Contact <u>data-safety@mca-ltd.com</u> to assess your organisation's exposure to data risks.

Data Safety Questionnaire

1.	Context
	   a) What does your organisation do?
	   b) What is the context of the work?	

2.	What does your organisation do with data?
	   a) Does your organisation use or produce data?
	   b) Does it feed data into other systems to use?
	   c) Does it feed data to other organisations?
	   d) Does it produce data for staff to use?	

3.	Specific use of the data
	   a) Who uses the data? (do you display or feed to other systems)
	   b) What do they do with it?	

4.	Responsibility and Accountability
	   a) Is there someone in your organisation responsible/accountable for data?
	   b) Who manages / maintains the data?
	   c) Is it clear who owns the data?
	   d) Who is responsible for procuring the data?	

5.	Can you draw a boundary for your organisation and its responsibility for data?	
6.	Is any of the data considered sensitive or critical for its intended purpose? For instance, is there data that has to be correct, accurate or timely in some way?	

7.	Are decisions affecting people or the environment made based wholly or partly on the data?
	   a) Could any of the data indirectly lead to harm via other systems or usage by other people?
	   b) Could any of this data directly cause harm?	

8.	Could this *safety-related* data be altered or changed in some way?
	For instance, could it be:
	   a) Lost or deleted
	   b) Out of date
	   c) Out of sequence
	   d) Wrongly merged together
	   e) Less acccurate than expected
	   f) Partly missing or incomplete
	   g) Modified unintentionally
	   h) Changed maliciously
	   i) Corrupted in a way which is hard to detect
	   j) Repeated in Multiple records for the same instance	

MISSION CRITICAL APPLICATIONS

Contact data-safety@mca-ltd.com to assess your organisation's exposure to data risks.

	Data Safety Questionnaire	

9.	What could be the effect in each these cases?
	  a) What harm to people or the environment might result?
	  b) Typically, what would go wrong?
	  c) How often might this problem arise?
	  d) What could be the worst-case scenario?	

10.	Are there protections in place to detect safety-related data problems?
	These might include:
	  a) Someone would spot the problem
	  b) Validation checks
	  c) Review on change
	  d) Regular inspections / checks / audits
	  e) Comparisons with other data (e.g. the previous set of data)
	  f) Data quality process
	  g) Technical measures on the data itself: checksums, digital signatures, CRCs, etc.	

11.	Risk Assessment and Review
	  a) Has an audit or review activity been conducted to establish the nature and scale of safety-related data in your organisation?
	  b) Has a risk assessment been undertaken to look at the specific data-related issues?	

12.	Support and Guidance
	  a) Is there any guidance or standards available to assist in managing safety-related data?
	  b) Are there any tools and infrastructure to support the management of such data?	

13.	Would tool support help manage data quality and data assurance in your organisation?	

14.	Collaboration
	  a) Would you like to collaborate to develop sector-specific customizations of the guidance and the RADISH tool?
	  b) Would you be happy for your answers to be used anonymously in further work?	