TRIP RISK LEVEL ASSESSMENT

| FACTOR | VERY LOW (1) | LOW (2) | MEDIUM (3) | HIGH (4) | VERY HIGH (5) |
| --- | --- | --- | --- | --- | --- |
| **Journey** | Travel journey is **not** likely to involve exposure to security threats for team members, participants, other stakeholders.  Any incidents are likely to have **negligible** impact. | Travel journey is **somewhat** likely to involve exposure to security threats for team members, participants, other stakeholders.  Any incidents are likely to have **minor** impact. | Travel journey is **reasonably** likely to involve exposure to security threats for team members, participants, other stakeholders.  Any incidents are likely to have **moderate** impact. | Travel journey is **likely** to involve exposure to security threats for team members, participants, other stakeholders.  Any incidents are likely to have **major** impact. | Travel journey is **highly** likely to involve exposure to security threats for team members, participants, other stakeholders.  Any incidents are likely to have **critical** impact. |
| **Destination** | Destination experiences **rare** security threats (crime, terrorism, civil unrest, conflict, arrest, surveillance).  Any incidents are likely to have **negligible** impact. | Destination experiences **occasional** security threats (crime, terrorism, civil unrest, conflict, arrest, surveillance).  Any incidents are likely to have **minor** impact. | Destination experiences **periodic** security threats (crime, terrorism, civil unrest, conflict, arrest, surveillance).  Any incidents are likely to have **moderate** impact. | Destination experiences **frequent** security threats (crime, terrorism, civil unrest, conflict, arrest, surveillance).  Any incidents are likely to have **major** impact. | Destination experiences **constant** security threats (crime, terrorism, civil unrest, conflict, arrest, surveillance).  Any incidents are likely to have **critical** impact. |
| **Information** | Very low digital threats because actor(s) have **zero** capabilities and/or are highly unlikely to target travellers.  Information content / sharing is **not likely** to result in security incidents. | Low digital threats because actor(s) have **low** capabilities and/or are unlikely to target travellers.  Information content / sharing is **somewhat** likely to result in security incidents. | Medium digital threats from **somewhat** capable actor(s) who could potentially target travellers.  Information content / sharing is **reasonably** likely to result in security incidents. | High digital threats from **capable** actor(s) with known intent to target similar travellers.  Information content / sharing **likely** to result in security incidents. | Very high digital threats from **highly capable** actor(s) with known intent to target the travellers.  Information content / sharing is **highly likely** to result in security incidents. |
| **Activity** | Activity is **not** likely to involve exposure to security threats for team members, participants, other stakeholders (e.g., closed meeting in very low risk destination). | Activity is **somewhat** likely to involve exposure to security threats for team members, participants, other stakeholders (e.g., conference in low risk destination). | Activity is **reasonably** likely to involve exposure to security threats for team members, participants, other stakeholders (e.g., conference in medium risk destination). | Activity is **likely** to involve exposure to security threats for team members, participants, other stakeholders (e.g., dialogue in high risk destination). | Activity is **highly likely** to involve exposure to security threats for team members, participants, other stakeholders (e.g., fieldwork in very high risk destination). |
| **Stakeholders** | Travel **does not** involve fixers, partners, grantees, fellows, other stakeholders. | Travel involves fixers, partners, grantees, fellows, other stakeholders who are **unlikely** to be targeted. | Travel involves fixers, partners, grantees, fellows, other stakeholders who are **somewhat** likely to be targeted. | Travel involves fixers, partners, grantees, fellows, other stakeholders who are **sometimes** targeted. | Travel involves fixers, partners, grantees, fellows, other stakeholders who are **frequently** targeted by capable threat actors. |
| **Travellers** | Traveller profile or visibility factors are likely to have **negligible** impact on their risk exposure.  Traveller is **highly** **experienced** with similar travel and has **highly** relevant securitytraining. | Traveller profile or visibility factors are likely to have **minor** impact on their risk exposure.  Traveller is **significantly** experienced with similar travel and has **relevant** security training. | Traveller profile or visibility factors are likely to have **moderate** impact on their risk exposure.  Traveller is **reasonably** experienced with similar travel and has **less** relevant security training. | Traveller profile or visibility factors are likely to have **major** impact on their risk exposure.  Traveller is **somewhat** experienced with similar travel and has **no relevant** security training. | Traveller profile or visibility factors are likely to have **critical** impact on their risk exposure.  Traveller is **not experienced** with similar travel and has **no** security training. |

Notes

1. The indicators above are provided for guidance. It is unlikely that every factor and indicator will be highly relevant for every trip. Additionally, some of the language in a single indicator may apply, but other language in the same indicator may not. As such, we recommend **a common-sense approach**.
2. The risk scores should be identified **without any consideration of their consequences** (e.g., required level of mitigations and approval).
3. Where you are unsure between two risk scores, **escalate to the higher risk score**. This ensures appropriate mitigations and approval.
4. The **highest risk score** **dictates the trip risk level**, for any given factor.
5. If the travel is a **multi-destination trip**, conduct a threat assessment for each destination and use the highest trip risk level, for any given factor, for the entire trip.
6. Trips with a **VERY LOW**, **LOW** or **MEDIUM** trip risk level are **reviewed and** **approved by the relevant manager/project manager** and should follow the relevant guidance in the Travel guidance and procedure.
7. Trips with a **HIGH** or **VERY HIGH** trip risk level are **reviewed and** **approved by the director or deputy director** and should follow the relevant guidance in the Travel guidance and procedure.