COMP7705 Project

Detailed Project Proposal

Project Title:	Cybersecurity Compliance and Reporting Platform
Mentor:	Dr. P.S. Vivien Chan
Student 1 (Leader)	YIP Wankit, Daniel 3036383678
Student 2	CHAN Cheung Hei 3036381280
Student 3	SONG Insu 3036199596
Student 4	WONG Kwun Yuet Shavonne 2013534309
Student 5	YEUNG Hiu Ying 3036379976

Aim

1. Summary

Hong Kong faces an increasing number of cybersecurity threats, including phishing, ransomware, and malware attacks, which pose risks to organizations, financial assets, and critical infrastructure. As digitalization expands, businesses must comply with evolving cybersecurity regulations, such as the upcoming Protection of Critical Infrastructure (Computer System) Bill (2026). However, many organizations encounter challenges in cyber incidents management due to limited resources, complex regulations and fragmented reporting processes, leading to inefficiencies and compliance risks.

To address these challenges, our team, a combination of teammates from technology, risk and legal backgrounds, is introducing the Cybersecurity Compliance and Reporting Platform through this project. This integrated solution incorporates key functionalities such as incident severity classification, regulatory compliance tracking and standardized reporting. After research, our team will leverage machine learning, NLP and cryptographic security to be the basic components for development. The platform will be empowered by an AI-powered chatbot for assessing incident severity, automated report generation, secure data storage using IPFS and real-time regulatory updates to help organizations maintain compliance efficiently.

After performing the research of online resources from various government departments, our team plan to include legislation and regulatory requirements from the Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC) and Privacy Commissioner for Personal Data etc. as the scope for compliance guidance. The project will be executed in several phases including research, development, testing and final reporting with regular progress update provided. Our team targets to complete the project by July 2025. The platform aims to enhance compliance management by making it more efficient and reducing reporting unalignment while strengthening cybersecurity oversight. Ultimately, it offers a standardized and effective solution for managing cybersecurity incidents and tackling the pain points.

2. Introduction

Background

Hong Kong faces increasing cybersecurity threats. According to The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) statistics [25], common attacks including phishing attacks, ransomware, web server and app attacks and malware attacks (botnets) pose significant risks to the organizations and endangering personal data, financial assets and critical infrastructure for IT environment. This evolving threat landscape is intensified by the digitalization of more businesses in Hong Kong. With the rising trend mentioned above, organizations are expected to strengthen their cybersecurity measures in their IT environments. In addition, more regulatory requirements and guidelines will be introduced to protect the public interest and ensure the stability of various industries. An upcoming legal requirement, the Protection of Critical Infrastructure (Computer System) Bill, is expected to be fully implemented by mid-2026.

Problem Statement and Motivation

Organizations in Hong Kong face considerable challenges in cyber incident handling, including addressing complex regulatory expectation and determination incident severity and preparing incident reporting materials due to the limited resources such as experience, knowledge and expertise. Cybersecurity threats are becoming more sophisticated, further complicating these challenges. While aforementioned problems cause delays and operational disruptions, this highlights the need for an integrated platform to streamline and reduce the time spent on the workflow and ensure the consistence on cybersecurity compliance and reporting. Unlike traditional incident reporting tracking, this project is empowered by cutting-edge technologies, including NLP, AI and machine learning to integrate regulatory requirements, severity classification, standardized incident reporting into a single platform. Additionally, application of a decentralized file system (IPFS) ensures tamper-proof and transparent audit trails for cybersecurity incidents. This project will significantly enhance cybersecurity compliance, reduce incident reporting inefficiencies and enhance data management of incident cases for businesses.

Objective and Expected Deliverables

This project aims to design and develop an intelligent, AI-driven and decentralized cybersecurity management solution, tentatively named "Cybersecurity Compliance and Reporting Platform" to assist organizations in Hong Kong with:

- Incident Severity Classification: The platform features an AI chatbot that helps users classify the severity of cybersecurity incidents and provides real-time regulatory guidance to ensure consistency on incident severity determination.
- AI-Powered Incident Reporting: It allows users to input key details and instantly create standardized reports for submission to the suggests the appropriate government departments for reporting. During the incident case input stage, reviewers can always provide comments and request for clarifications quickly, making the reporting process smoother and more efficient. Report generation function enables users to generate incident reports with standardized and clear format for both external and internal reporting.
- Secure Data Storage & Encryption: The platform ensures secure and tamper-proof data storage using IPFS (Inter-Planetary File System), making all records immutable and highly available. Strict access controls and RSA encryption protects incident reports, ensuring that only authorized entities can access sensitive information. This approach guarantees data confidentiality, integrity, and compliance with cybersecurity regulations.
- Regulatory Compliance & Knowledge Management: The regulatory dashboard keeps organizations updated on the latest cybersecurity laws and compliance requirements. The knowledge base is regularly updated to reflect new regulations, reducing the risk of non-compliance. The platform also integrates AI-powered search (RAG framework), which retrieves and provides the most up-to-date regulatory information when users seek

compliance guidance. This ensures accurate and reliable recommendations for cybersecurity reporting.

- Streamlined Compliance & Efficiency: The platform serves as an all-in-one compliance tool, combining incident classification, reporting, and regulatory tracking in one place. By automating these processes, it helps organizations save time, reduce manual effort, and minimize errors in cybersecurity incident reporting. The system's structured workflow ensures faster response times, greater accuracy and improved regulatory compliance, making it a practical solution for managing cybersecurity risks.

Brief Literature Review

3. Brief Literature Review

Currently in Hong Kong, there is no mandatory regulatory requirement for reporting cybersecurity incidents to regulatory authorities. At the same time, there is a wide array of guidelines across various industries, issued by regulators such as the Securities and Futures Commission (SFC), alongside multiple entities to which reports may be submitted, such as the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Police Force. While organizations and individuals may voluntarily report incidents to these authorities, the absence of a standardized reporting format or clear guidance on which authority should handle specific reports creates a fragmented and inconsistent framework. This fragmentation can result in confusion, reduced effectiveness and utility of the reports, or even a reluctance among organizations and individuals to report incidents altogether.

Studies have criticized the lack of a national-level cybersecurity incident reporting policy across the public and private sectors, highlighting significant consequences. These include insufficient sharing of lessons learned, uncoordinated and redundant defensive actions, and increased vulnerability to cyber-attacks due to limited real-time information sharing [2]. Without a regulatory framework or standardized policy, the incident reporting rate is believed to remain low. Beyond the absence of clear reporting policies, research has explored other factors contributing to low reporting rates. It has been observed that users may be more inclined to report technical issues rather than security breaches, especially when there is no perceived benefit to making such reports [3]. Additionally, feelings of shame and embarrassment associated with publicizing cybersecurity incidents have been identified as barriers to reporting breaches to law enforcement [4].

While these studies do not specifically analyze the context of Hong Kong, the unique challenges of the local regulatory landscape—marked by a patchwork of industry-specific guidelines and the lack of mandatory incident reporting policies—exacerbate the issue. In light of this, we believe that even in the absence of national-level legislation mandating cybersecurity incident reporting, there is an urgent need for a centralized platform. Such a platform could consolidate existing rules and guidelines, offering users a one-stop, private, and secure solution for making informed decisions about reporting incidents. A centralized system would enable organizations and individuals to navigate the complexities of the current framework with greater ease, ensuring confidentiality while facilitating compliance with the various reporting requirements.

This project aims to address the challenges posed by the absence of mandatory reporting regulations and the lack of streamlined support for cybersecurity incident reporting. By developing an intelligent platform, our goal is to provide users with up-to-date guidance on the latest cybersecurity-related rules and guidelines. The platform will also be capable of generating incident reports tailored to satisfy the requirements of all relevant authorities, thereby simplifying and standardizing the reporting process. In designing this platform, we propose to draw on [the European Commission's guidance on a risk-based approach, which emphasizes the importance of analyzing incidents that have caused or have the potential to cause substantial harm, as well as identifying cyber threats to competent authorities [5]. Additionally, we intend to incorporate insights from research indicating how robust incident reporting systems and effective cybersecurity management practices can mitigate employee stress and address challenges related to artificial intelligence (AI) in cybersecurity contexts [6].

By leveraging these principles and addressing the specific needs of Hong Kong, this project seeks to create a practical, centralized solution to improve cybersecurity incident reporting, enhance regulatory compliance, and ultimately strengthen the region's overall cybersecurity resilience.

Proposed Methodology

4. Scope of Work

The Protection of Critical Infrastructures (Computer Systems) Bill specifies eight in-scoped industries as critical infrastructures: Energy, Information Technology, Banking and Financial Services, Air Transport, Land Transport, Maritime Transport, Healthcare Services and Telecommunications and Broadcasting Services.

While the Bill designates specific regulating authorities for the Banking and Financial Services and Telecommunications and Broadcasting Services sectors, it does not explicitly assign regulating authorities for the remaining sectors. However, the Bill establishes a Commissioner of Critical Infrastructure (Computer-system Security) along with designated authorities, serves as the regulating authority for critical infrastructures.

The platform will cover regulatory frameworks (listed below) in Hong Kong that mandate incident reporting for cybersecurity breaches, data breaches, online operational failures, service disruptions and compliance violations. Operators within these eight sectors are required to report specific information to the Commissioner and designated regulatory authorities to ensure the security of their critical computer systems

- General for all industry
  - Hong Kong Law
    - Protection of Critical Infrastructures (Computer Systems) Bill [7]
  - Privacy Commissioner for Personal Data
    - Guidance on Data Breach Handling and Data Breach Notifications [8]
  - Hong Kong Police – Any cyber incidents related to criminal activities
- Banking and financial services
  - Hong Kong Monetary Authority (HKMA)
    - Guideline on Authorization of Digital Banks 25 Oct 2024 [9]
    - Guideline on Supervision of Stored Value Facility Licensees Sep 2016 [10]
    - Guideline on Oversight of Designated Retail Payment Systems Sep 2020 [11]
    - Supervisory Approach on Cyber Risk Management 29 Nov 2024 [12]
    - Risk Management of E-banking 25 Oct 2024 [13]
    - Incident response and management procedures 22 June 2010 [14]
    - General Principles for Technology Risk Management 24 June 2003 [15]

        - Operational Resilience 31 May 2022 [16]
        - Operational Risk Management 25 July 2022 [17]
        - Business Continuity Planning 31 May 2022 [18]
    - Securities and Futures Commission [19]
        - Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading 27 Oct 2017 [20]
    - Insurance Authority
        - Guideline on Cybersecurity [21]

5. <u>Core Components</u>

The platform will be built to streamline incident severity classification, regulatory compliance tracking and standardized incident reporting by integrating a rule-based chatbot with an automated severity classification system for incident severity assessment, intelligent incident reporting suggestions, decentralized storage for secure data management and a continuously updated regulatory knowledge base. Technologies such as Natural Language Processing (NLP), machine learning and cryptographic security will be adopted. These components work together to reduce manual effort and improve accuracy. Hence, it assists in enhancement on the overall efficiency of cybersecurity compliance and reporting management.

At the front end, users can access a web-based chatbot to input the summary on the details of incident cases. This rule-based chatbot operates based on a structured decision-making framework that aligns with Hong Kong's regulatory requirements, including the Personal Data (Privacy) Ordinance (PDPO) and other relevant legal frameworks. It evaluates incident characteristics based pre-defined criteria such as the type of data impacted, financial loss and regulatory reporting obligations to provide accurate and real-time reporting guidance. After the incident severity analysis, the user can consider whether the incident should be recorded on the platform. Users will be directed to the incident reporting aids if they decide to use the platform for monitoring specific incident cases. There is an incident input form for standardized incident reporting. Users are required to input the incident cases in detail. The chatbot will be tested and refined using simulated scenarios to ensure reliability. Additionally, a regulatory dashboard for displaying compliance requirements and policy updates will enable organizations to stay informed about changes in cybersecurity laws timely.

The backend is responsible for data processing and automation. To understand the incident that happened, NLP engine is the best fit technique for extracting insights from cyber incident details input by the user. Those details may contain both structured (e.g., financial losses, incident categories) and unstructured (e.g., detailed descriptions) data which are subject to further data processing. In the next workflow, an Incident Severity Classification Model categorizes incident severity based on insights provided by NLP engine and leverages machine learning techniques including rule-based models, Random Forest algorithms and fine-tuning methods such as Grid Search and SMOTE to provide recommendation in incident severity. As incident details is unlikely to share publicly, it may be the difficulty for our team to gather enough incident cases from Hong Kong. Therefore, our team will take references from some repository. The model is trained on datasets such as the European Repository of Cyber Incidents (EuRepoC) and Non-Profit Cyber Incident Repository (NPCIR) [27] [28]. To ensure performance accuracy, it is evaluated using metrics like F1 Score, Precision, and Recall. Additionally, the platform automates regulatory compliance tracking, monitoring legal updates and recommending necessary actions. An automated report generation module further simplifies reporting by formatting incident data into standardized reports for submission to regulatory authorities.

The storage system is developed with security and reliability in mind. The platform will employ a decentralized storage system using IPFS (Inter-Planetary File System) to prevent tampering and ensure high availability [24]. Compared with centralized data storage, IPFS distributes files across multiple nodes is chosen as this can mitigate the risks associated with hardware failures, cyber threats and natural disasters to provide higher resilience [25][26]. Incident information representing the existing vulnerabilities to the organization. Therefore, it is essential to put more effort into ensuring data security. The system also integrates RSA asymmetric encryption to ensure that incident reports remain confidential and can only be accessed by authorized parties [27]. Reports are encrypted with the organization’s public key for internal use and with the regulator’s public key for external submission through access control mechanisms. This can ensure data integrity and regulatory compliance. To handle a particular incident, many parties in the organization may need to contribute expertise on it.

A real-time reviewer feedback system enables different parties to request clarifications and collaboration. Hence, this assists in improving the efficiency of incident reporting and response.

With our proposed solutions, the platform helps reduce compliance burdens, enhance cybersecurity risk management, and streamline the incident reporting process. This enables organizations to overcome challenges related to resource limitations. Additionally, it helps minimize reporting errors, ensure timely regulatory submissions, and stay ahead of evolving cybersecurity requirements, ultimately strengthening their overall security posture and regulatory compliance.

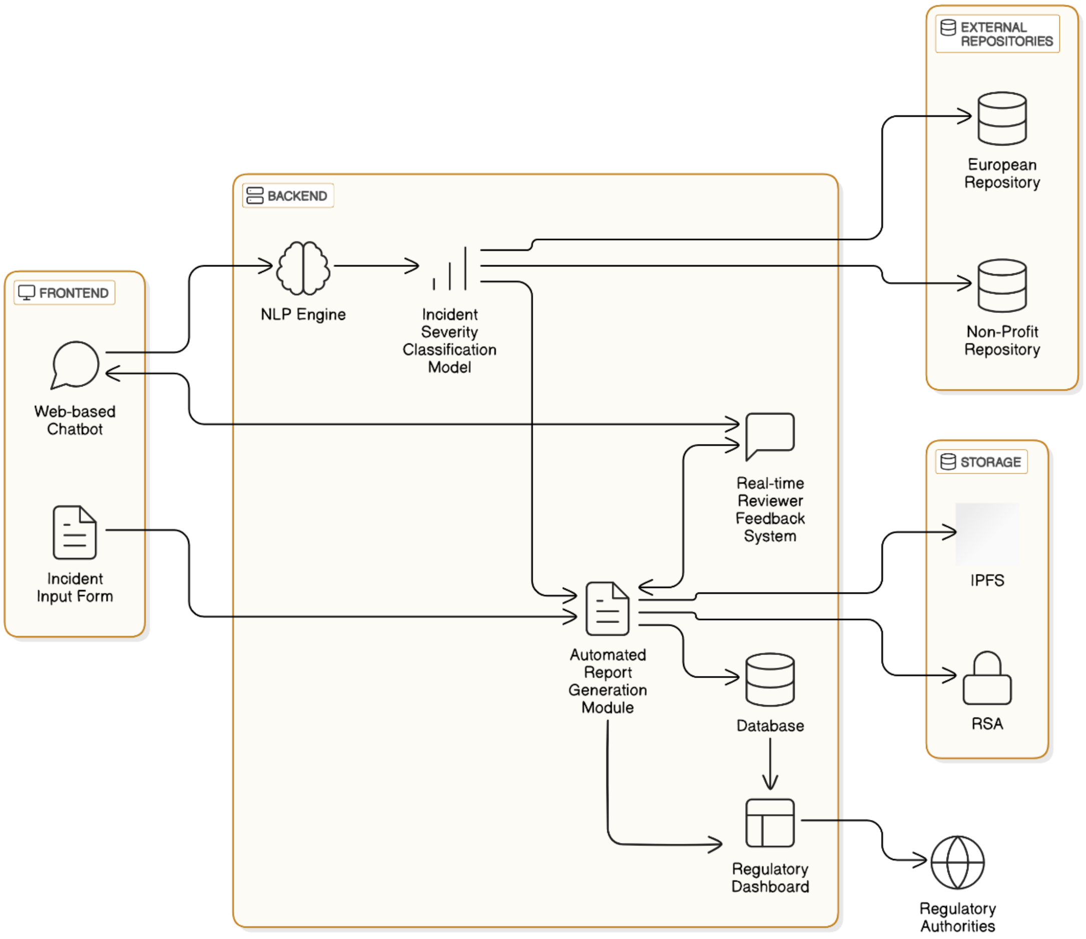

Figure 1: Architecture of Cybersecurity Compliance and Reporting Platform

5.1 Chatbot Assistance

Rule-based Chatbot

The Chatbot will be a rule-based chatbot, centered around a structured decision-making framework created by identifying key factors relevant to cybersecurity incidents, such as the type of incident, the data impacted and the specific regulatory requirements in Hong Kong to help on cybersecurity incident analysis, severity determination and associated reporting obligations.

An examination of applicable legal and regulatory frameworks will be conducted, such as the Personal Data (Privacy) Ordinance (PDPO) and guidelines from various regulators as well as findings from research papers to establish the thresholds of the incident determination criterion. Rules will then be designed to link incident characteristics to these criteria enabling Chatbot to provide relevant recommendations. Each rule will be tailored to address specific conditions, such as the scale of the breach or the sensitivity of the data involved, resulting in a systematic and logical process for evaluating incidents. These rules can be implemented through decision trees or programmed into a chatbot framework using tools like Dialogflow and Rasa.

To ensure accuracy and reliability, we will implement an iterative design and testing process for the Chatbot. The Chatbot's logic will be tested using simulated incident scenarios to confirm that it can correctly identify reporting obligations and provide precise guidance.
Set out below is a sample conversation:

- Chatbot: “What type of incident are you reporting? Select one:
    1. Data breach
    2. Service disruption
    3. Other”
- User: “Data breach.”
- Chatbot: “Does the breach involve personal data of Hong Kong residents? (Yes/No)”
- User: “Yes.”
- Chatbot: “Does the breach pose a real risk of significant harm to individuals? (Yes/No)”

- User: “Yes.”
- Chatbot: “Under [REGULATION/GUIDELINES], you are required to notify [REGULATOR] within [NUMBER] hours. Would you like guidance on how to submit a report? (Yes/No)”
- User: “Yes.”

Incident Severity Classification

The Chatbot module assistant will allow the user to seek advice on the severity classification of the incidents and provide guides on reporting the incident. This function will implement an incident classification model that predicts the severity of cybersecurity incidents based on the features extracted from the NLP-based Information Extraction function. The steps to build this classification model are detailed below.

1. Data Exploration and Preprocessing
    - Exploratory Data Analysis: To understand incident features dataset constructed earlier, we will examine its structure and visualize it to identify patterns and detect anomalies.
2. Model Building
    - Train-Testing Data: We will divide the dataset into training and testing data sets (70:30).
    - Baseline Rule-based Model: To establish a performance benchmark will construct a rule-based model by leveraging expert knowledge. This baseline provides a reference point for evaluating more complex models.
    - Machine Learning-based Models: We will consider more advanced machine learning models such as Random Forest to enhance classification performance.
3. Model Evaluation

- Performance Metrics: We may consider metrics such as F1 Score, Precision, and Recall for evaluating the model’s performance. Furthermore, we may employ cross validation.

4. Model Improvement

- Finetuning: We may optimize model performance through techniques like Grid Search or Random Search to find the best configuration. To address class imbalance, we may apply strategies such as Synthetic Minority Over-sampling Technique (SMOTE).

NLP-based Information Extraction

Cybersecurity reports contain both structured data, like expected financial losses and incident categories, and unstructured data, such as detailed incident descriptions. This makes it challenging to analyse and use the information effectively. To address this, we propose an NLP-based Information Extraction function. This function analyse those cybersecurity incident details inputted by user using techniques like named entity recognition and keyword extraction to pull out important features and insights. By converting unstructured text into a structured format, our solution will make it easier to query, analyse, and report data. To build the dataset of cyber security incident features, we consider leveraging public datasets including the European Repository of Cyber Incidents (EuRepoC) and Non-Profit Cyber Incident Repository (NPCIR) [27] [28].

5.2 Incident Reporting Aids

Automated Report Generation

The platform provides an automated report-generation feature to standardize the incident report and simplifies the process of reporting. Users only need to fill in the blank, inputting the necessary information about the incident that occurred, our platform will automatically generate the standardized incident report and send it to the government department selected by the user.

Intelligent suggestions for reporting

Under different circumstances, the user may report the incident to multiple government departments at the same time. Our platform includes a feature that will detect the input incident data and suggest the appropriate departments to report to. This feature ensures that no reports are overlooked, directs them to the appropriate authorities, simplifies the reporting process, and enhances compliance.

Real-Time Reviewer Feedback

The real-time feedback feature provided allows reviewers to leave comments and request additional information as needed. This feature will speed up the incident report process by cutting down the back-and-forth of edit requests.

Reporting Guidance

The reporting guidance function leverages incident severity and descriptions in the report to provide guidance on how to report the incident. When generating guidance, it retrieves the rules and guidance applicable to the user’s organization and industry by accessing the information from a knowledge database. Serious incidents may need immediate escalation and reporting to a specific government department, while for minor incidents, our platform will recommend the user to make internal reporting according to the policies of their own organisations.

Knowledge Base Maintenance

Our platform, for the purpose of this project, will maintain an up-to-date knowledge base with a cut-off time 31 March 2025, tentatively. This knowledge base will include all relevant laws, regulations, and guidelines available at that point. To ensure the system remains current, our team will periodically monitor official government and regulatory websites, to identify new laws, guidelines, or updates, if any. These updates will be assessed for relevance and then entered into the knowledge base, and obsolete content will be removed.

5.3 Integration of Decentralized File System

Decentralized Utilization of Decentralized Storage System

For adopting the distributed storage system, our project utilizes IPFS (Inter-Planetary File System). IPFS is a protocol for peer-to-peer file sharing, which was introduced over 10 years ago with the purpose of replacing the location-based protocol such as HTTP. With the adoption of IPFS, our system provides immutable and highly available storage for the users by distributing the stored files to multiple nodes in the network and addressing them with their content [24].

Centralization of data storage can lead to a fatal result of data loss from various unexpected incidents, such as hardware or software breakdown, cyber threats, or even natural disasters.

As all the data is stored in one single endpoint, the loss of data from these incidents cannot be recovered in the worst scenario. Thus, our project utilizes a decentralized file system to store important data in a highly available and secure manner. As the data is saved in distributed nodes across a network by pinning it to multiple endpoints of the network, it can ensure the data is available even if one endpoint is unavailable [25][26].

As IPFS protocol exploits the content of data for addressing and identifies the data with its cryptographic hash, it guarantees integrity of the data making it immutable. Integrity of the incident reports is an important matter for regulators when they check the legal aspects of the reported incidents.

Since IPFS doesn’t provide a functionality to encrypt data for storage, our project proposes employment of RSA encryption which makes use of asymmetric key pairs. For example, the file to be uploaded is encrypted with the recipient’s public key, and the recipient decrypts the file with their private key. This manner ensures that communication between the sender and the recipient is secure.

Asymmetric key Encryption

By implementing RSA (asymmetric key pairs) encryption for sending and receiving the incident reports, the confidentiality of the reports can be guaranteed [27]. To describe, both reporting entity and the regulators have a pair of public and private keys for data encryption and decryption.

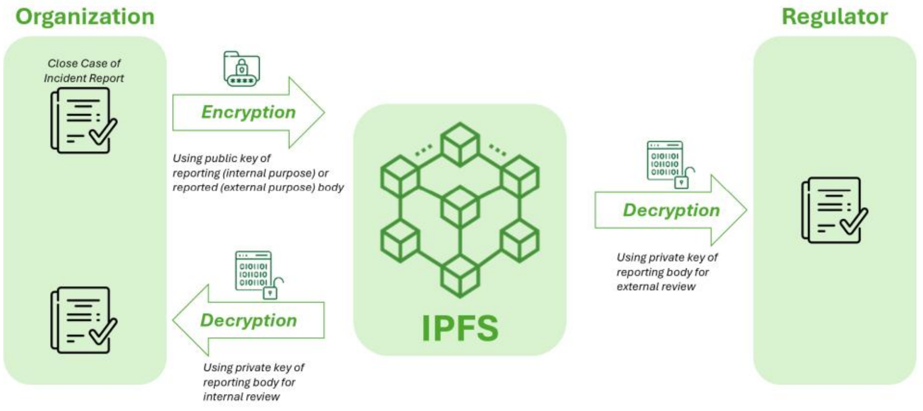
Organization
Close Case of Incident Report
Encryption
Using public key of reporting (internal purpose) or reported (external purpose) body
Decryption
Using private key of reporting body for internal review
IPFS
Decryption
Using private key of reporting body for external review
Regulator

Figure 2: Encrypted File Sharing with IPFS and RSA Key Pairs

Access Control and Data Utilization

Using asymmetric encryption method, access control of the uploaded reports can be implemented as well. For internal use of the report submission, the report is encrypted with the submitting organization’s public key so that only itself can decrypt the report. Similarly, the report is encrypted with the regulator’s public key for regulator to check the compatibility of the report in terms of the regal compliance. This enables access to data only for authorized parties.

6. Reference

[1] Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT). (2025). Hong Kong cyber security outlook 2025: Phishing hits five-year high, vulnerabilities in supply chain and AI content hijacking emerge as key risks. Retrieved from https://www.hkcert.org/press-centre/hkcert-unveils-hong-kong-cyber-security-outlook-2025-phishing-hits-five-year-high-vulnerabilities-in-supply-chain-and-ai-content-hijacking-emerge-as-key-risks-over-half-of-enterprises-fear-cyber-attacks-on-iot-digital-signages

[2] De Los Santos, S. (2016). The impact of an absent national cybersecurity attack reporting policy (Doctoral dissertation, Colorado Technical University). Colorado Technical University.

[3] Briggs, P., Jeske, D., Coventry, L., & Tryfonas, T. (2017). The design of messages to improve cybersecurity incident reporting. In Proceedings of the International Conference on Cybersecurity and Resilience (pp. 3-13). Springer International Publishing.

[4] Agbodoh-Falschau, K. R., & Ravaonorohanta, B. H. (2023). Investigating the influence of governance determinants on reporting cybersecurity incidents to police: Evidence from Canadian organizations’ perspectives. Technology in Society, 74, 102309.

[5] Schmitz-Berndt, S., Bellekens, X., Hindy, H., Onwubiko, C., Erola, A., Rege, A., Jaatun, M. G., & Rosati, P. (2023). Refining the mandatory cybersecurity incident reporting under the NIS directive 2.0: Event types and reporting processes. In Proceedings of the International Conference on Cybersecurity and Resilience (pp. 343-351). Springer.

[6] Muthuswamy, V. V., & Esakki, S. (2024). Impact of cybersecurity and AI-related factors on incident reporting suspicious behaviour and employees' stress: Moderating role of cybersecurity training. International Journal of Cyber Criminology, 18(1), 83-107.

[7] Hong Kong Legislative Council. (2024). Bill document. Hong Kong Special Administrative Region. Retrieved from https://www.legco.gov.hk/yr2024/english/bills/b202412061.pdf

[8] Office of the Privacy Commissioner for Personal Data (PCPD). (n.d.). Guidance note on data breach notification. Retrieved from https://www.pcpd.org.hk//english/resources_centre/publications/files/guidance_note_dbn_e.pdf

[9] Hong Kong Monetary Authority (HKMA). (n.d.). Guideline on Authorization of Digital Banks. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/Guideline_on_Authorization_of_Digital_Banks_eng.pdf

[10] Hong Kong Monetary Authority (HKMA). (n.d.). Guideline on Supervision of Stored Value Facility Licensees. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Guidelines-on-supervision-of-SVF-licensees_Eng.pdf

[11] Hong Kong Monetary Authority (HKMA). (n.d.). Guideline on Oversight of Designated Retail Payment Systems. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Guidelines-on-oversight-of-RPS.pdf

[12] Hong Kong Monetary Authority (HKMA). (2024, November 29). Supervisory Approach on Cyber Risk Management. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20241129e2a1.pdf

[13] Hong Kong Monetary Authority (HKMA). (2024, October 25). Risk Management of E-banking. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20241025e1a1.pdf

[14] Hong Kong Monetary Authority (HKMA). (2010, June 22). Incident response and management procedures. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2010/20100622e1.pdf

[15] Hong Kong Monetary Authority (HKMA). (n.d.). General Principles for Technology Risk Management. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf

[16] Hong Kong Monetary Authority (HKMA). (2022, May 31). Operational Resilience. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220531e1a1.pdf

[17] Hong Kong Monetary Authority (HKMA). (n.d.). Operational Risk Management. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-1.pdf

[18] Hong Kong Monetary Authority (HKMA). (n.d.). Business Continuity Planning. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-2.pdf

[19] Securities and Futures Commission (SFC). (n.d.). Cybersecurity regulations. Retrieved from https://www.sfc.hk/en/Regulatory-functions/Intermediaries/Supervision/Search-regulations-by-topic/Cybersecurity

[20] Securities and Futures Commission (SFC). (n.d.). Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading. Retrieved from https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading

[21] Insurance Authority of Hong Kong (IA). (n.d.). Guideline on Cybersecurity. Retrieved from https://www.ia.org.hk/en/legislative_framework/files/Guideline_on_Cybersecurity_English.pdf

[22] Stiftung Wissenschaft und Politik. (n.d.). European Repository of Cyber Incidents (EuRepoC). Retrieved from https://www.europoc-repository.com

[23] Kean University. (n.d.). Non-Profit Cyber Incident Repository (NPCIR). Retrieved from https://www.kean.edu/npcir

[24] Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. https://arxiv.org/abs/1407.3561v1

[25] Diallo, E. H., Abdallah, R., Dib, M., & Dib, O. (2024). Decentralized Incident Reporting: Mobilizing Urban Communities with Blockchain. Smart Cities 2024, Vol. 7, Pages 2283-2317, 7(4), 2283–2317. https://doi.org/10.3390/SMARTCITIES7040090

[26] Elvas, L. B., Mataloto, B. M., Martins, A. L., & Ferreira, J. C. (2021). Disaster Management in Smart Cities. Smart Cities 2021, Vol. 4, Pages 819-839, 4(2), 819–839. https://doi.org/10.3390/SMARTCITIES4020042

[27] Singh, G., & Supriya, S. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications, 67(19), 33–38. https://doi.org/10.5120/11507-7224

#Milestones

Tasks		***Estimated completion time***	***Estimated number of learning hours***
1	Research • Detailed Study of overall solutions	10 March 2025 (Submission deadline for Detailed Project Proposal)	50
2	Research • Specify the user requirements for each module • Defined detail task list for each module • Develop the website for project progress tracking	17 March 2025	50
3	Development • Data preparation • Frontend website design • Adding role-based access control on the frontend website • Incident input form design	24 March 2025	50
4	Development • NLP Engine • Machine learning model training • Incident severity classification model	30 April 2025	300
5	Development • IPFS integration • Encryption and data security controls • Report generation function • Review and feedback function • Connect to provide AI chatbot	31 May 2025 (Submission deadline for Interim Report and presentation)	400
6	Report • Interim Report preparation including Entire project processes, Challenges and solutions, Testing results analysis and Future work and enhancements	31 May 2025 (Submission deadline for Interim Report and presentation)	100
7	Testing & Evaluation • Testing such as User acceptance testing (UAT) • Defined new task list after the UAT	16 June 2025	30
8	Testing & Evaluation • Necessary adjustments to address the issues found from the testing • AI chatbot accuracy and reliability finetune • Any adjustments on the models	7 July 2025 (Project Progress Updates 4)	300
9	Report • Final Report preparation • Project Website	15 July 2025	120

10	Report • Presentation preparation	End of July 2025	100
			Total: 300*5 = 1500

Deliverables

Items	
1	Incident Severity Classification: The platform features an AI chatbot that helps users classify the severity of cybersecurity incidents and provides real-time regulatory guidance to ensure consistency on incident severity determination.
2	AI-Powered Incident Reporting: It allows users to input key details and instantly create standardized reports for submission to the suggests the appropriate government departments for reporting. During the incident case input stage, reviewers can always provide comments and request for clarifications quickly, making the reporting process smoother and more efficient. Report generation function enables users to generate incident reports with standardized and clear format for both external and internal reporting.
3	Secure Data Storage & Encryption: The platform ensures secure and tamper-proof data storage using IPFS (Inter-Planetary File System), making all records immutable and highly available. Strict access controls and RSA encryption protects incident reports, ensuring that only authorized entities can access sensitive information. This approach guarantees data confidentiality, integrity, and compliance with cybersecurity regulations.
4	Regulatory Compliance & Knowledge Management: The regulatory dashboard keeps organizations updated on the latest cybersecurity laws and compliance requirements. The knowledge base is regularly updated to reflect new regulations, reducing the risk of non-compliance. The platform also integrates AI-powered search (RAG framework), which retrieves and provides the most up-to-date regulatory information when users seek compliance guidance. This ensures accurate and reliable recommendations for cybersecurity reporting.
5	Streamlined Compliance & Efficiency: The platform serves as an all-in-one compliance tool, combining incident classification, reporting, and regulatory tracking in one place. By automating these processes, it helps organizations save time, reduce manual effort, and minimize errors in cybersecurity incident reporting.