# ANNEX B. SECURITY PLAN

This annex outlines the essential elements for writing a security plan for trucking operations. This template uses the five-step model managing trucking security risk which is introduced in ROADSEC Chapter 4 as the basis.



A security plan is the cornerstone of secure trucking operations that sets the basis for a strong security culture and strong security practice. A company security plan should cover at least the following steps, themes and elements:

1. Allocate security responsibilities to competent and qualified persons who have appropriate authority and high motivation to carry out their security related tasks. Nominate the head of security, preferably a senior expert with strong skills and substantial experience in trucking security.
2. Assess security risks of trucking operations. Refer to ROADSEC toolkit Chapter 4.2 “Assess Risk”. Involve key business partners – including shippers, freight forwarders, carriers, security service providers, and insurance experts – in the risk assessment, if possible.
3. Define measures to be taken to mitigate security risks in trucking operations. Refer to Chapter 4 of the ROADSEC toolkit keeping in mind specific requirements and needs of your company regarding key layers of trucking security management.
* Design & planning;
* Process control & visibility;
* Assets & data protection;
* Human resource management;
* Business partner management;
* Aftermath capabilities; and
* Disruption of criminal activities.

Consider also state-of-the-art technologies presented in ROADSEC Annex D “Freight transport security technology horizon.”

Pay regard to applicable laws, regulations, standards, internal company policies when selecting trucking security measures.

Study closely the security measures recommended or required by EU AEO, UK Border Force, TAPA EMEA and others, by consulting the ROADSEC Annex E “Existing freight transport security standards and good practices.”

1. If necessary, tailor ROADSEC Chapter 3 and/or Annex A to match the exact security measures and tips applicable to your truck drivers.
2. Organize appropriate training and awareness building among the drivers using materials particularly from ROADSEC Chapter 3 and Annex A, as well as Chapter 4. Consider hiring security trainers from the outside of your company or send your drivers to a trucking security course.
3. Establish communication and reporting procedures to collect driver feedback and help the drivers to report suspicions and crime incidents. Refer to ROADSEC toolkit Annex G “Security incident reporting forms” and the Chapter 4.6.2 “Capture data for security performance monitoring”.
4. Create procedures for periodic evaluation and update of security plans and procedures. Consider recommendations of the ROADSEC Chapter 4.6 “Monitor & Revise.” Collect feedback from drivers and consider the drivers’ needs and wishes in day-to-day trucking security management.
5. Ensure that only authorised people access information in the security plan on a need-to-know basis. Establish necessary cyber security safeguards to protect digital information as well.

Altogether, when designing security plans, managers should consider the five-step model and guidelines of ROADSEC Chapter 4, which guides them through the most important aspects and themes of the modern-day trucking security management. Use also Chapter 3 and Annex A – potentially tailored versions - of the ROADSEC toolkit to communicate key aspects of trucking security to truck drivers.