Risk Management Software criteria

System functions and characteristics:

Field, etc.	Description/requirement	Score
Business Objectives	Ability for the software to identify business objectives to which the risk(s) will relate. Linking/referencing objectives to risks and controls is a key requirement.	
Risk Identifiers	Unique identifier or risk index also possibly to identify functional area (i.e. Finance, HR, Commercial, etc.)	
Description of risk	Ability to describe the risk in sufficient detail to inform the assessment process. Better RM systems would also have a library of risks pre-recorded and editable for use to adapt for its own register. Should be able to cross-reference to controls, etc.	
Appetite/tolerance	Ability to identify risk attitude, appetite, tolerance or limits for the risk and/or target for control of risk and desired level of performance. Appetite should be capable of being determined on a risk-by-risk, or 'theme', basis rather than applying a global level of appetite to all risks. The system should be able to report on whether the inherent or residual risks are within stated appetite.	
Risk Owner	Ability to assign risks to a named person (ideally from a list of staff/look up table).	
Risk assessment	Ability to measure factors such as likelihood and impact and potentially for areas such as project risk aspects such as velocity, proximity and propinquity. The system should also be able to define an appropriate scoring approach. The better and more advanced systems software will enable this scoring to be customised so that it reflects specific needs. Supporting narrative/descriptors for each measure should be available and or customisable.	
Inherent Risk Score	A field which produces a 'score' based on the data above.	
Controls/mitigating actions	The system should be capable of identifying controls and their status/effectiveness in the mitigation of inherent risk. It should also be able to record different data relationships (i.e. one risk with one control; one risk with many controls, many risks with many controls, etc.). Typically this would include information such as: ▪ Existing control mechanisms and activities and controls; ▪ Control frequency; ▪ Level of confidence in existing controls; ▪ Procedures for monitoring and review of risk performance. An existing library/drop down menu would be advantageous as well as the ability to cross-reference controls to risks.	
Control Owner	Ability to assign controls/actions to a named person (ideally from a drop down list of staff/look up table) and the ability to assign dates for actions to be completed.	
Control effectiveness	Ability to record view/opinion as to their effectiveness and capable of being reported alongside inherent and residual scores as well as the stated appetite. Better systems will also include the resource implications of operating controls.	
Control cost and frequency	Can the system record the cost of operating the control (in terms of people, money and time? Further, can the system identify the frequency of the control's operation (i.e. daily, weekly, monthly, etc.)	
Control attestation	Are the results of any controls captured?	
Residual risk information	The system should be able to show residual impact, likelihood and risk scores through the use of the above data (i.e. controls and their effectiveness).	
Loss experience /incident logging	Previous incidents and prior loss experience of events related to the risk should be capable of being recorded to provide an evidence base for the scoring of risks – this should include the ability to attach documents, PDFs, etc.	
Benefit experience	Similar to the above points but from the perspective of an opportunity risk, where an actual benefit has been realised, i.e. that the outcome of a risk is a positive result.	

Field, etc.	Description/requirement	Score
Risk aggregation and escalation	Is there the facility to aggregate data for the same risks that occur at multiple times or in multiple functions or locations to establish an enterprise-wide position for a 'group' of risks? Where there are different levels or tiers of risk (say to reflect the organisational structure and management responsibilities, is there the ability to escalate risks that exceed agreed thresholds or limits and are worthy of being reported upwards?	
Potential for risk improvement	▪ Potential for cost-effective risk improvement or modification; ▪ Recommendations and deadlines for implementation; ▪ Responsibility for implementing any improvements.	
Assurance data	Capable of recording (possibly in a comments field/free format) sources of, or gaps in, assurance.	
Risk history	Ability to record the history and movement of risk over different time periods.	
Audit trails	For example the ability to list the history of risk scores over a stated period to show and why they have changed, etc.	

Other considerations:

Area	Description/requirement	Score
Reporting	Capable of reporting by any type or combination of fields above and through use of filtering (e.g. a list of risks grouped by risk owner – such as Director of HR, etc.). Graphical outputs also such as heat-maps, risk/control matrices, etc.	
Ease of use/access	Availability to users: ▪ Usable on traditional desktop/laptop devices; ▪ Usable on smart devices; ▪ Mobile/remote working; ▪ Real-time data; ▪ Available 24/7; ▪ Simultaneous use/record or file-locking; ▪ Multiple users/licences – flexibility of options and pricing on number of licences; ▪ Dynamic or automated updating and reporting (i.e. through email alerts).	
Integration issues	Ability to connect, integrate or transfer data with other organisational systems.	
Storage and security	Is the data and system an 'on premise' or cloud solution? What retention periods are there – how long is data kept for? GDPR? Is there an archiving facility? Where is the data held and are there protections such as escrow agreements, etc.? Is the ownership of the software and data clear from any contract or agreement (clarity on issues such as who are the data controllers and processors)? Data accessed, sent or created remotely – secure and encrypted?	