March
2026

# ORGANIZATIONAL LEVERAGE POINTS FOR COUNTERINTELLIGENCE PROFESSIONALS

JOB AID

CDSE Center for Development of Security Excellence

# Introduction

This Job Aid provides a foundational framework for counterintelligence (CI) and security professionals to identify and act upon organizational leverage points. This proactive approach allows professionals to strategically multiply their impact and build a lasting security culture by shifting focus from reacting to individual incidents to identifying fundamental opportunities to address vulnerabilities and their root causes.

## What are Organizational Leveral Points?

Organizational leverage points are specific places in an organization where focused energy can produce disproportionate effects across the entire enterprise. For the CI professionals, organizational leverage points are opportunities to scale their unique expertise, integrating CI principles into organization's mechanics, culture, and workforce. Thoughtful integration has a force multiplying effect, which amplifies security awareness, capability, and resilience far beyond what a CI team alone can achieve.

## A Framework for Organizationl Leverage

There are three broad categories of organizational leverage points: Operational, Policy, and Cultural. While some may be "owned" by security, the majority likely fall under other functional areas. Identifying a leverage point is only the first step; the true challenge is gaining the access and influence required to create change. Building relationships and maintaining partnerships with key stakeholders is the difference.

**Definition**: Organizational leverage points are specific areas within an organization—such as its processes, policies, or culture—where small, focused intervention can produce significant and widespread improvements across the entire enterprise. Definition: Organizational leverage points are specific areas within an organization—such as its processes, policies, or culture—where small, focused intervention can produce significant and widespread improvements across the entire enterprise.

# Category 1: Operational Leverage Points

Operational leverage points are potential opportunities to influence tangible infrastructure, systems, and business processes and workflows. They can have immediate impact as well as inform decisions with lasting implications.

| Point of Integration | CI Application & Example | Potential Stakeholder(s) |
|---|---|---|
| **IT Architecture and Design Decisions** | Participate in IT architecture reviews to influence fundamental system design and shape access control models before deployment.<br><br>*"Are we introducing foreign technology?"*<br><br>*"Does new software allow for adequate activity logging?"* | Cybersecurity, IT |
| **Threat Detection Workflow** | Collaborate with Insider Threat team to define CI-relevant indicators for their behavioral analytics and anomaly detection.<br><br>*"Let's define what a CI-related concern is and establish a protocol to notify us (the CI Team)."* | Cybersecurity, IT, Security |
| **Vendor Approval Process** | Enhance the procurement approval process by developing a role to evaluate from the CI perspective.<br><br>*"There is a real benefit in reviewing for foreign ownership, control, and influence (FOCI) concerns."*<br><br>*"These are not concerns that would be revealed by cybersecurity evaluations."* | Procurement, Supply Chain Risk |
| **Applicant Vetting Process** | Inform interview and hiring process by establishing CI-relevant risk indicators, techniques to evaluate, and processes to notify CI Team should concerns arise.<br><br>*"We need to integrate some interview techniques for identifying deepfake applicants or applicants using deepfake technology."*<br><br>*"Let's refine some of our questions on our new hire application."* | Human Resources, Legal |

# Category 2: Policy Leverage Points

Policy leverage points focus on codifying CI-relevant concepts or requirements into the formal rules, governance structures, and strategic goals of the organization. They inform the acceptable parameters for how the organization operates.

| Point of Integration | CI Application & Example | Potential Stakeholder(s) |
|---|---|---|
| **Strategic Business Dealings** | Shape pre/post decision-making regarding mergers, acquisitions, joint ventures, and partnerships.<br><br>*"This joint venture could create sudden and dramatic changes to an organization's risk surface. A more comprehensive due diligence effort that incorporates a CI review is absolutely necessary."* | Executive Leadership, Legal, HR, IT, Cybersecurity |
| **Visitor Management** | Ensure visitor protocols account for all risk scenarios and are applied enterprise-wise.<br><br>*"Our red team review shows a real need to establish a screening process for foreign national visitors and 'no visitor' zones for sensitive areas. And this needs to be consistently applied across all sites."* | Security, IT |
| **"Acceptable Use" Determinations** | Influence decision-making on how the workforce can transfer data, internally and externally.<br><br>*"Our metrics show extensive employee data transfers using removable media, despite access to more secure transfer tools. We strongly recommend strengthening the Organization's written policy and technical IT policies."* | Cybersecurity, IT |
| **Travel Risk Management** | Shape the corporate travel policy to better account for evolving geopolitical risk landscape.<br><br>*"In addition to conducting pre-travel security briefings and post-travel debriefings, there are certain locations where employee IT devices are also at much greater risk. We should consider addressing that risk through IT Policy as well."* | Security, Legal, HR, Cybersecurity, IT |

# Category 3: Cultural Leverage Points

Cultural leverage points are the most transformative and lasting. They focus on changing the fundamental beliefs, mindsets, and day-to-day behaviors that collectively define the organization's security culture.

| Point of Integration | CI Application & Example | Potential Stakeholder(s) |
|---|---|---|
| **Employee Onboarding** | Shape the new hire onboarding experience to establish security as a core value which they'll carry beyond Day 1.<br><br>*"Let's create a more engaging session where a senior leader welcomes new employees and frames security as a critical part of the company's culture and success."* | Executive Leadership, HR |
| **Workforce Engagement** | Foster concept of "Organizational Citizenship", where employees embrace a collective responsibility, which permeates into all functional areas, including security.<br><br>*"Let's launch a campaign around the idea we're all in a position to observe, engage, help, and be positive agents of change. A workforce with a sense of collective responsibility is our strongest asset."* | Executive Leadership, All |
| **Performance Measurement** | Encourage formal inclusion of new core competencies within performance reviews that drive positive behavior.<br><br>*"We should consider adding 'organizational citizenship' as an area of evaluation."* | Executive Leadership, HR |

# Conclusion

By shaping conversations around key Operational, Policy, and Cultural leverage points, a CI professional's influence expands beyond their direct role, embedding security principles into the core elements and culture of the enterprise to create a lasting security impact.