Demonstrating Value > Operational Excellence >

Operational Excellence in Contract Security Performance Measurement

Created by George Campbell, Security Executive Council Emeritus Faculty

This report continues our series of considerations for the application of operational excellence (OpEx) concepts to corporate security programs (see the first in the series, Defining Best Practices in Global Security Operations Centers). The focus in this edition is on measuring the performance of security service providers. The Security Executive Council believes that there needs to be a more in-depth consideration of what constitutes "excellence" in these operations given the consistent growth of outsourcing to guard service companies.

If there is one core service provided by corporate security organizations across the globe, it is the provision of a menu-driven suite of physical security services that are delivered by primarily hourly staff on a 24/7/365 basis. As of 2014, the U.S. contract security officer service market included somewhere in the neighborhood of 8,000 companies employing over one million personnel. This highly competitive business annually totaled $20B in revenue and was marked by aggressive acquisition of smaller regional companies.[1]

The Affordable Care Act and other cost factors are driving companies that currently employ in-house security officers to outsource these services, thus potentially adding to this employment pool. However, it is generally accepted that companies employing in-house security officers apply higher standards of recruitment, education and training, provide better compensation and benefits and realize higher and more consistently delivered levels of service excellence than outsourced services; so increased outsourcing potentially lowers quality of service.

[1] White Paper on the U.S. Contract Security Industry, www.robertperry.com, July, 2014

Defining Operational Excellence

According to Wilson Perumal & Company, "Operational Excellence is the execution of the business strategy more consistently and reliably than the competition. It is evidenced by results. Given two companies with the same strategy, the Operationally Excellent company will have lower operational risk, lower operating costs, and increased revenues relative to its competitors, which create value for customers and shareholders."[2] At its core, it's about increasing the perception of stakeholder value by delivering superior performance and results.

Proof of superior results: Where a security practice can be shown to deliver consistently superior results to an alternative process, it could be advertised as having achieved a level of excellence. The key is in the ability to measure the "superior result," and that requires detailed task and process analyses that are consistent elements in virtually all business excellence disciplines. When a security activity is peer-reviewed or benchmarked against available standards or best practices and exceeds qualitative measures of performance, value may be claimed. This is about a proven level of clearly superior service. The demonstration of a level of superior results requires performance metrics to establish reliability and validity.

The challenge: It is ironic that a discussion of service excellence in this industry has to be tempered by a popular movie image of Paul Blart, Mall Cop. A more intellectual analysis of the industry by Michigan State University concluded, "Despite playing a more important role in the wake of 9/11, the security guard industry remains plagued by inadequate training and standards in many states. Formal training of the one million-plus private security officers is widely neglected; a surprising finding when contrasted with other private occupations such as paramedics, childcare workers and even cosmetologists. By and large, security guards say they're unprepared to handle problematic people and physical altercations and to protect themselves. They strongly endorse the need for systematic and standardized training in the industry."[3] One might well question the legitimacy of OpEx in this industry if basic selection and training standards cannot be universally established and verified.

The lack of standards is reflected in the frequent frustration expressed by many chief security officers, security managers and procurement executives who receive commitments for gold level service from winning bidders and then experience inadequate recruitment pools, poor management, shoddy performance, excessive and unacceptable turnover rates, or loss of quality performers either through attrition or re-assignment to new contracts. One challenge that is difficult to manage for both parties is the inadequate regional recruitment supply. This occurs when the job market is so

[2] http://www.wilsonperumal.com/blog/a-better-definition-of-operational-excellence

[3] Security Guard Industry Lacks Standards & Training, M. Nalla & A. Henion, Michigan State University, June, 2014

robust that only the less qualified remain available for hire. On the flip side, these jobs may be temporary positions for the well qualified who are holding for an appointment in another pending position.

The fact that the security guard industry still characterizes itself as providing “guards” says volumes on the difference between a proprietary security service and the outsourced model. The former is totally focused on recruiting and retaining quality employees who are culturally attuned to quality service, while the latter focus on low-cost, often marginally employable individuals.

This is a highly fragmented and competitive industry; one that may be both incapable and unwilling to accept and really own the depth and breadth of performance measures essential to an OpEx model. But if security executives do not push measurably qualitative performance requirements, then the market will seek its own level, and bronze performance will be the standard rather than gold or silver.

This challenge is clearly tied to the absence and/or inadequacy of contractual standards and measurable expectations. RFPs (request for proposals) and contractual requirements are uniformly developed around hours of pre- and in-service training, background vetting, turnover, invoicing, post assignments and so on.

We need standards to establish qualitative measures of performance, and that is at the heart of the OpEx opportunity. We need to collectively ensure that the service provider’s team remains focused on service excellence, customer responsiveness and, of most critical importance in these duties, the proactive mitigation of risk to the customer’s people and operations. This paper will offer up several examples of performance measures and metrics for consideration.

Why operational excellence is particularly relevant to these services: More often than not, the typical first on-premise contact an employee or visitor has with an organization is with a uniformed or business-attired contract security officer. This staff contact represents the Security organization to that individual and informs an impression of brand. The perception of competence and quality in that interaction is critical, and the results are essential to the perception of care and of excellence in safe and secure business operations. The notion of operational excellence in these hourly-compensated services is important for several reasons:

- These are the first responders, the staff who have the 24/7 mission to expertly address the whole range of personal safety, security and business resilience incidents.
- Critical bench strength: They fill time-sensitive availability gaps in an emergency (fire, rescue/EMT and police) as well as pivotal positions staffing 24/7 critical process monitoring centers.

- Key service providers: Personnel are often required to oversee and respond to anomalies in a variety of operationally sensitive business, cultural and organizational processes.
- They are the often the primary staff for customer and business-facing concierge, supply chain and other dependencies.
- In the more competitive job markets, these companies struggle to find and retain quality staff to fill these shift-based programs. Turnover can be excessive and disruptively high.
- The market tends to set a standard that does not adequately drive excellence in performance standards.

In the Security Executive Council's (SEC) reviews of these operations, we find a wide variety of scope and performance-related detail in the contracts that are typically valued at millions of dollars annually and stand out as the single largest line item in the security department's budget. Often based on these levels of expenditure, the application of more detailed contractual requirements and a service level agreement (SLA) are provided as financial incentives to excel and penalties where performance is below a specified standard.

Industry Best Practices

Given the multi-billion-dollar nature of this business, one would think that our industry would have developed and vetted a comprehensive collection of proven if not best practices in this area of security services. These accepted guidelines or standards could then be easily translated to a measures-based set of excellence descriptors. We might expect the industry's representative, the National Association of Security Companies (NASCO) to have led this effort. At the time of this writing, however, little evidence of this has been unearthed. ASIS International has published a variety of guidance materials[4], the Department of Justice has funded projects documenting the scope and nature of the business[5], and in 2013 the Interagency Security Committee published Best Practices for Armed Security Offices in Federal Facilities, which only discusses recommended practices for training.

A potential model is found in the Risk-Based Performance Standards published in May 2009 by the Department of Homeland Security. This document provides industry guidance for implementation of the Chemical Facility Anti-Terrorism Standards. From an

[4] Quality Assurance & Security Management for Private Security Companies Operating at Sea (2013), Management System for Quality of Private Security Company Operations- Requirements with Guidance (2012) and currently is seeking comments on a proposed Guideline: Private Security Officer (PSO) Selection & Training.

[5] The Private Security Industry: A Review of the Definitions, Available Data Sources & Paths Moving Forward; K. Strom et al, December, 2010, Doc. # 232781

OpEx perspective, each standard provides clear descriptions of required security measures and associated metrics for evaluating compliance with site security requirements. This format enables consideration of incrementally rigorous performance standards for higher-risk facilities, many of which can be applied to OpEx program application.

Evidence of superior results in contract security services: There are a host of service-related variables that should be locally considered and defined in the contract. This ensures the necessary connection with the specific risk management and service level requirements appropriate for the sites to be staffed by the service provider. Carefully consider the proximity of these 24/7 security services to the customer and the direct connection to the risk management mission, as they should entail clearly measurable success factors. Moreover, they point to the kinds of KPIs we should be building to direct and assess the performance of our vendor's operations. Consider the factors in Table 1 for service excellence and value.

Success Factors	KPI Focus
1. Higher qualitative recruitment standards to provide sustained levels of competency in the employee base.	Management knows that service excellence is all about the quality of its people. Longevity can be a big plus.
2. Active encouragement and support of employees in education, professional certification and self improvement.	Willingness to invest in personal improvement and resident knowledge to mitigate risk of turnover and disruption.
3. Improved quality of reporting for collective knowledge.	Aids in mitigating litigation and outcome severity, enables trending and scorecards.
4. Active engagement at all levels in performance measures and metrics.	Process measurement and engagement, scorecard development, constant improvement efforts, feedback to customer on internal process defects, personnel development and risk management quality assurance.
5. Aggressive defect identification and elimination in service delivery tasks.	
6. Self-directed postmortems and after-action reviews.	
7. Sustained levels of independently obtained "high" and "very high" customer satisfaction survey results	Engagement and commitment to the quality of the customer relationship enables measurably improved risk awareness and service responsiveness for improved stakeholder brand protection and confidence in results.
8. Notably higher levels of customer connection and business unit knowledge.	
9. A sustained and positive connection with the customer's workforce and business operations.	
10. Lower rates of attrition.	Employee satisfaction & engagement in customer relationship, longevity & local knowledge.
11. Strong supervisory presence with	Strong, quality-focused 24/7 site supervision is

Success Factors	KPI Focus
correspondingly strong maintenance of service-level quality management and employee performance measurement.	the key to shift-based service excellence and total quality management.
12. Faster, better response to incidents and calls for service.	These results are assured when the vendor team is committed to service excellence.
13. Vendor management's commitment to and experience in developing improved methods of service delivery and adding measurable value to the customer's operations.	Service excellence begins at the top. This is about maintaining a focus on seeking out better ways to support the customer's unique needs at lower cost. This supports a focus on innovation, pushing quality down into the customer-facing service levels, and it opens opportunity for applying labor-reducing technologies.
14. Demonstrated willingness to identify opportunities for cost containment and/or reduction.	
15. Vendor-directed initiative in proactive risk identification and mitigation.	A critical focus of the site supervisory team and a documented process. Direct contribution to first call remedy rates & qualitative/timely response.
16. Perceptible levels of pride in all aspects of work performance.	A sense of purpose and ownership instilled by management and the supervisory team. Pride breeds an engaged, self-starting commitment to quality.

Table 1.

When you see these factors at work, the results are obvious. They collectively add up to a service provider capability for delivering sustained levels of performance excellence. Service teams show a commitment to become an integrated part of the business, and their value is both clearly perceptible and measurable by stakeholders and customers.

Service excellence and the ability to deliver the competent resources: The success factors listed above go beyond what is typically found in contract specifications and service level agreements.

Some organizations specify a variety of skills to address areas of life safety, emergency response, command center, specialized business support or the customer's regulatory requirements; all separately priced to address the added cost of recruitment, training and processing or certification. Many of the providers advertise a sliding scale of service levels intended to attract the consumer to an ostensibly higher level (and higher cost) of customer service skill. Interestingly, the brochures appear to focus on the concierge functions and related incumbent personality and appearance issues rather than a broader scope of security skills.

Many proprietary security programs successfully fill highly specialized line security functions and compensate them at competitive rates, so the model to provide a more selective and priced set of OpEx-based competencies by contract service providers is totally feasible. RFPs and contract documents need to clearly specify performance standards.

Selecting and engaging the service provider: Every organization brings its own well-established procurement processes to the acquisition of security services, too often without a well-documented assessment of service requirements to drive subsequent bid and contract documents. There are a variety of complexities in the contracting of security services that, if not considered, can result in increased board risks, liability, and poor execution of service. Some of the complexities include inadequate general liability coverage, workers compensation coverage, umbrella coverage, bond coverage, co-employment risks, hidden fees, inadequate licensure, sub-standard vetting, unacceptable levels of training.

Where performance expectations are not clearly spelled out in RFPs and specifications, bidders will take the natural path of least cost and most convenience. If levels of operational excellence are to be sought in procurement documents, the following must be thoroughly described:

1) each of the elements of superior performance for the full scope of security operations;

2) the skills and competencies that are required to consistently deliver and achieve the specified level of service;

3) the specific measurements for each type and level of service and how the measures will be applied and the metrics reported.

The contract must establish a mutually agreed, legally binding framework that includes measurable performance specifications aligned with defined service levels and productivity objectives calculated to improve security task efficiency and lower cost of operation. Specific service level objectives should be tied to defined security success factors such as those seen in Tables 1 (above) and 2 (below). Provisions for both incentive rewards and penalties are essential ingredients in the contract terms and service level agreement.

A note on co-employment: Many security executives who have experience with large contracts think this issue is a non-starter. They believe that client oversight, performance monitoring and directed engagement on task performance are essential, particularly given the proximity of the services to the customer-facing, risk management mission. While we encourage discussion with supplier management and legal counsel, we also state our firm belief that it is the corporate security executive who will be held accountable for a notable breach in security, a defect in a regulatory requirement, or a deficient response resulting in litigation. Knowledgeable oversight is a reasonable element of duty of care. Our suppliers are our agents, and while we can specify our requirements in contracts, the delivery of security services represents a shared, collective responsibility. The active measurement and directed feedback on performance is not only acceptable, it's our duty.

Managing the Service Level Agreement

Developing, maintaining and managing an SLA is neither a casual nor a simple process. It requires dedicated resources and will likely cost you more than the vanilla service levels most often marketed and delivered. Effective management of an SLA for operational excellence is not an exercise in hands-off, part-time engagement. Nor should it be left to an overworked contract specialist with little or no knowledge of the security program or the nuances of the various elements in the agreement. You must be dedicated and experienced to manage continuing SLA administration, relationship management and quality oversight.

OpEx demands measurable standards of performance from the contractor and all assigned personnel. Measuring requires the detailed work of defining what, why, how, by whom and when. Service-level management provides for continual identification, monitoring and review of the levels of service specified in the SLA. The central role of service-level management makes it the natural place for metrics to be established and monitored against a specific target. ***If you have committed a component of your program to a disciplined operational excellence process, be prepared to invest the time and effort to manage it conscientiously.***

Many organizations utilize an SLA as a part of their contract with the security vendor to commit the provider to specific deliverables and service levels. First and foremost, this agreement is a means of establishing and communicating clear expectations of service quality. It should be a collaborative process between the parties. This is particularly true when defining what is meant by "service excellence" and the elements of measurement.

Maintaining lines of communication on performance elements will avoid conflict on the content and adequacy of services and aid in resolution when differences do occur. The objective is to establish consistency in measuring service effectiveness, especially where the SLA will apply to multiple sites and (possibly) multiple vendors with identical contact terminology. The agreement should clarify the division of responsibilities. This can be very important due to the dependencies that typically exist between various components in the physical security infrastructure, the facilities, and business continuity teams and other organizational elements that rely on these security operations for task accomplishment.

Counting versus measuring: From an OpEx perspective, SLAs are typically organized around quantitative measures. However, they tend to use transactional (counting) criteria rather than more qualitative measures that can really focus on service excellence. Table 2, shown below, provides some examples.

KPI/SLA Factor	Qualitative Consideration
Turnover: Average number of employees who left during the period (voluntary & involuntary)	Report summarizing root causes of turnover in excess of target and steps taken to stabilize
Tour conduct: Percent of checkpoints correctly registered	Number of hazards detected, mitigated and eliminated during tours
Incident reports completed and submitted on time	Quality rating of reporting, supervisory review and satisfactory resolution of reporting defects
Response time or Time Service Factor (TSF)	Percent meeting combined dispatch & response target time with satisfactory resolution of initiating event
Customer satisfaction scores (percent satisfactory)	Percent of unsatisfactory with known causes and verifiable elimination of root causes
Corrective action plans (percent compliance)	Analysis of plans by type and location to connect the dots, isolate root causes and ensure systemic mitigation of issues
Service quality	Often calculated on staff appearance, courtesy, helpfulness and other hospitality factors rather than the fundamental of security service quality
Service level improvements submitted & adopted	Improvement that measurably contributes to increased productivity at reduced cost, eliminated hours of required service or improved risk outcomes within acceptable total cost of ownership (TCO)
Number of customer requests for support	Number processed with satisfactory vs. unsatisfactory resolution as defined by the customer
Key process cycle time	Percent achieved vs. missed with proven steps to eliminate defects
🚫 Total hours required for the reporting period vs. total hours staffed	These are basic contractual compliance measures that dilute the relevance of the metrics contained in the SLA
🚫 Invoice accuracy	
🚫 Hours of training delivered	

Table 2

Are you prepared to manage your Service Level Agreement? SLA scoring may be arrayed as lowest/unacceptable to highest/exceptional (1-5 or 1-10) with financial penalties levied for below the set standard and awards for above. As may be seen in the qualitative considerations in the above table, the more difficult task for some is identifying and/or maintaining a database on the factors to use to rate or rank various elements in the SLA. Counting is much easier and less time consuming than evaluating the real quality and value of task performance.

Several corporate supplier management programs have established multi-level standards that drive the monthly or quarterly performance rating scheme. Here is an example:

- **Gold** - Supplier performance meets or exceeds expectations for all elements of the work
- **Silver** - Supplier performance for most elements meets or may exceed expectations
- **Bronze** - Supplier performance for selected elements meets expectations. Corrective actions for identified opportunities and problems are being addressed.
- **Yellow** - Supplier performance does not meet expectations for multiple elements and corrective actions have not yet been identified or implemented
- **Red** - Supplier performance clearly does not meet expectations and recovery is not likely in a timely manner. Performance on identified evaluation elements contains serious problems for which corrective action(s) were ineffective. Constitutes Notice of Termination.

Complications of multi-site SLA administration: Many supplier management and organizational business models budget and align contract administration locally. Thus, each site or region may set unique contractual standards, evaluate and rate supplier performance on its own, and sanction or compensate based on established review results. What are potentially missing are the linked and consolidated common denominators that enable the critical performance-based assessment of the supplier. Are this quarter's concerns in Region 1 the same as those in Regions 3, 4 and 7? If so, this escalates the accountability for resolution to a corporate representative rather than dealing with each set of issues locally with differing approaches and results.

Complications of multiple-supplier SLA administration: Similar but more serious issues can crop up when multiple suppliers are selected in an umbrella security service delivery model. This is especially true in multi-national or larger national contracts where no single source may be available or satisfactory, and several uniquely located and compliant suppliers are selected. Establishing a common set of expectations (as well as terminology or service descriptions) and oversight when dealing with multiple business cultures and levels of sophistication can significantly impact administration of SLA administration, service evaluation and a common baseline of service excellence.

Key Performance Indicators

In both the multi-site and multiple-supplier situations, identifying the critical few key performance measures that may be tracked across all suppliers in all locations will enable ongoing, consolidated overview and reporting on critical performance issues. It is particularly important to make a clear connection between the performance indicators and the four overarching business drivers briefly discussed below.

1. **Sensitivity and criticality of business process.** The higher the sensitivity and criticality of the business process, the more absolute should be the requirement for operational excellence in service management and delivery. Where the client's business operations possess higher degrees of exposure to threat, risk, interruption and loss, a shared contribution of oversight by corporate security management and total commitment to task accomplishment by the supplier's team are absolutely essential to the core risk management mission.

   Achieving performance excellence in these services clearly supports a primary mission of the security organization: assurance of safe and secure workplaces. The total scope of Corporate Security's service is rightly measured by timely and qualitative response to emergency and crisis events. Operational excellence for safe and secure workplace protection results in increased productivity, lower insurance cost, increased worker morale, and reduced incidence of injury and fatality.

2. **Proactive all-hazard risk mitigation.** In reactive security operations, best practices are absolutely critical. But events in this space comprise a small part of the available time of these operations. It is in the considerable balance of routine operational time where we may find increased scope and value. Opportunities to be more proactive have incented many security service providers to expand their suite of offerings. Technology installation and systems integration facilitate anomaly detection and situational awareness by more reliably seeking out hazards and risks before they occur. This requires hazard-focused planning and shift-based operations. As is demonstrated in Figure 1 below, OpEx practices directed to specific risk reduction initiatives can yield high value results and contribute in quantifiable ways to Security's value proposition.

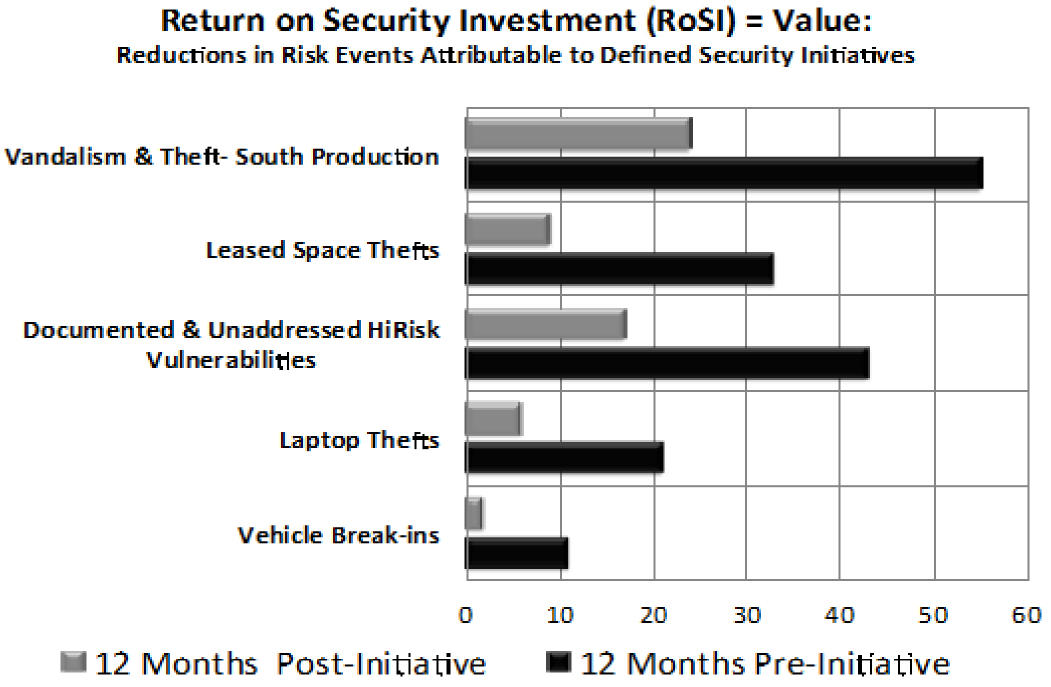


Figure 1

3. **The supplier's contribution to Security's value proposition.** At its core, operational excellence is about both real and perceived value. Where the Security department prioritizes best practices and measurable service excellence, value will be clearly advertised and delivered. Consider these four perspectives on value:

    - We may find value when the cost of a secured business process is less than the consequences from risk of interruption over time. This requires the receiver of services to see the provider as actively addressing their exposure to risk. Appropriately focused KPIs will provide that perspective.
    - The cost is additive or incrementally greater, but those at risk feel measurably safer and more productive. KPIs that clearly measure quality and risk mitigation results will provide this perspective.
    - An incremental increase in asset protection is achieved at reduced cost to the customer. This addresses a recommended KPI where the vendor actively seeks out opportunities to reduce cost.
    - A customer's expectation or service level is consistently exceeded.

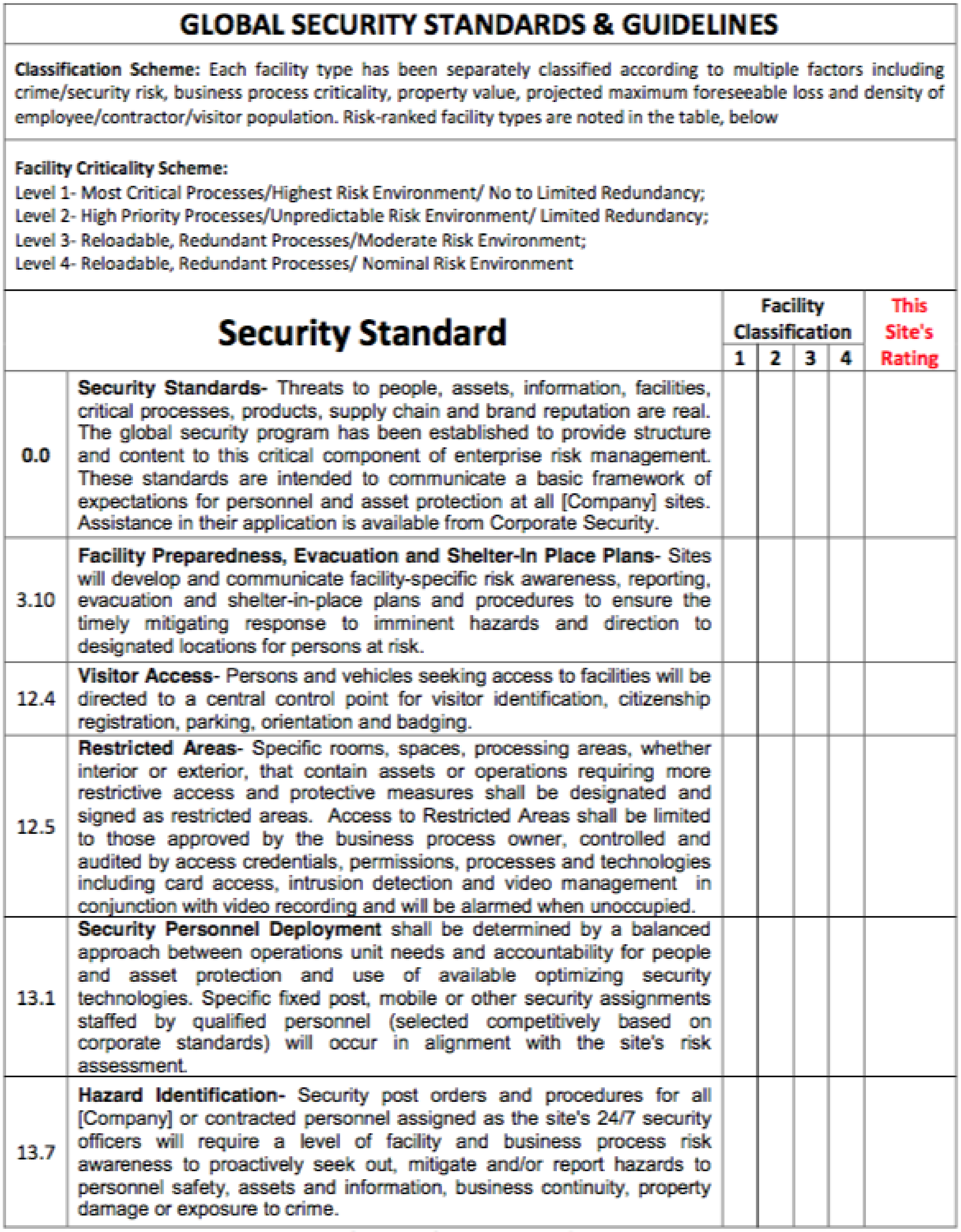
    The challenge here is how to get the supplier to own that requisite level of commitment and ingrain the essential best practices in their 24/7 operations. As may be seen in figures 3 and 4, this paper proposes fourteen KPIs and measures that we believe may serve that objective.

4. **Highly responsive customer service.** These supplier-based services may be the only direct contact the customer has with the security organization. When we can define a level of performance results that deliver a measurable benefit (like less risk or faster, better response), we can not only improve performance but also positively influence the perception of value by key constituencies or stakeholders. To that end, there are multiple points of potential convergence between a supplier and the organization’s Security stakeholders. These need to be plotted on the scalable matrix of best practices.

These four drivers form the quadrants of qualitative measurement that need to be factored into a performance management scheme for contract security services. They provide structure for more specific objectives and consideration of what constitutes best practices.

Performance Excellence Is Linked to Security Policy, Standards and Guidelines

Performance excellence and superior results in security operations cannot be achieved without a tangible connection to an established set of guidelines. A more formally grounded governance infrastructure provides for policy and standards that support aligned procedures and post orders. In Table 3 we see a few examples from a much larger set that have been tied to a site risk classification scheme. Standards establish measurable targets for key performance indicators and directly link to a set of management expectations.



GLOBAL SECURITY STANDARDS & GUIDELINES

Classification Scheme: Each facility type has been separately classified according to multiple factors including crime/security risk, business process criticality, property value, projected maximum foreseeable loss and density of employee/contractor/visitor population. Risk-ranked facility types are noted in the table, below

Facility Criticality Scheme:
Level 1- Most Critical Processes/Highest Risk Environment/ No to Limited Redundancy;
Level 2- High Priority Processes/Unpredictable Risk Environment/ Limited Redundancy;
Level 3- Reloadable, Redundant Processes/Moderate Risk Environment;
Level 4- Reloadable, Redundant Processes/ Nominal Risk Environment

Security Standard		**Facility Classification**				**This Site's Rating**
		1	**2**	**3**	**4**	
0.0	**Security Standards-** Threats to people, assets, information, facilities, critical processes, products, supply chain and brand reputation are real. The global security program has been established to provide structure and content to this critical component of enterprise risk management. These standards are intended to communicate a basic framework of expectations for personnel and asset protection at all [Company] sites. Assistance in their application is available from Corporate Security.					
3.10	**Facility Preparedness, Evacuation and Shelter-In Place Plans-** Sites will develop and communicate facility-specific risk awareness, reporting, evacuation and shelter-in-place plans and procedures to ensure the timely mitigating response to imminent hazards and direction to designated locations for persons at risk.					
12.4	**Visitor Access-** Persons and vehicles seeking access to facilities will be directed to a central control point for visitor identification, citizenship registration, parking, orientation and badging.					
12.5	**Restricted Areas-** Specific rooms, spaces, processing areas, whether interior or exterior, that contain assets or operations requiring more restrictive access and protective measures shall be designated and signed as restricted areas. Access to Restricted Areas shall be limited to those approved by the business process owner, controlled and audited by access credentials, permissions, processes and technologies including card access, intrusion detection and video management in conjunction with video recording and will be alarmed when unoccupied.					
13.1	**Security Personnel Deployment** shall be determined by a balanced approach between operations unit needs and accountability for people and asset protection and use of available optimizing security technologies. Specific fixed post, mobile or other security assignments staffed by qualified personnel (selected competitively based on corporate standards) will occur in alignment with the site's risk assessment.					
13.7	**Hazard Identification-** Security post orders and procedures for all [Company] or contracted personnel assigned as the site's 24/7 security officers will require a level of facility and business process risk awareness to proactively seek out, mitigate and/or report hazards to personnel safety, assets and information, business continuity, property damage or exposure to crime.					

Table 3- Sample Standards & Guidelines

Policies and standards are designed to provide operational direction and control. They also provide alignment with related key performance indicators. For example, using the Hazard Identification (13.7, above) standard, a guard force KPI could be "number of hazards proactively identified, documented and mitigated per shift." In a large facility, it is difficult to envision a well-trained and motivated security operation not being able to identify and document multiple hazards or security defects.

Seeking Service Excellence

When a large global manufacturing company wanted to examine their notion of service excellence, they brought a small team of their line Security managers together and laid out a set of key performance measures. Each KPI included an associated audit process so that the team could fully understand how the data to support measurement would be gathered and validated. Each manager oversaw a number of contracted security staff serving diverse (but globally representative) profiles of business operations, customer requirements, and threat/risk exposures. The team's exercise took 19 guard force performance measures and ranked them from 1 (low value) to 5 (highest value). Their rankings are seen in Figure 2, below.

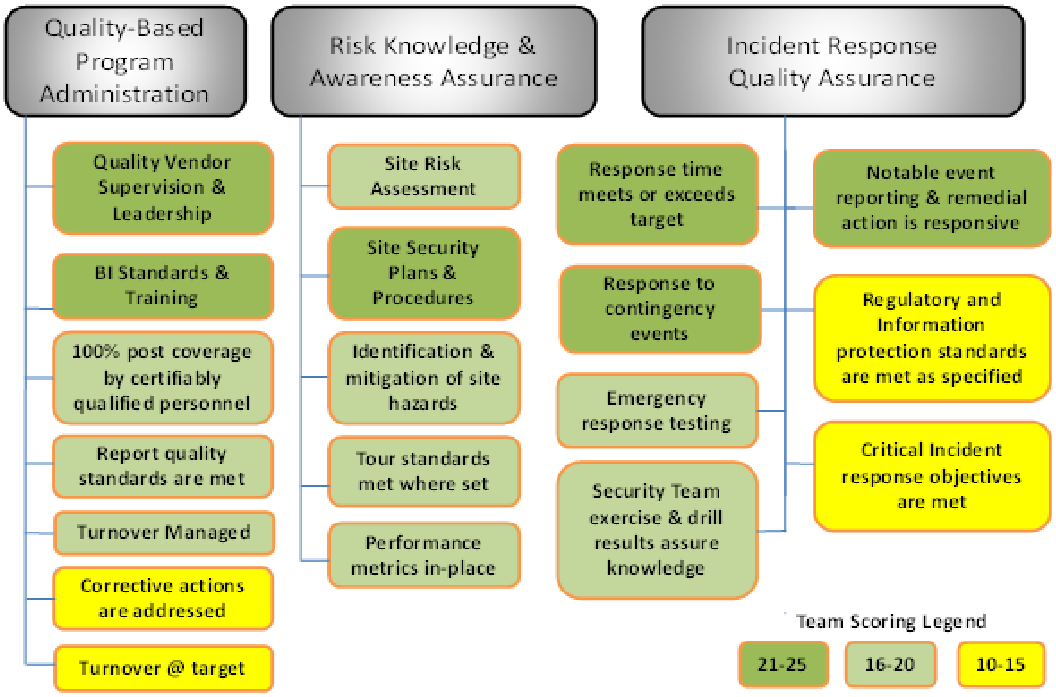

Quality-Based Program Administration
Quality Vendor Supervision & Leadership
BI Standards & Training
100% post coverage by certifiably qualified personnel
Report quality standards are met
Turnover Managed
Corrective actions are addressed
Turnover @ target
Risk Knowledge & Awareness Assurance
Site Risk Assessment
Site Security Plans & Procedures
Identification & mitigation of site hazards
Tour standards met where set
Performance metrics in-place
Incident Response Quality Assurance
Response time meets or exceeds target
Response to contingency events
Emergency response testing
Security Team exercise & drill results assure knowledge
Notable event reporting & remedial action is responsive
Regulatory and Information protection standards are met as specified
Critical Incident response objectives are met
Team Scoring Legend
21-25
16-20
10-15

Figure 2 – Key Performance Indicators Selected for Manager Team Ranking

The Security managers' discussion determined that knowledgeable, customer-focused first line supervision drives quality and performance excellence. We know this is where the critical values, mentoring, motivation, and oversight of the standards is found, yet so many job specifications, service level agreements, and performance metrics are focused on transactional contract terms that have to be complied with in any case.

Within the ranking shown in Figure 2 we see the top third clearly emphasizing key areas of performance: leadership, the quality of incident knowledge and response, security planning and standards. The middle group focused on tactical readiness, risk awareness and staff quality. Thus, 80% of the choices went directly to qualitative measures. Given the relevance of the lowest four, the discussion acknowledged the value but noted that these few should be addressed as contractual compliance matters and generally viewed as zero-defect factors.

Excellence in Action: Measuring Key Performance Indicators

The following discussion lays out two sets of proposed KPIs that were developed through the above exercise. The first set focuses on quality of supervision and the second on excellence in prevention and response activities. Together they provide an actionable set of considerations for an OpEx-supportive service level agreement. Note the qualification: actionable. As you weigh the measures in the following KPIs, consider how each one could be applied in three distinct contexts:
1) in the SLA portion of the contract
2) in the administrative processes of day-to-day operations by the vendor and
3) by the administrator of the contract/SLA in the Security organization.

Each of these players brings a set of unique and potentially conflicting perspectives to this process of SLA administration. The contract has to be enforceable but, especially with regard to the SLA, leave room for collaboration and creativity.

Measuring and reporting on leadership, supervision and program administration - As displayed in Figure 3 below, this organization has centered one set of its performance management requirements precisely where it belongs: on the supervisors who are charged with establishing and maintaining the quality standards and the designated leaders who interact with the customer and every assigned officer 24/7/365. The seven measures displayed in the following chart are directed to leadership and program administration and focus the team’s performance clearly on the competencies of the site supervision team.

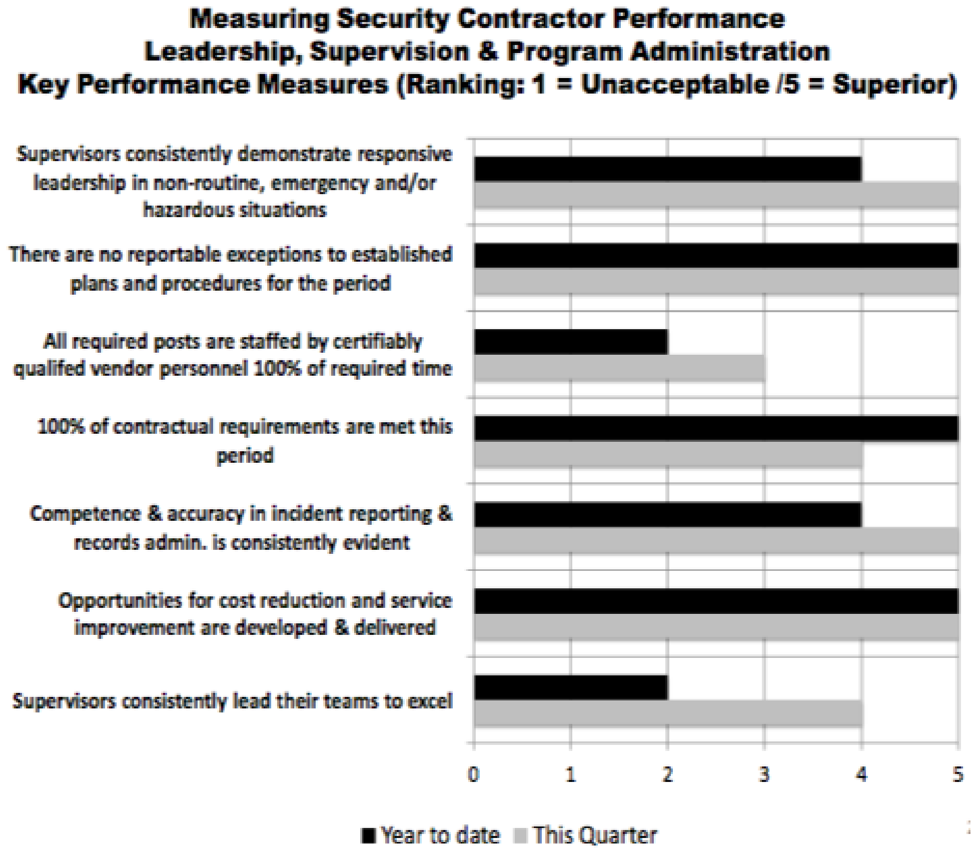


Figure 3 – Supervisory KPIs

Supervisors consistently lead their teams to excel. How do you define business or operational excellence in your company and why shouldn't it be applied to your contracted security team? You have to work with the supplier to spell out how this measurement would be demonstrated in your unique operational environment. This is one of those measures that requires discussion and development of examples, but the discussion alone will have great benefits for the shared notion of service excellence and leadership.

Opportunities for cost reduction are developed and delivered. Why wouldn't you charge the supplier's on-site team leaders to seek out opportunities to reduce cost and improve service levels in key areas of operation? If they need to add cost to address your increase in scope, where can these costs be absorbed by reducing less value-based work? All too often we see scope creep as new tasks are added without ever probing what work was unproductive or outdated and could be eliminated.

Competence and accuracy in incident reporting is consistently evident. These are the records that keep you advised of risk and responsiveness, not to mention the first things requested in litigation discovery. The supervisor's competence in quality and accuracy is mandatory.

100% of contractual requirements are met this period. The contract directs compliance on contractual details, so don't waste space in the SLA just repeating these items. The supervisors need to oversee these elements daily.

Independent review affirms that customers have trust and confidence in the contractor's team. The key here is "independent review." This relationship needs to be periodically measured by your own staff or representative to gain reliable feedback on performance. Use incident reports for input.

There are no reportable exceptions to established plans or procedures this period. A flat zero tolerance seems to make perfect sense. Should exceptions be noted, they should be accompanied by detailed documentation of supervisory findings and recommended remediation.

Supervisors consistently demonstrate responsive leadership in non-routine, emergency and hazardous situations. This is the basic measure of how they lead from preparation to execution. Expect good leadership when all is well. Measurably outstanding leadership when confronted with the infrequent crisis or the clearly hazardous situation is the mark of excellence.

Measuring & reporting on response to threat and risk. It goes without saying that customers expect flawless response when there is an incident that threatens their safety or security. In the typical operational environment, events like these are extremely infrequent - but they are possible, and conditions that contribute to their higher likelihood are variables for which effective preparation is the foundation of superior results. The IT security sector has seen dramatic escalation in threat probability and consequence over the past couple of decades. The insider always persists as a serious risk.

Acquiring or locating a business operation in a high crime or disaster-prone site presents a whole new set of strategic and tactical requirements for organizations whose prior experience was perceived as safe, secure and resilient. The 24/7 officers are the first responders for whatever may occur and should be staffed and deployed to respond to critical events significantly faster than external public safety resources.

In this next example (Figure 4), the security organization maintains the supervisory emphasis while raising the bar on performance expectations related to incident response and management. It would be worthy of a serious discussion if you were to get pushback from the vendor on any of these measures.

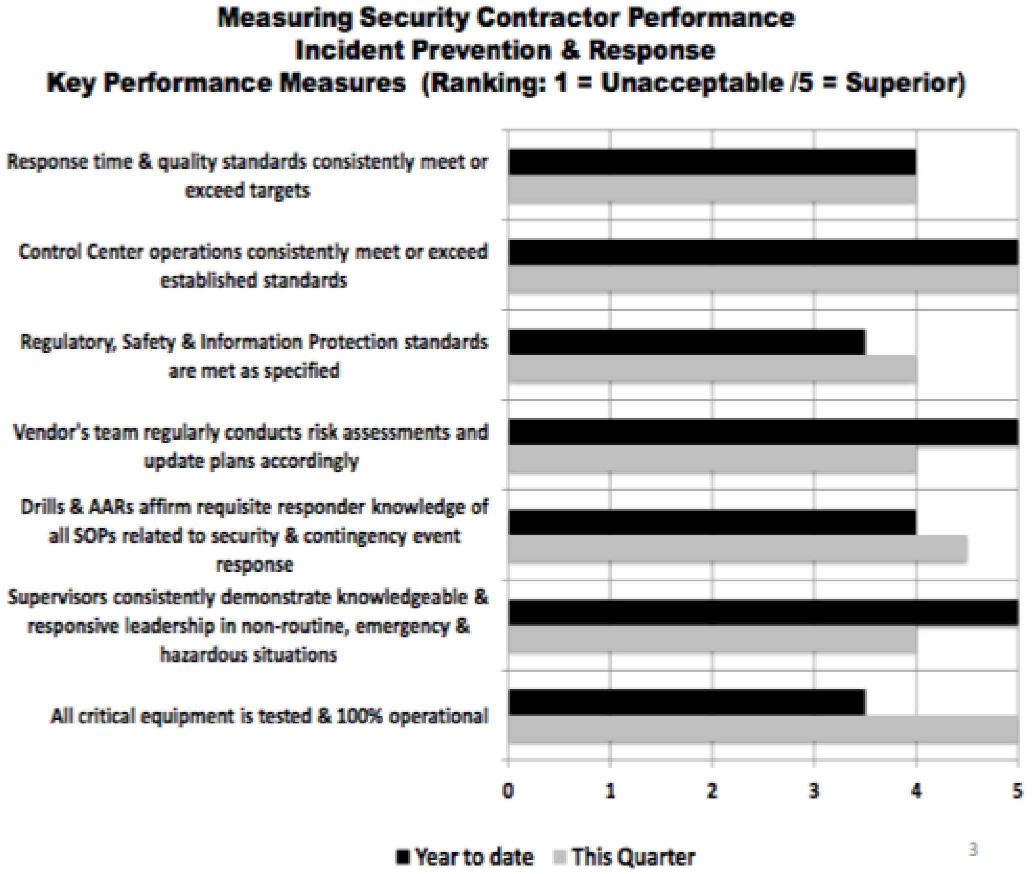


Figure 4- Incident Prevention & Response KPIs

Security Service team regularly assesses site risk and updates plans. Maintaining a thorough understanding of a site's exposure to threat and risk is a fundamental responsibility of the Security organization. Your supplier's team arguably needs to be at the center of this process. When they are the responders, they see and document the hazards 24/7 and (should) recognize anomalies and changes in the threat profile.

Response time & quality standards consistently meet or exceed targets. You will have events that require your responders to get there fast and know what to do with total assurance when they arrive.

Regulatory, safety and information protection standards are met as specified. This is all about foreseeability and why we have established patrol plans, tour standards and response guidelines to ensure that officers and supervisors are being proactive in inspecting and identifying foreseeable hazards as well as addressing specified business needs.

Control center operations consistently meet or exceed standards. Your control center operation is a key element in qualitative response to risk events and customer service. In this example, the organization has established clear performance standards for call management, incident documentation, response assistance and situational awareness.

Supervisors consistently demonstrate knowledgeable and responsive leadership in non-routine, emergency and hazardous situations. As noted in the first example, we have to focus performance measurement squarely on the supervisors and lead officers. They are the focal point for quality management and performance excellence and play a particularly critical role regarding incident prevention and response. This is where the results have to be consistently and flawlessly delivered.

Drills & AARs affirm requisite responder knowledge of all SOPs related to security & contingency event response. Good supervisors will ensure preparedness even if your contingency procedures have not specified a scenario. After-action reviews should be an established routine after any notable event, and what is learned about everything from vulnerability to procedures to training and more is totally worth the effort. Similarly, exercises and drills ensure responsiveness and knowledgeable action when it is most needed.

While there are many processes to choose from, these seven provide a solid cross-section that support this set of mission-critical functions. Each one contributes to the overall assessment of service excellence.

Security's reliance on technology and related service providers. The expansive growth of technology in the physical security space has brought a whole new set of players, opportunities and challenges to performance management. Where the client has an on-site control and communication center, the contract security team typically will staff it. Alternatively, Security (or Facilities) may engage a third party central station service for basic alarm monitoring, notification and response. An example of one set of performance measures is seen below (Figure 5).

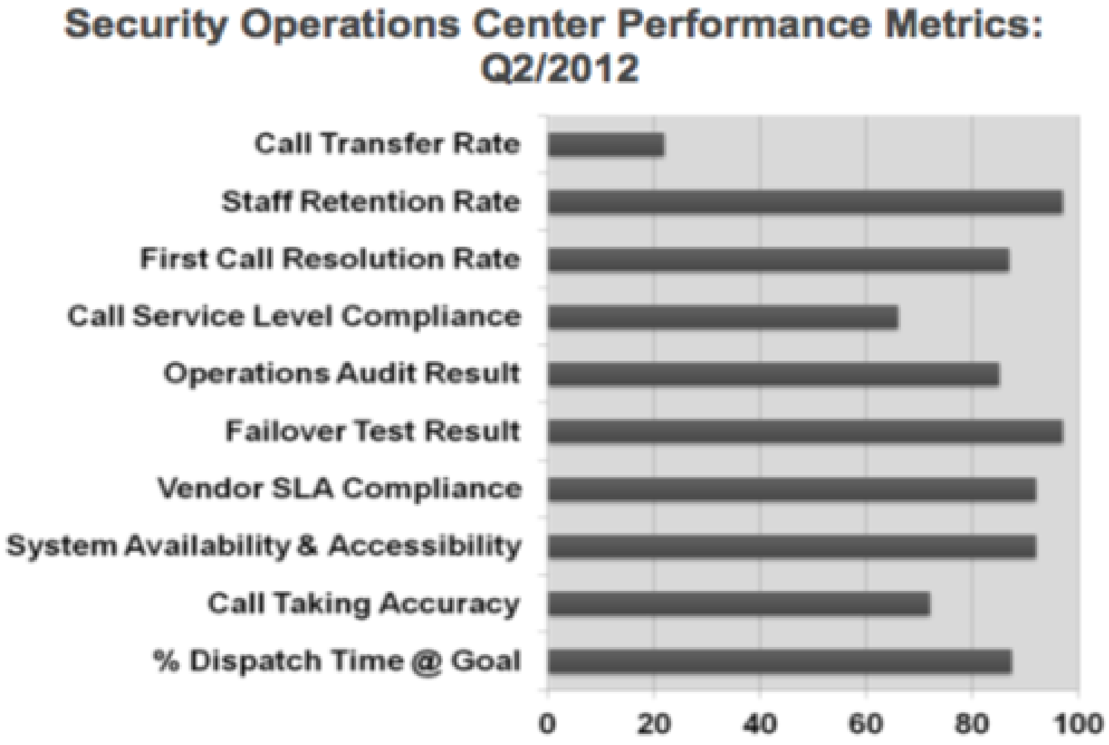


Figure 5 – Security Operations Center Measures

We have published a separate treatment of operational excellence in proprietary Global Security Operations Centers (GSOCs)[6]. Owing to the critical role these services deliver, incorporating measurable performance specifications and SLA requirements in contracts with them is essential.

A Different Business Model

If we had a clean slate for an organization's contracted physical security model that included many of the elements we see in Figure 6, what would a service provider's business model have to look like?

[6] Defining Best Practices in Global Security Operations Centers, Security Executive Council, March, 2014.

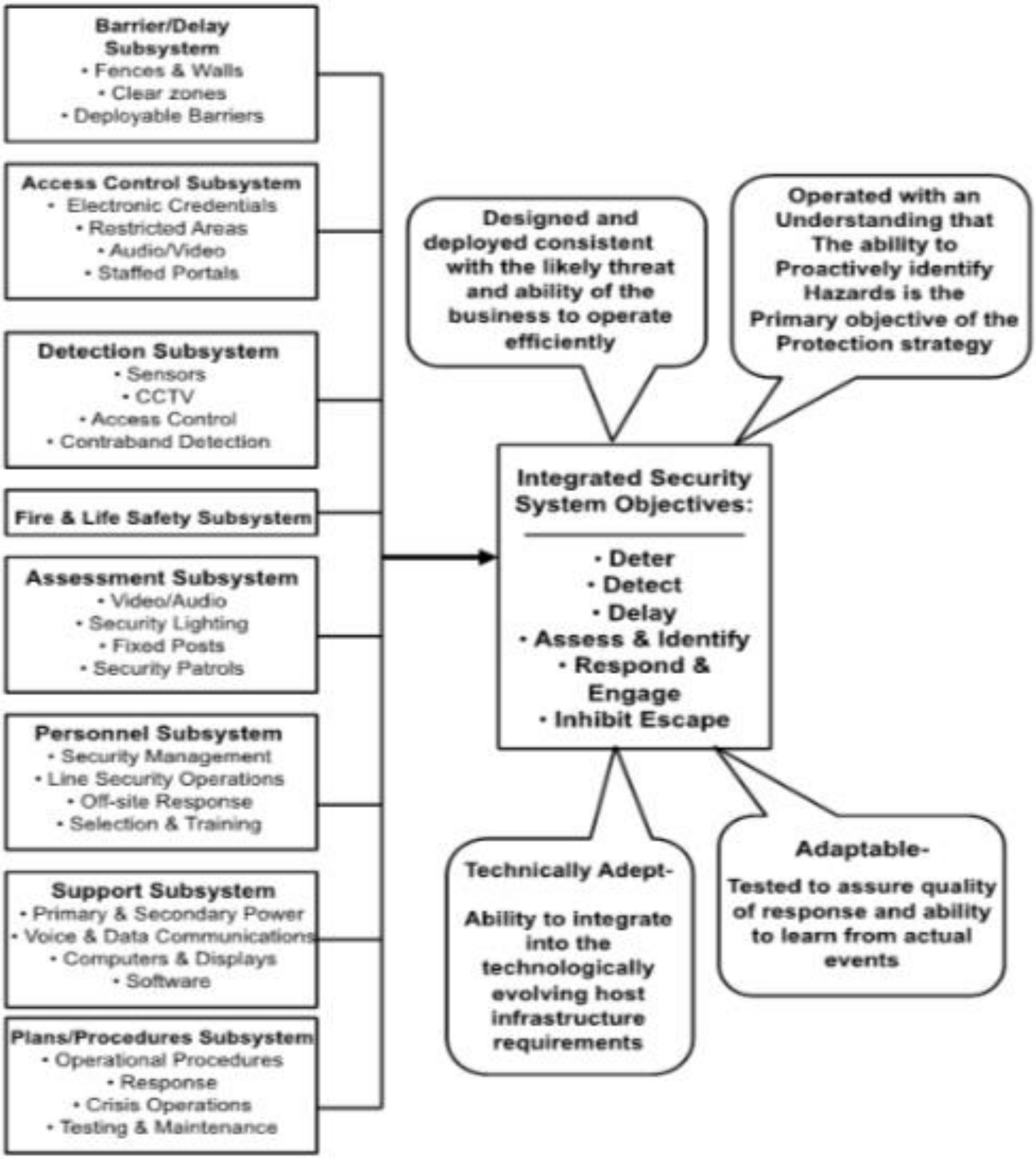


Figure 6 – Elements of an Integrated Physical Security Program

All of these elements could be provided by contracted service organization.

Many security service providers have seen the opportunity and are blending technology into their established customer relationships. Alf Goransson, President and CEO of Securitas, alluded to the opportunity as follows:

> "There is a clear trend in the security industry: labor is becoming more expensive and complex, with new rules and regulations every year. Technology is developing fast and becoming less expensive, and in combination with a new generation of high-capacity telecom networks, the transmission of images and videos is becoming more viable and secure.
>
> This is enabling us to change our service content and offer better security at a lower or equal cost, which is a critical shift in those countries where salary costs are relatively high. In addition, video analytics and intelligent cameras are enabling us to determine suspicious or dangerous behavior at an early stage, thereby minimizing the risk of business interruption.
>
> In short, we can detect potential crime before it happens, and do it more cost- efficiently than before. A pretty good value proposition!
>
> This combination creates a paradigm shift and a brilliant opportunity for security companies that are able to make investments in technology, monitoring and response capacity, and have the financial strength to invest in the required equipment. Security companies that do nothing will not survive over the long term – and this will simply be a matter of time, since creating customer value by only selling guarding hours will become increasingly difficult."[7]

Mr. Goransson sees the part of the opportunity that is easily attached to the manned functions he is already supplying: command center video monitoring. Real examination requires a vendor that is capable of engaging the customer with a holistic approach to risk and service-based requirements rather than through the lens of its core "guard force" model of selling hours with a bit of technology attached.

We have seen the less than enthusiastic results of an SLA factor that sets a target for identifying opportunities to eliminate manpower-intensive posts in favor of technology. Some providers are serious about a challenge like this and actively collaborate with an integrator or technology supplier to identify and deliver a value-added solution. But what if the supplier could do it all? What if they were to provide a wholly integrated suite of physical security services, grounded on a solid foundation of risk assessment, and incorporating the responsive mix of people, technology, process and truly OpEx-engaged supervision and management? Could a model like this be as culturally attuned as a proprietary organization while delivering consistently measurable quality at a more competitive price?

[7] White Paper on the U.S. Contract Security Industry, Robert H. Perry & Associates; Greensboro, NC; July, 2015, page 4

Closing Thoughts

Service cost and stakeholder investment are two prerequisites that linger as potentially significant variables for the reality of operational excellence. On one hand we should ask if organizations that rely upon these suppliers would be willing to pay a premium for incrementally higher-quality service levels that may contribute to OpEx and best practice KPIs; the most notable being the sum of risk event outcomes and security cost. On the other, we should legitimately ask if these security service companies would need to or want to make the investment that it might take to deliver this level of service. Regardless, the initiative will not come from the service sector; it must come from the Security executives that recognize the duties and benefits of excellence in these core security services.

How should we specify and judge the performance of our contracted security service providers? What should we expect from a supplier who is providing a service that may be called upon to save a life, alert and protect our employees from harm or eliminate a hazard that could threaten our customers and continuity of our business operations? This discussion has not intended to influence organizations that are satisfied with minimal performance requirements and low-bid responses from service providers that are, in any case, clueless regarding operational excellence. These notes are intended for those who are interested in evaluating how to measurably engage and work to improve the performance of their security contractor; to exceed the expectations of their Brand.

If you accept that the security officer may be the only contact a typical employee has with the security organization, doesn’t it follow that this contact may have defined how the whole security program is perceived? How can you not demand anything but operational excellence from that officer and from his or her employer? If you seriously consider the reasoning behind operational excellence in security operations and the few examples that are used here, perhaps the idea of opening a dialogue with your service provider on the opportunity for both parties is worth the effort.

Visit the Security Executive Council website for other resources in the Demonstrating Value: Operational Excellence 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/