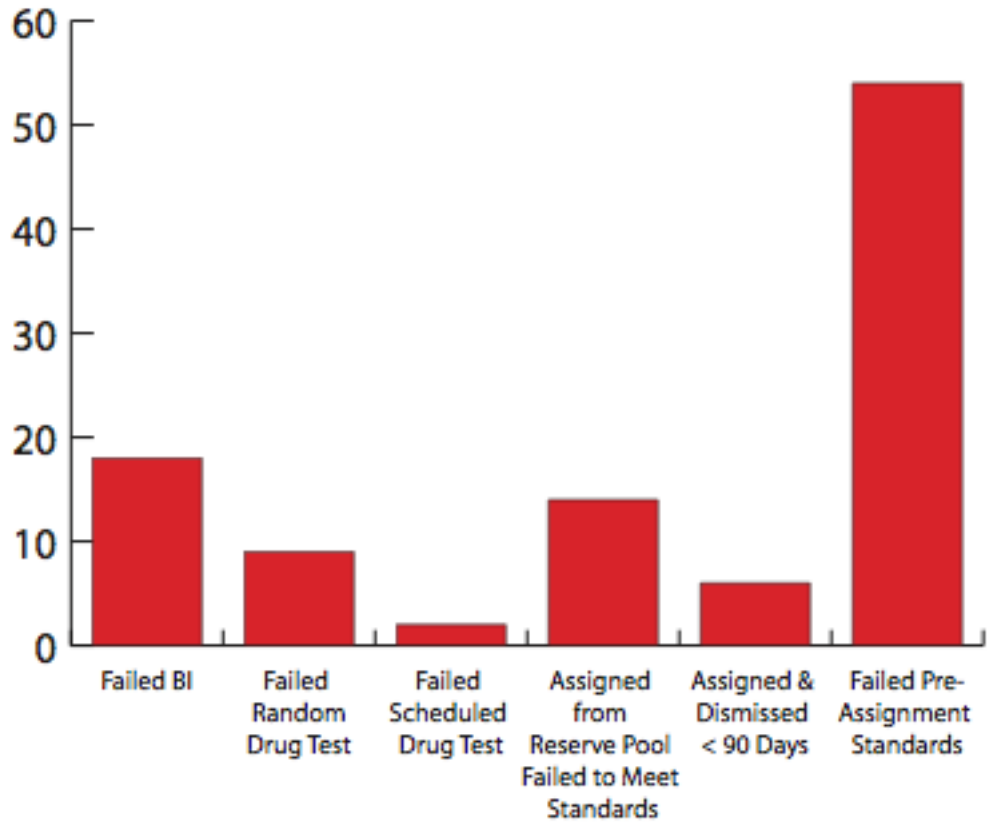
Security Contract Compliance Auditing

George Campbell

Originally Published in Security InfoWatch

October 2012

Security Contract Compliance Auditing



Contracts with product and service suppliers are an integral part of many corporate security service delivery programs; in fact, many companies spend millions of dollars annually for thousands of hours of service from contract guard vendors.

Ensuring the effectiveness of performance terms and related compliance monitoring is a critical management objective that requires knowledgeable and engaged resources, along with the right data for performance measurement. Too many organizations rely solely on the vendor's own periodic reporting for compliance assessment. Service level agreements

(SLA) typically apply a relatively small sample of performance requirements across different aspects of the contractual agreement.

The company in this month's example chart is concerned with co-employment risk and takes a relatively hands-off oversight posture. The vendor is required to ensure that all personnel who may be assigned under this contract are submitted for background investigation and drug testing — both administered by contractors of their choosing. Hiring, training and retention standards are specified, and the contract indicates that the company's security contract administrator may audit compliance. This audit function is assigned to the purchasing department, and the company is heavily into outsourcing and lean management.

A new director of security has correctly prioritized a thorough review of operations, and this contract represents 62 percent of the corporate security budget. The vendor is required to submit a variety of data pursuant to the SLA, so the security director places a request to Purchasing for audit reports, with this result: There are none.

It turns out that the purchasing department is "too busy with RFPs" to engage in audits. The security operations manager who "owns" these services also serves as a lead investigator for site incidents and has relied on facility managers and the vendor's supervisory team to jointly manage guard operations.

The security director has seen a variety of signs in incident reports, shift reviews and simple observation of post assignments that this vendor may require more active oversight. His subsequent review of one report provided by the vendor confirms his concerns. It shows that in the past two quarters at the company's two largest sites, 103 individuals slated for assignment or actually assigned have been dismissed or reassigned, likely to other clients with lower retention standards. This represents a 32 percent rejection rate for the quarter.

Of more immediate concern is the finding that 70 percent of this group either failed to meet pre-assignment standards or had to be dismissed prior to the end of their 90-day probationary period. A deeper dive indicates that

turnover has spiked over the past three quarters and the supervisory team has been reassigned to a new contract in another part of the region. Follow-up discussions with selected facility staff further reveal that service quality has deteriorated and response times have noticeably increased in areas requiring a response time of no more than five minutes.

Clearly, something is amiss either in this vendor's recruitment efforts or in the available pool of candidates. It is also clear that the company has totally failed to exercise its responsibilities in basic contract management, and this one metric report is only the tip of the iceberg.

Ask Yourself: If you were presented with this set of facts and concerns, what steps would you take to immediately improve the quality of personnel and service from your guard force contractor? What other data would you demand from the vendor? What steps should be taken internally to ensure the appropriate level of contract compliance? If your actions with this vendor created co-employment concerns from Purchasing and Legal, how would you answer them? What would be an appropriate response from the vendor's management?

George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, Measures and Metrics in Corporate Security, may be purchased at https://www.securityexecutivecouncil.com/secstore/index.php?main_page=product_info&cPath=77_65&products_id=324. The SEC draws on the knowledge of security practitioners, experts and strategic partners to help other security leaders initiate, enhance or innovate security programs and build leadership skills.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com