Attachment B
City of Redmond Functional Risk Management System Requirements

INSTRUCTIONS FOR COMPLETING FUNCTIONAL REQUIREMENTS

1) Supplier Response

For each numbered line item requirement, the vendor must indicate Y, 3P, C, F, or N with an "X" in the Supplier Response column, according to the following legend:

Y	Fully supported by the current release of the software.
3P	Supported with third party software (i.e. software not directly owned or controlled by the supplier submitting the proposal).
C	Customization is required to meet the requirement (e.g. changes to the underlying code must be made; a new table must be created; etc.) This causes additional upgrade work in order to implement new versions or upgrades.
F	Future functionality: Supported in the next release of the software.
N	Not supported.

2) If the Supplier responds with **3P**, **C**, or **F**, the supplier must provide additional information in the comments column:
   - For "**3P**", the supplier must explain what third party software application or service is required, any integration requirements, and the vendor's relationship with this third party.
   - For "**C**", the supplier must explain the nature and amount of customization required, and experience with the same or similar modifications.
   - For "**F**", the supplier must explain the functionality in the new release, the expected general availability release timing and provide surety that the functionality will be included.

3) The Supplier must also identify which module(s) the required functionality is part of in the final column (as applicable).

The information must be completed and submitted in the format provided.

Attachment B
City of Redmond Functional Risk Management System Requirements

		Key Functional Criteria **R** = Required **I** = Important **N** = Nice to Have **E** = Explore	**Supplier Response** **Y**	**3P**	**C**	**F**	**N**	**Comments** *if supplier responds with 3P, C, or F, additional information must be provided as noted on Instructions page. Note applicable modules.
		Requirements						
1	**R**	Employees can submit incidents directly into the system.						
2	**E**	Citizens can submit incidents directly into the system.						
3	**N**	Employees may enter an incident in draft mode and save it temporarily before completing and submitting for supervisor review.						
4	**I**	Incidents may be queried, filtered or sorted by a variety of criteria (such as claimant, date, status, keyword, type).						
5	**I**	Incident review should be enabled by work-flow to supervisor or other relevant city staff based on type.						
6	**N**	Allowable values within certain data fields should be restricted (such as dates, type of incident).						
7	**N**	Default values should be available where applicable (e.g. date = current date).						
8	**N**	Field format masks should be available where applicable (e.g. date, phone number).						
9	**R**	Security features should limit visibility of certain incident information to personnel outside of risk management.						
10	**R**	Ability to edit information within an incident is controlled by security.						
11	**I**	Ability to configure incident types and content and associated workflow.						
12	**I**	Ability to establish and modify workflow rules based on content.						
13	**N**	Ability to escalate and delegate within workflow.						
14	**N**	Ability to associate a new incident to a parent incident (e.g. a broken water pipe may result in multiple claims from the same incident; a						

		citizen and an employee both make separate entries on the same incident).						
15	**I**	Risk management personnel can edit information related to the incident.						
16	**N**	Estimates of damage amount can be entered at different stages of incident review.						
17	**R**	Supporting documentation can be "attached" to an incident record (e.g. photographs, emails, scanned documents).						
18	**I**	An incident can reference a police report.						
19	**I**	Ability to include "tracking" only incidents (also could be used for "near misses").						
20	**I**	Ability to set reminders for follow-up.						
21	**R**	Records can be archived and deleted as appropriate pursuant to records retention schedules.						
22	**N**	Records can be exported to a Records Management system for archival.						
23	**R**	Ability to track related costs of an incident (e.g. investigation, city repaired damage, external repairs).						
24	**R**	Ability to track cost recovery within an incident (e.g. recovery of city costs related to damaged city property).						
25	**R**	Ability to track the status of each incident.						
26	**I**	Easily accessible data for reporting within "Business Intelligence" type tool such as Power BI.						
27	**I**	Ability to reopen "closed" incidents if needed.						
		Incident Data Requirements						
28	**R**	Employee name (should self-populate, but can be changed).						
29	**I**	Employee position.						
30	**R**	Type of Incident (property, vehicle, citizen)						
31	**N**	Witness						
32	**R**	Other Person Involved						
33	**I**	Employee phone.						
34	**I**	Employee department.						
35	**I**	Employee division.						

36	**R**	Date of incident (editable by Risk Management).						
37	**R**	Date incident reported (auto-populates).						
38	**R**	Vehicle Number						
39	**R**	Description of incident (text field).						
40	**R**	Location of incident (text field).						
		Technical Requirements						
41	**I**	Migrate data from our current in-house application.						
42	**R**	Describe support hours and Service Level Agreements.						
43	**R**	Describe how sensitive data is stored. If encrypted, what type of encryption?						
44	**I**	Does the system integrate with Active Directory Federated Services (ADSF)? If not, describe the user name and password management and protection.						
45	**I**	If citizen entry is supported, describe how user names and passwords are protected and the process for recovering credentials.						
46	**R**	Services have a geographic presence with reasonable proximity to Redmond, be within the United States, and have geo-redundancy.						
47	**R**	Describe how the solution protects against DDOS attacks and others.						
48	**R**	Describe your approach to applying security updates including how frequently they are applied						
49	**R**	Describe the disaster recovery plan including, but not limited to, frequency of backups for servers and systems, recovery procedures and frequency of testing those procedures, any disaster recovery service levels in terms of recovery point objective, recovery time objective and fail over plans and options.						
50	**R**	Describe the access we will have to our data outside the system for reporting or other uses.						