Risk Management

An initial product risk assessment must be performed after establishment of the requirements. The purpose of the assessment is to determine which (parts of) the software could contribute to hazardous situations that can lead to harm of the patient and/or operator. Risks are estimated on probability and severity and risk control measures are to be taken. These measures can result in a redesign of the software (changing or adding requirements), changing or adding health care procedures, warnings to the operators via the instruction manual or via the software. All risks must be mitigated to an acceptable level. A risk-benefit analysis (does a medical benefit outweigh the risk) is part of the risk management report.

Risk management is a continuous process: it is invoked initially, after the design phase, before final release and during maintenance phase if feedback from the market is received. All risk related documentation together is called the Risk Management File (RMF)

For medical devices, the ISO14971 is the de-facto standard for risk management.
The IEC62366 (see section Usability), defines how use errors are taken into account in the risk process.
The IEC62304 details out the risk process for software and ads a risk level (A, B, C) that defines that the higher the risk of a module more quality evidence is required.