Integrity risks in times of geopolitical tensions

How organizations can strengthen governance, controls and resilience during and after periods of tension

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

Geopolitical dynamics and continued uncertainty contribute to challenges impacting trade routes, energy markets and cross border payments.

In such environments, organizations may be required to operate at speed, often under limited oversight, rapidly changing regulations and increased operational complexity. These considerations may have implications beyond financial and regulatory outcomes, including reputational and operational impacts.

Changes to procurement process, evolving sanctions obligations, third party dependencies, workforce dynamics and changing operating conditions can increase exposure to integrity risks across organizations.

Traditional control frameworks, designed for stable operating environments, may require adaptation in the face of urgency, uncertainty and resource constraints.

The discussion will focus on the below topics:

How geopolitical changes reshape the integrity risk landscape

What can organizations do to adapt their governance and control response during periods of geopolitical uncertainty and transition.

As geopolitical dynamics becomes a persistent feature of the global operating environment, organizations that fail to anticipate and respond to integrity risks arising from geopolitical changes expose themselves to potential financial loss, regulatory scrutiny, reputational impact and strategic challenges.

This paper is intended to support senior leaders, risk professionals and compliance teams in understanding these risks and strengthening resilience in an era of sustained geopolitical uncertainty.

Emergency procurement and contracting risk

01

Emergency procurement and contracting integrity risks arise when organizations procure goods or services rapidly, often bypassing standard procurement processes. The urgency to secure critical supplies – such as fuel, logistics support, security services, IT infrastructure or emergency facilities – reduces competitive tension and weakens scrutiny.

Typical schemes

- Price gouging, inflated invoices and "emergency premium" abuse
- Collusion with vendors, kickbacks and bid steering
- Ghost suppliers or shell entities created to exploit urgent demand
- Contract splitting to bypass thresholds and approvals

Strategic focus areas

- Logistics and transportation services
- Fuel, energy supply and critical spares
- Security, defense and guarding services
- IT, cybersecurity and emergency systems support
- Temporary facilities, housing and infrastructure
- Crisis advisors, consultants and dedicated service providers

Geopolitical tensions can create an integrity risk "spike" during active disruption as organizations operate under urgency, unpredictability and evolving oversight conditions.

What causes this?

These integrity risks are typically driven by a combination of structural and behavioral control weaknesses, including the following:

- Relaxation or suspension of competitive tendering and sourcing requirements
- Weak or unclear emergency procurement policies and approval frameworks
- Inadequate price benchmarking or independent cost validation
- Reduced segregation of duties due to resource constraints
- Limited or no third-party due diligence on newly onboarded suppliers
- Poor visibility over cumulative emergency spend and exceptions
- Insufficient documentation and audit trails for emergency decisions

What can organizations do?

- Establish a crisis procurement governance framework with clearly defined approval thresholds, decision rights and non-negotiable controls
- Require minimum price validation (benchmarking, rate cards or independent estimates) even during emergencies
- Use pre-approved emergency supplier panels and framework agreements where possible
- Enforce beneficial ownership declarations and sanctions screening for high-risk suppliers
- Apply maker-checker controls for contract awards and payments
- Monitor cumulative spend to detect contract splitting and threshold abuse
- Flag emergency contracts in enterprise resource planning (ERP) systems for enhanced post-event review

Trade, sanctions and cross-border integrity risk

02

Geopolitical dynamics often trigger rapid changes in sanctions regimes, trade restrictions and routing patterns, creating confusion and compliance blind spots. For example, such issues occur when counterparties conceal a sanctioned party's involvement (ownership, control and end user), misrepresent the origin or destination of goods. They may also alter trade documentation to move controlled items, dual-use products or funds across borders.

Typical schemes

- Concealing beneficial ownership (front companies and layered intermediaries)
- Misrepresentation of origin or end use, falsified certificates and re-routing shipments
- Over or under-invoicing, phantom shipments and dual invoicing
- Use of "high-risk corridors" and grey market sourcing

High-risk areas

- Cross-border procurement, imports or exports and freight forwarding
- Trading (commodities, refined products, chemicals and metals)
- Agents or intermediaries, distributors and brokers
- Letters of credit, trade finance instruments and documentary collections
- Customs clearance, certificates of origin and end user certificates
- Re-exports and trans-shipment arrangements

What causes this?

- Inadequate or outdated sanctions screening (entities, vessels and goods)
- Weak visibility of beneficial ownership and "control" structures
- Overreliance on third-party self certifications or declarations without verification
- Limited governance over agents and intermediaries (commission abuse)
- Fragmented trade documentation controls (manual processes and inconsistent checks)
- Weak escalation protocols when sanctions guidance changes mid-transaction

What can organizations do?

- **Sanctions controls embedded into the transaction flow:** screen at onboarding and before shipment or payment; apply holds until cleared
- **Beneficial ownership validation for high-risk counterparties and intermediaries:** require structured attestations and documentary proof
- **Trade document integrity checks:** standardize verification of origin or end-use, harmonized system (HS) codes, vessel tracking (where relevant) and routing logic
- **Intermediary governance:** clear justification for agents, transparent fee structures and enhanced monitoring for unusual commissions
- **Dynamic compliance updates:** a "sanctions change bulletin" process with rapid procedure updates, training and mandatory re-check triggers
- **Audit and analytics:** anomaly detection for abnormal pricing, routing, repeated intermediaries and inconsistent trade document

Payment integrity risk

03

Payment processes often become more decentralized and time-sensitive. This creates opportunities for unauthorized payments, duplicate payments, manipulation of bank details and diversion of funds through informal or weakly controlled channels.

Typical schemes

- Urgent payments processed without full review
- Vendor impersonation or executive impersonation
- Bank account changes without proper verification
- Duplicate or split invoices
- Emergency disbursements with limited support

High-risk areas

- Emergency disbursements, ad hoc transfers and time-sensitive supplier payments
- Vendor master data changes (bank accounts, addresses and contacts)
- High-value categories: fuel, logistics, security and spares
- Cash advances, petty cash, travel or security allowances
- Foreign currency conversions, settlement terms and off-cycle payment runs

What can organizations do?

- **Bank detail change controls:** call-back verification to known numbers, dual approval and cooling off-periods for high-risk changes
- **Payment integrity monitoring:** daily analytics for duplicates, split invoices, unusual bank geographies, rush payments and round amounts
- **Reinforce matching controls:** enforce three-way matching where possible and require strong exception documentation where it is not.
- **Segregation of duties:** separate vendor creation, master changes, invoice approvals and payment release
- **Emergency payment governance:** defined criteria, limited channels and centralized logging of emergency approvals
- **Rapid reconciliations:** daily bank reconciliations for crisis accounts and emergency fund

Third-party supply chain integrity risk

04

Changes in operating conditions often require organizations to source from new vendors, alternate routes and unfamiliar logistics partners. This increases exposure to quality issues, counterfeit goods, short shipments, falsified delivery confirmations and diversion of goods in transit.

Typical schemes

- Supply of counterfeit or substandard goods
- Shipment shortfalls or substitution of materials
- False delivery confirmations
- Diversion of goods in transit
- Collusion between internal staff and vendors or logistics providers

High-risk areas

- Critical spares, controlled goods and high-value parts (aviation and industrial)
- Medical supplies, pharmaceuticals and personal protective equipment (PPE)
- Fuel and lubricants
- Construction materials and temporary works
- Freight, warehousing, last-mile distribution and customs clearance
- Distributor networks and reseller channels

What causes this?

- Vendor onboarding without adequate due diligence or quality validation
- Weak receiving and inspection processes; limited independent verification
- Poor inventory governance (inadequate cycle counts and tracking gaps)
- Lack of batch or serial traceability for critical items
- Overreliance on logistics providers' documentation without validation
- Limited oversight of distributor or reseller pricing and returns

What can organizations do?

- **Tiered third-party due diligence:** enhanced checks for new or high-risk vendors and crisis categories
- **Authenticity controls:** inspection protocols, sample testing, approved specifications and vendor certifications
- **Strengthen logistics controls:** independent proof-of-delivery, GPS or time stamping and reconciliations against dispatch records
- **Inventory integrity:** cycle counts, surprise audits and serialization or batch tracking for critical items
- **Contractual protections:** audit rights, penalties for counterfeit or substitution and clear acceptance criteria
- **Supplier performance monitoring:** exception reporting on delays, defects and repeated discrepancies

Cyber-enabled integrity risks: deepfakes, impersonation and remote trust failures

05

Geopolitical situations create environments that amplify cyber threats and targeted fraud campaigns, as threat actors exploit distraction, remote work and crisis communications. Organizations are also facing a new dimension of technology-enabled threats, including deepfake-enabled impersonation, synthetic identity abuse and artificial intelligence (AI) – assisted social engineering.

Typical schemes

- Executive voice or video impersonation to approve urgent payments
- Fake vendor or partner communications requesting account changes
- Manipulated recordings or fabricated evidence used to support false claims
- Synthetic candidates or contractors entering sensitive workflows
- Account compromise used to alter procurement or payment data

High-risk areas

- Finance or procurement mailboxes and vendor portals
- Payment approval workflows and ERP access rights
- Remote access or VPN, privileged accounts admin tools
- Helpdesk and identity reset processes
- Incident response vendors and emergency IT or cyber purchases

What causes this?

- Weak multi-factor authentication (MFA) coverage and poor privileged access management
- Inadequate verification for urgent instructions and payment changes
- Over-permissioned user access in ERP during crisis role changes
- Limited monitoring of anomalous logins and transaction patterns
- Inconsistent incident response processes and delayed containment
- Threat actors can also use AI for voice cloning and social engineering to impersonate trusted individuals and compromise an environment
- Traditional crisis management protocols are often inadequate in addressing the rapid pace of AI-related threats

What can organizations do?

- Investing in AI tools for threat detection and response and learning to use AI as an ally in countering cybercrime
- Out-of-band verification for urgent payment requests and vendor changes
- MFA everywhere, especially for finance systems and privileged accounts; tighten conditional access rules
- **Privileged access management:** least privilege, time-bound admin access and frequent access reviews
- **Fraud and cyber monitoring integration:** alerting for anomalous payments, logins, email rule creation and ERP changes
- **Crisis communications protocol:** one authoritative channel for instructions to reduce impersonation
- **Rapid phishing defense:** targeted awareness bursts, simulated phishing and quick reporting or triage

Reconstruction and capital project integrity risk

06

As recovery begins and operations begin to stabilize, large reconstruction programs and capital spending can create a second wave of integrity risk such as bid rigging, inflated change orders, manipulated bill of quantities (BoQs), false progress reporting and materials substitution.

Following periods of geopolitical tensions, organizations face reconstruction spending, regulatory catch up, claims activity and large-scale normalization of operations. This process often reveals hidden losses and enables new integrity risk exposures.

Typical schemes

- Inflated variations and change orders
- Manipulated BoQs
- False or overstated progress reporting
- Materials substitution and quality failures
- Collusion across contractors and subcontractors

Strategic focus areas

- Major infrastructure rebuilds (roads, utilities and public buildings)
- Engineering, procurement and construction (EPC) contracts, subcontractors and site services
- Change orders, variations and claims
- Materials procurement and quality certification
- Milestone certification and progress payments

What causes this?

- Weak tender governance and poor contractor vetting
- Inadequate cost engineering and independent estimates
- Loose change-order controls and weak scope definition
- Limited quality assurance or inspection capacity
- Poor segregation between project management and certification roles

What can organizations do?

- Independent cost estimates and benchmarking; change-order boards
- Strengthen change-order review and approval governance
- Milestone certification independence; site verification and quality assurance (QA) or quality control (QC) strengthening
- Contract compliance audits; transparent procurement where feasible
- Subcontractor visibility and beneficial-ownership checks
- Strong documentation and digital project controls (progress evidence)

Claims, compensation and recovery program risk

07

Insurance claims, compensation requests and relief related reimbursements often increase sharply. Where review teams are stretched and evidence standards vary, organizations may face inflated losses, duplicate claims, unsupported damage evidence and limited oversight of third parties involved in assessment or repair.

Typical schemes

- Overstated or duplicate claims
- Unsupported damage evidence
- Repeated submissions across different programs
- Overreliance on external assessors
- Weak separation between assessment, approval and payment

Strategic focus areas

- Property and business interruption claims
- Damage assessments and repair contracts
- Government compensation funds and relief grants
- Medical and injury-related claims

What causes this?

- Poor verification standards and inconsistent evidence requirements
- Limited cross-checks for duplicates across systems
- Overreliance on third-party assessors without oversight
- Weak separation between assessment, approval and payment
- Overreliance on third-party assessors without oversight
- Weak separation between assessment, approval and payment

What can organizations do?

- Standardized validation, integrity risk scoring and duplicate detection
- Independent review of high-value claims and audit trails
- Vendor governance over assessors or repair partners
- Data-sharing or cross program matching where legally possible

Contract disputes and force majeure

08

Force majeure (FM) clauses are frequently invoked to address genuine disruptions; however, they also present an increased risk of misuse.

Periods of geopolitical tension or operational disruption may weaken oversight, increase urgency to maintain continuity of operations and create information asymmetry between contracting parties. These conditions can result in FM claims being misrepresented, exaggerated or inappropriately applied. Common abuses include false or overly broad invocation of FM to avoid contractual penalties, inflate costs, justify non-performance or renegotiate unfavorable contracts.

Typical schemes

- Broad or unsupported force majeure notices
- Claims that do not clearly link the event to actual non-performance
- Inflated standby, idle time, demurrage or disruption costs
- Repeated requests for extensions, repricing or scope adjustment
- Limited visibility over subcontractor or pass-through claims

Strategic focus areas

- Construction, infrastructure and reconstruction projects (post damage)
- Standby costs, demurrage, delay claims and idle equipment charges
- Subcontractor and supply-chain – dependent expenditures

What causes this?

- Weakened governance and controls due to emergency timelines and reduced verification capacity
- Ambiguously drafted FM clauses lacking clear causal, evidentiary and proportionality requirements
- Information asymmetry, especially where access to sites or third-party verification is limited
- High financial pressure on contractors facing cash-flow constraints or margin erosion
- Evolving oversight mechanisms, including delayed audits, inspections and dispute resolution
- Limited understanding of the legal distinction between impossibility and commercial hardship
- Overreliance on self-certification by suppliers, contractors or local partners

What can organizations do?

- Appoint an independent consultant to assist with contract disputes
- Strengthen contractual and governance frameworks
- Enhance evidence and verification requirements
- Validate supporting evidence independently where feasible
- Apply targeted financial and forensic oversight
- Enable crisis-mode monitoring and dispute management over change orders, delay claims, standby charges, etc

What leaders should do now

To manage integrity risks effectively during and after periods of geopolitical tension, organizations should prioritize the following actions:

Reinforce ethics and integrity through consistent leadership communications, decisions and actions

Scrutinize emergency approvals and decision rights; enforce non-bypassable controls (e.g., sanctions screening, bank detail verification)

Increase senior visibility over high-risk spend, payment changes, third-party onboarding and contractual claims

Implement targeted monitoring for deepfake impersonation, cybercrime and payment integrity risks

Provide regular management and board updates on integrity risks, incidents and response actions

Maintain a central exception register capturing emergency decisions, rationale, approvers and evidence

Establish a cross-functional crisis integrity governance cell to review exceptions and control weaknesses

Conclusion

Geopolitical dynamics fundamentally alter the integrity risk landscape. Such tensions demonstrate that fraud risks do not arise solely from malicious intent, but from urgency, weakened controls, regulatory complexity and operational pressures. Organizations that rely on pre-disruption governance frameworks are unlikely to manage these risks effectively. Resilience requires a deliberate shift from static integrity risk controls to adaptive, crisis- ready governance, combining speed with accountability. Organizations that anticipate disruption-driven integrity risks, invest in practical controls, and institutionalize lessons learned will be better positioned to protect public funds, shareholder value and trust. This protection applies both during times of challenges and throughout recovery.

Thank you

Continuing the conversation

Alexander Sokolov
Partner, Forensic Leader – Middle East, Forensic & Integrity Services, Ernst & Young Professional Services (Professional LLC)
alexander.sokolov@ae.ey.com

Abubakr Ibrahim
Partner, Forensic & Integrity Services, EY Consulting LLC
abubakr.ebrahim@ae.ey.com

Charbel Mehanna
Partner, Forensic & Integrity Services, EY Consulting LLC
charbel.mehanna@qa.ey.com

Philip Mennie
Partner, Forensic & Integrity Services, EY Consulting LLC
philip.mennie@ae.ey.com

Tarek Rayyan
Partner, Forensic & Integrity Services, EY Consulting LLC
tarek.rayyan@ae.ey.com

Hussam Adili
Partner, Forensic & Integrity Services, Ernst & Young Professional Services (Professional LLC)
hussam.adili@sa.ey.com

Thank you

Continuing the conversation

Dhritimaan Shukla
Partner, Forensic & Integrity Services,
EY Consulting LLC
dhritimaan.shukla@ae.ey.com

Robert Chandler
Partner, Forensic & Integrity Services,
EY Consulting LLC
bob.c@sa.ey.com

Ihsaan Ahmed
Partner, Forensic & Integrity Services, Ernst &
Young Professional Services (Professional LLC)
hsaan.ahmed@sa.ey.com

Hamdan Haman
Partner, Forensic & Integrity Services,
EY Consulting LLC
hamdan.hamdan@ae.ey.com

Mohammad Shaaban
Partner, Forensic & Integrity Services,
EY Consulting LLC
mohammad.shaaban@ae.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

The MENA practice of EY has been operating in the region since 1923. Over the past 100 years, we have grown to over 8,500 people united across 27 offices and 14 countries, sharing the same values and an unwavering commitment to quality. As an organization, we continue to develop outstanding leaders who deliver exceptional services to our clients and who contribute to our communities. We are proud of our accomplishments over the years, reaffirming our position as the largest and most established professional services organization in the region.

EYG no. 002935-26Gbl

ED None.

ey.com