1.5.1 (5.1)	**Risk Management**. What challenges and risks do you anticipate in delivering the required service for this project?	**Pages:** 5	**Points:** 75

A Confident and Experienced Implementing Partner. Torchlight has the regional experience and contextual confidence to understand and manage the diverse challenges and risks within this project ensuring the project remains focused on achieving the agreed outcomes. We ensure *added value* through our wider knowledge and understanding of the political, security, and Rule of Law considerations impacting Lebanese life, informed through the delivery of multiple HMG programmes over the past 5 years.

Key Risks Matrix. We see the challenges and risks breaking down into three broad categories:

1. Programme delivery.
2. Political risks.
3. Security and environmental risks.

The Risk Matrix below captures the key risk factors, by broad category, which we judge would likely have the most impact on the delivery programme. The Matrix is based on a combination of risk likelihood and risk rating by consequence and impact. Information used in formulation of risk levels was in part informed by monitoring of recent security incidents across the country and in particular, areas of planned operation.

There are 2 specific risks that are detailed in the Risk Matrix but elaborated here:

1. Credibility of messaging. To achieve the greatest impact, all messaging will derive directly from the results and qualitative findings of the research component. Wherever possible in the project, we propose to have the TA design any content produced and disseminated to provide maximum credibility, cultural nuances, narrative, language and effectiveness. Our in-country leads will also be responsible for oversight of this process. We have also incorporated message-testing opportunities through our iterative process which will allow us to continually refine our messaging throughout the course of the programme. Throughout the programme, we are accessing existing cultural concepts, networks and narratives rather than creating artificial or contrived new messaging and pathways.
2. Mitigating the risk of non-aligned messaging. Whilst the testimonies of former terrorist fighters (FTFs) offer authentic and effective CVE messages, we are cognisant of the risk of accounts – both from FTFs as well as activists or other parties – inadvertently promoting extremism or radicalisation, or in some way pushing narratives that are contrary to the objectives of this programme. As such, all testimonies will be reviewed by our expert in jihadist narratives, our project lead for their CVE expertise and our in-country expert for cultural nuance. The script will be provided to the Authority for approval in advance to ensure the content does not reinforce ideological or political statements that are contrary to our goals or could compromise HMG.

Experienced and proficient in proactively managing risks to staff, partners and beneficiaries. Our project management approach is founded on PRINCE 2, adapted and developed for delivering HMG programmes in Fragile and Conflict Affected States (FCAS). We accept the Duty of Care and Safeguarding responsibilities for employees, subcontractors, agents, partners and third parties/beneficiaries affected by our activities. These obligations are taken seriously and with 7 years' experience, including the safe delivery of over 18,000 days in FCAS and complex environments, we have developed clear processes and procedures to ensure we address these responsibilities effectively. We use highly credible risk management sources, including Northcott Global Solutions, FCO travel advisory services, and our own analysts for in-country security monitoring. We utilise a layered proactive initiative including: formal in-country dynamic risk assessment and mitigation; detailed property and site security plans; strong and effective communications; working in close partnership with all stakeholders, including local authorities; providing appropriate and ongoing environmental security training/briefings, and continually honing, testing and enforcing our comprehensive Company Operating Procedures (COPs), which keeps management of risk as a central tenet. All project staff will undergo pre-deployment Hostile Environment Training, as well as cyber and communications security education and awareness training.

Due diligence procedures. Torchlight operates an ISO 9001:2015 accredited supply chain management system supported by best practice. Our Supplier Evaluation Guide provides an auditable framework for the selection and ongoing management of suppliers. Evaluation criteria include financial checks, governance and statutory declarations, and past performance references. Internal financial controls and segregation of duties ensure the financial integrity of our supply chains. Suppliers are provided a contract linked to activity and invoices are subject to a 3-stage review approved by the Finance Director. Our supplier evaluation and internal financial controls, together with project team oversight, provide a robust framework for preventing fraud. All Torchlight staff undergo mandatory Anti Bribery & Corruption training, which is reinforced within COPs. All suppliers are made to contractually acknowledge adherence to the UK Bribery Act 2010. We would take quick and decisive action if attempted fraud is detected, ensuring full disclosure to the Authority.

Risk/Threat	Affect/Impact	Likelihood (1-5)	Risk Level	Mitigation
Programme Delivery Risks				
Lack of support for the programme, Target Audience participation & access to PRCs	Detrimental impact on Torchlight's ability to deliver the project.	**3**	**Moderate**	We have built a broad and persistent team using recognised HMG experts aligned with NGOs with local knowledge, influence, and access. This approach affords us the highest probably of success whilst remaining sensitive to the conflict dynamics. Challenges around messaging and counter-messaging are described on Page 1 of this section.
Gender sensitivity.	Any perception of gender inequality associated with the project may have reputational risks for both Torchlight, our implementing partners, and the Authority.	**2**	**Moderate**	Torchlight actively integrates gender sensitivity into all its programmes. Any activity that is deemed as counterproductive in achieving this is appropriately and proportionately responded to. We will institute specific measures to enhance counterpart human rights compliance, promote gender inclusion and ensure conflict sensitivity across the programme – all of which will enable rather than hinder delivery. This will include all members of our programme team signing a commitment to respect and uphold these values. Our technical advisers and programme management staff have extensive and specific experience in these areas across a range of other sensitive HMG-funded security sector reform programmes.
Safeguarding.	There is a risk to vulnerable persons associated with the project.	**2**	**Moderate**	Torchlight has implemented a Safeguarding policy which all employees, associates, and contractors are required to adhere to. There are no known safeguarding risks from within the wider team.
Further call-down expertise required & potential rotation of staff.	Capability gaps may delay project delivery and distort workstream timelines; having potential knock on effects with wider programming.	**2**	**Moderate**	With an established core of 45 full-time employees, supported by a network of 300+ specialists, we have the inherent ability to access wider professional technical expertise in a timely manner, either as individual experts or as part of our integrated multi-disciplinary teams.

Threats to project staff, partners and beneficiaries. Including from terrorism and negative, potentially violent impact of association with C-Daesh programme being made known among violent extremist community.	Any successful or attempted attacks against our project staff, partners, HMG or members of the Target Audience engaged in our programme is likely to have a destabilising effect on the programme delivery, including access to sites, personnel and willingness to continue.	**3**	**High**	All staff will undergo pre-deployment Hostile Environment Awareness Training (HEAT). Using Threat/Risk monitoring services, newsfeeds and local information, Torchlight will monitor the security situation and liaise with the Authority and partner organisations regarding threats/risks on route and in the vicinity of accommodation and project-focused sites (ie. hotels, refugee camps, border regions, stakeholder locations). **This programme will not be overtly branded as a CVE/C-Daesh programme and at no stage will we disclose HMG involvement in this programme.**
Political risks				
Host nation conflict with neighbouring states. Borders with Israel remain susceptible to potential conflict and the eastern and northern borders with Syria remain fragile through foreign fighter movement.	The security situation could deteriorate to such a degree that operations in Lebanon and Beirut would be untenable.	**2**	**Moderate**	We will seek to collaborate with the Authority, our local implementing partners and key Lebanese stakeholders in the security sector to ensure appropriate prioritisation and access to areas to carry on work with the limited resources available. Using Threat/Risk monitoring, newsfeeds and local information, we will monitor the security situation and liaise with our local partners on the most appropriate course of action.
Internal politics/breakdown in political process.	Possible impacts include; freedom of movement, availability of TA, degradation of the critical national infrastructure and the use of the international airport resulting in delay / suspension of the programme delivery.	**2**	**Moderate**	We will engage actively with principal points of contact to ensure appropriate prioritisation and availability to areas and people to carry on work with the limited resources available. We will seek assurance from our local partners of commitment to the programme.
Security and Environment Risks				
Cyber. There is a risk of direct targeting by extremist groups and/or nation states, including Lebanon (eg. Russia, Iran, Israel, Syria, Saudi and the Gulf States) seeking to either influence, disrupt or discredit projects of this kind. There is also a high probability of indirect risk from cyber criminals conducting social engineering or malware attacks.	Computer security breaches leading to data loss, corruption or covert espionage may compromise personnel security, undermine the credibility of our project and the reputation of stakeholders. This in turn could lead to lack of confidence by the Target Audience in the project and willingness of staff and partners to continue.	**3**	**High**	All staff will undergo pre-deployment cyber security training using our proprietary GCHQ- and ISSP-accredited online **CybSafe** platform, with regular refresher sessions during the project lifecycle. Project IT will employ BitLocker encryption, VPN software, Egress encrypted email and shared secure workspaces. Torchlight employs a remote-managed security service to monitor IT activity and keep AV software updated. All ports will be disabled, and removable devices will not be permitted. IT will be secured in workplace and residential accommodation.

Communications. There is a risk from interception of mobile, fixed line and unencrypted radio communications by nation state actors and extremist groups, as well as the accessing of personal and project-specific social media platforms.	The interception of voice and data communications, and monitoring of personal social media platforms could compromise personnel security and the integrity of the project. This in turn could lead to a lack of confidence by the Target Audience in the project and willingness of staff and partners to continue.	**2**	**Moderate**	All staff will undergo pre-deployment communications security training to include how to secure social media accounts; encrypted email for personal use (eg. ProtonMail) and secure messaging applications (eg. Wickr, Signal and WhatsApp). End-to-end encrypted VOIP video conferencing systems via VPN; Egress encrypted email and shared secure workspaces for project information and all laptops to be installed with AES 256 encryption (bitlocker).
Civil unrest. Local demonstrations and protests can bring parts of the country/Beirut into lockdown.	Local demonstrations prevent freedom of movement and can cause increasing levels of violence in localised or widespread areas of the city or region, hampering ability to conduct activity with End User.	**3**	**High**	In addition to utilising our local networks, we will maintain a close watch on the local and regional political news, indicators and warnings. These can be maintained through close collaboration with our local partners and regular updates from Threat/Risk groups and newsfeeds.
Reputational risk.	The sensitive nature of this project can potentially put Torchlight and the Authority into a situation where inappropriately framed publicity of any sort, actual or fictitious illicit activity are connected to our delivery. This may require extraction from the project for a protracted period or the transfer of delivery to another organisation due to the potential stigma associated with the implementing partner.	2	**Moderate**	Torchlight will maintain constant vigilance throughout its delivery and interaction with stakeholders to ensure any evidence or rumours of activities such as Human Rights violations are identified, scrutinised and managed through official chains to either prevent leakage of fictitious information or ensuring that the perpetrators are identified and held to account. **At no stage will we disclose HMG involvement in this programme.**
Kidnap. There is a threat of kidnapping by groups (includingDaesh and Daesh-affiliated groups) operating in border areas of the country and potentially in/around refugee camps.	The impact of team members being kidnapped is likely to be very high and result in an inability to deliver the project. The impact on families, friends and colleagues would be significant. Would likely result in concerted efforts by HMG and Host Nation to recover individual(s).	**2**	**Moderate**	All staff will undergo pre-deployment HEAT training. Coordination with local liaison partners will ensure project members avoid all high-risk areas, unless required by the programme. Conduct risk assessment and produce security plans, including communications schedules and regular calls. Torchlight has established operational procedures and insurances that will be escalated / implemented in line with threat levels.
Corruption. Corruption remains a problem in Lebanon and is particularly prevalent amongst public sector worker where wages remain low.	The impact of corruption extends from poor or no delivery of contracted services from in-country suppliers, team member(s) breaking UK, national and international anti-bribery and	**3**	**High**	Team members to undergo UK Anti-bribery and corruption training and education prior to deployment. Provision of direction and guidance from Torchlight Head Office regarding 3rd party supply

	corruption laws, and subsequent risk of detention, punishment or deportation, significant risk to the reputation of the project, as well as UK HMG and Torchlight, resulting in delays, retraction of Host Nation support or cancellation of project.			contracts and/or suspected bribery/corruption incidents. Robust and supported Whistle Blowing Policy.
Road Travel. Lebanon has a poor road safety record. The risk of death, injury or detention pending a trial/hearing if team members are involved in a Road Traffic Collison is 9 times greater than in the UK.	Impacts range from minor delays to project activities if vehicles are damaged, to possible detention by local law enforcement, injury and /or fatalities, which may result in significant delay or cancellation of the project.	**4**	**High**	All staff will undergo pre-deployment HEAT training and defensive driver awareness training. Project vehicles should be selected on the basis of safety and survivability. Team members to travel in pairs where possible. All vehicles to be equipped with medical, hazard warning and full recovery equipment.
Environmental risks mainly revolve around earthquakes. Due to the two fault lines (Yamuna/Roman) running through the country, seismic activity is common and daily, though rarely severe. Earthquakes usually range between 4 and 5 on the Richter Scale and can cause property damage.	Impact is low, as we do not envisage operating in the Mount Lebanon area. Any serious seismic activity could cause travel disruption or lack of cadre personnel could delay on programme delivery. Damage to property. Off duty activities could be affected.	**2**	**Moderate**	Formulate earthquake drills based on local best practice. All vehicles to be fully equipped with recovery and first aid equipment. Communications plans and schedules to be implemented. Avoid high risk areas during extreme weather conditions.
UXO. Threat of Mines, IEDs and UXO. Various factions over the years have seeded anti-vehicle and anti-personnel mines as well as cluster bombs. This threat is mainly around the border areas in the north-east of Lebanon (borders with Syria by Da'esh and HTS) and along the southern border areas (Israeli Forces).	Impacts include loss of life or serious injury to project staff or implementing partners, postponement or cancellation of programme.	**3**	**High**	Coordination to ensure all high-risk areas avoided, unless essential need to travel there for the programme. Seek local advice and adhere to Mine Field Markers and warnings and stick to known and maintained paths and metalled roads.
Power cuts. Frequent power cuts due to demand for power and subsequent energy surges, especially throughout the holiday and summer months.	Frequent power cuts can have a significant impact on the tempo of delivery and access to IT infrastructure.	**3**	**High**	Where possible, use back up power options. Utilise Laptops where possible with spare batteries. Keep charged whenever power is available. Utilise UPS (large and laptop-sized options) if the power situation becomes untenable.