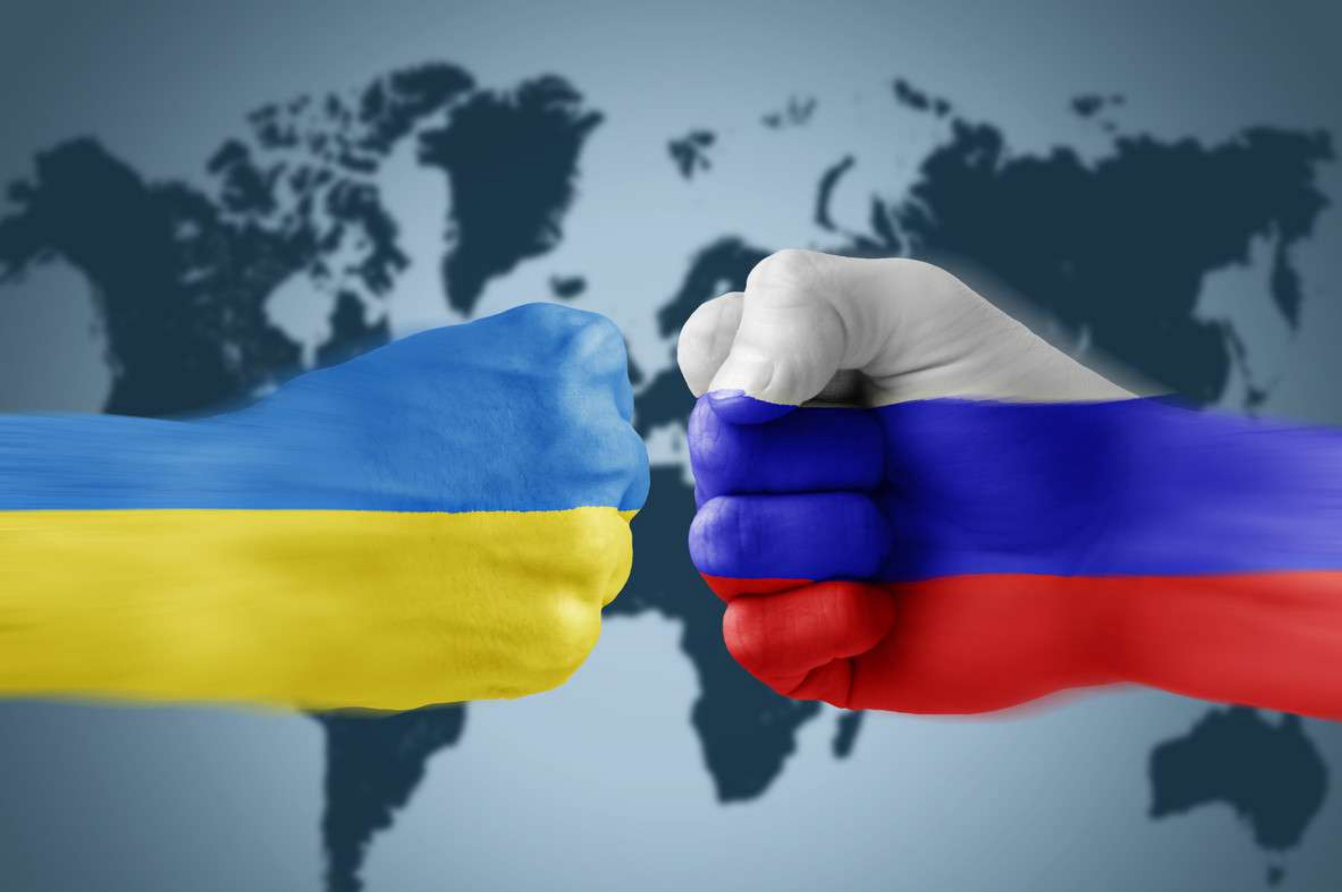


White Paper

Recommendations for international acting enterprises in the Russia-Ukraine War 2022

controllit

Business Continuity Management

Content

Introduction

The current acts of war in **Ukraine** and the conflict with **Russia** are not only concerning us in the media, politically and personally, they also have a massive impact on business activities and the European economy. Business and activities in and with **Belarus** as well as Ukraine's **neighbouring countries** and Russia are also in the spotlight.

The (mostly still voluntary) sanctions against Russia are already having far reaching economic consequences. Numerous companies are reacting by restricting their business activities, are in a holding pattern or are ending their activities completely. Where production and distribution have been or are being shut down, it is a matter of coordinated phasing out and securing goods, assets and real estate.

From the automotive industry (manufacturing and distribution), transport (especially aviation), banking and insurance, energy, entertainment, industry and manufacturing, logistics, technology, telecommunications to sporting goods manufacturers, production and distribution of household goods and furniture stores, there is a corresponding response.

The impact on the battleground Ukraine itself is devastating, and neighbouring countries, not only in the border areas, as well and other Europen countries are also involved.

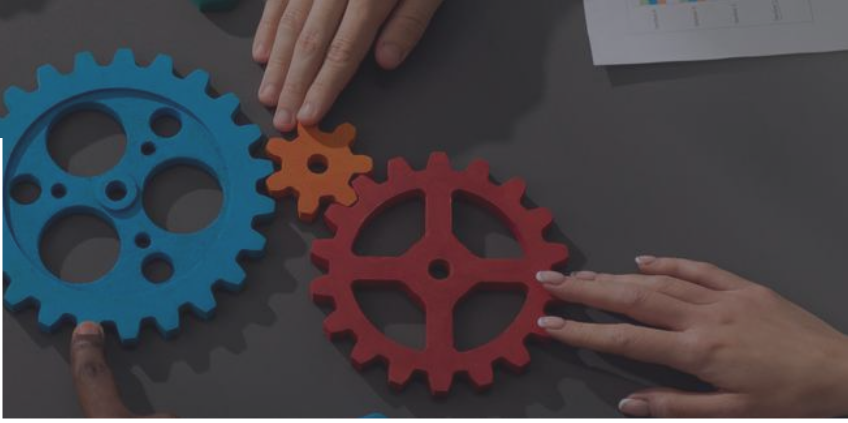
Introduction

The consequences for cost development are noticeable (a credit programme by the state development bank in Germany has been announced), the export forecast of the DIHK (German Chamber of Industry and Commerce) has been significantly lowered and production interruptions, even at indirectly affected locations, are looming due to challenges in the supply chains. In addition, there is a possible shortage and probable price increase for raw materials.

Last, but not least, direct **concern and care** for employees is a defining issue: this is where corporate responsibility and accountability becomes relevant, from evacuating employees to providing the best possible care for employees who want or need to stay on site.

With these recommendations for action, we want to provide **orientation** based on the classic staff perspective and identify **options for the following topics**:

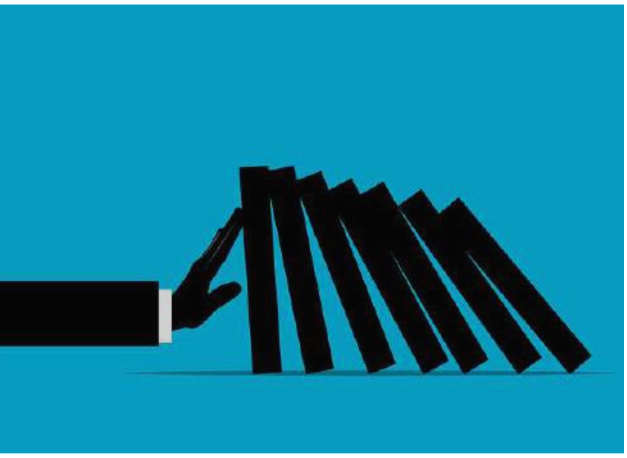
- Human Resources (incl. Safety)
- Evaluation (inc. Security)
- Operations
- Logistics
- Communication
- IT, Information security and data protection



Action recommendations

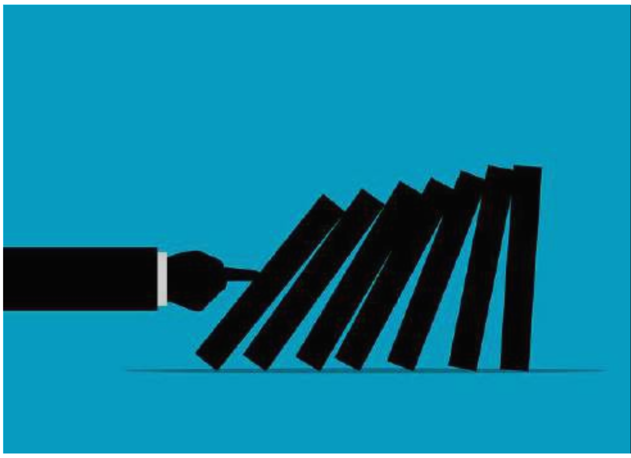
In principle, we also recommend solid and far-sighted preparation in the current conflict (if available: Use of your company's escalation levels and thresholds) and the development of step-by-step plans or scenarios.

The concrete preparation primarily serves the purposeful assessment (ideally based on your updated thresholds and prioritisations, if applicable). The use of step-by-step plans or scenarios supports companies in flexibly adapting to the concrete situation. On the other hand, reactive preparation also serves the purpose of targeted coordination and control in all phase-out, rest and decommissioning scenarios. Here there is a noticeable difference between a targeted, proactively controlled approach and simply "dropping it". Even when returning to normal operations, a step-by-step plan provides structure and flexible confidence in action.



Depending on the situation, the procedures for companies with activities in the directly operating or affected countries Russia, Ukraine and Belarus are on a different level than in the neighbouring countries. However, the issues and your interface management are very similar. In the neighbouring countries, it is a question of both the perspective of being affected in the border regions and a possible expansion of the conflict.

In the following chapters, we give you concrete recommendations for action on the topic areas and raise necessary questions.



Human Resources

The staff sector can be well structured and evaluated with the interface partners human resources and security. On the one hand, of course, it is important to ensure the physical safety and health of the staff, but on the other hand, it is also important to proactively manage skills (abilities, skills, qualifications) including the Single Points of Knowledge (SPOKs) of your company.

The most essential question in the war zone, direct sanction zone or border zone is that of physical security. But the situation can also change dynamically in neighbouring countries.

→ Check your staff security: Do your travel arrangements correspond to the current situation (travel restrictions, etc.)?

→ Determine which staff you need, should or want to evacuate (not only in the immediate war zone).

→ Consider whether your staff are national employees in their their home country or staff from other countries (possibly with the nationalities of the conflict parties). Also consider the need and possibility of evacuating family members of the local staff.

→ Always follow the recommendations of the Federal Foreign Office (in Germany) and, of course, the authorities in the respective country.

Human Resources

- → Identify the options and means available for leaving/evacuating. Presumably there are offers of support on the one hand for the use of means of transport, but also of a financial nature on the other hand.
- → Check whether there is support from the federal government, the state, other institutions or private security companies and whether your company's insurance will cover it.
- → Look at the timetable. Which immediate activities are necessary, which activities can be prepared and implemented in which environment in which time frame?
- → Plan the alternative locations of your staff. In a war-torn region, temporary departure/exit to neighbouring countries may be advisable under time pressure. Inform yourself and those affected about the appropriate contact points (e.g. embassies).
- → If you can control the departure activities, the medium-term occupationally meaningful place of employment must definitely be included in the consideration of the safe destination region.
- → It may be advisable to carry out a comprehensive investigation to find out which of the skills that are now being freed up are needed where. Are there perhaps already considerations about corporate replacement solutions or the need for other, secure locations?
- → Also consider whether and which local staff are needed to secure your goods and assets, for monitoring activities or entrepreneurial activities in the event of a targeted discontinuation or reduction of your business operations.
  The perspective of your local staff and the other staff on site can be a good decision-making aid here.
- → Last, but not least, employees from directly affected areas are likely to need psycho-social support. Are there other mental health challenges for staff?

Evaluation

Determining a situation picture in a war zone is always a challenge with some unknowns. It is therefore advisable to use both official and media information as well as individual information and compile it into a company-specific situation picture. In addition, there are companies and services in Germany that specialise in such services. Your communication professionals (communication department, etc.) and security officers as well as your direct employees, partners and/or service providers on site are relevant information partners. You will also receive valuable feedback on the feasibility of your measures via your local contacts.

To develop your phased plan on the basis of the situation picture, it is also important to know whether you are talking about a complete discontinuation, a controlled or a limited reduction of your business activities. In addition, there are of course all combination variants that you should consider and evaluate. In addition, the situation in Ukraine, Russia, Belarus as well as neighbouring countries can have a rebound effect on your entire business. Ideally, you should also consider the dependencies in the international environment of your business organisation.

→ Check which parts of the company are currently affected and to what extent. Define the scope of your analysis in consultation with your management (currently we recommend a perspective of at least six months). What damage has already occurred and is foreseeable (mid to long term)?

Evaluation

- Include the dependencies of your other products, production and supply chains in the consideration. Are there "monopolies" or core business activities?
- Check how your customers, employees and their families and markets are affected.
- Find out about the assessment and perspectives of your direct local contacts.
- Also determine how the exchange of information with the local contact partners can be maintained in the mid to long term.
- Determine the local resource situation and local requirements (staff incl. know-how, buildings, IT, service providers as well as material status, warehousing, logistics, etc.).
- Information on the supply, transport and security situation in Ukraine, Russia, Belarus and neighbouring countries is also recommended for resource assessment and planning.
- When gathering information, pay attention to the reliability of the sources, question situation information critically and regularly and communicate central situation information within your company.
- Try to get ahead of the situation by outlining and evaluating potential future scenarios of conflict and market for your company and designing appropriate responses.
- Check your eligibility and take advantage of federal funding and/or loan programmes.
- Monitor and evaluate your current shareholdings at appropriate (possibly shorter) intervals to keep an eye on fluctuating prices and act and communicate accordingly.

Operations

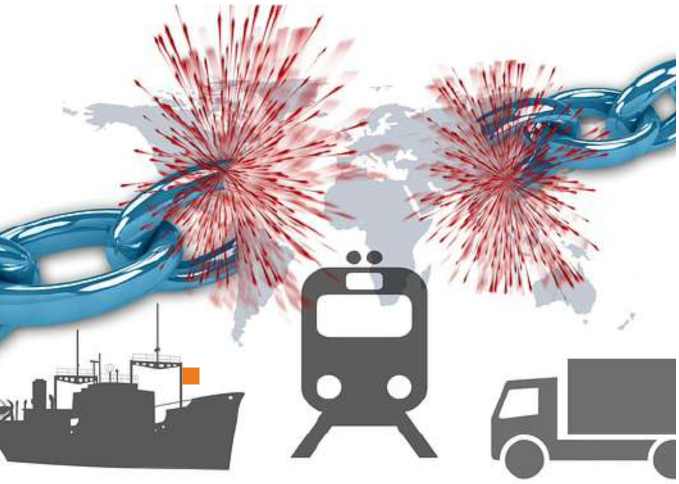
When making decisions and adjusting your measures, it is advisable to adapt to the situation in a really flexible way using your decision-making model (e.g. FORDEC). In particular, look again at possible support options and use your thresholds and prioritisations in the recommended level model.

- → Make sure your prioritisations are adapted to the situation or will be modified at short notice.
- → Check weather and by which non-affected parts of your business compensation measures can be implemented.
- → Check whether and which alternatives and expansion options exist in your business field.
- → Determine whether and which internal and external interfaces are available.

Logistics

Since Covid-19, the sensitivity of goods movements in connection with warehousing and transport has come into focus. In the context of armed conflicts, this area requires special coordination and organisation in the countries concerned: Ukraine, Russia, Belarus and neighbouring countries. In turn, it is advisable to react flexibly and confidently to the situation with the help of your step-by-step plan. Use the interfaces in controlling, risk management, local representatives and your management at the strategic level as a source of information.

- Ensure your priority products and customers are up to date.
- Determine the current technical and material availability incl. equipment of your warehouses, vehicle fleets, other means of transport and freight routes (see also Evaluation).
- Check your alternatives: Are there choices to other storage facilities (incl. splitting), service providers, carriers, transport means and routes?
- Determine the requirements of your alternatives. Are there any special features or obstacles? Maybe a combination of alternatives makes sense?
- Check which qualitative and quantitative losses are acceptable.
- Evaluate the choices for security (please also include the mid to long-term perspective), cost-effectiveness (time and costs) and feasibility (staff requirement, shelf life of your goods, IT requirements, use of manual processes if necessary, etc.).
- Keep an eye on legal or contractual requirements and the impact on your company's reputation and image, as well as on a location that can be used for a longer period of time.
- Ensure that your alternatives are also effective and efficient across countries. It is advisable to check the freedom of your transport chains and supply flows also with reference to the country of origin and arrival as well as the documentation requirements.



Communication

The communication department of your company is significantly challenged in all crises in terms of the volume to be handled and the quality demand. The internal and external perception of your crisis management is shaped by the corporate communications department and decisively determines the success of your crisis management.

It is the same in the current war situation: the attitude and presentation of your company contributes significantly to its future sustainability. It is advisable to activate the lived support of marketing and other corporate reserves for communication in due time.

- → Align the options of the communication strategy according to the situation. Specifically filter the strategically useful steps and make a targeted preselection.
- → Check and adapt your wording templates (especially in line with the specific preselection).

Communication

Coordinate with the management what proactive statements and what attitude you want to communicate, even without direct involvement, in Ukraine, Russia, Belarus and neighbouring countries. For example, does taking sides with Ukraine fit in with your business activities? Also instruct your employees in this regard and recommend or forbid such partisanship or proactive solidarity.

Activate your media monitoring to identify developments for your company at an early stage.

Observe the overall company communication externally (e.g. also what happens in your hotlines) **and internally** (what feedback do you receive from the employees?).

Prepare all communication media (internal/external/social media) to suit the target group. Pay attention to the proactive and reactive gradations.

Secure your resource pool: Do you have sufficient staff for active crisis communication (activate your supporters internally and externally)? Do you need additional language skills?

IT, Information security and data protection

One of the first and most impressive responses in the IT environment in Germany was the announcement by the hacker group Anonymous that they had declared cyber war on Russia. However, there are professionals at the other end of the line, especially in Ukraine and Russia. Therefore, protection in the area of IT, information security and data protection is extremely important (in an already sensitive field) in order to prevent damage to your company in the mid and long term (even if it is only unintentional collateral damage).

- If you do not already have one, **set up an awareness and sensitisation programme**. Focus on regular communication, especially with regard to current incidents and examples, without exaggerating the situation.
    - Emplyoees in general
    - Employees with special IT or increased rights (adminstrators)
    - Employees who work with particularly sensitive and critical data (R&D, Finance)

- **Secure your operational readiness against a DDoS attack in five key areas:**
    - Carrying out service validations
    - Confirm authorised mitigation service contacts
    - Review and update runbooks
    - Conduct operational readiness exercises
    - Update emergency communication methods

IT, Information security and data protection

- **Implement geo-blocking.**

- **Check whether the patches for vulnerable systems are done at a secure level.** In particular, previously postponed (security) patches should be prioritised.

- **Segment your network to protect against the threat of ransomware.**

- Minimise risks by **updating your current authorisation and access policies and prioritising the projects and items that are currently open.**

- **Critically review whether you are or have been sourcing current or past IT outsourcing, procurement or services from Belarus, Ukraine or Russia.** If so, consider the possibility that these systems may no longer be available or may be compromised.

```
each: function(e, t, n) {
    var r, i = 0,
        o = e.length,
        a = M(e);
    if (n) {
        if (a) {
            for (; o > i; i++)
                if (r = t.apply(e[i], n), r === !1) break
        } else
            for (i in e)
                if (r = t.apply(e[i], n), r === !1) break
    } else if (a) {
        for (; o > i; i++)
            if (r = t.call(e[i], i, e[i]), r === !1) break
    } else
        for (i in e)
            if (r = t.call(e[i], i, e[i]), r === !1) break;
    return e
},
trim: b && !b.call("\ufeff\u00a0") ? function(e) {
    return null == e ? "" : b.call(e)
} : function(e) {
    return null == e ? "" : (e + "").replace(C, "")
},
makeArray: function(e, t) {
    var n = t || [];
    return null != e && (M(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) :
},
inArray: function(e, t, n) {
    var r;
    if (t) {
        if (m) return m.call(t, e, n);
        for (r = t.length, n = n ? 0 > n ? Math.max(0, r + n) : n : 0; r > n; n++)
            if (n in t && t[n] === e) return n
    }
```

- **Prepare to shut down and disconnect your IT infrastructure in the countries mentioned above.** Also think about backing up and/or deleting critical company information.

- **Review and update (as appropriate) your ITSC plans.**

Prospects

The duration of the Ukraine war and its consequences can hardly be estimated at present, hopes for a settlement of the hostilities are high, but so is the certainty about long-term effects.

The "return to normal operations" after the stabilisation of the crisis within a company and the termination of the active deployment of the crisis team therefore requires (as always) concrete measures and, in this particular case, a sensitive approach.

Step-by-step plans and scenarios are also suitable for this purpose and can be flexibly adapted to changing situation developments.

- → Check whether the official national and international requirements and framework conditions allow or even support the resumption of your business operations.
- → Does it make sense to take over part of your business?
- → Determine the local availability and operational capability of your company: Are the required resources (staff incl. know-how, buildings, IT, service providers as well as material, warehouse availability, logistics, etc.) available?
- → Check the relevance (reputation, other interests) and the economic viability (incl. the sales market) of resuming/partially resuming your business operations.
- → Develop a time and step-by- step plan for the restart (from 0 to 100 usually does not work smoothly). An individual site consideration is indeed recommended.
- → Involve relevant stakeholders in due time (local employees, suppliers, service providers, customers, etc.).

Prospects

- Check and adapt your business concepts to the development of the situation (from security to occupational health and safety, etc.).
- Warn your employees explicitly about cyber attacks via social engineering (usually e-mails with malware), even in the long term.
- Organise a fully comprehensive handover to the business units that are now operating independently again.
- Communicate clear information lines and reporting channels. Be aware of possible re-escalation. So check and update your thresholds and priorities.
- Use all the means of your communication professionals for a coordinated, company-conform and appropriate communication (internal/external/social media).

Controllit AG
Kühnehöfe 20
22761 Hamburg
Germany
www.controll-it.de

Status: 18 March 2022

Controllit AG is your partner for Business Continuity Management (BCM). Since our foundation, we have been developing integrative concepts and products for business continuity management, IT service continuity management and crisis management. We help you with strategic, organisational and technical concepts to secure your business processes against threats and to provide for emergencies.

Photo credits: P. 1 :iStock.com/Aquir; P. 3: iStock.com/designer491;
P. 4: iStock.com/designer491, iStock.com/ake1150sb;
P. 5: iStock/comalphaspirit; P. 6: iStock.com/Andranik Hakobyan,
iStock.com/vege; P. 7: iStock.com/vege, P. 11: iStock.com/OstapenkoOlena;
P. 12: iStock.com/SurfUpVector