#### Coventry University

School of Computing, Engineering and Mathematics



##### Lecturer

##### TSUI CHUN MAN, LEO

### Security (VTC6005CEM) module Coursework1

###### Table of contents

[Introduction 3](#_bookmark0)

[Current situation 3](#_bookmark1)

[Staff management 3](#_bookmark2)

[IT infrastructure 4](#_bookmark3)

[Information security risks 4](#_bookmark4)

[Application security risks 5](#_bookmark5)

[Access control risks 6](#_bookmark6)

[Data leakage or loss issues 6](#_bookmark7)

[IT infrastructure risks 7](#_bookmark8)

[Conclusion 8](#_bookmark9)

[Reference 8](#_bookmark10)

# Introduction

The concept of information security refers to protecting information and its critical elements, such as the hardware and software that store, transmit and use data. Policy, education, training, awareness, and technology are applied to protect information assets' confidentiality, integrity, and availability (Kim & Solomon, 2018). It protects information from unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction.

Today, A computer may keep connecting with billions of computers through the internet, which means the potential hackers may also be billions. Besides this, the awareness of information security is increasing nowadays. Information security issues may cause loss of the organization, customers, revenue, and market share and may also increase their additional costs or damage their reputation (Whitman & Mattord, 2021).

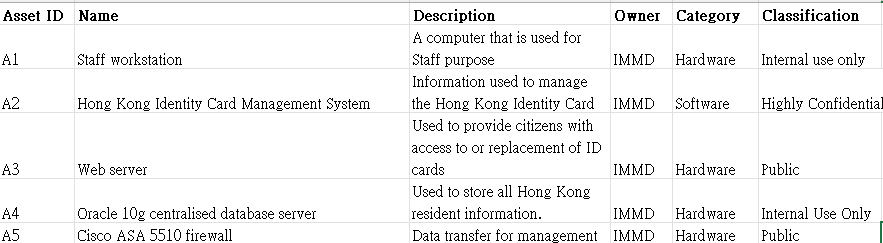
HKID Card Management System allows HK citizens to schedule appointments to apply for their HKID card. Users need to fill in their personal information in the system. This report assesses and evaluates the security risk of this system and its assets and provides possible controls to mitigate those risks.

# Current situation

## Staff management

The staff of the Immigration Department of the Hong Kong Government are divided into three categories Junior staff, Approving staff and System admin to run the HKID card management system. These three types of staff are responsible for different tasks in the HKID Card Management System.

## IT infrastructure



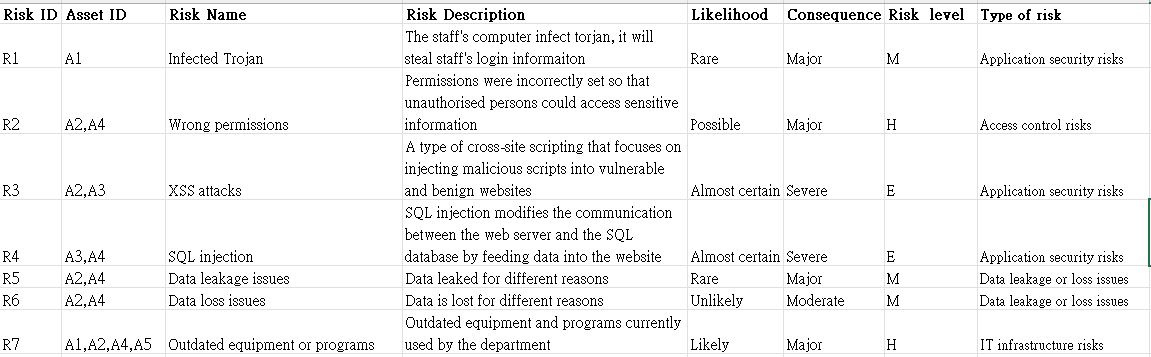
There are currently 100 workstations running windows 8 and windows 10 for internal staff and a window 2016 server running the Hong Kong Identity Card Management System with anti-virus software installed.

The department has a web server deployed in the Demilitarized Zone (DMZ) for providing online booking function of HKID card to the public.

For data storage, the department uses an oracle 10g centralised database server for storing personal data of Hong Kong residents.

A Cisco ASA 5510 firewall is deployed between the gateway and the Internet and uses a default rule set to control incoming and outgoing traffic to the system.

# Information security risks



A risk analysis of the current departmental staff management and IT

infrastructure has identified seven risk possibilities which can be categorised into four types of risk. Application security risks , Access control risks, Data leakage or loss

issues and IT infrastructure risks.

## Application security risks

As the department is responsible for the operation of the HKID Card Management System, which includes the booking of applications or replacement of HKID cards, users are required to input their personal data into the system and are

therefore exposed to application security risks. Common application security issues include SQL injection vulnerabilities and cross-site scripting attacks.

SQL injection is one of the most serious vulnerabilities on the web, ranking as one of the top ten application security risks in the 2013 Open Web Application Security Project (OWASP) (McWhirter et al., 2018). SQL injection allows an attacker to modify the communication between a web server and a SQL database by sending carefully crafted input data to a website in order to perform operations that exceed the application's intended functionality (Erdődi et al., 2021; McWhirter et al., 2018). By

inserting or falsely generating query-related input fields into the system to transform them into SQL queries, attackers can perform remote processes and escalate their privileges on the database management system to extract data from the database that they would not normally have access to. In extreme cases, an attacker could continuously change the database, or even send remote commands to be executed on the web server using a SQL injection vulnerability (Erdődi et al., 2021; McWhirter et al., 2018).

XSS is defined by OWASP as "a type of cross-site scripting that focuses on

injecting malicious scripts into vulnerable and benign websites", Cross-site scripting (XSS) vulnerabilities pose a serious threat to the security of modern applications (Tariq et al., 2021). These malicious scripts can be written in a variety of client-side scripts, namely JavaScript, VBScript and ActionScript, making XSS attacks highly diverse (Malviya et al., 2021). XSS attacks have the potential to cause serious consequences, including personal identity theft, sensitive internal information

leakage, alteration of browser functionality, denial of service attacks, etc (Malviya et al., 2021). These attacks occur when a malicious user uses a web application to execute or send malicious code on another user's computer, and because XSS attacks are so easy to create and difficult to fully mitigate, any application that requires user input is susceptible to XSS attacks (Rodríguez et al., 2020; van Gundy & Chen, 2012).

The corresponding application security controls for common application security risks are relatively easy to implement. Firstly, corresponding input restrictions need to be set for different users in the system input interface to prevent malicious users from entering malicious code scripts in the input interface to confuse the attack, then,

before running the data entered by different users, the data entered by different users needs to be authenticated and filtered for double protection for the system.

## Access control risks

In today's society, data has become an asset of economic significance and it is

important that it is shared securely in order to use it more effectively. Access control plays an important role, and with the increase in insider-induced information security incidents in businesses and government agencies around the world, systems need sensible access control policies or mechanisms that balance information sharing and protection, thereby bringing greater benefits to the application and its users (Helil et al., 2017; Ma et al., 2020).

The department's current access controls may be inadequate, as the current restrictions on access to data by different users are not sufficiently strict and clear, and the fact that most staff have the same access rights can lead to confusion and when problems arise it is difficult to hold people accountable.

On the other hand, both the public and internal staff need access to the database when using the system. Many access privileges are misconfigured and difficult to

detect, making the system vulnerable to attackers using misconfigured access controls to access sensitive information that should not be made public (Truong, 2021).

Application security controls to address issues arising from access control risks

include identifying different users, including internal staff and members of the public, before they can use the system, for example by requiring them to log in and ensuring that different users are using sufficiently strong passwords. In addition to this, The need to ensure a secure access environment and it is necessary to clearly identify the permissions of different accounts and to restrict access to different permissions and ensure that the system does not use the root account unless necessary.

## Data leakage or loss issues

As the department is responsible for the management and storage of Hong Kong Identity Card data, which is personal and private, it is also a highly sought-after target for foreign governments, organised cyber criminals and hacktivists (Andersson et al., 2022).

There is a risk of data leakage or data loss due to misconfiguration by IT professionals, mismanagement by careless staff, malicious users and system errors (Vodopyan, 2021). The reason for this is that in recent years there has been an increase in the number of data leaks and losses caused by insiders because of

misconfigurations by it professionals that have allowed some staff or users to gain unauthorised access to the database, The misconfiguration of user privileges has also increased the likelihood of users taking the wrong actions (Helil et al., 2017; Ma et al., 2020). On the other hand, due to the importance of the data stored in the department, many malicious users may compromise the system through different network attacks such as SQL injection, Trojan horse and XSS attacks to gain access to the data stored in the system.

The consequences of a data leakage or loss could be serious and have a negative impact on the department's reputation (Andersson et al., 2022).

Application security controls to address data leakage and loss include configuring proper database access management to prevent unauthorised users from accessing database data, and using strong encryption for data encryption in the database to reduce the possibility of malicious users gaining access to correct data, thereby reducing the loss of data in the event of a breach or loss.

## IT infrastructure risks

Firstly, Windows 8 operating system for internal staff workstations and the windows 2016 server for the Hong Kong Identity Card System were all experiencing problems. The model number or version is out of date. The need for staff to use obsolete operating systems for their daily work and for the provision of services to the public because the operating systems used by the department are at or near the end of their life cycle.

According to Microsoft, the lifecycle of the Windows 8 operating system ends on 12 January 2016 and no further updates, including bug fixes, feature improvements and security solutions, will be available for the system (Microsoft, n.d). Mainstream support for Windows 2016 Server has also ended and there will be no more non- security updates for Windows 2016 Server, and users will not be able to request product design and feature changes (Microsoft, 2022).

Secondly, the oracle 10g centralised database server equipment used to store information on Hong Kong residents was severely out of date.

According to Oracle's Oracle's Lifetime Support Policy, the oracle 10g centralised database server currently used by the department was withdrawn from support in July 2013 (Oracle, 2022).

In addition, the department's Cisco ASA 5510 firewall, which is deployed at the gateway to the Internet to control traffic and prevent attacks, was also suffering from equipment obsolescence.

According to cisco's End-of-Life Policy, the Cisco ASA 5510 firewall also cease

to be supported on 30 September 2018 (Cisco, 2020).

This makes the systems vulnerable to attack as the operating systems used by the departments are not up to date with the latest security updates and most malware or hackers are able to accurately target older versions of the systems and exploit fixed vulnerabilities in newer versions, making it easy for criminals to break into the department's systems potentially causing service interruptions, sensitive personal

information leaked, loss of reputation and credibility etc (Navarro, 2021). Outdated equipment and software are prone to malfunction, which can lead to slowdowns, restarts and even programs shutting down on their own, these failures make the work of staff difficult and have the potential to cause crashes in the operating system and

loss and corruption of data and this is a serious problem for the public sector(Navarro, 2021).

Application security controls to address IT infrastructure risks focus on the replacement of equipment and systems currently used by the department and system updates to ensure that the equipment used by the department is still supported to avoid problems caused by IT infrastructure risks.

# Conclusion

In conclusion, this report investigates the security risks of the Immigration Department and identifies the various types of security risks and consolidates them

into four types of security risks and provides the corresponding handling methods for these four types of security risks to enable management to understand the system security situation and allocate a budget based on the analysis.

# Reference

Kim, D., & Solomon, M. (2018). *Fundamentals of Information Systems Security*. Jones & Bartlett Learning.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage.

Helil, N., Halik, A., &amp; Rahman, K. (2017). Non-zero-sum cooperative access control game model with User Trust and Permission Risk. Applied Mathematics and Computation, 307, 299–310. https://doi.org/10.1016/j.amc.2017.03.006

Malviya, V. K., Rai, S., & Gupta, A. (2021). Development of web browser prototype

with embedded classification capability for mitigating Cross-Site Scripting attacks. Applied Soft Computing, 102, 106873. <https://doi.org/10.1016/j.asoc.2020.106873>

Ma, K., Yang, G., &amp; Xiang, Y. (2020). RCBAC: A risk-aware content-based access control model for large-scale text data. Journal of Network and Computer Applications, 167, 102733. <https://doi.org/10.1016/j.jnca.2020.102733>

Microsoft. (n.d.). Windows 8 - Microsoft Lifecycle. Microsoft Docs. Retrieved May 16, 2022, from <https://docs.microsoft.com/en-us/lifecycle/products/windows-8>

Microsoft. (2022, April 2). Fixed Lifecycle Policy - Microsoft Lifecycle. Microsoft Docs. Retrieved May 16, 2022, from [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/lifecycle/policies/fixed)

[us/lifecycle/policies/fixed](https://docs.microsoft.com/en-us/lifecycle/policies/fixed)

Navarro, P. (2021, June 10). Top 5 risks of using outdated software in your company.

Business 2 Community. Retrieved May 16, 2022, from

[https://www.business2community.com/tech-gadgets/top-5-risks-of-using-outdated-](https://www.business2community.com/tech-gadgets/top-5-risks-of-using-outdated-software-in-your-company-02412185) [software-in-your-company-02412185](https://www.business2community.com/tech-gadgets/top-5-risks-of-using-outdated-software-in-your-company-02412185)

Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166, 106960. <https://doi.org/10.1016/j.comnet.2019.106960>

Tariq, I., Sindhu, M. A., Abbasi, R. A., Khattak, A. S., Maqbool, O., & Siddiqui, G. F. (2021). Resolving cross-site scripting attacks through genetic algorithm and

reinforcement learning. Expert Systems with Applications, 168, 114386. <https://doi.org/10.1016/j.eswa.2020.114386>

Truong, J. (2021, November 4). 5 Common Identity and Access Management Security Risks. HackerNoon. Retrieved May 17, 2022, from [https://hackernoon.com/5-](https://hackernoon.com/5-common-identity-and-access-management-security-risks) [common-identity-and-access-management-security-risks](https://hackernoon.com/5-common-identity-and-access-management-security-risks)

van Gundy, M., & Chen, H. (2012). Noncespaces: Using randomization to defeat cross-site scripting attacks. Computers & Security, 31(4), 612–628.

<https://doi.org/10.1016/j.cose.2011.12.004>

von Solms, R., &amp; van Niekerk, J. (2013). From information security to cyber security. Computers &amp; Security, 38, 97–102.

<https://doi.org/10.1016/j.cose.2013.04.004>

Vodopyan, E. (2021, February 10). What Is Data Leakage? Netwrix. Retrieved May 17, 2022, from https://blog.netwrix.com/2021/02/10/data-leakage/