

F.5.2 SOFTWARE RISK MANAGEMENT

Objective:

Software risk management is a proactive and disciplined approach to assess and control software risks.

Criteria:

1. Potential software risks are identified as required by the grading level.
2. Likelihood and consequences of the safety software failure are determined.
3. Risks are prioritized.
4. Risk avoidance, mitigation, and/or transfer strategies are created.
5. Risks are monitored.

Approach:

Determine the existence of software risk management planning. This may be evident in a standalone document or embedded in another document. As applicable, ensure that the risk management planning specifies the following:

- scope of the risk management activities;
- risk management policies and process (for both technical and managerial) under which risk management is to be performed are defined;
- identification of the technical and managerial risks and likelihood and potential safety consequences of using software risk taxonomies as a guide;
- establishment of risk thresholds for the safety software application;
- risk avoidance, mitigation, or transfer options; and
- management techniques to address risks throughout project life-cycle, including tracking, decision, and feedback points.