CY4930 - GRC AI Agent

Alp Berrak and Carter Jules

Feature			Sub-Feature		
#	**Name**	**Description**	**#**	**Description**	**Assigned To**
1	Regulation Database	Database that contains all data regulations applicable	**a**	All regulations that apply to the business sector are accounted for	Carter
			b	Easily updatable in order to account for new regulations/additional sectors	Carter
			c	Formatted such that LLM can easily parse	Carter
2	NIST Database	Database that contains all NIST recommended system features	**a**	All NIST recommendations accounted for	Alp
			b	Easily updatable for new recommendations	Alp
			c	Formatted such that LLM can easily parse	Alp
	Additional Config Database	Database that contains additional recommendations that add onto NIST that are specific to the business/finance sector	**a**	Easily updatable for new recommendations	Carter
			b	Formatted such that LLM can easily parse	Alp
3	Example Database	Database that contains example prompts for LLM training use	**a**	Example prompts that cover a variety of cases/system configs	Carter

			b	Variations of format to properly train the LLM	Alp
4	Good System Example Database	Database that contains examples of well built systems for LLM training use	**a**	Several examples of well built out systems	Carter
			b	Variation is size/complexity of system and purpose of system	Alp~
5	Output Format	How the output should be formatted every time AI Agent is used	**a**	Specific order of output in order to make output info easily digestible by user	Carter
6	Weak Feature Detection	LLM trained to identify weak features in a given system	**a**	LLM trained to know weak features	Alp
			b	LLM trained to detect weak features in larger system config and list them in output	Carter
7	Strong Feature Detection	LLM trained to identify strong features in a given system	**a**	LLM trained to know strong features	Carter
			b	LLM trained to detect strong features in larger system and list them in output	Alp
8	Not Following Regulation Detection	LLM trained to identify when a system is not following a regulation correctly	**a**	LLM trained to know what system configs don’t follow regulations via example instances	Alp
			b	LLM trained to detect when a particular system config doesn’t follow a regulation and list it in output	Carter

9	Following Regulation Detection	LLM trained to identify when a system is following a regulation correctly	**a**	LLM trained to know what system configs do follow regulations via example instances	Carter
			b	LLM trained to detect when a particular system config does follow regulation and list it in output	Alp
10	Recommendation Output	LLM outputs recommendations for upgrading a given system correctly	**a**	LLM can process a system in order to correctly identify what areas can be improved - trained on examples of weak system and their improvements	Carter
11	Identifying Regulations Output	LLM outputs list of regulations a system must follow correctly	**a**	LLM can identify what regulations apply based on locations and sector (only business in this case)	Alp
12	Input Parser	LLM able to parse through given input config file	**a**	LLM can correctly parse the different parts of system config	Carter
			b	LLM can apply regulation and NIST databases to the input it has parsed	Alp
13	Input Flexibility	LLM able to parse through variations of input config file	**a**	The input config file does not have to be a strictly formatted input - can work with variations of input	Carter
14	Frequent Input Nodes	AI Agent has built in nodes to work with frequent inputs more efficiently	**a**	LLM can identify when particular part of a system config is frequently seen	Carter

			b	LLM can correctly move to node based on the frequent input given	Alp
15	User Input Protection	Build out security for database	**a**	Input sanitation	Alp
			b	Rate limiting	Carter
			c	Data encryption	Alp
16	Nodes for if clauses	Nodes in the AI Agent that work through the input via if statement	**a**	A node for accounting for location - is location mentioned in input	Carter
			b	A node for accounting for something out of scope of the AI Agent	Carter
			c	A node for input that contains all the information needed to run analysis	Alp
			d	A node for input that only wants to know regulations to follow	Alp