	Objectives	Activities	Main Guidance Material	Outputs
Establish Context	Key stakeholders and necessary approvers are identified Interfaces are defined and controlled The Data Safety assessment is planned Data Artefacts are identified	Describe the organisational context Describe the system context Plan the assessment Identify Data Artefacts	Organisational Data Risk (ODR) assessment Data Safety Culture questionnaire System lifecycle, producers and consumers Supplier data maturity questionnaire Data Types	A list of key stakeholders and necessary approvers for data safety activities An interface control plan or list of control measures An estimate of the level of data-related risk (e.g., an ODR rating) A plan for the remaining parts of the data safety assessment A collection of Data Artefacts
Identify Risks	Generic and historic examples of data-related issues are reviewed Risks are identified and linked to Data Artefacts and Data Properties	Review the general, historical perspective Conduct a top-down approach Conduct a bottom-up approach Update planning documents	Historical accidents and incidents Generic ways data can cause problems Data Properties Hazard and Operability Study Guidewords	A description of the process used for risk identification List of risks linked to Data Artefacts and associated Data Properties Plans updated to account for quantity and complexity analysis
Analyse Risks	The required Data Safety Assurance Levels are established and justified The required Data Safety Assurance Levels are analysed as part of system safety activities	Establish Data Safety Assurance Levels Analyse DSALs as part of system safety activities	Data Safety Assurance Levels (DSALs) Relationship between DSALs and other Integrity Levels	A DSAL (and supporting justification) for each identified risk
Evaluate and Treat Risks	Data Safety requirements are identified, documented and reviewed Methods used to provide Data Safety assurance are defined and implemented Evidence of compliance with the Data Safety requirements is documented, reviewed and approved	Review each risk and either: Avoid, Accept, Transfer, or Treat Establish treatment methods for relevant risks Implement and verify treatment methods	Methods and Approaches tables	A record of the agreed responses to each of the identified risks Data Safety requirements that follow from these responses A record of the treatment adopted for each of the identified risks An assessment as to whether the risk has been suitably mitigated