BSCF BUSINESS SERVICE CENTER FORUM

AMCHAM SLOVAKIA

#FUTUREREADY

PARTNERS KINSTELLAR Deloitte.

CRISIS MANAGEMENT & FRAUD INVESTIGATION IN THE BSCF SECTOR

Policy recommendations for business services and shared service operations in Slovakia.

Business services and shared service operations have become a cornerstone of Slovakia's economy since the dawn of the new millenium, supporting global organizations across finance, procurement, IT, HR, and customer operations. While these structures create efficiencies and scalability, they also introduce unique risk concentrations. Centralized processes, cross border reporting lines, high data volumes, and hybrid working environments mean that fraud incidents and compliance crises can escalate quickly and across multiple jurisdictions.

This policy paper provides practical recommendations for compliance, legal, audit, and operational leaders working in business services and captive finance environment. It reflects lessons learned from investigations, crisis responses, and regulatory matters affecting shared service centers in Slovakia.

The most critical period in any crisis is often the first 48 hours. During this phase, organizations must focus on stopping ongoing misconduct, preserving data and other evidence, defining the scope of the investigation, and establishing clear governance structures. Early missteps, particularly around data handling or internal communications, can undermine legal privilege, weaken regulatory defenses, and create unnecessary operational disruption.

The recommendations presented here aim to support the Business Service Center Forum (BSCF) community in Slovakia associated within the American Chamber of Commerce in building stronger crisis readiness, integrating legal and forensic expertise, and strengthening long-term resilience.

WHY THE BSCF SECTOR FACES UNIQUE CRISIS RISKS

Shared service centers and captive business functions operate differently from traditional corporate structures. These differences create specific investigative and compliance challenges.

Centralization of financial or operational processes can create high impact exposure when controls fail. A single weakness in procurement, payroll, or vendor onboarding may affect multiple markets simultaneously. Teams are often geographically distributed, with local employees reporting into regional or global management structures. This can complicate decision making during crises, particularly where employment law, data protection, or regulatory obligations differ across jurisdictions.

Hybrid work environments further increase risk. Employees may access sensitive systems remotely, use multiple communication platforms, or rely on shared devices. Investigations must therefore address not only misconduct but also digital evidence preservation in complex technical environments.

The intense transformation of the sector with AI brings a new set of fraud and non-compliance risks, while internal control systems did not adapt yet.

Organizations sometimes assume that local operations carry only local regulatory exposure. In reality, BSCF operations frequently fall within the scope of global anti-corruption regimes such as the U.S. Foreign Corrupt Practices Act (FCPA) or the UK Anti-Bribery Act, particularly where payments, approvals, or data flows cross borders.

GOVERNANCE IN THE FIRST 48 HOURS OF A CRISIS

Effective crisis management begins with clear governance. Organizations should establish a defined response structure that separates fact finding from disciplinary decision making and aligns operational leadership with legal oversight.

A crisis steering group should be formed quickly, typically including senior management, legal counsel, compliance, HR, and where appropriate forensic specialists. Roles and reporting lines must be clear from the outset. Uncoordinated responses often result in duplicated work, inconsistent messaging, or premature conclusions.

Immediate priorities during the first 48 hours include:

- stopping ongoing misconduct or control failures
- preserving electronic and physical evidence
- limiting unnecessary internal communications
- defining who has access to investigation information on a need to know basis

Organizations should resist the instinct to conduct informal internal reviews before establishing a structured investigation framework. Early unstructured actions can damage legal privilege and complicate later regulatory engagement. They may also lead to losses of critical evidence. Therefore the initial steps of the crisis response should be properly planned.

SCOPING THE INVESTIGATION: LEGAL AND OPERATIONAL ALIGNMENT

Defining the scope of an investigation is one of the most critical steps in managing risk. Scope determines which data is collected, which employees are interviewed, and how findings are ultimately assessed.

A well-structured scoping process aligns legal objectives with operational realities. Leaders must understand whether the investigation is primarily aimed at internal remediation, potential regulatory exposure, or anticipated litigation. These objectives influence both the methodology and the resources required.

Regulatory considerations should be assessed early. Shared service centers may trigger obligations under anti-corruption laws, sanctions and AML regimes, whistleblower protections, or data protection rules. Understanding potential exposure helps organizations avoid either under investigating serious risks or over expanding investigations unnecessarily.

Clear scoping also helps manage employee expectations and maintain business continuity. Investigations that grow without defined boundaries can disrupt operations and create uncertainty within teams.

DATA PROTECTION, PRIVACY AND LEGAL PRIVILEGE

Data handling is often the most sensitive aspect of an investigation within the BSCF sector. Shared service environments typically manage large volumes of personal and financial data across multiple jurisdictions, making privacy compliance a central concern.

Organizations should involve legal counsel before collecting or reviewing employee data. Proportionality assessments and clear documentation of investigative purpose can help demonstrate compliance with data protection requirements. Technical teams should avoid accessing or copying employee devices without proper forensic protocols, as this may compromise evidence integrity or legal defensibility.

Legal privilege is another critical consideration. Investigations that are directed by legal counsel and structured appropriately may benefit from privilege protections, depending on jurisdiction. However, privilege expectations differ between legal systems, and organizations should not assume that practices common in the United States automatically apply in European contexts.

Clearly defining the "client" of the investigation, whether the legal department, the board, or senior management, helps protect confidentiality and ensures consistent communication.

EVIDENCE PRESERVATION AND DIGITAL FORENSICS

Digital evidence plays a central role in most modern investigations. Emails, messaging platforms, access logs, and financial systems often contain key information about potential misconduct.

Organizations should issue preservation instructions promptly once a credible concern arises. Automated deletion policies may need to be paused, and relevant accounts or devices secured. At the same time, business continuity must be maintained, which requires coordination between legal teams and IT specialists.

Remote work environments create additional challenges. Employees may use personal devices or cloud-based collaboration tools, and investigators must consider how to collect data without violating privacy expectations and disrupting operations and to minimize the risk of losing important evidence.

Early involvement of forensic specialists can help ensure that evidence is preserved in a defensible manner and that technical analysis aligns with investigative goals.

CONDUCTING INTERVIEWS IN A BSCF ENVIRONMENT

Employee interviews are often a key source of information during investigations, but they must be conducted carefully to maintain fairness and credibility.

A distinction should be made between fact finding interviews and confrontational interviews aimed at accountability. Early interviews should focus on understanding processes and gathering context rather than assigning blame. Mixing investigative interviews with disciplinary meetings can create confusion and increase legal risk.

Multilingual teams and cross cultural dynamics are common in shared service environments. Investigators should consider language preferences, cultural expectations, and remote communication challenges when planning interviews.

Preparation is essential. Interview sequences should be aligned with available evidence so that discussions remain structured and objective.

FINANCIAL ANALYSIS AND FORENSIC ACCOUNTING

Forensic accounting plays an important role in identifying patterns of misconduct that may not be immediately visible through operational reviews. Shared service centers often manage high volumes of transactions, making data driven analysis particularly valuable.

Common areas of focus include vendor payments, procurement processes, expense reimbursements, and segregation of duties. Analysts may look for unusual payment patterns, duplicate vendors, or transactions occurring outside normal approval channels.

The goal of forensic analysis is not only to identify specific instances of fraud but also to understand systemic weaknesses that allowed misconduct to occur and remain undetected for months or years.

REPORTING AND DECISION MAKING

Investigation reporting should support clear decision making rather than simply documenting activity. Reports should be structured, factual, and proportionate to the risks identified.

A typical report may include:

- scope and objectives
- methodology
- factual findings
- risk assessment
- recommended actions

Organizations should avoid speculative conclusions or overly legalistic language that may limit flexibility in later discussions with regulators or employees. Separating factual findings from legal analysis can help maintain clarity and protect confidentiality.

Senior leadership should receive concise summaries that allow for timely decisions on remediation, disciplinary measures, or regulatory engagement.

DISCLOSURE AND REGULATORY STRATEGY

Decisions about whether to disclose findings to regulators or law enforcement require careful analysis. Disclosure may reduce regulatory exposure in certain circumstances, but premature or incomplete disclosures can create additional risk.

Organizations should consider the nature of the misconduct, jurisdictional exposure, and potential parallel proceedings. Cross border coordination is particularly important where shared service activities support multiple markets.

Communication strategies should be aligned across legal, compliance, and public relations teams to ensure consistency and avoid unintended admissions.

REMEDIATION AND BUILDING LONG TERM RESILIENCE

The end of an investigation should mark the beginning of long-term improvement. Effective remediation goes beyond disciplinary action and focuses on strengthening systems, processes, and culture.

Common remediation steps include redesigning approval workflows, enhancing monitoring controls, updating training programs, and improving escalation channels. Leadership messaging plays a critical role in reinforcing ethical expectations and restoring trust within teams.

Organizations that treat remediation as a strategic opportunity often emerge stronger and more resilient after a crisis.

KEY TAKEAWAYS FOR THE BSCF COMMUNITY

The experience of crisis management across the BSCF sector highlights several consistent lessons:

- The first 48 hours are critical for protecting evidence and defining strategy.
- Legal, forensic, and operational teams must work as an integrated unit.
- Investigations should be planned before data collection begins.
- Clear governance structures reduce confusion and support faster decisions.
- Long term resilience depends on thoughtful remediation, not only immediate fixes.

By combining legal insight, forensic expertise, and operational awareness, organizations can respond to fraud risks in a way that protects both business continuity and regulatory standing.