



Using Private Investigative Expertise to Enhance Corporate Compliance

By: Billy Marlin CFE, CBA

bmarlin@veritasap.com

Executive Partner

Veritas Assurance Partners, LLC

June 26, 2025

Risk management consultants with expertise in investigations and intelligence (RMC) can significantly strengthen corporate compliance programs by bringing specialized investigative skills, forensic capabilities and discreet information-gathering techniques.

Strategically utilizing RMC in the compliance function typically results in:

- Faster resolution of complex cases
- Fewer violations identified in regulatory reviews
- Increased voluntary disclosure of minor violations before they escalate
- Significant reduction in repeat violations through more effective deterrent measures.

Here's how organizations can effectively integrate independent investigation and intelligence consulting services into their compliance functions:

Core Contributions to Compliance Programs

1. Third-Party Due Diligence Enhancement

- **Vendor/partner/employee Due Diligence and background checks** beyond standard database searches.

- **Beneficial ownership verification** through international asset tracing.
- **Reputation assessments** via discreet field inquiries and local source networks.
- **Supply chain verification** including unannounced site visits and subcontractor identifications.

Our Insight:

Thorough background checks often identify incompatible affiliations and adverse reputational issues that often results in increased chances for potential unethical behavior. The level of validation and the extent of the searches should be commensurate with the level of potential risk associated with the position of the individual and/or company. From our own experience in dealing with hundreds of investigations for over three decades, it pays to be proactive as the reputational, legal and financial cost of unethical violations is often miniscule when compared to the cost of a thorough due diligence or background check.

Sometimes the most relevant evidence is unexpected and comes from indirect relationships as in a recent case where the subject, who had an out of wedlock child with the client, was attempting to blackmail him. Our investigative approach was substantially modified to include mitigating risks to our client's personal safety when a due diligence on the subject revealed close affiliations with two criminal groups dedicated to illicit drug trafficking.

2. Internal Investigation Support

- **Covert surveillance** for suspected code of conduct violations and other potential illicit behavior.
- **Digital forensics** including recovery of deleted electronic communications and metadata analysis.
- **Witness interviews** locating potential witnesses and using law enforcement techniques to uncover concealed information.
- **Document authentication** including handwriting analysis and forgery detection.

Our Insight:

Substantive evidence in electronic form is often overlooked. When properly collected using advanced investigative tools, hard drives, telephone text messages often provide solid evidence on intent and collusion on theft, procurement and fraud matters. The use of advanced tools often allows trained investigators to retrieve data even after being erased from the electronic device.

In two recent cases, recovered electronic evidence has been the basis for identifying those responsible for bribery schemes within our clients' procurement process. These schemes resulted in the selection of unqualified suppliers and purchases of overpriced equipment and services.

3. Fraud Detection & Prevention

- **Asset searches** to identify hidden interests of employees or partners and verify the congruence, or lack thereof, between the official income level of these individuals and their lifestyle or standard of living.
- **Social media deep dives** using specialized tools to detect questionable behavior and connections.
- **Whistleblower validation** through independent corroboration of allegations.
- **Pattern analysis** identifying anomalies in expense reports and procurement patterns.

Our Insight:

A comprehensive profile of a vendor/partner/employee in a sensitive function should include their social media profile. We often use social media postings to establish spending habits including vacations, automobiles, personal and business affiliations etc. Social media postings can also be a valuable tool to establish personal and business connections between the subjects of an investigation.

On a recent multi-million dollars bank fraud matter we uncovered personal connections and traced the current whereabouts of several suspected perpetrators by accessing their social media interactions and meta data from two cellular phones used by the fraudsters.

Strategic Implementation Framework

Phase 1: Risk Assessment Integration

- Work with compliance officers to **identify high-risk areas needing investigative support**.
- Develop protocols for **when and how to engage investigators**.
- Establish clear **chains of custody** for evidentiary purposes.

Phase 2: Proactive Monitoring

- Implement **discreet employee screening** for sensitive positions.
- Conduct periodic **function-based exercises** for testing compliance controls.
- **Monitor dark web** for company data leaks or credential sales.

Phase 3: Investigation Response

- **Preserve digital evidence** using forensic standards.

- **Maintain investigation logs** meeting legal requirements.
- **Prepare findings** in formats suitable for civil, criminal and regulatory submission.

Specialized Compliance Applications

Anti-Bribery/Corruption

- **Undercover operations** at high-risk trade shows or conferences.
- **Payment pattern analysis** identifying unusual transactions.
- **Travel verification** confirming purported business activities.

Trade Sanctions Compliance

- **Vessel tracking** to verify claimed shipping routes.
- **Corporate veil piercing** identifying sanctioned entities using shell companies.
- **End-user verification** through international field networks.

Data Privacy

- **Breach source identification** through digital forensic techniques.
- **Dumpster diving audits** (where legal) testing document disposal practices.
- **Social engineering tests** evaluating employee susceptibility.

Best Practices for Effective Collaboration

1. **Legal Alignment:** Ensure all methods comply with company ethics and local privacy/employment laws.
2. **Documentation Standards:** Maintain investigation files that would withstand regulatory scrutiny.
3. **Training Integration:** Have RMCs train compliance staff on red flag recognition.
4. **Technology Leverage:** Utilize specialized RMC tools like advanced OSINT platforms.
5. **Reporting Protocols:** Structure findings to support both internal discipline and potential regulatory disclosures.

Conclusion

Adding the resources and expertise of a reputable RMC can be a force multiplier for compliance teams. These are the key advantages of utilizing independent investigative and intelligence services:

- **Anonymity:** Avoid tipping off subjects during sensitive probes.
- **Containment of Sensitive Information:** It is easier to avoid information leaks and maintain Confidentiality.
- **Specialized Skills:** Access to surveillance, forensic accounting, or cyber-investigation tools.
- **Jurisdictional Reach:** PIs with local expertise can navigate foreign legal/regulatory systems.
- **High-Risk Geopolitical Environments:** Using PIs to investigate vendors, partners, or employees in jurisdictions with limited public records or high corruption risks provides a better chance for identifying relevant issues not recorded in public record searches.

By combining corporate compliance frameworks with professional investigative methodologies, companies can enhance the performance of their compliance function to create a robust defense against regulatory risks while maintaining the flexibility to address emerging threats proactively.

