LORICA

LORICA PAPERS

Operational Coordination in Private Security

Why Private Security Is an Ideal Proving Ground for Shared Operational Infrastructure

Series Industries
Version 1.0
Published June 26, 2026

Introduction

Over the past two decades, the operating model of the private security industry has evolved significantly. While firms continue to maintain internal workforces, an increasing share of client work now depends on trusted networks of subcontractors, specialized providers, and regional partners. Executive protection companies routinely extend their geographic reach through partner organizations. National guarding providers subcontract work outside their primary markets. Global security firms coordinate hundreds of independent companies to support multinational clients.

This evolution has made the industry substantially more capable. Organizations no longer need to employ every specialist internally or establish offices in every location in order to serve complex customer requirements. Instead, they assemble trusted teams from networks that may span multiple companies and jurisdictions.

That shift has also introduced a different operational challenge. Coordinating work across multiple independent organizations is fundamentally different from managing work within a single company, yet much of the software supporting the industry was designed around the latter operating model.

The challenge has evolved from managing a security company to coordination a security network – yet most industry software remains organization-centric.

Internal Efficiency and External Coordination

Over the past twenty years, security companies have invested heavily in systems that improve internal operations. Scheduling platforms manage employee assignments. Human resources systems maintain personnel records. Credential management platforms track licenses and certifications. Payroll, accounting, and customer relationship systems streamline administrative processes and improve visibility within the organization.

These systems remain essential, but they generally assume that the company performing the work is also the company employing the personnel.

Increasingly, that assumption no longer reflects how many security organizations operate.

Large client engagements frequently require several independent companies to work together. Each organization maintains its own personnel records, credential information, pricing structures, communication channels, and operational procedures. Those systems may function well individually, yet relatively little infrastructure exists to help them coordinate effectively with one another. As partner networks expand, the amount of coordination required grows accordingly.

This distinction is becoming increasingly important. Internal efficiency remains essential, but operational success increasingly depends on how efficiently organizations coordinate beyond their own boundaries.

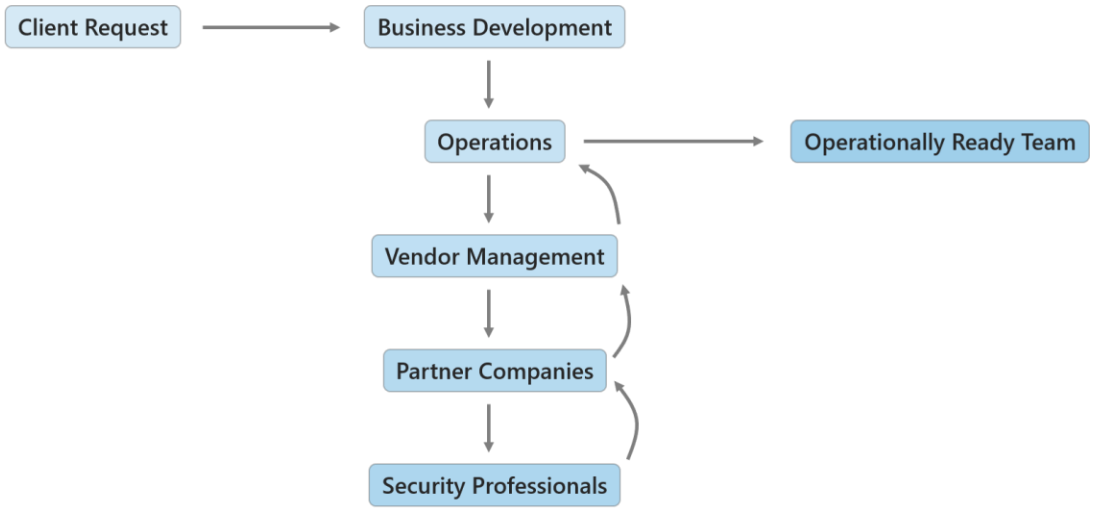
A Typical Request

Consider a common enterprise request. A client contacts a national security provider seeking executive protection support for an upcoming trip to Texas. In addition to several executive protection agents, the assignment requires a Technical Surveillance Counter-Measures (TSCM) sweep before the principal arrives.

The request typically begins with Business Development or Operations. The organization first determines whether it has appropriately qualified personnel available internally. If sufficient resources already exist, planning can proceed quickly. More often, however, at least part of the request must be fulfilled through external partners.

Operations and Vendor Management begin identifying companies capable of supporting the assignment. Those vendors determine whether they have qualified personnel available and, if not, may contact trusted subcontractors or independent contractors within their own networks. At the same time, Business Development frequently requires pricing information before responding to the client. That pricing depends on which vendors ultimately participate, what personnel they can provide, travel considerations, and other operational factors.

Information begins moving in several directions simultaneously.



At each stage, decisions depend on information that often resides in different departments or different companies. Personnel availability, credential status, pricing, geographic coverage, client requirements, and operational readiness must all be evaluated before the organization can confidently commit resources.

None of the individual steps are inherently inefficient. Each organization is making reasonable operational decisions based on the information available to it. The challenge is cumulative. Every

additional organization introduces another layer of communication, verification, pricing, and coordination before a definitive response can be provided to the client.

The limiting factor is often not finding qualified personnel. It is reaching confident operational decisions quickly enough to meet customer expectations.

Operational Readiness

The private security industry has traditionally measured operational strength by the size of an organization's workforce, geographic footprint, or specialized capabilities. Those factors remain important, but they are increasingly complemented by another competitive advantage: the ability to move rapidly from an initial client request to an operationally ready team.

Organizations that can quickly evaluate available resources, identify trusted partners, verify qualifications, assemble appropriate personnel, and communicate confidently with customers are generally better positioned to pursue new opportunities and respond to changing operational requirements.

As companies expand geographically, pursue acquisitions, or deepen their partner networks, this challenge becomes more pronounced. Every additional relationship increases capability while also increasing the amount of coordination required to transform customer demand into operational execution.

Operational readiness is therefore becoming less dependent on how efficiently individual organizations manage their own workforces and more dependent on how efficiently trusted organizations can make decisions and coordinate work together.

An Emerging Operating Model

Existing software will continue to play an essential role in managing employees, schedules, payroll, credentials, accounting, and customer relationships. Those systems solve important problems and are deeply embedded within the industry's daily operations.

At the same time, a complementary category of operational infrastructure is beginning to emerge. Rather than replacing existing systems, this infrastructure focuses on improving how information and work move between trusted organizations. It enables companies to identify qualified personnel more quickly, coordinate with established partners more effectively, respond to customer requests with greater confidence, and expand their operational networks without proportionally increasing administrative complexity.

This represents a natural evolution of the industry's software requirements. As private security becomes increasingly networked, the systems supporting it will increasingly need to facilitate operational coordination across organizations rather than simply manage activity within them.

A Different Approach

Lorica is being developed around this observation.

Rather than replacing scheduling platforms, HR systems, credential management software, or customer relationship tools, Lorica is intended to complement those systems by improving the flow of operational information between organizations. The platform focuses on the processes that occur between an initial customer request and an operationally ready team, including staffing

requests, credential readiness, pricing, trusted partner relationships, and cross-company coordination.

The objective is straightforward: reduce the time and effort required to transform customer demand into operational execution.

Whether an organization is coordinating a local executive protection assignment or activating a global network of trusted partners, the underlying challenge is increasingly the same. As the industry's operating model continues to evolve, we believe the software supporting it will increasingly evolve in the same direction.

This document reflects our current thinking and is intended to encourage discussion with security operators, customers, and investors. We expect both the platform and these ideas to continue evolving as we continue learning from organizations across the private security industry.