Cybersecurity Compliance and Reporting Platform

Project Progress Update 1

April 2025

Progress Overview

- Frontend of the Platform
- Dual Information Input Flow: (A) PDF Upload or (B) Form Filling
  - (A) PDF Upload – LLM model to extract information from the report
  - (B) Form Filling – Form design
- Pre-Reporting Evaluation Framework: Factors for Severity determination model
- Backend of the Platform

Frontend of the Platform for Incident Reporting Form

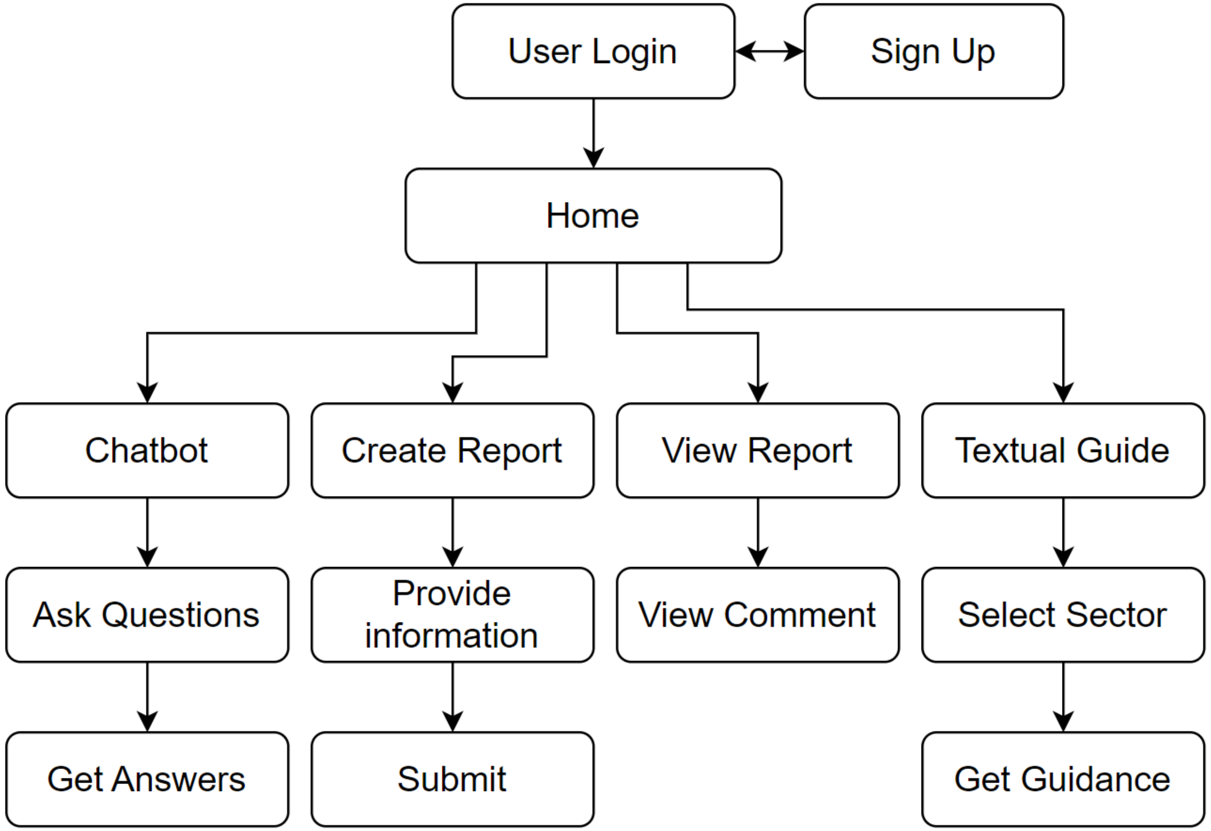
- **Frontend requirements:**
  - **Node: v20.11.1 +**
  - **NPM (Node Package Manager): v10.2.4 +**
  - **Framework: React JS v19.0.0 +**

- **Local chatbot backend requirements:**
  - **Python: v3.9 +**
  - **Ollama: v0.6.2 +**

- **Frontend design considerations:**
  - **To design Responsive web with seamless compatibility across diverse devices and screen sizes**
  - **To make intuitive navigations without confusion**
  - **To consider user needs and preferences**
  - **To user modular approach considering further updates**

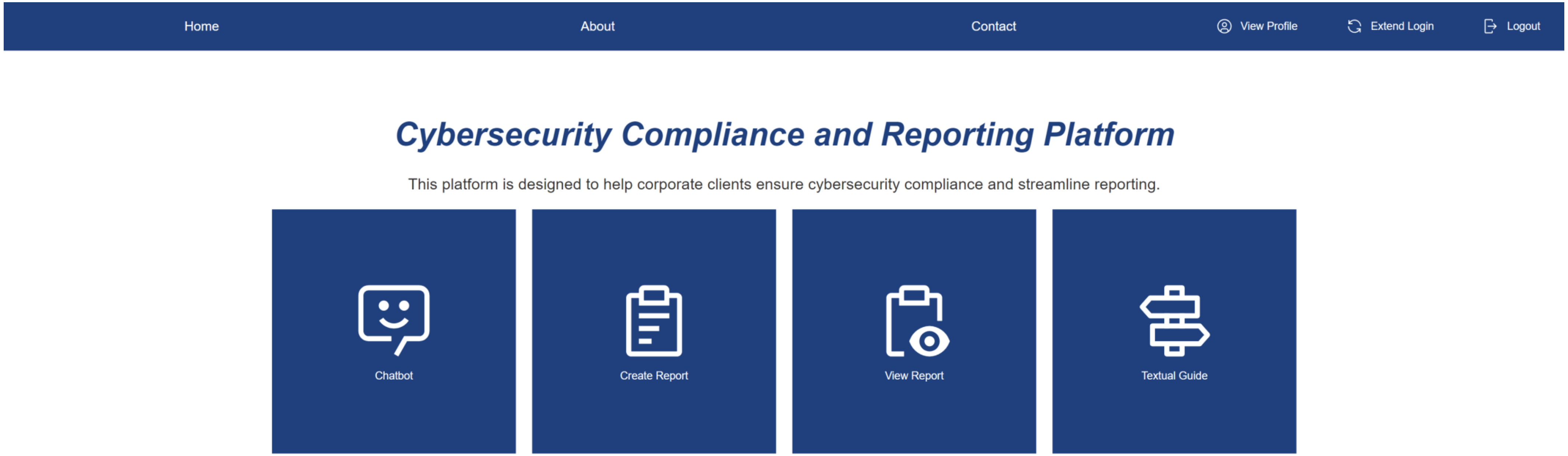
Frontend of the Platform for Incident Reporting Form

❖ Main Workflow of Client



Frontend of the Platform for Incident Reporting Form

- **Home**

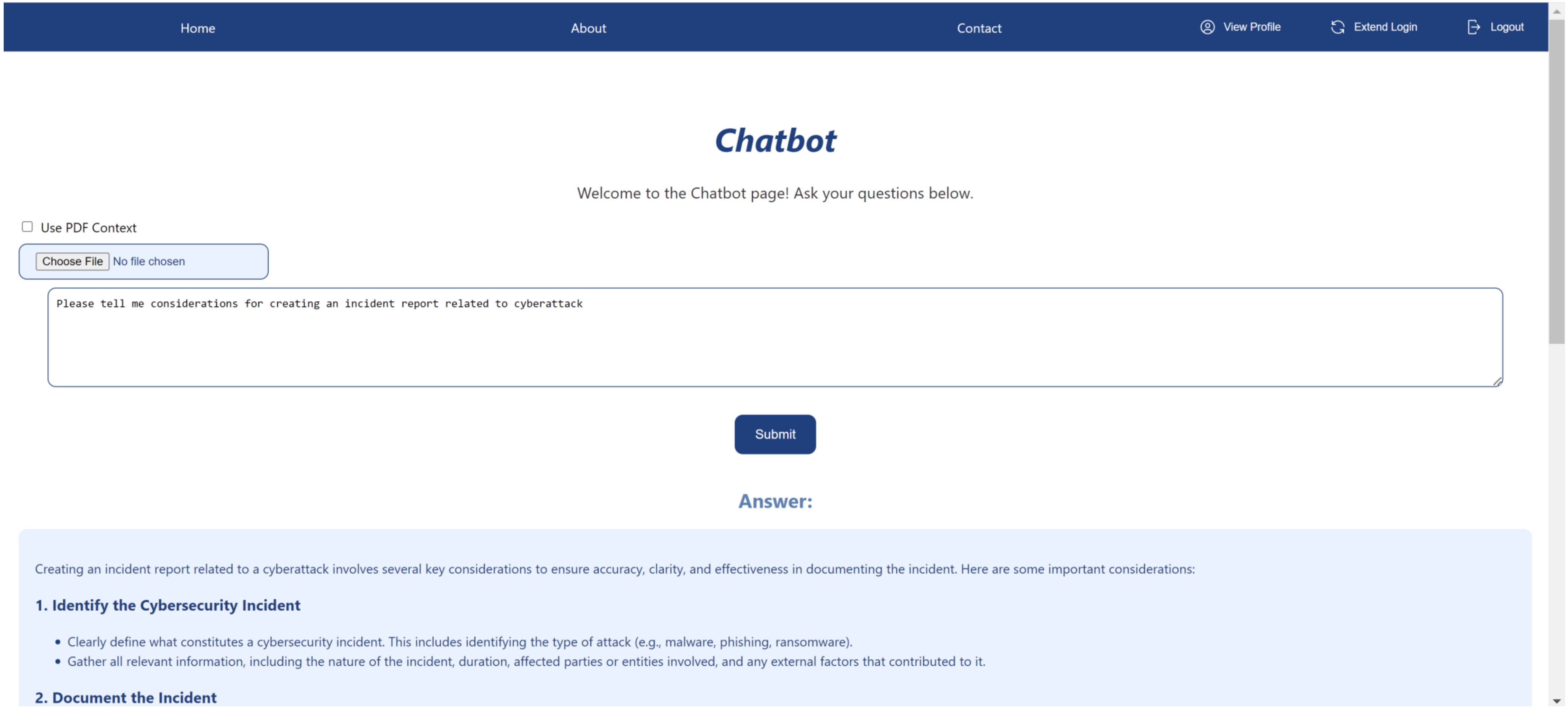


Cybersecurity Compliance and Reporting Platform

This platform is designed to help corporate clients ensure cybersecurity compliance and streamline reporting.

Frontend of the Platform for Incident Reporting Form

❖ Chatbot Page with Local LLM Integration



Chatbot

Welcome to the Chatbot page! Ask your questions below.

□ Use PDF Context

```
Please tell me considerations for creating an incident report related to cyberattack
```

Answer:

Creating an incident report related to a cyberattack involves several key considerations to ensure accuracy, clarity, and effectiveness in documenting the incident. Here are some important considerations:

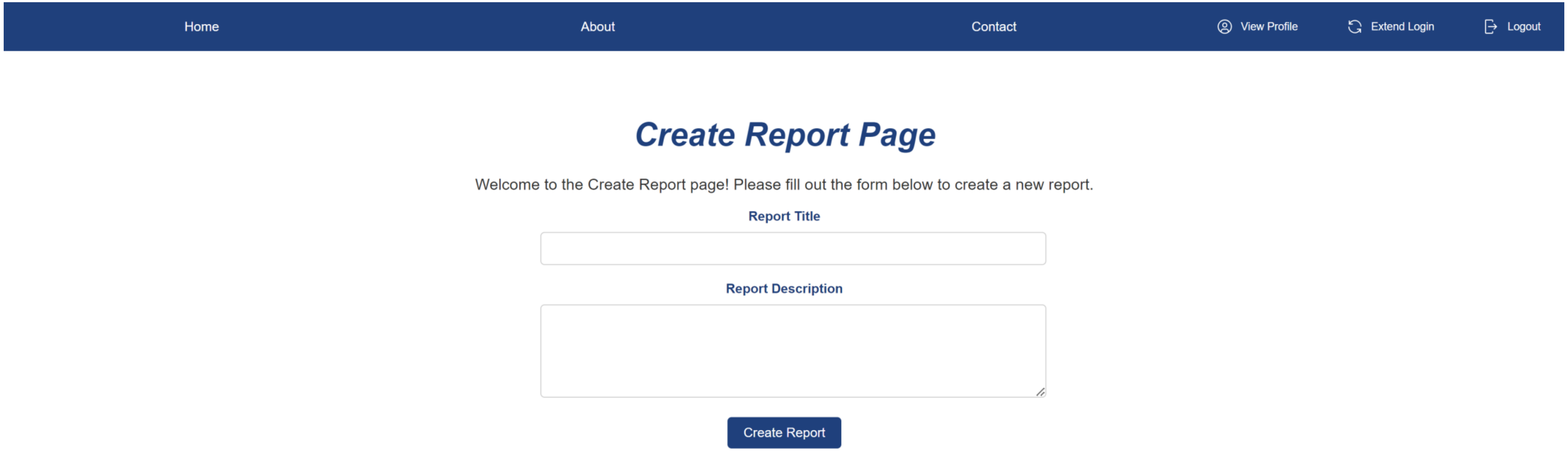
1. Identify the Cybersecurity Incident

- Clearly define what constitutes a cybersecurity incident. This includes identifying the type of attack (e.g., malware, phishing, ransomware).
- Gather all relevant information, including the nature of the incident, duration, affected parties or entities involved, and any external factors that contributed to it.

2. Document the Incident

Frontend of the Platform for Incident Reporting Form

❖ Create Report Page



Create Report Page

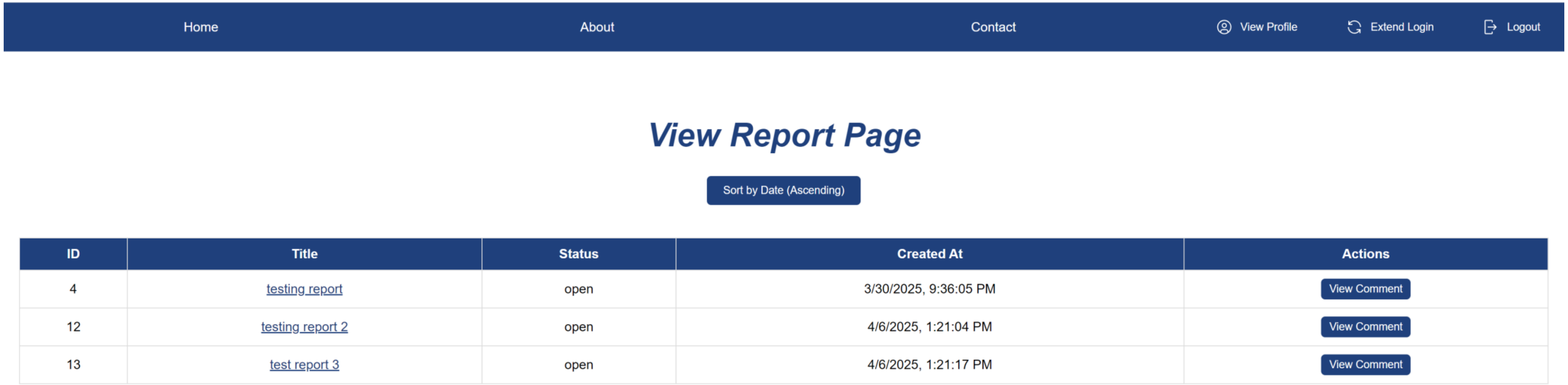
Welcome to the Create Report page! Please fill out the form below to create a new report.

Report Title

Report Description

Frontend of the Platform for Incident Reporting Form

❖ View Report Page

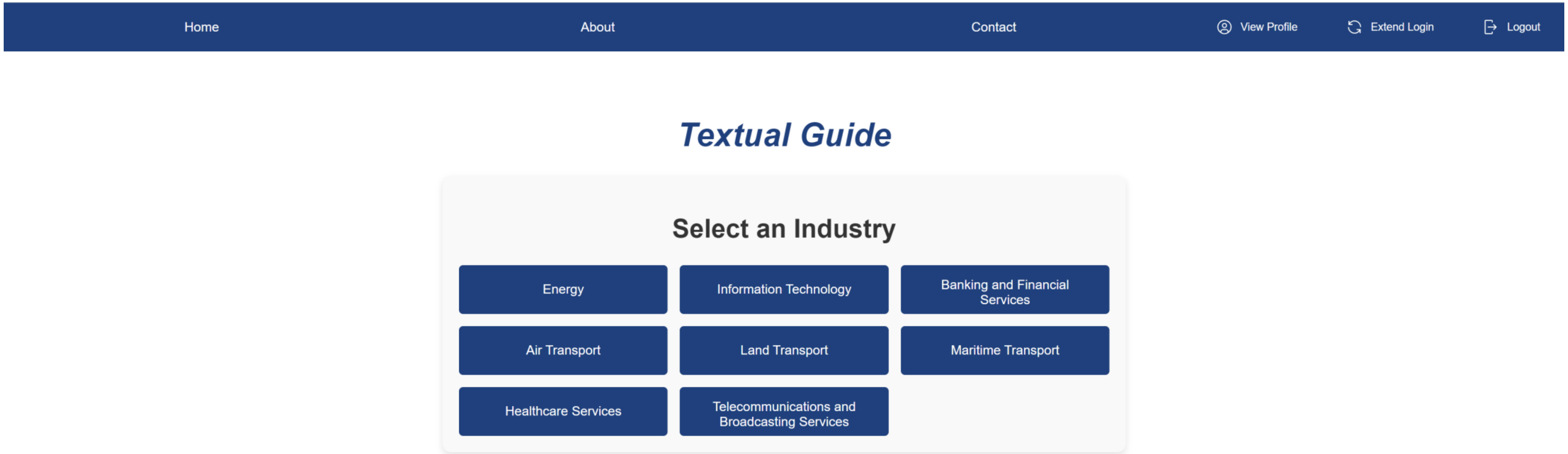


View Report Page

ID	Title	Status	Created At	Actions
4	testing report	open	3/30/2025, 9:36:05 PM	View Comment
12	testing report 2	open	4/6/2025, 1:21:04 PM	View Comment
13	test report 3	open	4/6/2025, 1:21:17 PM	View Comment

Frontend of the Platform for Incident Reporting Form

❖ Textual Guide Page

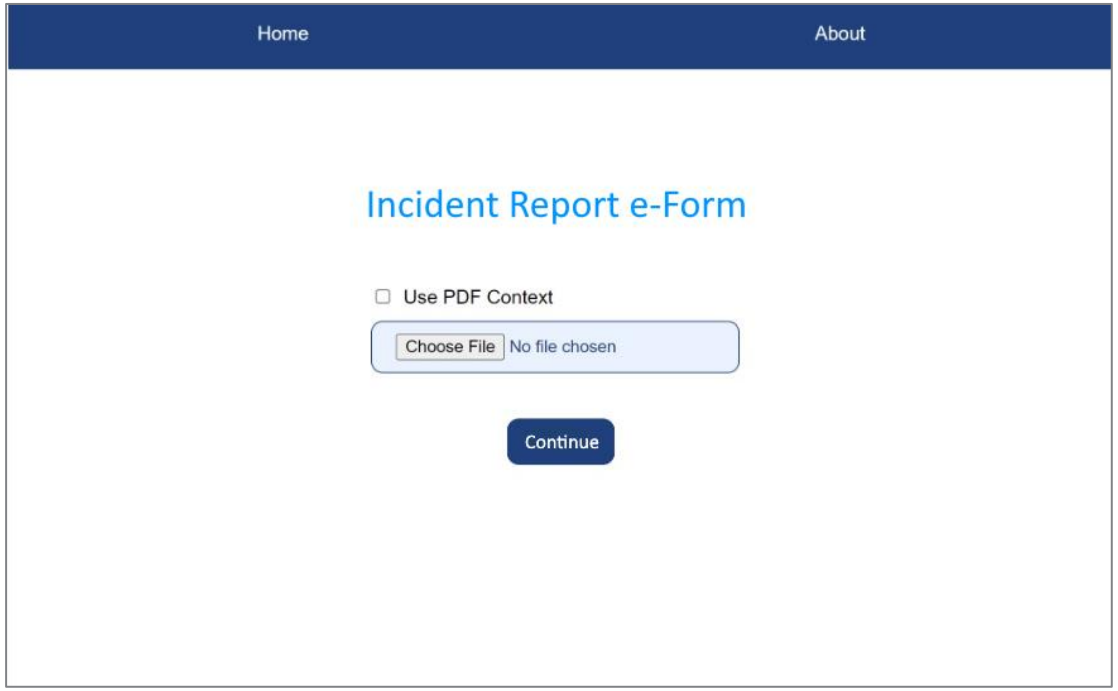


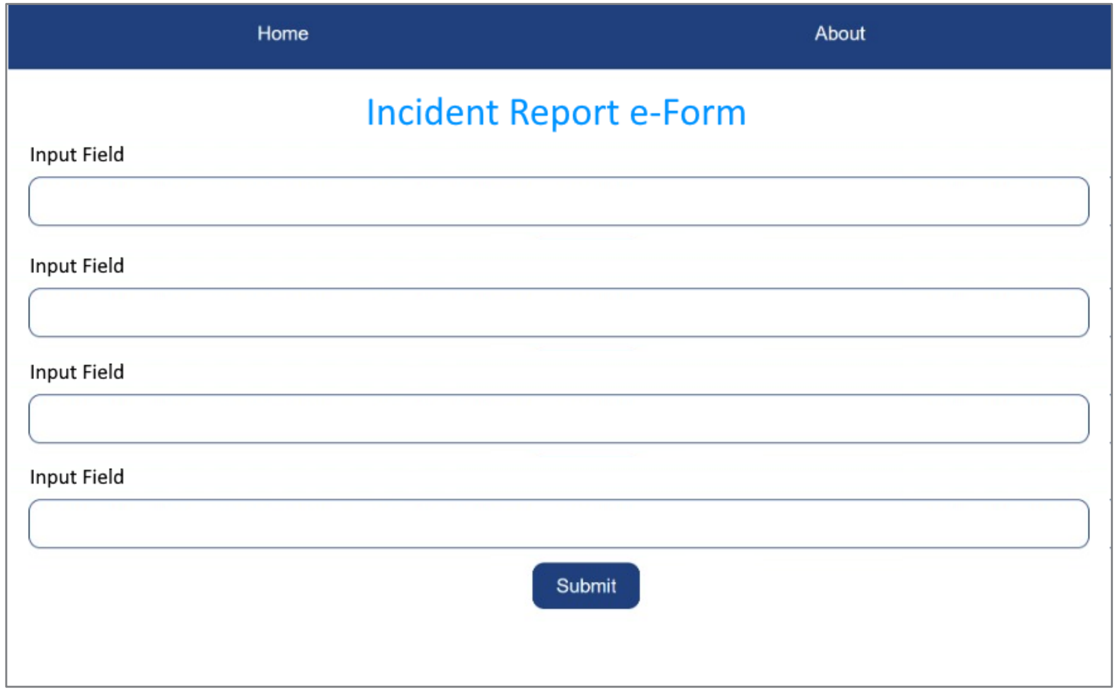
Textual Guide

Select an Industry

Frontend of the Platform for Incident Reporting Form

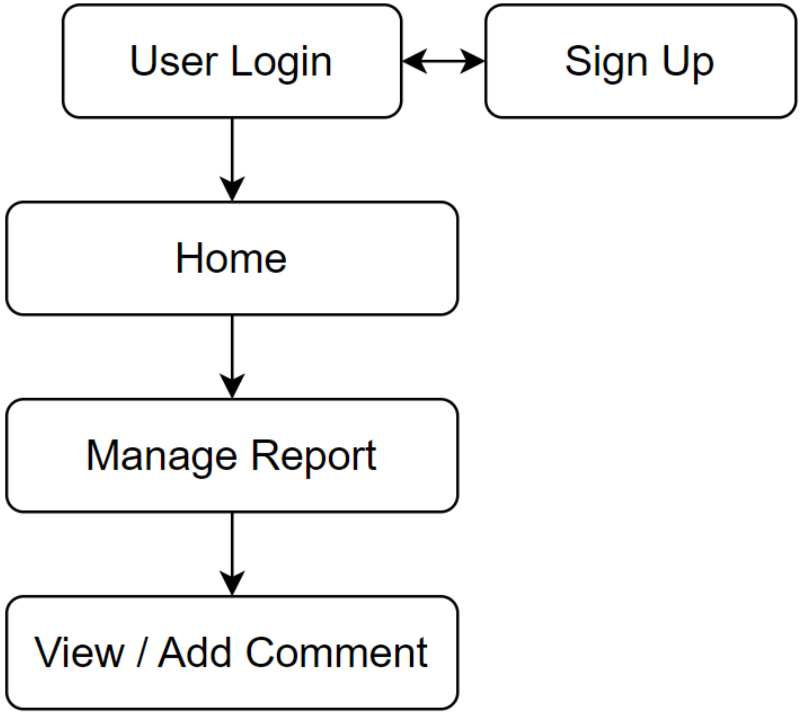
Tentative design (In progress)





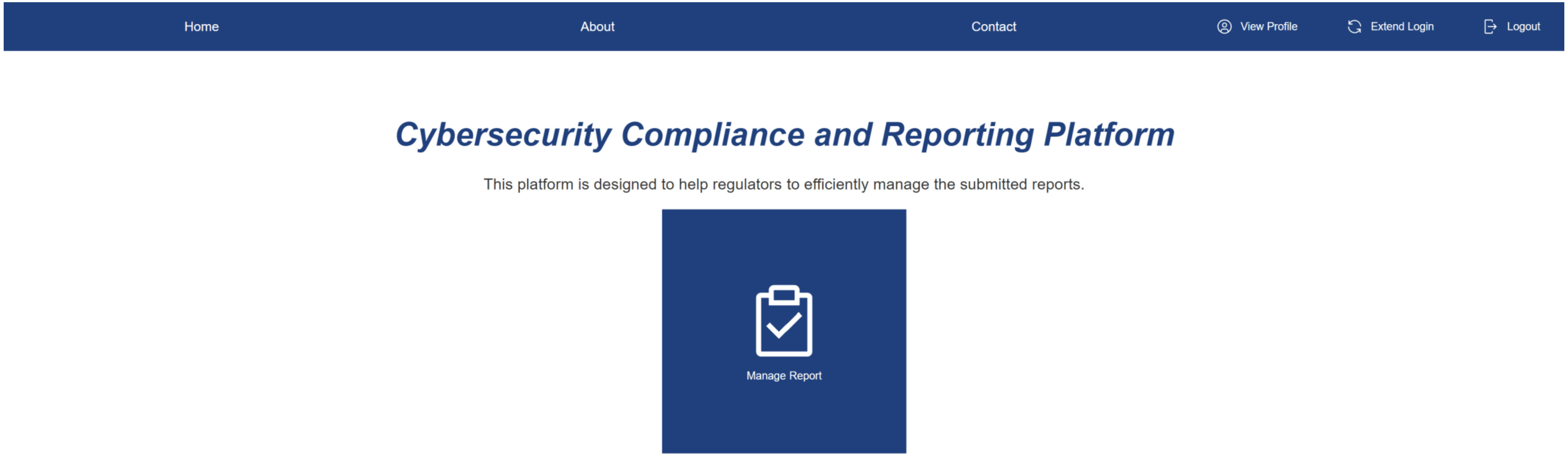
Frontend of the Platform for Incident Reporting Form

❖ Main Workflow of Regulator



Frontend of the Platform for Incident Reporting Form

❖ Home

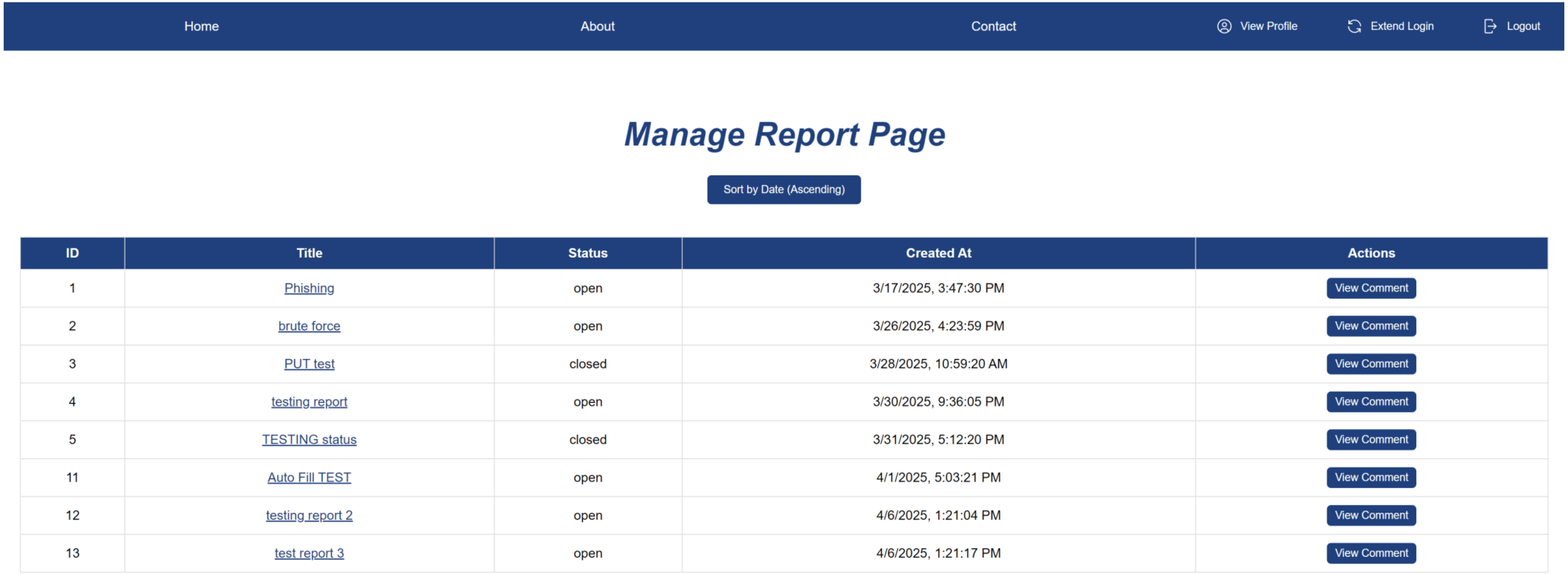


Cybersecurity Compliance and Reporting Platform

This platform is designed to help regulators to efficiently manage the submitted reports.

Frontend of the Platform for Incident Reporting Form

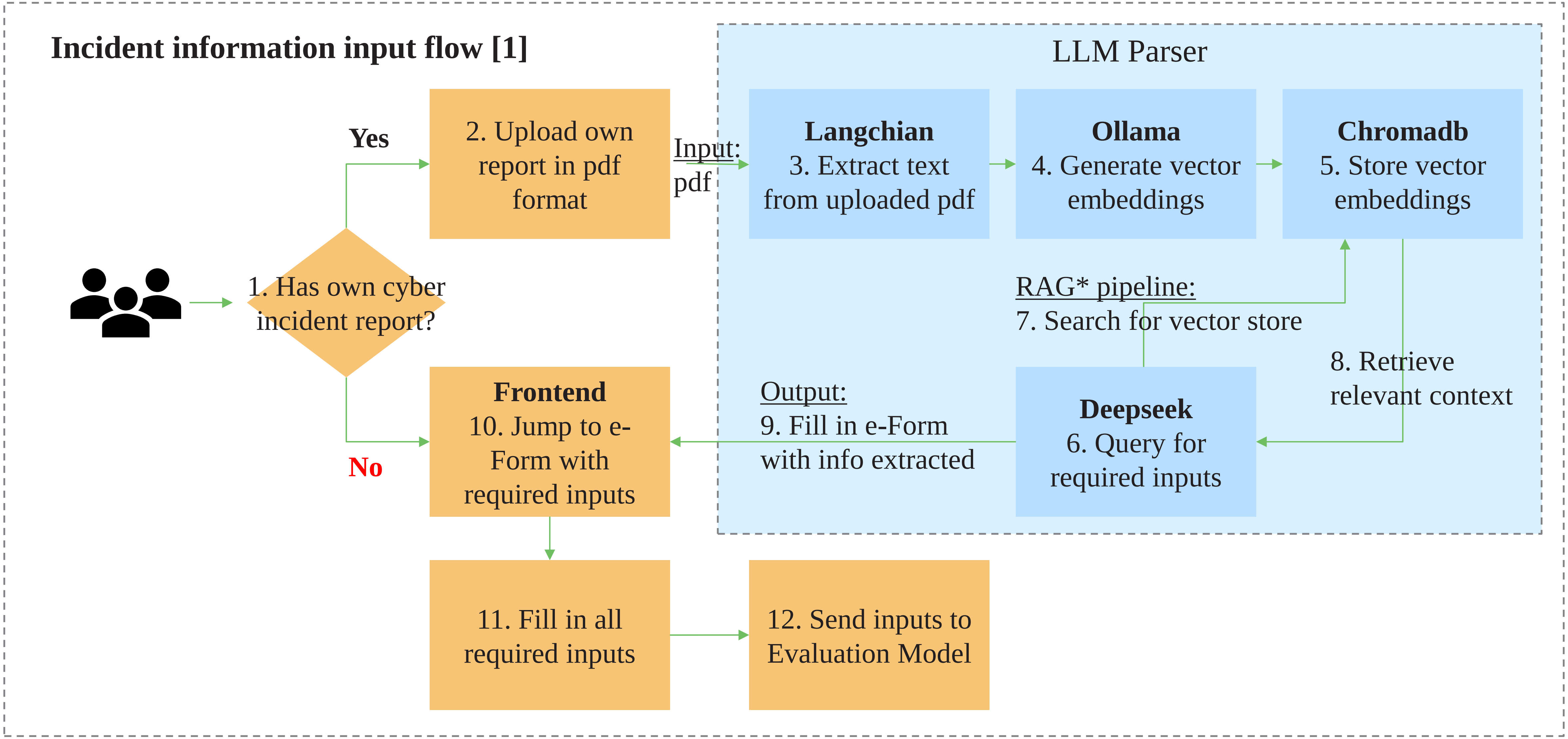
❖ **View Report Page**



Manage Report Page

ID	Title	Status	Created At	Actions
1	Phishing	open	3/17/2025, 3:47:30 PM	View Comment
2	brute force	open	3/26/2025, 4:23:59 PM	View Comment
3	PUT test	closed	3/28/2025, 10:59:20 AM	View Comment
4	testing report	open	3/30/2025, 9:36:05 PM	View Comment
5	TESTING status	closed	3/31/2025, 5:12:20 PM	View Comment
11	Auto Fill TEST	open	4/1/2025, 5:03:21 PM	View Comment
12	testing report 2	open	4/6/2025, 1:21:04 PM	View Comment
13	test report 3	open	4/6/2025, 1:21:17 PM	View Comment

Dual Information Input Flow: (A) PDF Upload or (B) Form Filling



Incident information input flow [1]
LLM Parser
1. Has own cyber incident report?
Yes
No
2. Upload own report in pdf format
Input: pdf
Langchian
3. Extract text from uploaded pdf
Ollama
4. Generate vector embeddings
Chromadb
5. Store vector embeddings
RAG* pipeline:
7. Search for vector store
8. Retrieve relevant context
Deepseek
6. Query for required inputs
Output:
9. Fill in e-Form with info extracted
Frontend
10. Jump to e-Form with required inputs
11. Fill in all required inputs
12. Send inputs to Evaluation Model

[1] https://www.datacamp.com/tutorial/deepseek-r1-ollama

*RAG (Retrieval-Augmented Generation): Process to optimize LLM output by incorporating context from external source.

(A) PDF Upload – LLM model to extract information from PDF report

Technologies implemented

Technology	Platform/Tool	Description and Justification
Pretrained LLM Model	Deepseek R1 [1]	DeepSeek-R1 is an open-source language model created by High-Flyer. It can perform **advanced logical reasoning and decision-making tasks with less cost**.
LLM Platform	Ollama [2]	A platform that lets you run large language models (LLMs) **locally on your machine**.
LLM Framework	Langchain [3]	A framework for building applications with large language models, enabling **easy retrieval and tool integration**.
Context Database	Chromadb [4]	A fast vector database for **efficient similarity searches** and embedding storage of context extracted from report.

[1] https://www.deepseek.com/, [2] https://ollama.com/, [3] https://www.langchain.com/, [4] https://www.trychroma.com/

(A) PDF Upload – LLM model to extract information from PDF report

Further work

Performance Evaluation

- **Gather sample incident reports** of different types.
- **Evaluate parsing performance** in terms of Accuracy, Precision, Recall and F1 score

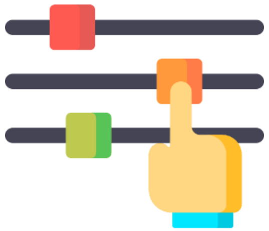
Finetuning and Improvement

1. Test and evaluate **different LLM models** [1]

Llama 3 Gemma 3 Qwen

2. Employ **prompt engineering** to guide the model's response

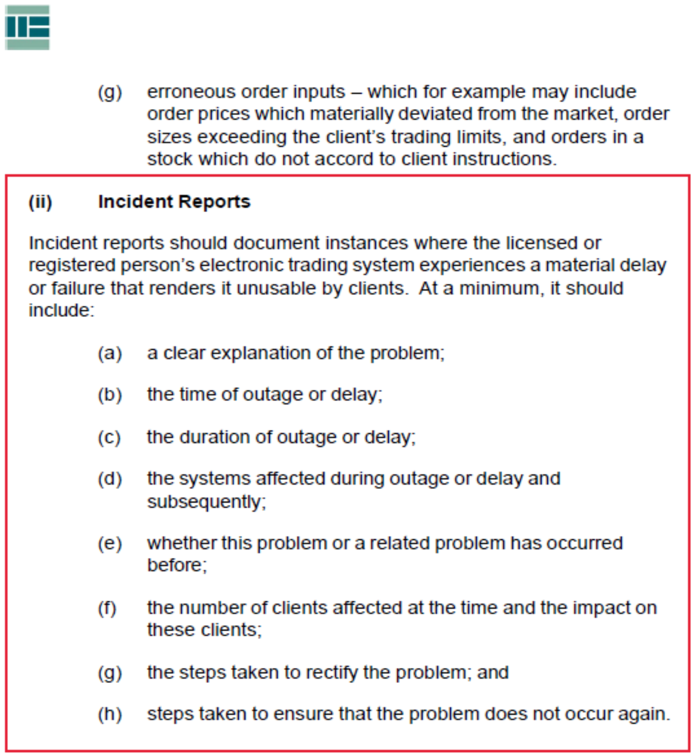
3. Finetune parameters to achieve better parsing performance



[1] https://ollama.com/library

(B) Form Filling – Form Design

Incident report content requirements



(g) erroneous order inputs – which for example may include order prices which materially deviated from the market, order sizes exceeding the client's trading limits, and orders in a stock which do not accord to client instructions.

(ii) **Incident Reports**

Incident reports should document instances where the licensed or registered person's electronic trading system experiences a material delay or failure that renders it unusable by clients. At a minimum, it should include:

(a) a clear explanation of the problem;

(b) the time of outage or delay;

(c) the duration of outage or delay;

(d) the systems affected during outage or delay and subsequently;

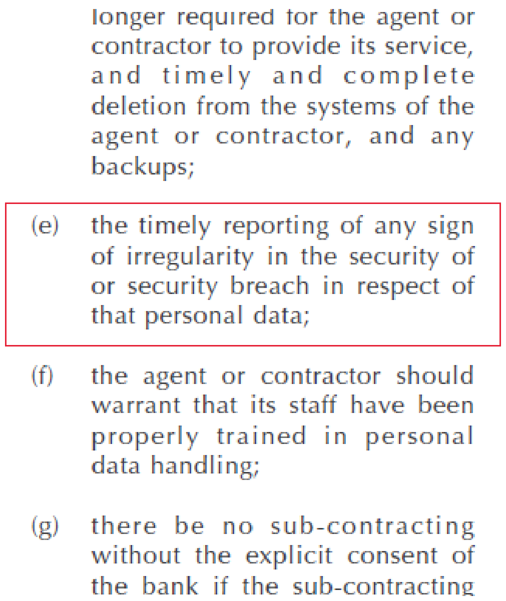
(e) whether this problem or a related problem has occurred before;

(f) the number of clients affected at the time and the impact on these clients;

(g) the steps taken to rectify the problem; and

(h) steps taken to ensure that the problem does not occur again.

SFC – Code of Conduct for Persons Licensed by or Registered with the SFC



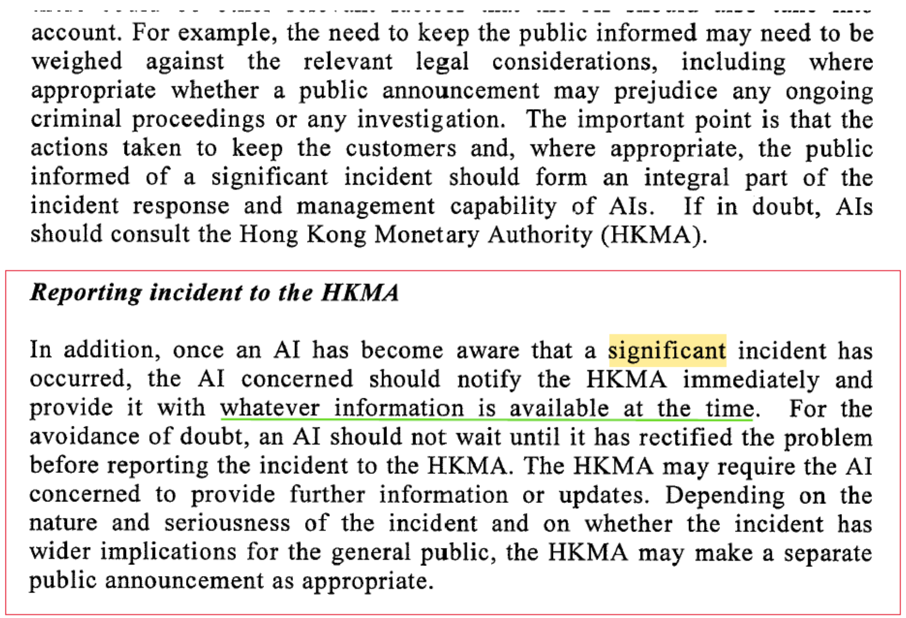
longer required for the agent or contractor to provide its service, and timely and complete deletion from the systems of the agent or contractor, and any backups;

(e) the timely reporting of any sign of irregularity in the security of or security breach in respect of that personal data;

(f) the agent or contractor should warrant that its staff have been properly trained in personal data handling;

(g) there be no sub-contracting without the explicit consent of the bank if the sub-contracting

PCPD – Guidance on Proper Handling of Customers' Personal Data (Oct 2014)



account. For example, the need to keep the public informed may need to be weighed against the relevant legal considerations, including where appropriate whether a public announcement may prejudice any ongoing criminal proceedings or any investigation. The important point is that the actions taken to keep the customers and, where appropriate, the public informed of a significant incident should form an integral part of the incident response and management capability of AIs. If in doubt, AIs should consult the Hong Kong Monetary Authority (HKMA).

Reporting incident to the HKMA

In addition, once an AI has become aware that a significant incident has occurred, the AI concerned should notify the HKMA immediately and provide it with whatever information is available at the time. For the avoidance of doubt, an AI should not wait until it has rectified the problem before reporting the incident to the HKMA. The HKMA may require the AI concerned to provide further information or updates. Depending on the nature and seriousness of the incident and on whether the incident has wider implications for the general public, the HKMA may make a separate public announcement as appropriate.

HKMA – Circular for incident response and management procedures (June 2010)

(B) Form Filling – Form Design

User profile design

#	Category	Key Attribute	Format
1	User basic information	User ID / Username	Free text
2	User basic information	Country / Jurisdiction (to tailor regulatory guidance)	Dropdown list
3	User basic information	Contact Email / Phone (for follow-ups)	Free text
4	Role and Access Level	User Role / function in the company (e.g., CISO, IT Manager, Compliance Officer)	Dropdown list
5	Role and Access Level	Decision-Making Authority for regulatory reporting (Yes/No – useful for assessing impact context)	N/A
6	Organization basic information	Organization Name	Free text
7	Organization basic information	Industry Sector (e.g., Finance, Healthcare, Education, Retail)	Dropdown list
8	Organization basic information	Business size SME / Large Enterprise	Dropdown list
9	Organization basic information	Number of employees	Dropdown list
10	Organization basic	Type of Customers (e.g.,	Form
11			
12			
13			
14			
	Bill		

Incident report content design

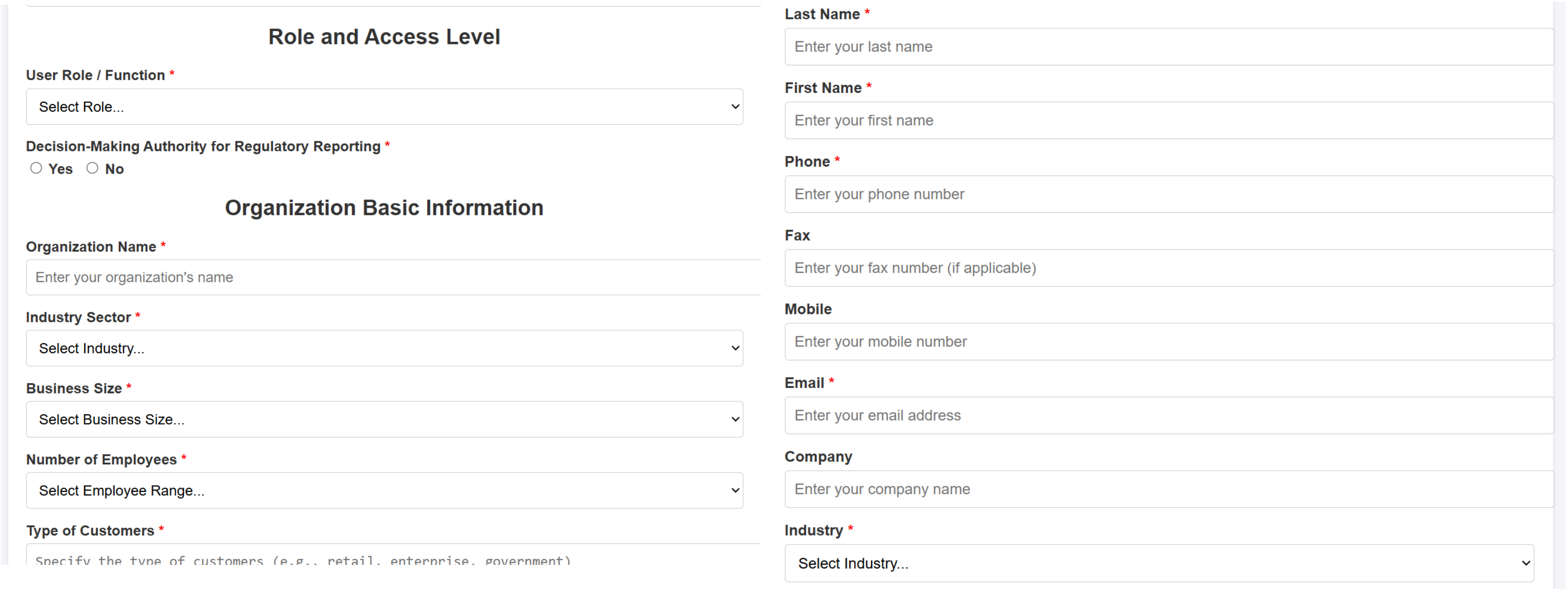
#	Category	Key Attribute	Format
1	Basic information	User ID / Username of the reporter	from user profile
2	Basic information	Date Reported	Date
3	Basic information	Time Reported	Time
4	Incident	Case number	Assigned
5	Incident	Incident Status: Ongoing / Contained / Resolved / Closed	Dropdown list
6	Incident	Incident Discovery Date	Date
7	Incident	Incident Discovery Time	Time
8	Incident	Date of Occurrence	Date
9	Incident	Time of Occurrence	Time
10	Incident	Incident Type (multi-select or dropdown):	Form
11	Incident	Confirmed fraudulent website / fraudulent applications / scams / fraud cases	Yes/No
12	Incident	Impacted systems	Free text
13	Incident	Summary of the incident	Free text
14	Detection source	Internal Monitoring / External Notification / Customer Complaint / Regulatory Notification / Others)	Dropdown list
15	Investigation	Description of the investigation and observation	Free text
16	Investigation	Re-occurrence	Yes/No
19	Root cause	Incident Origin	Form
17	Root cause	Any Zero-day vulnerability related	Yes/No
18	Root cause	Any external attack	Form
20	Impact	Affecting Critical infrastructure	Yes/No
21	Impact	Any news reported by mainstream media	Yes/No
22	Impact	Service disruption / unscheduled downtime affecting key / core business function for certain period	Yes/No
23	Impact	Operational Impact with suggested considerations	Dropdown list
36	Attachments	if any	Free text

Next Steps:
Deploy the designs on both the frontend and backend. Use real incident cases to evaluate the model's performance and refine both the model and system design accordingly.

Challenges and Solutions:
It is difficult to access incident cases with comprehensive impact details. We may need to create representative cases based on our actual work experience to facilitate evaluation and improvement.

(B) Form Filling – Form Design

Form design (in progress)



Role and Access Level

User Role / Function *

Select Role...

Decision-Making Authority for Regulatory Reporting *

○ Yes ○ No

Organization Basic Information

Organization Name *

Enter your organization's name

Industry Sector *

Select Industry...

Business Size *

Select Business Size...

Number of Employees *

Select Employee Range...

Type of Customers *

Specify the type of customers (e.g., retail, enterprise, government)

Last Name *

Enter your last name

First Name *

Enter your first name

Phone *

Enter your phone number

Fax

Enter your fax number (if applicable)

Mobile

Enter your mobile number

Email *

Enter your email address

Company

Enter your company name

Industry *

Select Industry...

Pre-Reporting Evaluation Framework

❖ Factors for Severity Assessment

If an incident is assessed as (1) meeting the reporting obligation criteria or (2) its severity score exceeds the defined threshold, the system will recommend reporting the incident to the relevant government authorities or industry regulators.

(1) Reporting obligations

When the user inputs whether the incident falls under any of the 5 defined scenarios, the system will recommend reporting to the relevant government departments, statutory bodies, or industry authorities based on the entity's sector or industry.

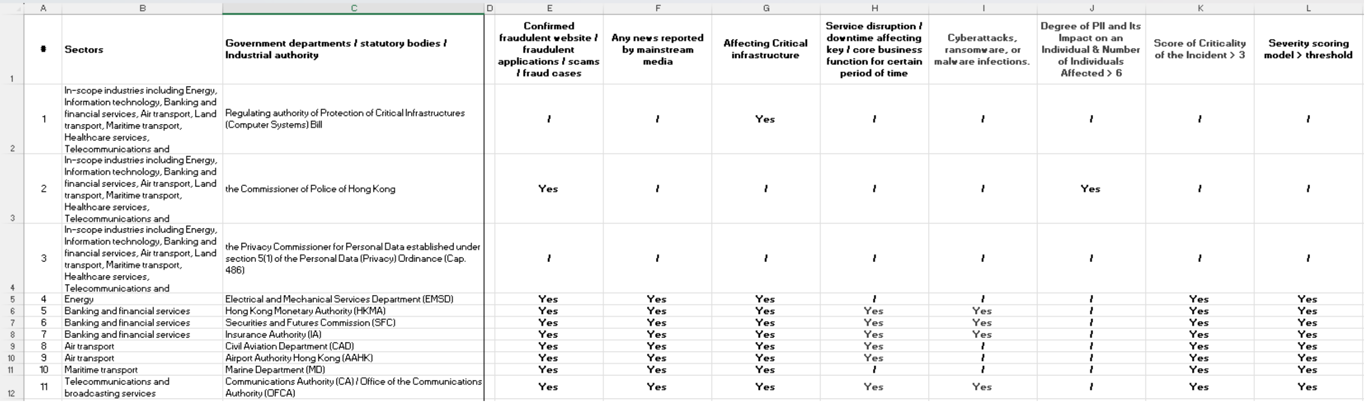
Confirmed fraudulent websites / fraudulent applications / scams / fraud cases

Any news reported by mainstream media

Service disruption / downtime affecting key / core business function for certain period of time

Affecting Critical infrastructure

Cyberattacks, ransomware, or malware infections



#	Sectors	Government departments / statutory bodies / Industrial authority	Confirmed fraudulent website / fraudulent applications / scams / fraud cases	Any news reported by mainstream media	Affecting Critical infrastructure	Service disruption / downtime affecting key / core business function for certain period of time	Cyberattacks, ransomware, or malware infections.	Degree of PII and Its Impact on an Individual & Number of Individuals Affected > 6	Score of Criticality of the Incident > 3	Severity scoring model > threshold
1	In-scope industries including Energy, Information technology, Banking and financial services, Air transport, Land transport, Maritime transport, Healthcare services, Telecommunications and	Regulating authority of Protection of Critical Infrastructures (Computer Systems) Bill	/	/	Yes	/	/	/	/	/
2	In-scope industries including Energy, Information technology, Banking and financial services, Air transport, Land transport, Maritime transport, Healthcare services, Telecommunications and	the Commissioner of Police of Hong Kong	Yes	/	/	/	/	Yes	/	/
3	In-scope industries including Energy, Information technology, Banking and financial services, Air transport, Land transport, Maritime transport, Healthcare services, Telecommunications and	the Privacy Commissioner for Personal Data established under section 5(1) of the Personal Data (Privacy) Ordinance (Cap. 486)	/	/	/	/	/	/	/	/
4	Energy	Electrical and Mechanical Services Department (EMSD)	Yes	Yes	Yes	/	/	/	Yes	Yes
5	Banking and financial services	Hong Kong Monetary Authority (HKMA)	Yes	Yes	Yes	Yes	Yes	/	Yes	Yes
6	Banking and financial services	Securities and Futures Commission (SFC)	Yes	Yes	Yes	Yes	Yes	/	Yes	Yes
7	Banking and financial services	Insurance Authority (IA)	Yes	Yes	Yes	Yes	Yes	/	Yes	Yes
8	Air transport	Civil Aviation Department (CAD)	Yes	Yes	Yes	Yes	/	/	Yes	Yes
9	Air transport	Airport Authority Hong Kong (AAHK)	Yes	Yes	Yes	Yes	/	/	Yes	Yes
10	Maritime transport	Marine Department (MD)	Yes	Yes	Yes	/	/	/	Yes	Yes
11	Telecommunications and broadcasting services	Communications Authority (CA) / Office of the Communications Authority (OFCA)	Yes	Yes	Yes	Yes	Yes	/	Yes	Yes

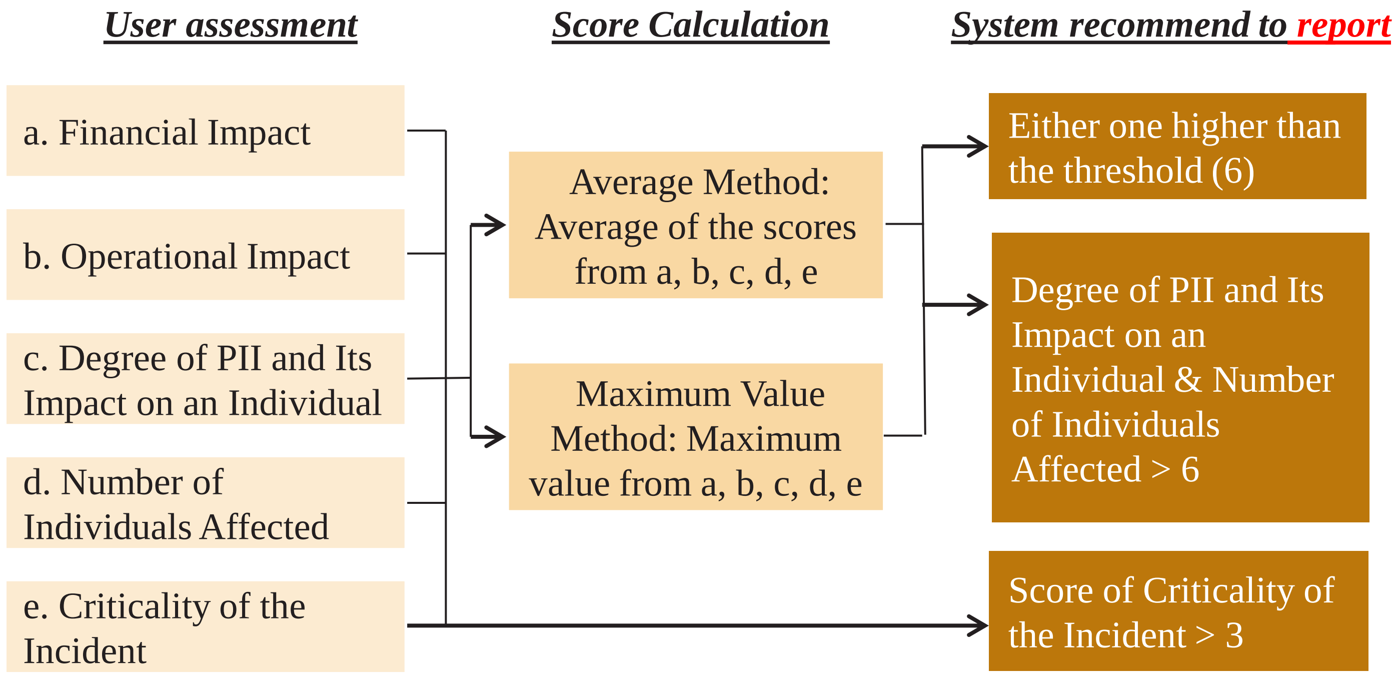
Pre-Reporting Evaluation Framework

❖ Factors for Severity Assessment

If an incident is assessed as (1) meeting the reporting obligation criteria or (2) its severity score exceeds the defined threshold, the system will recommend reporting the incident to the relevant government authorities or industry regulators.

(2) Severity Score > Threshold

The user needs to assess the impact of the incident across five key aspects. Based on this assessment, a severity score will be calculated. The system will recommend reporting to the relevant government departments, statutory bodies, or industry authorities based on the entity’s sector or industry.



User assessment

a. Financial Impact

b. Operational Impact

c. Degree of PII and Its Impact on an Individual

d. Number of Individuals Affected

e. Criticality of the Incident

Score Calculation

Average Method: Average of the scores from a, b, c, d, e

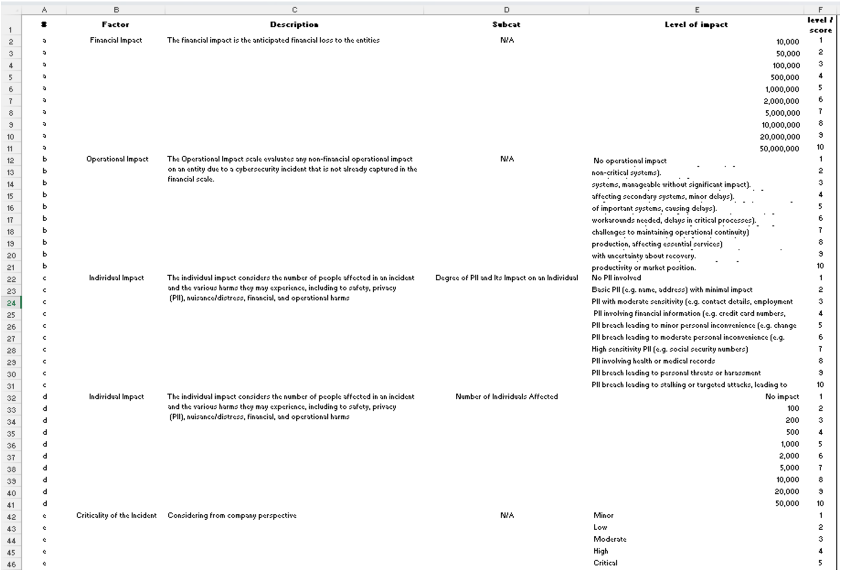
Maximum Value Method: Maximum value from a, b, c, d, e

System recommend to report

Either one higher than the threshold (6)

Degree of PII and Its Impact on an Individual & Number of Individuals Affected > 6

Score of Criticality of the Incident > 3



	A	B	C	D	E	F
1	#	Factor	Description	Subcat	Level of impact	level / score
2	a	Financial Impact	The financial impact is the anticipated financial loss to the entities	N/A	10,000	1
3	a				50,000	2
4	a				100,000	3
5	a				500,000	4
6	a				1,000,000	5
7	a				2,000,000	6
8	a				5,000,000	7
9	a				10,000,000	8
10	a				20,000,000	9
11	a				50,000,000	10
12	b	Operational Impact	The Operational Impact scale evaluates any non-financial operational impact on an entity due to a cybersecurity incident that is not already captured in the financial scale.	N/A	No operational impact	1
13	b				non-critical systems).	2
14	b				systems, manageable without significant impact).	3
15	b				affecting secondary systems, minor delays).	4
16	b				of important systems, causing delays).	5
17	b				workarounds needed, delays in critical processes).	6
18	b				challenges to maintaining operational continuity)	7
19	b				production, affecting essential services)	8
20	b				with uncertainty about recovery.	9
21	b				productivity or market position.	10
22	c	Individual Impact	The individual impact considers the number of people affected in an incident and the various harms they may experience, including to safety, privacy (PII), nuisance/distress, financial, and operational harms	Degree of PII and Its Impact on an Individual	No PII involved	1
23	c				Basic PII (e.g. name, address) with minimal impact	2
24	c				PII with moderate sensitivity (e.g. contact details, employment	3
25	c				PII involving financial information (e.g. credit card numbers,	4
26	c				PII breach leading to minor personal inconvenience (e.g. change	5
27	c				PII breach leading to moderate personal inconvenience (e.g.	6
28	c				High sensitivity PII (e.g. social security numbers)	7
29	c				PII involving health or medical records	8
30	c				PII breach leading to personal threats or harassment	9
31	c				PII breach leading to stalking or targeted attacks, leading to	10
32	d	Individual Impact	The individual impact considers the number of people affected in an incident and the various harms they may experience, including to safety, privacy (PII), nuisance/distress, financial, and operational harms	Number of Individuals Affected	No impact	1
33	d				100	2
34	d				200	3
35	d				500	4
36	d				1,000	5
37	d				2,000	6
38	d				5,000	7
39	d				10,000	8
40	d				20,000	9
41	d				50,000	10
42	e	Criticality of the Incident	Considering from company perspective	N/A	Minor	1
43	e				Low	2
44	e				Moderate	3
45	e				High	4
46	e				Critical	5

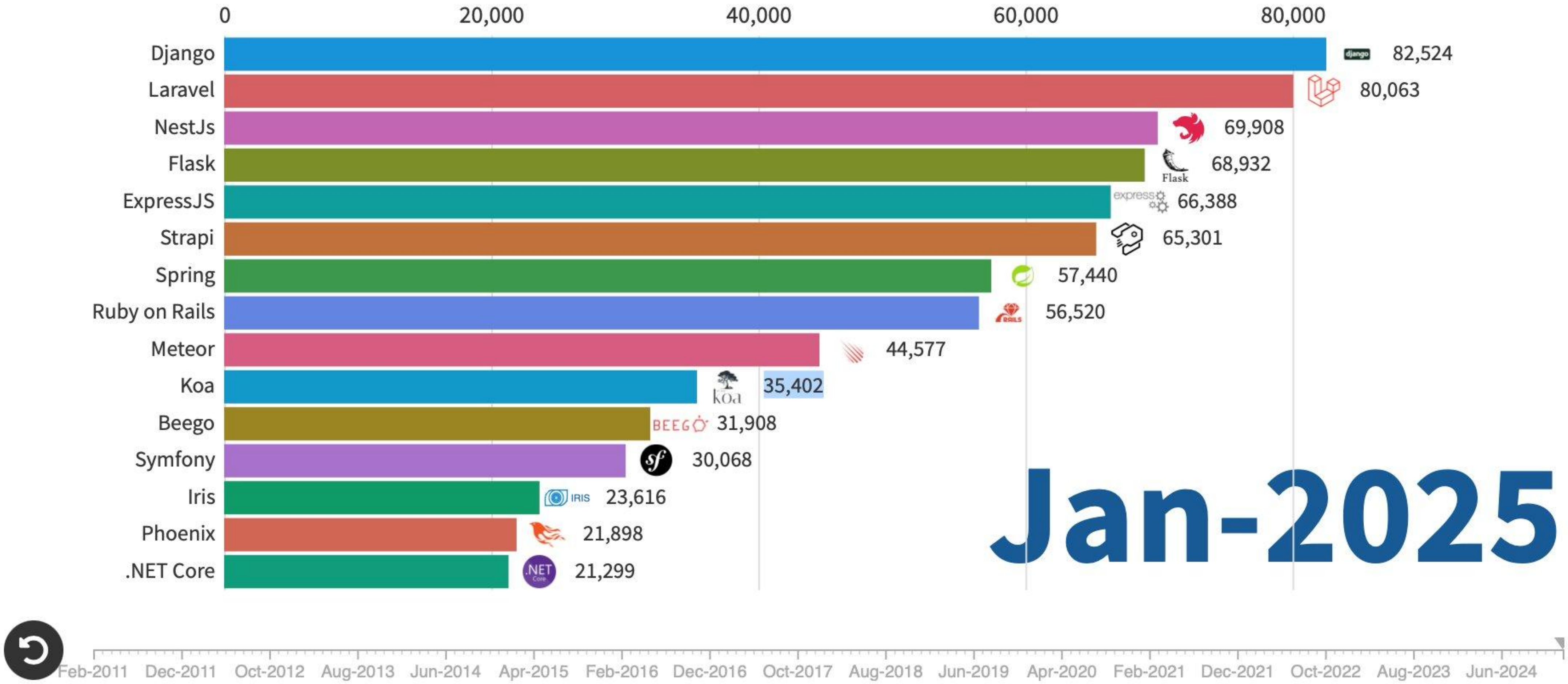
Conard, C. F. (2024). *Quantifying the severity of a cybersecurity incident for incident reporting* [Master's thesis, Massachusetts Institute of Technology]. DSpace@MIT. https://dspace.mit.edu/handle/1721.1/157124

Backend of the Platform for Incident Reporting Form

- **Backend Requirement:**
  - **Dynamic Website**
  - **Beginner Friendly**
  - **Strong Community and Ecosystem**

- **Our Choice: Django**
  - **Build-in features**
  - **ORM (Object-Relational Mapping) for database**
  - **Built on Python**

Most Popular Backend Frameworks



https://statisticsanddata.org/data/most-popular-backend-frameworks-2012-2025/

Updated Progress Summary

	Month				
	3	4	5	6	7
Detailed Project Proposal (10 March)	■				
1st Milestone (7 April) - Develop a website with role-based access control (sign-up, login, logout, etc.). - Implement functionality for submitting incident response reports.	■	■			
Project Progress Update 1 (7 April)		■			
Project Progress Update 2 (5 May)			▨		
2nd Milestone (1 June) - Further enhancing functionality of website and report generation functions. - Evaluation of pre-reporting evaluation framework. - Exploring practicality of additional features including Chatbot and IPFS.				▨	
Interim Report and Presentation (1 June)				▨	
Project Progress Update 3 (16 June)				▨	
3rd Milestone (7 July) - Transition from Proof of Concept (POC) to Production. - Finalize platform deployment and conduct user acceptance testing (UAT)					▨
Project Progress Update 4 (7 July)					▨
Project Report (18 July)					▨
Oral Examination (End of July)					▨