Cybersecurity Compliance and Reporting Platform

Project Progress Update 2

May 2025

Project Recap

- Aim: Streamline incident reporting and compliance using a single platform.
- Features:
  - Evaluate the severity of incidents.
  - Provide guidance on Hong Kong regulatory requirements.
  - Generate reports that fulfill Hong Kong regulatory requirements.
  - Storage of reports of incidents for regulators’ reference and handling.

(Recap from Progress update #1)

(A) PDF Upload – LLM model to extract information from PDF report → **(A) PDF Upload – LLM model to provide advice on the reporting decision**

(B) Form Filling – for role-based decision model to provide advice on the reporting decision

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 language processing capability with less computational cost.**
LLM Platform	Ollama [2]	A platform that enables **local deployment** of large language models (LLMs) and vector embedding models.
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.

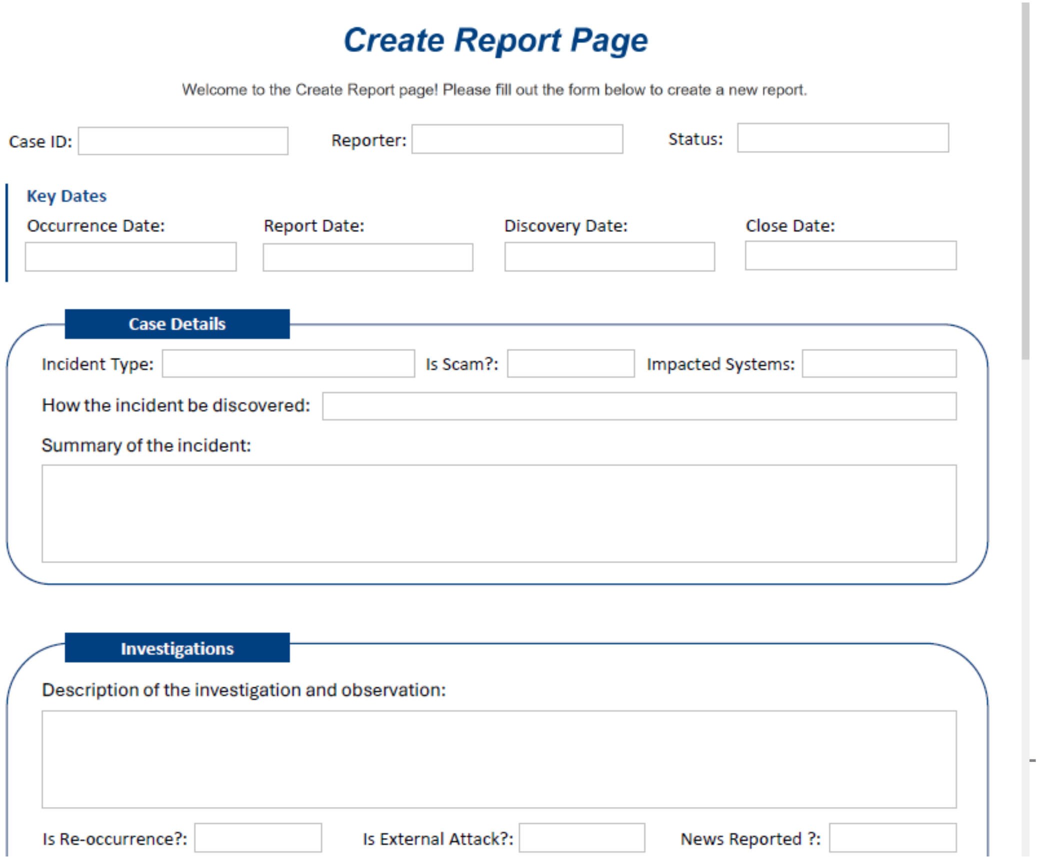
Incident report content design

#	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
24	Impact	Supporting Reason for Operational impact	Free text
25	Impact	Number of Individuals Affected with suggested considerations	Dropdown list
26	Impact	Supporting Reason for Numbers of affected customer	Free text
34	Recovery status	the status after the immediate actions	Free text
35	Other action	Action plan, futher enhancement to avoid reoccurence	Free text
36	Attachments	if any	Free text

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

Progress Overview

- ❖ Further improved functionality of frontend and backend of the Platform
  - ❖ Set up interface for data input for report
  - ❖ Substantiated the page for textual guidance for the regulatory requirements in Hong Kong
- ❖ Revised Pre-Reporting Evaluation Framework with reference to external references



Create Report Page

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

Case ID: Reporter: Status:

Key Dates

Occurrence Date: Report Date: Discovery Date: Close Date:

Case Details

Incident Type: Is Scam?: Impacted Systems:

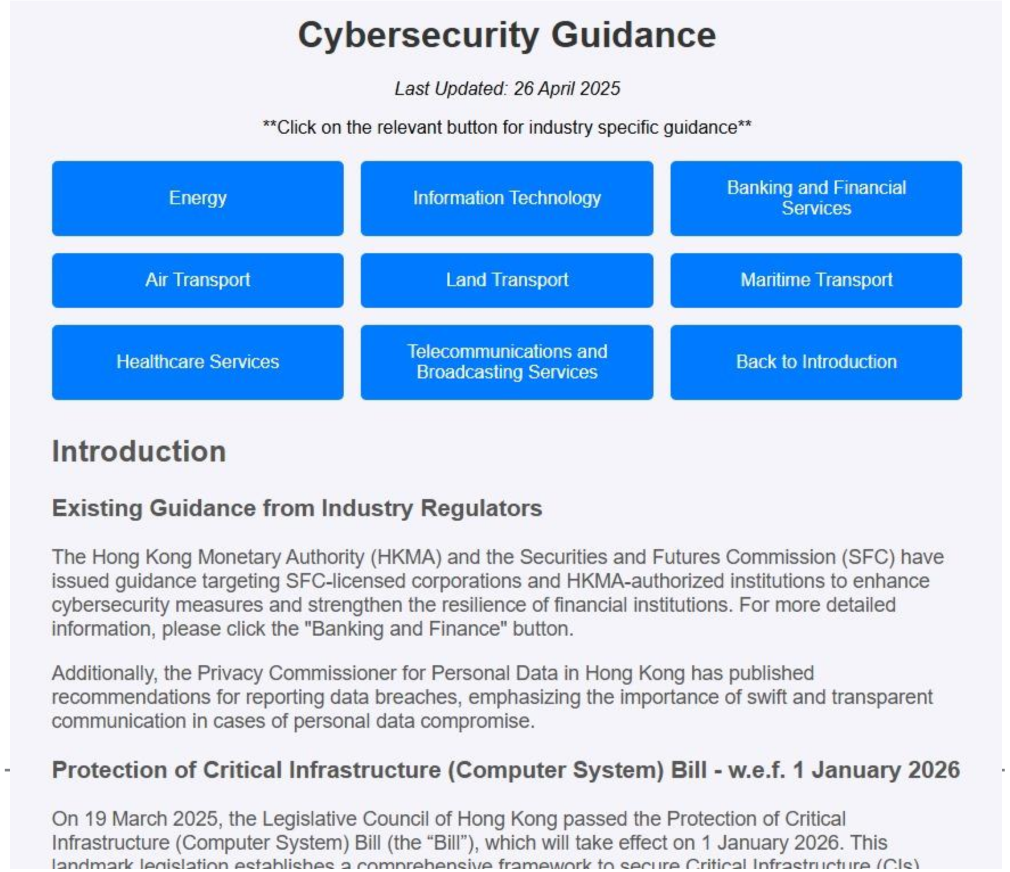
How the incident be discovered:

Summary of the incident:

Investigations

Description of the investigation and observation:

Is Re-occurrence?: Is External Attack?: News Reported ?:



Cybersecurity Guidance

Last Updated: 26 April 2025

Click on the relevant button for industry specific guidance

Introduction

Existing Guidance from Industry Regulators

The Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC) have issued guidance targeting SFC-licensed corporations and HKMA-authorized institutions to enhance cybersecurity measures and strengthen the resilience of financial institutions. For more detailed information, please click the "Banking and Finance" button.

Additionally, the Privacy Commissioner for Personal Data in Hong Kong has published recommendations for reporting data breaches, emphasizing the importance of swift and transparent communication in cases of personal data compromise.

Protection of Critical Infrastructure (Computer System) Bill - w.e.f. 1 January 2026

On 19 March 2025, the Legislative Council of Hong Kong passed the Protection of Critical Infrastructure (Computer System) Bill (the “Bill”), which will take effect on 1 January 2026. This landmark legislation establishes a comprehensive framework to secure Critical Infrastructure (CIs)

Pre-Reporting Evaluation Framework (Recap from Progress update #1)

❖ 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.

Mainly take reference from a research paper, maybe not enough.

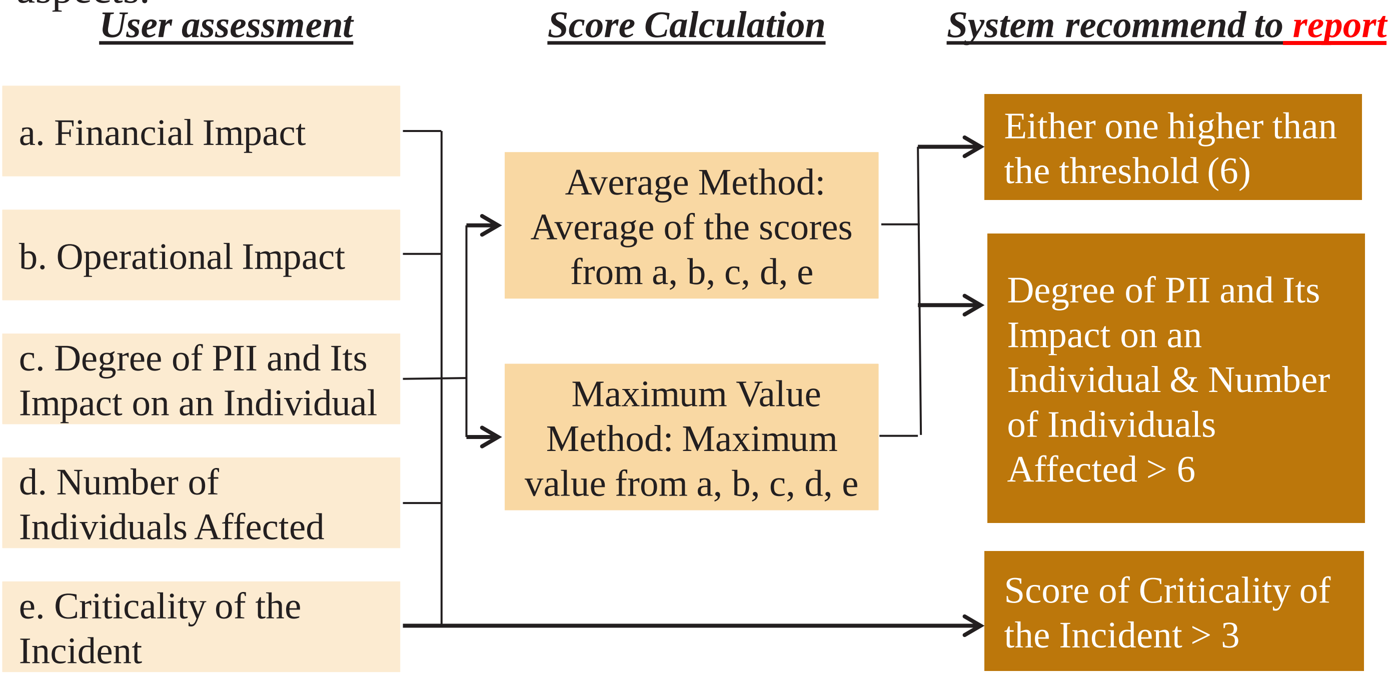
(1) Reporting obligations

When the user inputs whether the incident falls under any of the 5 defined scenarios

- 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

(2) Severity Score > Threshold

The user needs to assess the impact of the incident across five key aspects.



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

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

Revised Pre-Reporting Evaluation Framework

❖ **Factors for Severity Assessment**

Overall severity assessment methodology remains unchanged, slightly updated on “(1) meeting the reporting obligation” criteria, revised “(2) its severity score exceeds the defined threshold”. Some references as below:

A regulator is a government authority or independent body that creates and enforces rules (regulations) for specific industries to ensure fair practices, safety, and legal compliance. Therefore, using the frameworks adopted by the government as a reference for our model will provide strong support and credibility. In particular:

- Practice Guide for Information Security Incident Handling (February 2025)
- Practice Guide for IT Security Risk Management (July 2024)

The P&P used in HK government also take references from international standards including:

- ISO/IEC: These are two international standard-setting bodies that collaborate to create global standards, especially in areas of information technology and electronic systems.
- NIST: Stands for the National Institute of Standards and Technology. It’s a U.S. federal agency that develops standards, guidelines, and best practices to promote innovation and industrial competitiveness, especially in areas like cybersecurity, technology, and measurement science.

In addition, more reference from internation organizations:

- Format for Incident Reporting Exchange (FIRE) from Financial Stability Board
- Reporting of Aviation Security Occurrences and Incidents from International Civil Aviation Organization
- Security Incident Reporting from International Air Transport Association

Revised Pre-Reporting Evaluation Framework

❖ Factors for Severity Assessment

If an incident is assessed as (1) meeting the reporting obligation criteria or (2) its severity level 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 4 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
- Cyberattacks, ransomware, or malware infections
- Service disruption / downtime affecting key / core business function for certain period of time
- Affecting Critical infrastructure

Revised Pre-Reporting Evaluation Framework

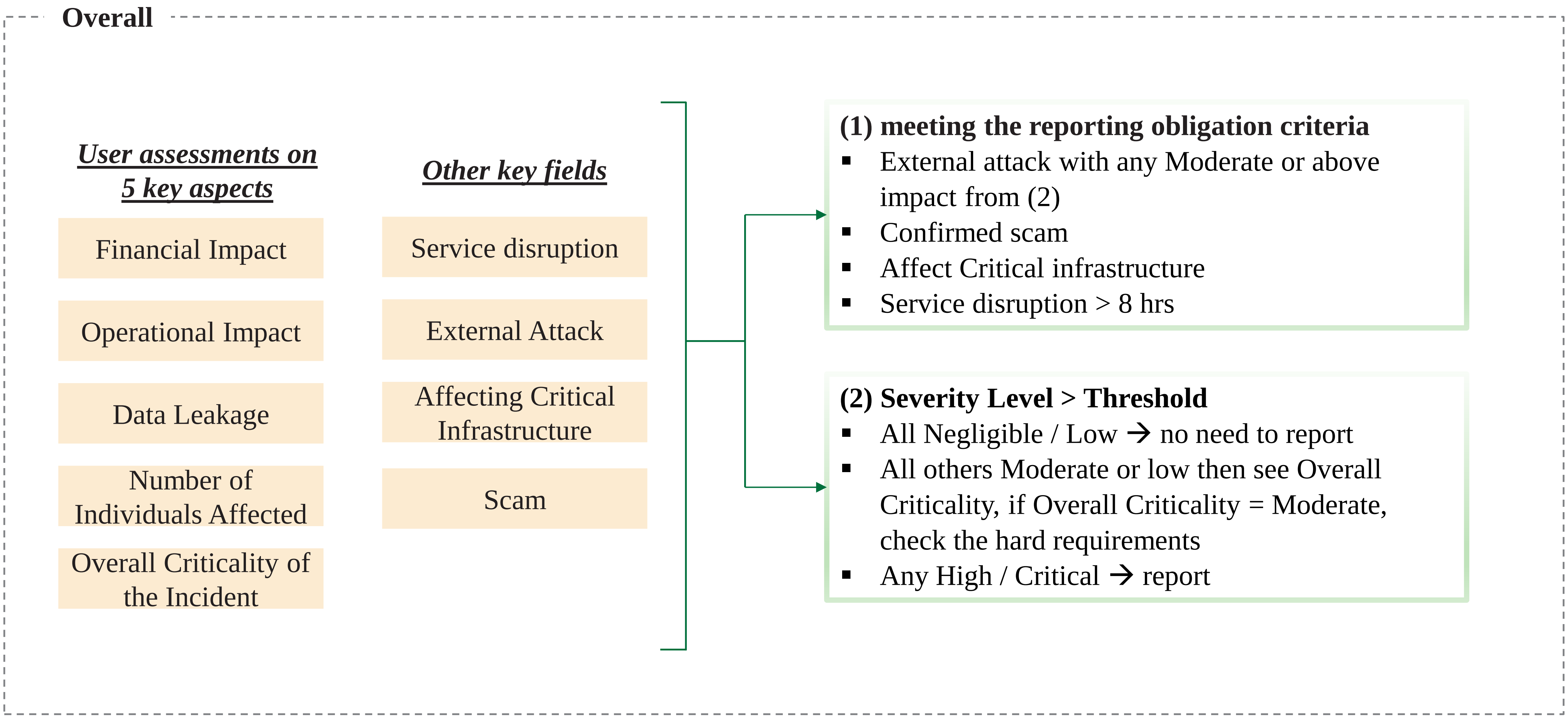
(2) Severity Level > Threshold

With references as mentioned in previous slides, revise the impact types and severity level as below

Impact Type from Frameworks adopted by the Government		Our considerations	Changes made
Confidentiality, Integrity, Availability (CIA Triad)	Section 3.4 – Incident Categorisation	Should be considered under different areas as they always intercorrelated	No
Operational Disruption	Section 4.2 – Incident Impact Assessment	Yes (Operational impact & service disruption)	No
Information Leakage	Section 4.2 – Incident Impact Assessment	Yes (PII impact)	Renamed as “Data Leakage”
System Compromise	Section 3.3 – Incident Identification and Recording	Yes, kind of included under Operational impact, Affecting Critical Infrastructure, Impacted Systems	No
Legal and Regulatory Consequences	Section 4.2 – Incident Impact Assessment	Yes, kind of included under Overall Criticality	No
Reputational Damage	Section 4.2 – Incident Impact Assessment	Yes, kind of included under Overall Criticality	No
Financial Loss	Section 4.2 – Incident Impact Assessment	Yes (Financial impact)	No

Level	Financial Impact	Operational Impact	Data Leakage	Number of Individuals Affected	Overall Criticality
Negligible	Financial loss is insignificant, with no noticeable effect on operations or services.	Minor inconvenience, no disruption to critical business functions, easily resolved without external intervention.	Exposure of non-sensitive information (e.g., public directories) with no risk to individuals.	No individuals affected, or exposure of non-identifiable public data. No action required.	Minimal impact, no legal, regulatory, or reputational consequences; routine business operations unaffected.
Low	Minor financial loss with limited impact on operations; easily absorbed without significant effort.	Slight delays or reduced performance in non-critical systems, minimal customer impact.	Limited exposure of PII (e.g., names, email addresses) with minimal risk; may require monitoring.	1-10 individuals affected; limited data (e.g., name, email). Minimal risk. Notification optional.	Limited impact, minor legal/regulatory concerns, reputational effect negligible; easily contained.
Moderate	Noticeable financial loss affecting specific departments or services; requires management attention.	Disruption in one or more non-critical processes; possible customer complaints; requires moderate resource allocation to fix.	Exposure of sensitive PII (e.g., ID numbers) affecting a group; potential for identity theft.	11-100 individuals; moderate sensitivity data (e.g., contact + ID number). Some risk, notification advisable.	Noticeable impact, potential for moderate legal or regulatory concern, some reputational risk; may require external communication.
High	Significant financial loss impacting multiple departments; may threaten organizational objectives.	Major disruption to critical business functions; significant customer dissatisfaction; potential legal or contractual implications.	Large-scale exposure of sensitive PII (e.g., financial, health data); significant risk to individuals.	101-1,000 individuals; sensitive data (e.g., health, financial). High risk, mandatory notification.	Significant legal/regulatory consequences, high reputational damage risk, business operations disrupted; reporting likely mandatory.
Critical	Severe financial loss jeopardizing the organization's viability; requires immediate executive action.	Total shutdown of critical operations; threatens the organization’s survival or national infrastructure; requires immediate executive and external action.	Massive breach of highly sensitive PII; severe risk to individuals and organizations; legal implications.	>1,000 individuals; highly sensitive data; major harm possible (identity theft, fraud). Regulator involvement.	Severe legal and regulatory fallout, national or cross-border implications, reputational crisis, major disruption to core services; immediate executive attention and mandatory reporting.

Revised Pre-Reporting Evaluation Framework



Overall

User assessments on 5 key aspects

- Financial Impact
- Operational Impact
- Data Leakage
- Number of Individuals Affected
- Overall Criticality of the Incident

Other key fields

- Service disruption
- External Attack
- Affecting Critical Infrastructure
- Scam

(1) meeting the reporting obligation criteria

- External attack with any Moderate or above impact from (2)
- Confirmed scam
- Affect Critical infrastructure
- Service disruption > 8 hrs

(2) Severity Level > Threshold

- All Negligible / Low → no need to report
- All others Moderate or low then see Overall Criticality, if Overall Criticality = Moderate, check the hard requirements
- Any High / Critical → report

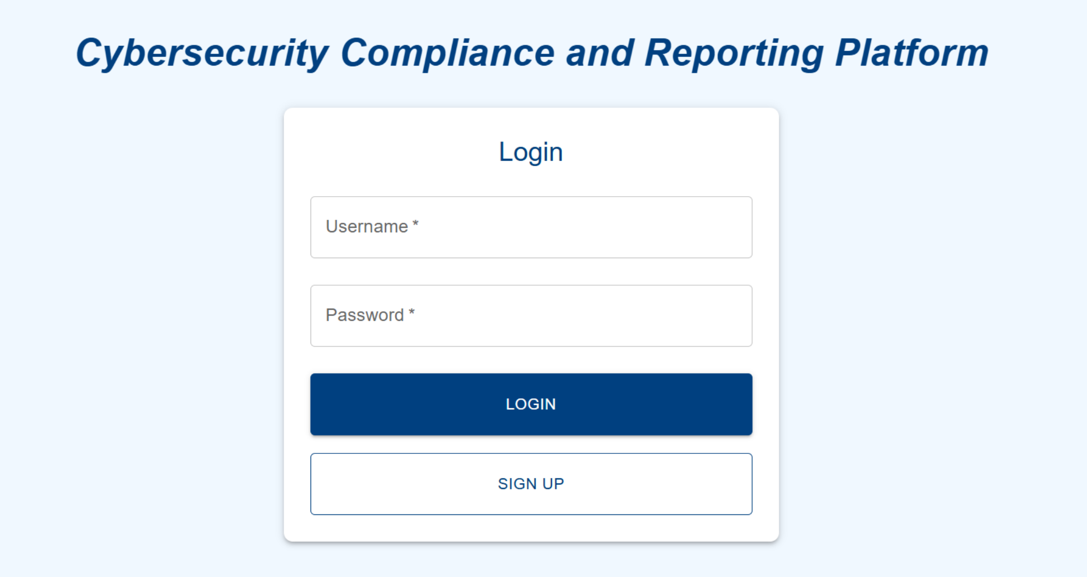
Demo

- We will now provide a demonstration.

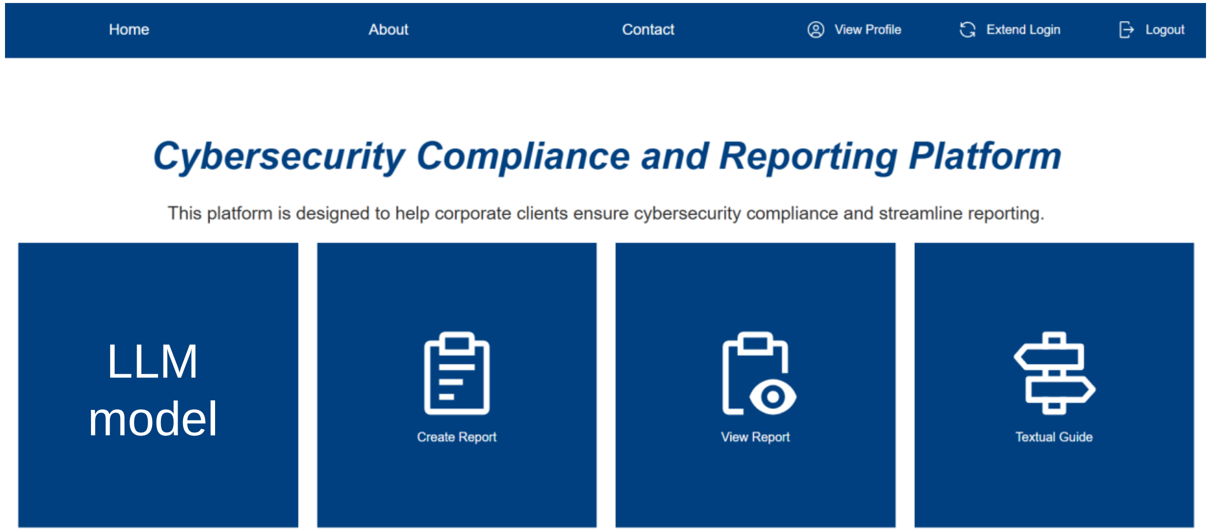
Demo – as a user

- Mainly on incident reporting record creation
- Seek guidance on reporting to regulators / escalation decision

Sign Up / Login to access the platform



Cybersecurity Compliance and Reporting Platform



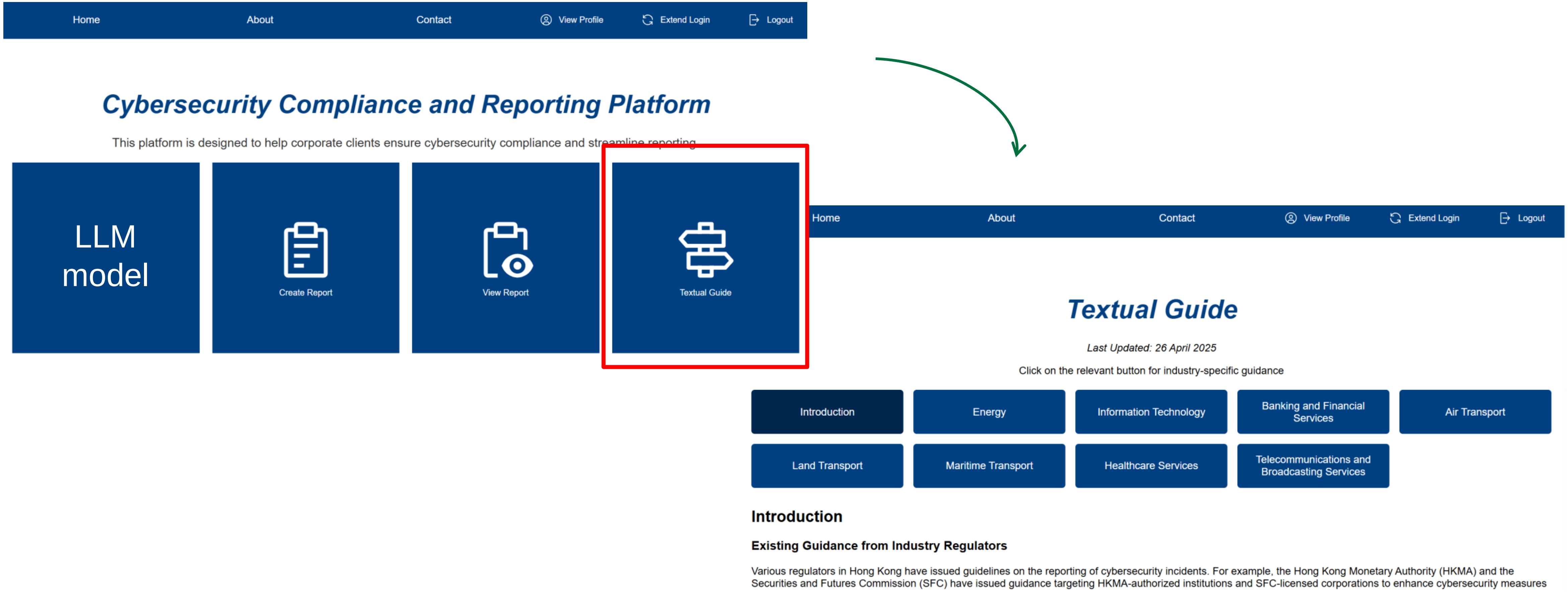
Cybersecurity Compliance and Reporting Platform

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

Demo – as a user

- Mainly on incident reporting record creation
- Seek guidance on reporting to regulators / escalation decision

Check out the Guide



Cybersecurity Compliance and Reporting Platform

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

Textual Guide

Last Updated: 26 April 2025

Click on the relevant button for industry-specific guidance

Introduction

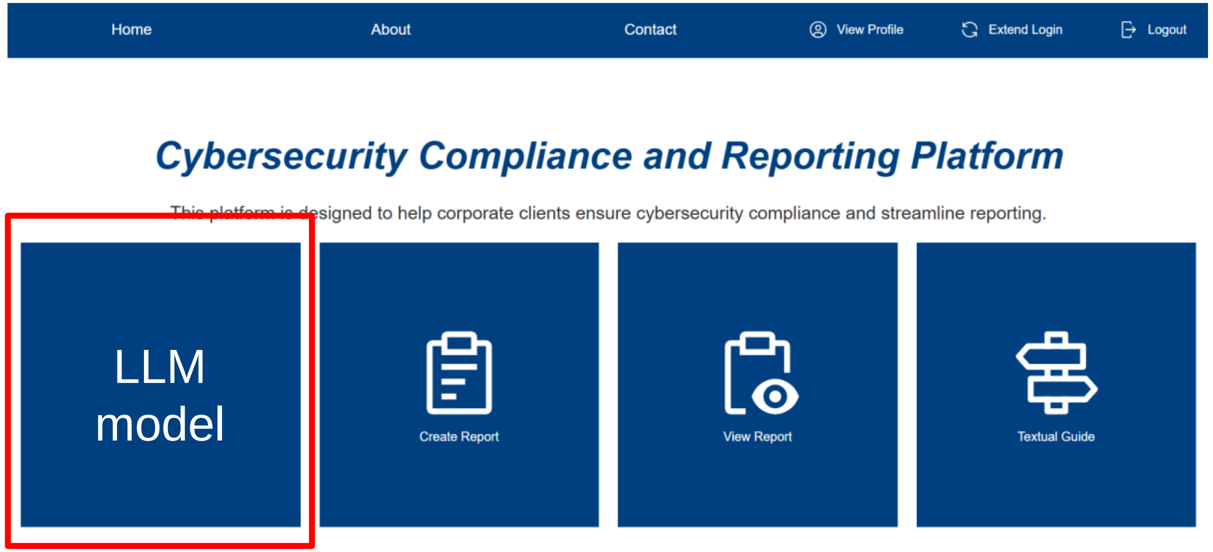
Existing Guidance from Industry Regulators

Various regulators in Hong Kong have issued guidelines on the reporting of cybersecurity incidents. For example, the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC) have issued guidance targeting HKMA-authorized institutions and SFC-licensed corporations to enhance cybersecurity measures

Demo – as a user

- Mainly on incident reporting record creation
- Seek guidance on reporting to regulators / escalation decision

Use (A) PDF Upload – LLM model to provide advice on the reporting decision (still under development)



Cybersecurity Compliance and Reporting Platform

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

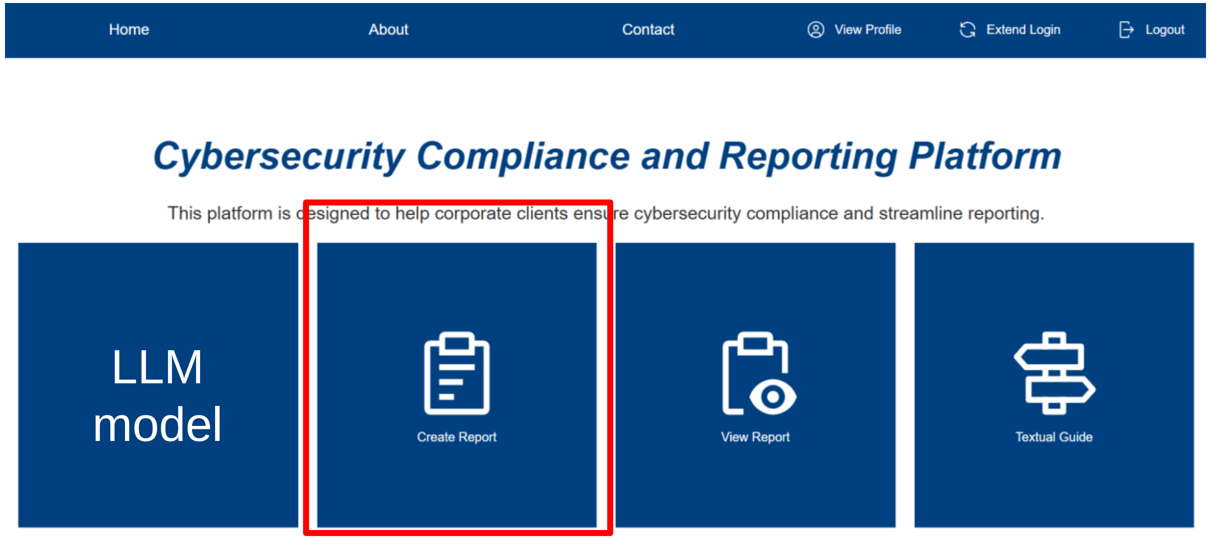
Upload PDF here

Still under development

Demo – as a user

- Mainly on incident reporting record creation
- Seek guidance on reporting to regulators / escalation decision

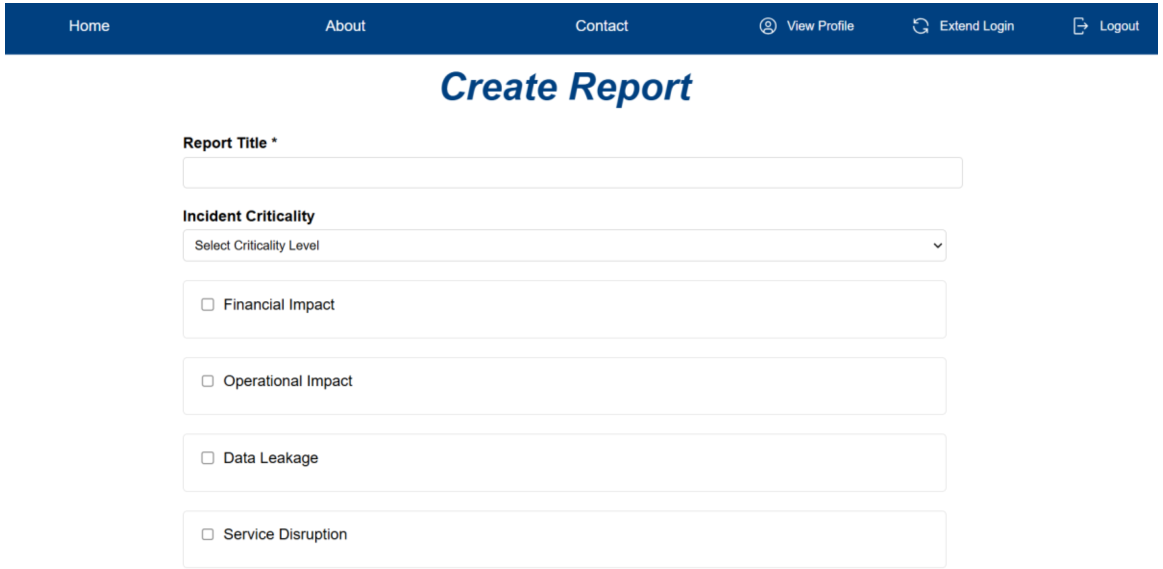
Use (B) Form Filling – for role-based decision model to provide advice on the reporting decision



Cybersecurity Compliance and Reporting Platform

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

Input incident details and associated impacts here



Create Report

Report Title *

Incident Criticality

Select Criticality Level

☐ Financial Impact

☐ Operational Impact

☐ Data Leakage

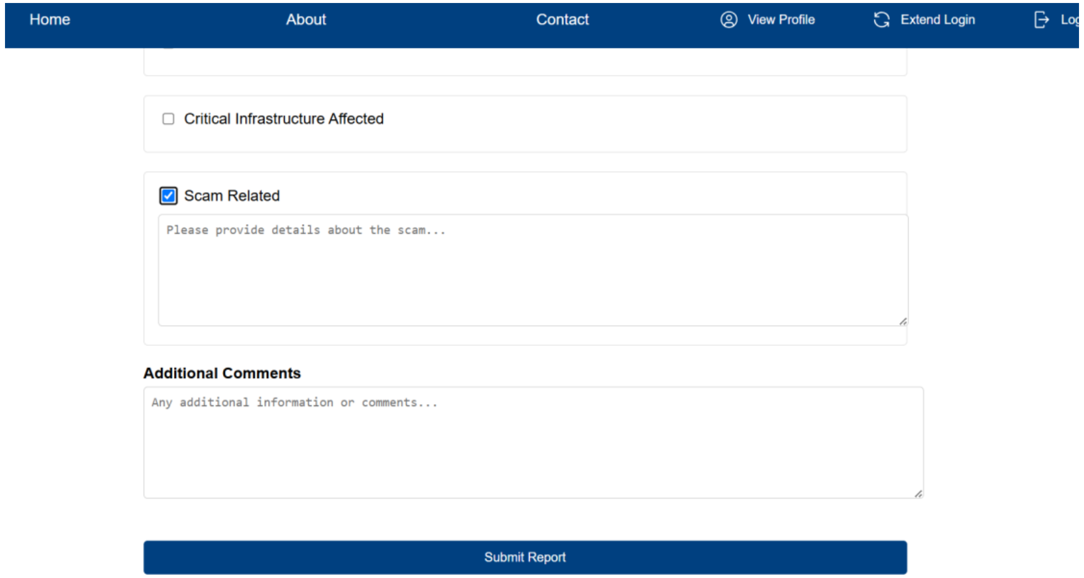
☐ Service Disruption

Demo – as a user

- Mainly on incident reporting record creation
- Seek guidance on reporting to regulators / escalation decision

Use (B) Form Filling – for role-based decision model to provide advice on the reporting decision

Submit the report



□ Critical Infrastructure Affected

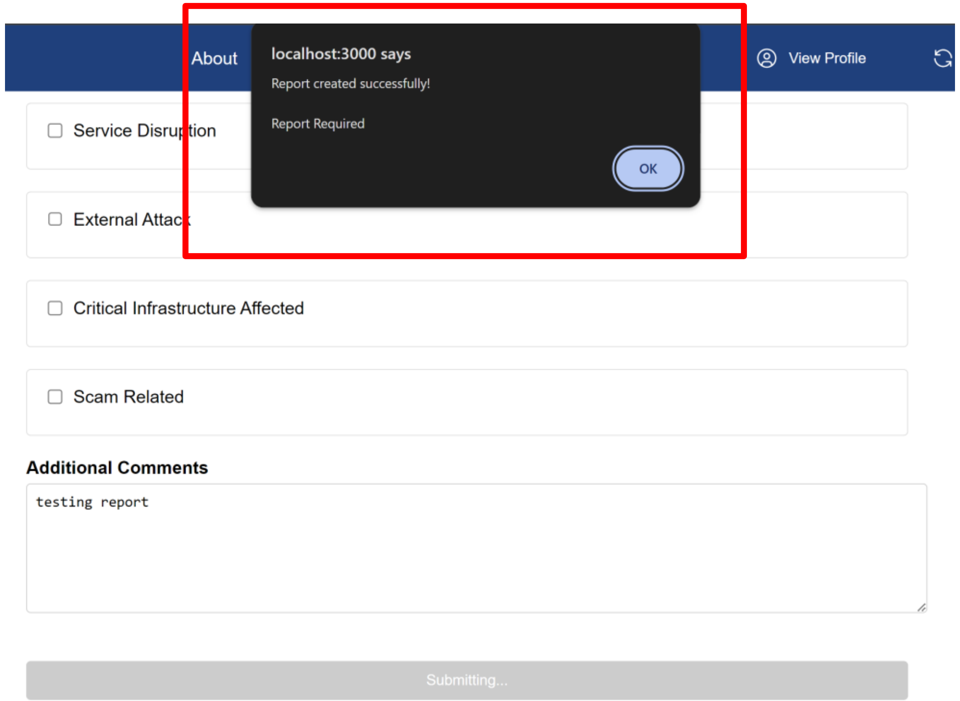
☑ Scam Related

Please provide details about the scam...

Additional Comments

Any additional information or comments...

Get the result “report” / “not report”



localhost:3000 says

Report created successfully!

Report Required

□ Service Disruption

□ External Attack

□ Critical Infrastructure Affected

□ Scam Related

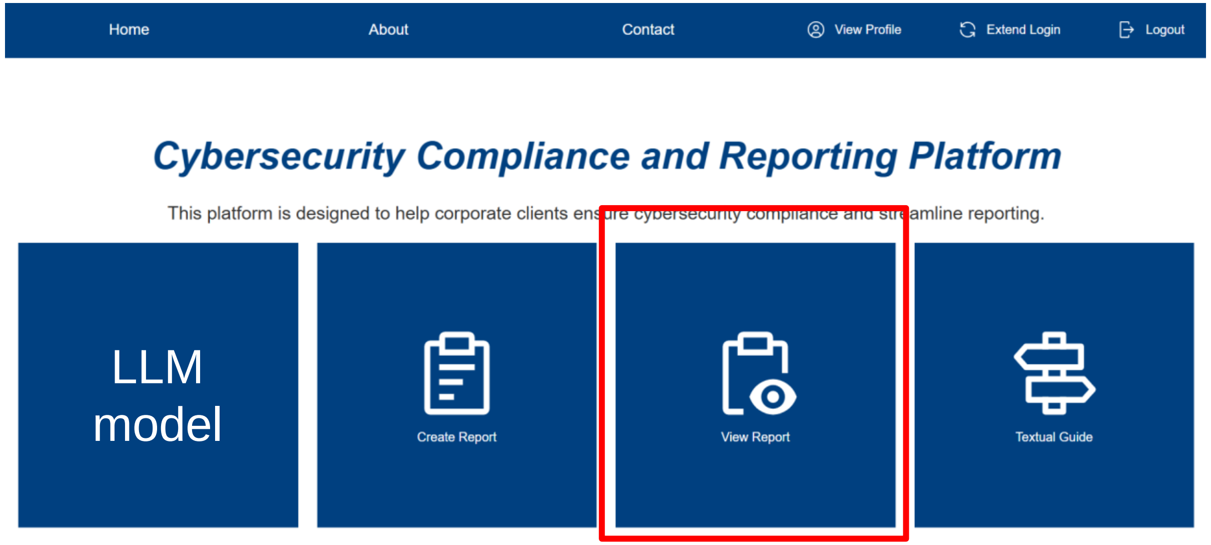
Additional Comments

testing report

Demo – as a user

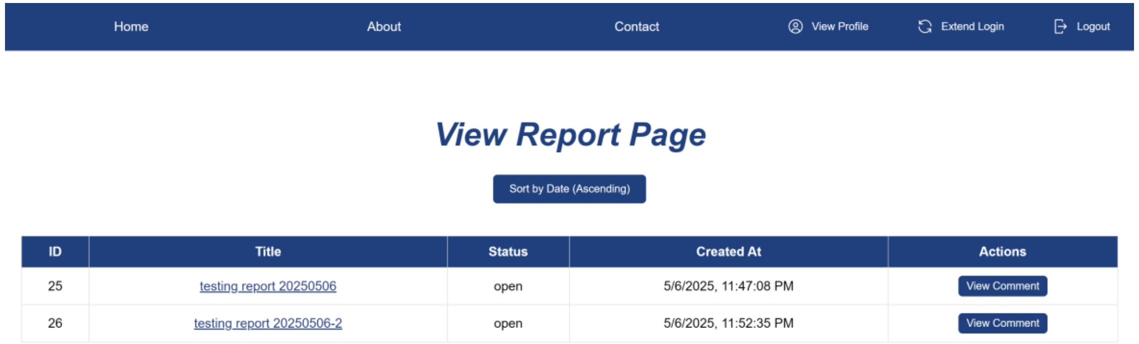
- Mainly on incident reporting record creation
- Seek guidance on reporting to regulators / escalation decision

Use (B) Form Filling – for role-based decision model to provide advice on the reporting decision



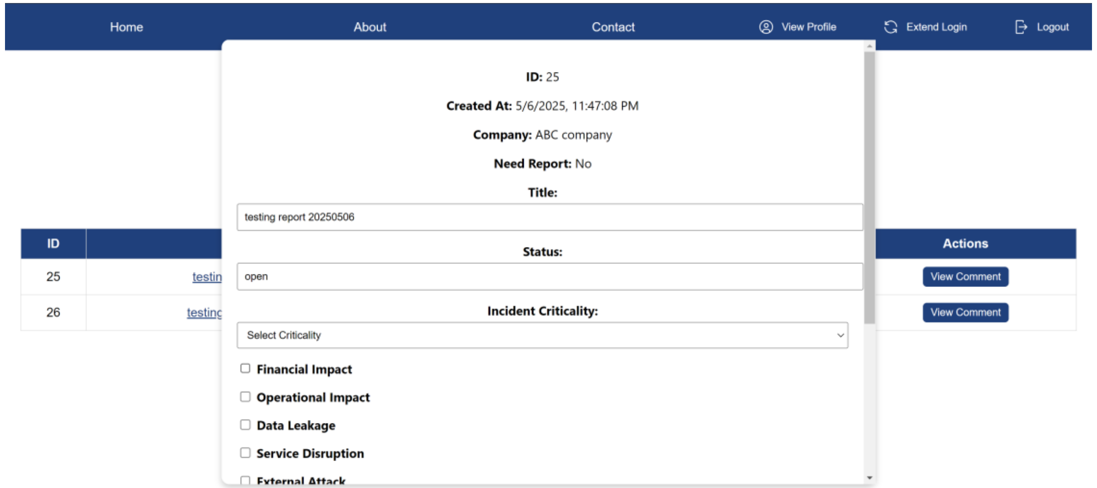
Cybersecurity Compliance and Reporting Platform

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



View Report Page

ID	Title	Status	Created At	Actions
25	testing report 20250506	open	5/6/2025, 11:47:08 PM	View Comment
26	testing report 20250506-2	open	5/6/2025, 11:52:35 PM	View Comment



ID: 25

Created At: 5/6/2025, 11:47:08 PM

Company: ABC company

Need Report: No

Title:

testing report 20250506

Status:

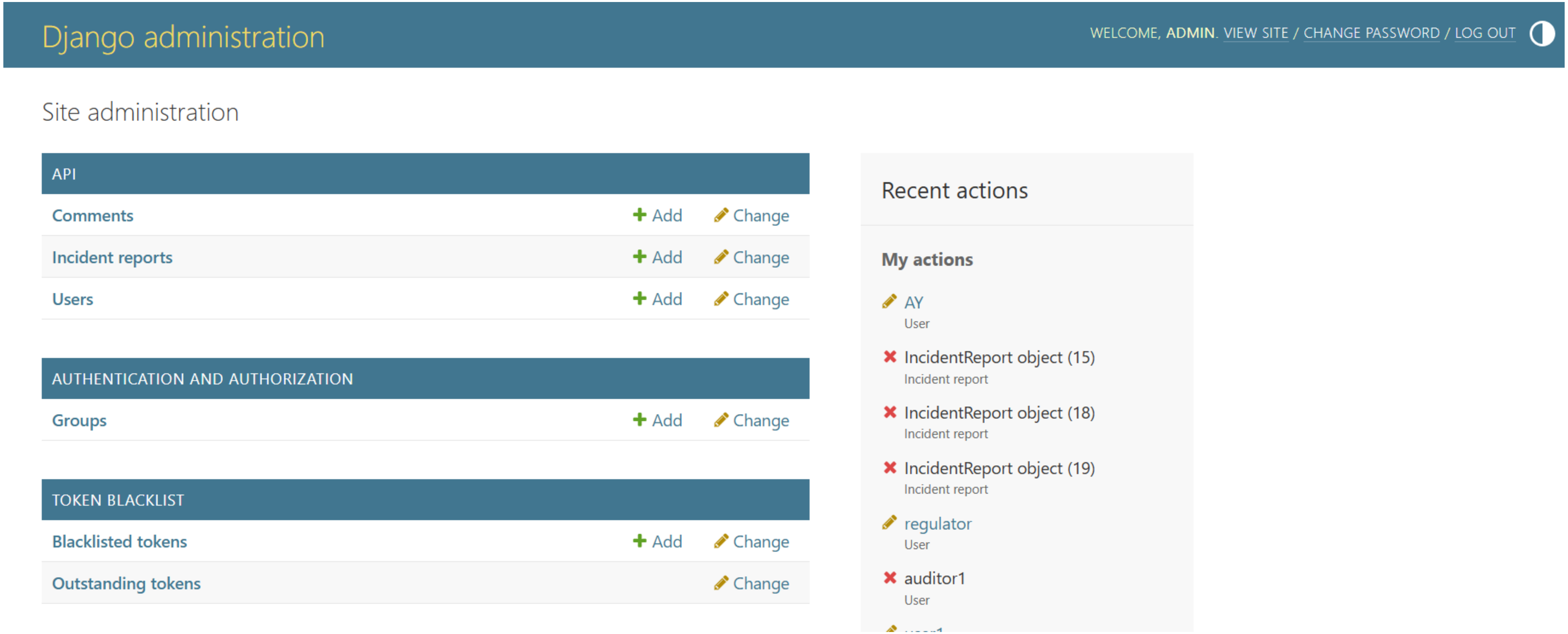
open

Incident Criticality:

Select Criticality

- □ **Financial Impact**
- □ **Operational Impact**
- □ **Data Leakage**
- □ **Service Disruption**
- □ **External Attack**

Demo – Administration



Django administration

WELCOME, **ADMIN**. VIEW SITE / CHANGE PASSWORD / LOG OUT

Site administration

API		
Comments	+ Add	✎ Change
Incident reports	+ Add	✎ Change
Users	+ Add	✎ Change

AUTHENTICATION AND AUTHORIZATION		
Groups	+ Add	✎ Change

TOKEN BLACKLIST		
Blacklisted tokens	+ Add	✎ Change
Outstanding tokens		✎ Change

Recent actions

My actions

✎ AY
User

✖ IncidentReport object (15)
Incident report

✖ IncidentReport object (18)
Incident report

✖ IncidentReport object (19)
Incident report

✎ regulator
User

✖ auditor1
User

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) - Presentation on the 1st Milestone		■			
Project Progress Update 2 (10 May) - Working towards the 2nd Milestone in relation to further enhancing functionality of website and report generation functions, and evaluation of pre-reporting evaluation framework.			■		
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)					▨