PREPARING FOR THE BUSINESS IMPACTS OF THE RUSSIA-UKRAINE CRISIS

The tragedy unfolding in Ukraine is first and foremost a humanitarian crisis. BDO deplores the violation of international law and military aggression in all its forms. We stand with the people of Ukraine.

Organizations with people, operations and other interests in Eastern Europe and the wider region should prepare for a variety of immediate and long-term ramifications. At BDO, our top priorities are the safety of our colleagues and their families on the ground and helping our clients navigate the impact of this conflict on their people and operations.

Within this briefing, we'll cover what organizations should anticipate in the days and weeks to come and tactical considerations, from personnel and safety planning to compliance with sanctions.

Keep in mind that the crisis is complex and fast-moving, and that every business' situation is unique. These tactical considerations are non-exhaustive and are solely intended to provide a starting point for further discussion.

BDO®

WHAT TO ANTICIPATE

- Significant civil unrest and humanitarian concerns
- Significant and enduring operational uncertainty and disruption
- Significant sanctions, trade controls, and regulatory compulsion
- Significant disruption to supply chains and commodity prices
- Long-term changes to trade relations
- Significantly higher insurance premiums and denial of coverage based on regional exposure

Of immediate concern to all organizations is the protection and safety of human lives. The humanitarian crisis, mass departure of civilians from the combat zone and anxiety about family and loved ones are escalating as events progress.

Organizations should anticipate temporary lack of, or permanent loss of, access to production sites and feedstocks, raw materials and finish goods inventory, etc. In many cases, the primary recourse for recouping these losses will be through insurance claims.

Global supply chain disruptions have already been exacerbated and could result in permanent changes that endure after military action. Companies may see disruption to production and distribution, food and water safety, raw and intermediate goods, as well as suppliers of parts and services. With certain businesses and operations ceasing in the region, companies should expect and plan for potential service disruption.

The commodity and capital markets are already seeing significant volatility increases. Market volatility may be long-lasting, especially for prices of and access to commodities such as oil and gas, refined fuels, staples such as wheat and barley, and critical elements including nickel, aluminum, copper and rare earth elements. Follow-on impacts from sanctions and other trade controls may lead to further price volatility and disruptions.

The new export controls on Russia cover electronics, computer, telecommunications, information security, sensors and lasers, navigation and avionics, marine, aerospace and propulsion. Select Russian banks have also been disconnected from the SWIFT system that banks use to effect global payment flows. Lack of access to SWIFT has been shown to be a critical tool to disrupt financial flows of capital, impacting the ability of banks to enable payments globally and sovereign access to foreign funds. Of similar and related concern, companies should be prepared for volatility in foreign exchange (FX) and at times the ability to transact in key FX pairs. More sanctions may follow.

Over the long term, organizations should assess how the effects of the sanctions unfold and how different actors will respond and potentially escalate, creating additional complexity and “knock-on” risk effects. For example, Russian cyberattacks on U.S. banks are increasing. Attacks on other critical infrastructure categories, social media elements and market disruptions may also intensify.

Finally, there should be attention paid to opportunistic cyber threat actors (both nation-state and otherwise) who may see an opportunity to exploit the crisis. Organizations should harden their security posture towards ransomware incidents or other cyber events that take advantage of distraction.

Ultimately, there is no crystal ball for how a violent attack by a heavily armed nation-state will unfold. Organizations that are focused on resilience to risk and performance will carefully consider their options over time for trade relations, logistics and transport, supply chain partners and vendors, investment options, compliance requirements—and above all else, human safety and security.

CONSIDERATIONS FOR ORGANIZATIONS WITH DIRECT AND INDIRECT EXPOSURE TO THE REGION

People, Security, and Human Safety:

- If you have not already, identify personnel in and near combat zones to potentially be evacuated in case of escalation of combat operations.
- Consider providing emergency funding, medical supplies or relocation assistance to affected employees, their families or impacted communities.
- If your business is a supplier of a critical service or product, consider offering free aid (e.g., food, fuel, transportation) or temporarily waiving fees for refugees.
- Increase employee and stakeholder education and communication, stressing operational security, personal safety, responsible use of social media, and protection of assets and devices.
- Relay critical information and news to personnel in Ukraine in case official channels are compromised.

Processes and Functions:

Situational Awareness

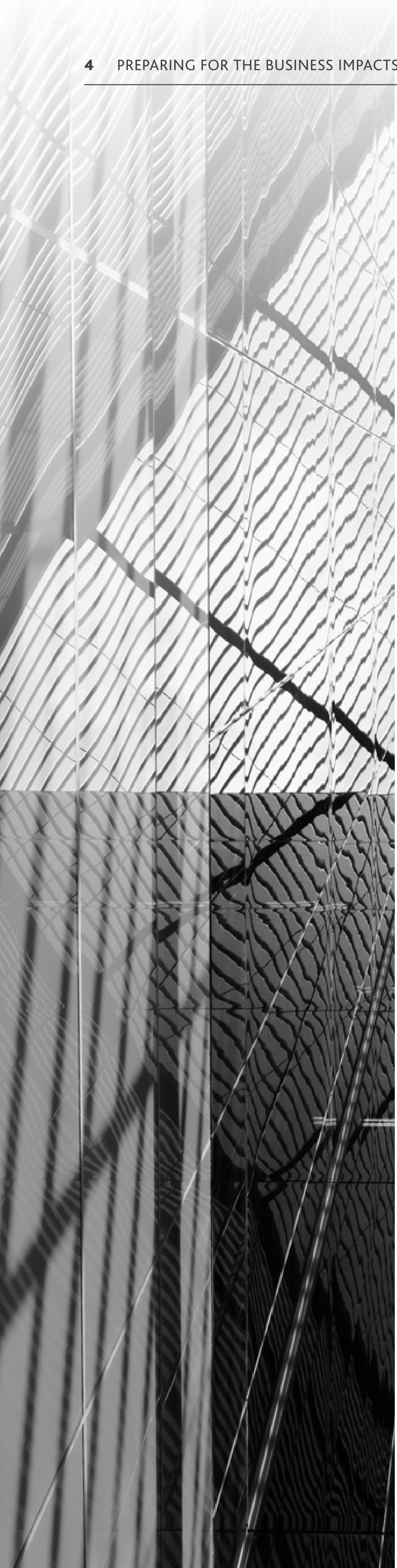
- Develop an in-depth understanding of the threats and operational environment. Identify risk scenarios, critical information requirements, and reliable sources for information.
- Establish a common operating picture which includes relevant information of interest to decision makers.
- Physically and digitally map assets you control and assets of interest which may also include adjacent stakeholders and suppliers.
- Monitor the dynamic legal regulatory environment and assess business impact.

Planning

- Review Business Continuity, Incident Response, and Disaster Recovery Plans, and socialize any specific updates to key stakeholders with responsibility/accountability for Business Continuity/Disaster Recovery (BC/DR).
- Review and monitor changing sanctions and regulatory/reporting regimes and consider rapidly implementing a sanctions tool if you don't already have one in place.
- Align and communicate with and between corporate compliance functions to stay informed of the changing regulatory landscape, including updated export controls on Russia and potentially other nation-states.
- Conduct ongoing crisis simulations to explore evolving risks and how they cascade.
- Analyze interdependencies between systems and processes, and second- and third-order consequences of the conflict (e.g., rising energy prices, strained regional infrastructure, affected IT dependencies).

Insurance

- Identify and document (ideally in a risk register) the current assets in terms of plant and equipment as well as inventory (work in progress, raw/intermediate/finished goods). Elements that are currently located in Russia, Ukraine and potentially Belarus will need special attention in case of complete loss.
- Review insurance coverage and begin the claims process.



Data Protection and Cybersecurity:

- Establish a dedicated cross-functional crisis management and incident response team.
- Review and document personal and sensitive data locations to ensure that the locations have the highest level of data protection.
- Review breach response and ransomware resiliency plans, processes and policies.
- Establish clear communications guidelines for employees and executives, including the retention of outside professionals to assist in the wake of a breach.
- Review vendor contracts to identify potentially vulnerable industries and companies to monitor activities more closely.
- Review vendor and third-party IT security, and ensure systems are current with appropriate patches and updates.
- Gain an understanding of remote access vulnerabilities and update accordingly.
- Review all ingress and egress points, access controls, network and critical system access and administrative privileges.
- Update subscriptions and closely monitor alerts from government agencies such as the Cybersecurity Infrastructure Security Agency, the National Institute of Standards & Technology, the Department of Homeland Security, and the FBI.
- Increase the frequency of monitoring and escalate suspicious activities.
- Isolate and segregate traffic between trusted and unknown points of origin.
- Assume that all traffic is suspicious until validated, and dismiss common geographic indicators like IP addresses, headers, or other primary and meta-identifiers as reliable.
- Increase the frequency of firewall and access control log reviews.
- Revisit data subject request processes and procedures to ensure that identity verification is continuous throughout the response process.
- Conduct tabletop incident response exercises and verify that business continuity and disaster recovery plans work.
- Review and test data backups – cognizant of fact that your network connection and data flow may be impacted significantly. Isolate backup data from rest of IT network and ecosystem.
- Consider a blockchain backup system that is immutable to change and vulnerabilities.

Payment & Banking Controls:

- Review foreign vendors to determine if any payment is intended to be paid or transferred to Russia or Belarus either directly or indirectly.
- Screen all prospective payments and currency transfers against the appropriate denied parties' lists maintained by various U.S. regulatory agencies. The U.S. government has added Russian entities and individuals to these lists and transferred others to more comprehensive and restrictive lists.
- Do not send any payments or funds to Russian banks or foreign banks' Russian subsidiaries.

National Security and Critical Infrastructure Protection:

- Review Industrial Control and SCADA systems risk profiles.
- Document Defense-in-Depth strategies and identify high risk systems and data.
- Develop or update a cyber forensics plan for control systems and controlled data.
- Review manual controls and overrides assuming that underlying network and technologies will be compromised or destroyed.
- Physically separate Industry Control Systems to mitigate overall risk.
- Evaluate interconnected technologies to identify potential threats.
- Establish direct access into the Industrial Control System and devices.
- Increase the frequency of phishing exercises to train professionals to recognize potential risks and to limit downloads of potential threats.
- Update website security settings to alleviate potential cross-site scripting and other vulnerabilities.
- Isolate SCADA and PCN system from the Internet and enterprise network using firewalls.

Supply Chain:

- Assess and quantify potential impact on inventory and assets such as factories, warehouses, or facilities.
- Assess risk to logistics and transport of goods, accounting for expected energy price increases and possible disruptions.
- Evaluate financial risk – does the organization have financial or other assets (e.g., receivables) located in or near the conflict area?
- Analyze suppliers and customers that are domiciled in or near areas of combat and adjacent geographies and assess how a disruption to these entities might affect the organization from multiple facets.
- Request that suppliers develop, evaluate, and share their own exposure assessment and refresh it in a consistent and timely manner as the situation evolves.
- Perform scenario modeling to build out alternative cost to serve or route to market plans to evaluate differing strategies to help manage the disruptions.

Export Controls:

- Review foreign customers, subsidiaries, affiliates, vendors, etc. to determine if any products, technology or information are intended to be shipped or transferred to Russia or Belarus either directly or indirectly.
- Review exports and/or transfers of U.S. goods, technology and information provided to foreign entities that manufacture products using these items to determine if the foreign-produced item is destined for Russia or Belarus.
- Determine if U.S. technology or information will be incorporated into or used in the production or development of any part, component or equipment produced or destined for Russia or Belarus.
- Screen all prospective export transactions against the appropriate denied parties' lists maintained by various U.S. regulatory agencies.
- Understand the new Foreign Direct Product Rule (FDPR) given that it can apply to customers in foreign countries of U.S. suppliers of, e.g., technology and software. [Read more about the new FDPR **here**].
- Review exceptions to licensing requirements carefully as these requirements are narrowly tailored for specific situations. When in doubt, seek the advice of compliance professionals.
- Carefully review the case-by-case scenarios under which a license for shipment to Russia may be approved, with the understanding a license will likely not be approved if it benefits the Russian government or defense sector.

Communication:

- Establish primary, alternate, contingent, and emergency communications protocols.
- Establish contact and a briefing cadence with key stakeholders to share information that is timely and targeted.

HOW BDO CAN HELP

BDO can support your organization through this challenging time. Our cross-disciplinary team of BDO professionals is here to help you assess your organization's risk exposure and develop a comprehensive mitigation plan.

CONTACT

JIM MACDONNELL
Managing Director, Risk & Insurance
703-245-0382 / jmacdonnell@bdo.com

CHAD FLEEGER
Managing Director, BDO
412-315-2360 / cfleeger@bdo.com

ELIZABETH CARTER
Director, Risk & Insurance
415-397-7900 / ecarter@bdo.com

KAREN SCHULER
Principal, Risk & GRC
301-354-2581 / kschuler@bdo.com

KEVIN RUIZ
Director, Risk & Insurance
408-352-3564 / karuiz@bdo.com

DAMON PIKE
International Tax Principal, Customs &
International Trade Services
561-207-3205 / dpike@bdo.com

BDO USA, LLP is a professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 70 offices and over 750 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 97,000 people working out of more than 1,700 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. www.bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.