Operating environment

Zinc, generally, assesses the operating environment across the Baltic States to be one of low risk. All three countries have stable political systems and a strong rule of law with either low or moderate levels of crime. Corruption is of moderate concern regionally; which Zinc has addressed by putting in place mitigation measures in the project's risk matrix. Physical risks (beyond those listed below) to project staff in-country are considered to be low. Zinc has contingency and emergency planning built into its risk management strategy in case of need.

However, this project faces distinct and complex challenges by operating across the Baltic States. The historical relationship between Russia and the Baltics, and their subsequent accession into NATO and the EU, has resulted in them becoming particular targets of Russian diplomacy, media and non-kinetic warfare, including disinformation. Although there is no expectation that Russia will attempt another Ukrainian style occupation, Russia destabilises those nations, including through funding of Russia-based media that propagates Russian influence. Through this, Russia attempts to exploit ethnic tensions, socially divisive issues (such as LGBT), and fuel anti-Western sentiment. Tactics include the dissemination of conspiracy theories, alternative narratives and "truths", and attempts to discredit groups or individuals. In some cases, this can extend to digital harassment, including cyber-attacks, physical harassment and intimidation of those speaking out against the Russian State and its Baltic policy. These risks are amplified by the involvement of foreign donors; Russian knowledge of UK funding could make project partners and beneficiaries targets for retaliation. We have multiple mitigation strategies in place, from designing the project in a way that avoids putting partners and beneficiaries in direct confrontation with Russian state-funded sources and provides them with tailored support to strengthen their resilience, to best in class information and data security, and emergency response and contingency plans to respond to any incident.

By understanding and adapting to the known context, Zinc has developed the toolset to deliver projects in this operating environment successfully. Policies and processes are designed to safeguard the people, assets and activities critical to the project, and satisfy our duty of care. The first stage in addressing the risk landscape is to identify the specific threats to the project, as set out below. We have detailed these threats and associated mitigation measures in the risk matrix.

Threats to the project

We have completed an initial assessment of potential risks and implications for the project and its staff. These are:

- Physical risk to the project staff, organisations, sites or events
- Digital targeting of project staff or associates via social media or other open sources of individual data
- Cyber-attacks, hacks or interception of project documents resulting in the publication of documentation
- Member activity not meeting journalistic or ethical standards
- Members' involvement in the project resulting in a higher level of scrutiny or interference than they can handle
- Corruption/kickback scandal or misuse of funds implication due to a third party's nefarious financial conduct
- Influencers afraid of losing editorial independence and/or Russian blowback and so unwilling to contribute
- Senior stakeholders across broadcast and large media outlets' disagreement with or disinterest in the project
- Counterparts do not see the importance of conflict and gender sensitivity and equality, causing lack of engagement in such themes in programming
- Reputational – people, groups and organisations working with UK companies easily discredited to Russian-speaking audiences
- The project inadvertently exacerbates tensions and/or perpetuates gender and social inequalities
- Low levels of capacity and/or commitment within beneficiary organisations means that the planned level and duration of support is insufficient to generate substantive and sustainable change

Risk Management

Zinc operates an enterprise risk management framework, allocating responsibility at all levels of the business. Risk is identified and managed through detailed project risk registers, such as the one attached. This register is reviewed at least monthly by the Project Director. In the event a risk rating exceeds the pre-defined risk appetite, it is escalated to the senior management team for further action. We will review all key risks with the Baltic Board quarterly, or when new critical or high risks are identified. This ensures agreed actions and mitigation measures are put in place.

Supply Chain

Zinc maintains a transparent and collegiate environment with sub-contractors (SC) and local organisations. We manage risk and performance through the supply chain by: robust due diligence; weekly emails and meetings with SCs/organisations and daily meetings with key individuals; quarterly reviews against key KPIs to pinpoint SC/organisations' partial or non-performance; and clearly defined procedures for dealing with poor performances and resolving disputes proactively. All SC agreements include a flow down of our contractual arrangement with the client.

Duty of Care (DoC)

Our commitment to duty of care and health, safety and security is a key enabler of successfully delivering our work. We ensure accountability and compliance by providing our staff with the correct training (including specialist training where required), information and equipment before deployment to enable them to carry out their obligations safely.

We monitor Duty of Care risks on an ongoing basis, and have detailed procedures and plans in place to manage an incident or emergency, including in the case of quick response and evacuation.

Due Diligence (DD) Policy
Toro Solutions, our long-term security partner, conducts due diligence evaluation on our behalf. This process will apply to all SCs/organisations/journalists/influencers. It includes: developed credit checks – applicable to those handling budgets or working in the finance department; developed criminal checks – covering convictions and outstanding court orders; political exposure checks; extremist activity; espionage and security service exposure, and; developed checks against immediate family – extremist political, criminal and security service exposure. Where manageable risks are identified, they will be incorporated into the risk register with clear mitigation measures tracked and actioned. Risks above a manageable threshold will result in termination of the particular activity.

Quality Control
Zinc is ISO 9001 certified with established processes to ensure delivery of services on time, to budget and exceeding client requirements. Quality assurance is tied to our Theory of Change with performance and quality review of inputs, outputs, outcomes and objectives. Overall responsibility for quality control sits with the Project Director, with weekly oversight from senior management.

Financial integrity/control
Our due diligence will encompass the financial integrity and standing of suppliers/partners engaged. This also covers the risk of money laundering or financing criminal activity. Where possible, we will obtain three independent quotes, and issue purchase orders for contracts with detailed requirements of quality and timelines. Invoices, when received, will be signed-off by the project team, then finance and paid through a dual authorisation process. Our Commercial Director ensures financial probity, and has a wealth of experience in implementing robust financial integrity controls and mitigations specific to this type of work.

Information security (InfoSec) policy
We fully encompass industry, security and legislative best practice into our InfoSec approach, including UK and European data protection legislation. Zinc is ISO 27001 accredited and Cyber Essentials Plus certified. We conduct annual internal/external penetration testing and electronic sweeps of premises, systems and devices. Where required, we recruit specialists to address specific project security. Systems are encrypted, secured by two-factor authentication and monitored for abnormal activity which, if detected, is recorded in our incident log with responses and resolution detailed in an incident report. Data is backed up and disaster recovery plans ensure effective recovery in the event of data unavailability. We permit granular access to data based on specific clearance levels. We use software which classifies content and alerts any potential exposure of sensitive information in real time, allowing us to take proactive action against data breaches.

Incident management
If a critical incident occurs, we will form an Incident Management Team and follow procedure to: prevent (further) harm; assure the affected people/stakeholders of an effective response; fulfil our Duty of Care and legal responsibilities; safeguard our information and reputation; and ensure effective business continuity.

Case Study: Institute of Statecraft Hack
When the Institute for Statecraft was hacked, Zinc activated its incident response team. It assessed the situation and immediately investigated potentially exploitable vulnerabilities related to the documents leaked. We set up social media listening to monitor mentions of the leak, Zinc, our projects and partners. We allocated actions and implemented mitigations to plan for further exposure. With no evidence of Zinc systems compromised, we formulated a communications response, contacted our partners, and provided support and training in secure ways of working to those individuals. We also updated our project and company risk registers with additional mitigation measures identified. We provided further training to all staff on cyber security, secure communications methods and working practices – communicating these expected standards and best practices to our partners. Scenario response training has ensured swift, organised and effective actions to further leaks. Zinc has continued to monitor the situation and implemented robust safeguarding procedures for the network and partners.

Safeguarding
The safeguarding risks are two-fold. There are those posed by the activity of hostile malign actors; and those created through the behaviour of staff and suppliers. Our safeguarding framework ensures:
1. Safe programme design and a commitment to a code of conduct that requires specific ethical behaviour from all staff, consultants and partners.
2. Proactive issue identification – including through a complaints and concerns procedure, whistleblowing function and survivor support.
3. Robust risk management overseen by our identified Safeguarding Officer.

Risk Register

						Before reduction measures (raw risk)						After current risk reduction measures (residual risk)				
Risk ID	Risk Category	Risk Description	Risk Context	Risk Consequences	Standing, or Temporary	Likelihood		Impact		Risk Rating	Mitigations - what can we do to reduce the risk?	Likelihood		Impact		Risk Rating
001	Reputation	Content generates overwhelming negative response from the general public to journalists/media outlets or implementing partners	There are multiple target audiences who hold differing attitudes, in a media space which is heavily influenced by Russian disinformation efforts	A negative audience reaction could limit ZN's efforts to engage with individuals and deliver project objectives. Further, it may demotivate the journalists/media outlets who might wish to leave the project	Standing	3	MODERATE	3	MODERATE	MODERATE	Network managers will be responsible for regular check-ins with the organisations to ensure transparency. ZN will monitor audience engagement, and update the client in case of major project disruption.	2	LOW	3	MODERATE	LOW
002	Security	Physical risk to project staff, organisations , sites or events	Journalists/media outlets can face physical and digital attack due to the nature of the project	Any attack/disruption may disrupt delivery and cause local journalists/media outlets to self censor and leave the project	Standing	3	MODERATE	4	HIGH	HIGH	Risk assessment, actions plans and crisis management by RSA.	2	LOW	3	MODERATE	LOW
003	Data	ZN IT system and the project's organisations may be subject to an attack or hack. Interception and publication of project objectives	The project is working in media space influenced by Russian State disinformation efforts. This environment includes threats to IT systems from hackers	A potential attack may seriously disrupt the project and adversely affect journalists/media outlets or ZN	Standing	2	LOW	4	HIGH	MODERATE	Communications will be conducted through secure means, in addition to sensitive information not being shared with organisations/individuals unnecessarily. ZN use accredited online services and follow strict security guidelines internally, to mitigate any potential risks. All staff undergo online security and IT training when they're engaged by ZN.	2	LOW	4	HIGH	MODERATE
004	Networks / groups / influencers / contributors	Media partners reluctant to cooperate with ZN or working against project objectives	Russian influence spreads widely across European media organisations, thus ZN must work sensitively	This could result in a hinderance of the campaign effectiveness and its digital reach across the intended media spaces, resulting in ZN not reaching the campaign objectives.	Standing	2	LOW	4	HIGH	MODERATE	Due diligence will be carried out internally on all media organisations involved in the project. Network Managers will build trusted relationships with these organisations and maintain ongoing communication throughout the project to ZN core project team.	2	LOW	4	HIGH	MODERATE
005	Reputation	Member activity does not meet journalistic or ethical standards	Regulatory bodies across the Baltics' media environment do little to ensure professional standards are adhered to	This could undermine their credibility and bring the project into disrepute	Standing	3	MODERATE	3	MODERATE	MODERATE	Close monitoring of Member activities by project team. Vetting of members. ZN Code of conduct disseminated to project's organisations/individuals	2	LOW	3	MODERATE	LOW
006	People	Individuals/organisations involved with project exposed to higher profile/scrutiny/level of interference (including physical security risk, online intimidation or cyber attack)	Individuals/organisations in the Baltics' media space can be subject to digital and physical harassment by the Russian state which can result in intimidation and consequently project disruption	Withdrawal/ self-censoring of individuals/organisations from the project	Standing	3	MODERATE	4	HIGH	HIGH	Callibration of activities to individuals'/organisations' capabilities and risk tolerance. Escalation of high-risk issues to Project Director.	2	LOW	4	HIGH	MODERATE
007	Finance	The project is implicated in a corruption/kickback scandal or misuse of funds incident due to local third parties'/partners' nefarious financial conduct with project funds.	Professional and ethical standards across the media environment in Baltic countries has much fluctuation with little regulatory oversight in real terms	Reputational damage to ZN/ the client. Financial loss, failure to deliver project deliverables	Temporary	3	MODERATE	3	MODERATE	MODERATE	ZN will include anti-bribery in contract with suppliers. Due Diligence will raise any previous examples of unlawful behaviour. ZN will conduct due diligence of the grants management process for BC before assigning contractual responsibility to the organisation.	2	LOW	2	LOW	LOW
008	Project Delivery	The project overlaps with other donor support, providing poor value for money and exacerbating the problem of commercial sustainability of media organisations in the region	HMG is approaching disinformation through numerous, simultaneous sensitive projects. It is likely that another project is operating in the same field. This project is part of a wider programme of HMG counter disinformation projects across the Baltic states	Reduced effectiveness of all projects due to overlapping responsibilities.	Standing	2	LOW	3	MODERATE	LOW	The project preparation process will include thorough due diligence of other donor activities and plans. Project proposals will contain clear paths to commercial sustainability of the media organisations.	2	LOW	2	LOW	LOW
009	Security	ZN staff are obstructed or impeded while travelling to region.	Malicious agents may attempt to block ZN activities in the region or immigration may question why individuals are travelling	Harm to staff, harm to equipment, delay in project delivery, unforeseen costs to project	Temporary	2	LOW	4	HIGH	MODERATE	All staff deployed to region will be given sufficient training and guidance, following ZN's travel procedure of pre-travel and post-travel assessments. Client to provide lines in case of any undue or unwanted attention.	2	LOW	3	MODERATE	LOW
010	Networks / groups / influencers / contributors	Social media personalities afraid of losing editorial independence	In an already divisive media environment rife with disinformation and dominant narratives, these personalities may well have concerns over freedom of expression	Influencers lose interest in the project and leave	Standing	3	MODERATE	3	MODERATE	MODERATE	We have committed to establishing complete editorial independence to allow as much freedom of expression as possible and keep FCO branding to a minimum. A code of conduct will also be disseminated amongst project members.	2	LOW	3	MODERATE	LOW
012	Partners / suppliers	Senior stakeholders across broadcast and large media outlets do not agree with the project or lose interest in it	In a media environment which is dominated by Russian TV, PSBs and large media outlets, these organisations may be resistant to engaging with our innovative and modern approach	PSBs and large media outlets leave the project	Standing	3	MODERATE	3	MODERATE	MODERATE	ZN will leverage BCME's pre-existing relationships with PSBs in an effort to ensure stakeholder buy-in from the inception phase to ensure local ownership in engaging with project. The process will be led by the Project Director. We will conduct continuous stakeholder analysis to identify where issues might arise and identify how we can mitigate the internally or in collaboration with the BB.	2	LOW	3	MODERATE	LOW
013	People	Counterparts do not see the importance of gender sensitivity and equality and are therefore unwilling to engage in topics	Gender sensitivity and equality is a controversial topic within a heavily dominated Russian media space	Project outputs do not meet the requirements of either our approach, or the FCO's requirements for gender sensitivity and equality resulting in the inability to achieve desired outcomes	Standing	3	MODERATE	3	MODERATE	MODERATE	The project's Gender Advisor will engage with all counterparts and media outlets on a quarterly basis to discuss how issues are important in their context and how to best produce content which is promoting equality and thus reaching a large audience base. They will be supported by our local staff on the ground and our PSB adviser to ensure all recommendations are relevant to the Baltic context.	2	LOW	3	MODERATE	LOW
014	Project Delivery	The project inadvertently exacerbates tensions by perpetuating gender and social inequalities	Gender sensitivity and equality is a controversial topic within a heavily dominated Russian media space	Resulting in counter-productive and damaging outputs, which cause the project to fail to meet its stated objectives and simultaneously losing the trust of stakeholders and the discredits the campaign brand in the eyes of the target audience	Standing	4	HIGH	3	MODERATE	HIGH	ZN has established an advisory panel, as well as regional experts, including a Gender and equality advisor who will review project outputs on a regular basis to ensure that content is achiveing stated objectives	2	LOW	3	MODERATE	LOW