GRC AI Agent

Alp Berrak and Carter Jules

Time Frame	*Task/Associated Subfeature*	*Description*	*Functional Testing Timeframe*	*Test Cases*	*Estimated Completion Date*
Milestone 1 - Data Compilation - 02/01 - 02/15					
02/01 - 02/04	Feature 1a	Compile list of all regulations applicable to the business sector	02/01 - 02/04	N/A	02/04
02/04 - 02/08	Feature 2a	Compile list of all NIST recommendations	02/04 - 02/08	N/A	02/08
02/08 - 02/12	Feature 3a	Compile examples input prompts	02/08 - 02/12	N/A	02/12
02/12 - 02/15	Feature 4a	Compile example good system configs	02/12 - 02/15	N/A	02/15
Milestone 2 - Database Build Out - 02/15 - 02/28					
02/15 - 02/22	Feature 1b	Develop database for regulations that is easily appendable	02/22 - 02/28	Test by appending new regulation	02/22
02/22 - 02/28	Feature 1c	Develop database for regulations that is easily parsable by LLM	02/22 - 02/28	Test by having LLM read through it (milestone 3)	02/28
02/15 - 02/22	Feature 2b	Develop database for NIST that is easily appendable	02/22 - 02/28	Test by adding new NIST recommendation	02/22
02/22 - 02/28	Feature 2c	Develop database for NIST that is easily parsable by LLM	02/22 - 02/28	Test by having LLM read through database (milestone 3)	02/28
02/22 - 02/28	Feature 3b	Develop database for example inputs that is easily parsable	02/22 - 02/28	Test by having LLM read through database (milestone	02/28

				3)	
02/22 - 02/28	Feature 4b	Develop database for example system configs that is easily parsable	02/22 - 02/28	Test by having LLM read through database (milestone 3)	02/28
Milestone 3 - Build the LLM - 03/01 - 03/31					
03/01 - 03/02	Feature 5a	Develop the output formatting	03/01 - 03/02	Test by reviewing Agent output	03/02
03/02 - 03/09	Feature 6a	LLM training to know weak system features	03/05 - 03/09	Test through reviewing Agent output for accuracy	03/09
03/02 - 03/09	Feature 7a	LLM training to know strong system features	03/05 - 03/09	Test through reviewing Agent output for accuracy	03/09
03/02 - 03/09	Feature 8a	LLM training to know system configs that don't follow regulations	03/05 - 03/09	Test through reviewing Agent output for accuracy	03/09
03/02 - 03/09	Feature 9a	LLM training to know system configs that follow regulations	03/05 - 03/09	Test through reviewing Agent output for accuracy	03/09
03/09 - 03/18	Feature 6b	LLM training to identify weak features within larger system	03/12 - 03/18	Test through reviewing Agent output for accuracy	03/18
03/09 - 03/18	Feature 7b	LLM training to identify strong features in system	03/12 - 03/18	Test through reviewing Agent output for accuracy	03/18
03/09 - 03/18	Feature 8b	LLM training to identify what configs don’t follow regulations in a larger system	03/12 - 03/18	Test through reviewing Agent output for accuracy	03/18
03/09 - 03/18	Feature 9b	LLM training to identify what configs follow regulations in larger system	03/12 - 03/18	Test through reviewing Agent output for accuracy	03/18
03/18 - 03/25	Feature 10a	LLM training to ensure correct recommendations are given based on user input	03/21 - 03/25	Test through reviewing Agent output for accuracy	03/25
03/18 - 03/25	Feature 11a	LLM training to ensure correct regulations are listed that must by followed given specific user	03/21 - 03/25	Test through reviewing Agent output for accuracy	03/25

		input			
03/18 - 03/25	Feature 12a	LLM training to ensure it can parse all parts of a system config correctly	03/21 - 03/25	Test through reviewing Agent output for accuracy	03/25
03/25 - 03/31	Feature 12b	LLM training to ensure it uses the training regulation and NIST data to get output	03/28 - 03/31	Test through reviewing Agent output for accuracy	03/31
03/25 - 03/31	Feature 13a	LLM training on variations of input to ensure that it still correctly process input and gives output	03/28 - 03/31	Test through reviewing Agent output for accuracy	03/31
03/25 - 03/31	Feature 14a	LLM can correctly identify what node to travel to based on input	03/28 - 03/31	Test through reviewing Agent output for accuracy	03/31
03/25 - 03/31	Feature 14b	LLM moves through AI Agent nodes correctly based on user input	03/28 - 03/31	Test through reviewing Agent output for accuracy	03/31
Milestone 4 - Security and Pentesting 04/01 - 04/20					
04/01 - 04/08	Feature 15a	Implement input sanitation to prevent attacks via user input	04/03 - 04/08	Pen Testing	04/08
04/08 - 04/15	Feature 15b	Implement rate limiting to prevent service overload	04/11 - 04/15	Pen Testing	04/15
04/15 - 04/20	Feature 15c	Implement data encryption for user input security	04/18 - 04/20	Pen Testing	04/20