Regtech Adoption Practice Guide

Issue #5: Cyber Risk Management

January 2022

HONG KONG MONETARY AUTHORITY
香港金融管理局

KPMG

Disclaimer

Regtech Adoption Practice Guide is a publication published by the Hong Kong Monetary Authority (HKMA). It should be noted that the sole purpose of this publication is to provide Authorized Institutions (banks) with information on the latest regulatory technology (Regtech) developments. The HKMA does not endorse any use cases, solutions and/or implementation guidance described in this adoption practice guide. If a bank intends to adopt a particular solution or implementation, it should undertake its own due diligence to ensure that the technology or approach is suitable for its circumstances.

Contents

1 Introduction **4**

1.1 Background 4

1.2 Purpose 5

2 Cyber Risk Management **6**

2.1 Key challenges 6

2.2 How can Cyber Risk Management Regtech solutions help? 7

2.3 Key considerations when adopting Cyber Risk Management Regtech solutions 8

3 Implementation guidance **10**

3.1 Formulate a cross-functional implementation team 10

3.2 Business case analysis 11

3.3 Vendor evaluation 11

3.4 Proof of concept testing 12

3.5 Ongoing measures 13

4 Regtech use cases **14**

4.1 Use Case #1 Securing Containers – Changing landscape of containers 14

4.2 Use Case #2 Implementation of data protection solution against remote working scenario 16

A Appendix **17**

A.1 Acknowledgements 17

A.2 Relevant regulatory requirements and/or guidance 17

01 Introduction

1.1 Background

The value of Regtech in banking is coming to the fore in Hong Kong, offering clear benefits to banks, customers and regulators. In November 2020, the HKMA released a two-year roadmap to promote Regtech adoption in Hong Kong, as laid out in a White Paper titled "Transforming Risk Management and Compliance: Harnessing the Power of Regtech".[1] The White Paper identified 16 recommendations across five core areas to accelerate the further adoption of Regtech in Hong Kong.

The White Paper acknowledges that since 2019, the HKMA published a series of "Regtech Watch" newsletters, introducing banks to Regtech use cases on the adoption of innovative technology to enhance risk management and regulatory compliance. The banks interviewed for the White Paper cited these newsletters as a valuable source of information and guidance, especially the actual or potential Regtech use cases that have been rolled out or are being explored in Hong Kong or globally.

The White Paper identified 26 specific application areas of Regtech that can benefit banks. There are significant opportunities and a strong desire from the industry for the HKMA to develop and issue "Regtech Adoption Practice Guides" around these application areas.

As a successor, this Regtech Adoption Practice Guide (Guide) series builds on the "Regtech Watch" newsletters to include common industry challenges, guidance on implementation and examples of what others have done successfully to overcome adoption barriers. The Guides are to supplement other ongoing HKMA initiatives such as the Banking Made Easy initiative, Fintech Supervisory Sandbox and the Fintech Supervisory Chatroom. Ultimately, the Guides should enhance the sharing of experience related to Regtech implementation in the industry, which will help further drive Regtech adoption in Hong Kong.

This fifth Guide of the series focuses on Cyber Risk Management Regtech solutions. The inaugural Regtech Watch[2] newsletter, which promotes Regtech usage in

[1] Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf

[2] Regtech Watch Issue No.1, HKMA (November 2019), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191112e1a1.pdf

Hong Kong through sharing observed Regtech use cases with the industry, focused on Cyber Risk Management. This Guide will provide more guidance on the implementation of these solutions. As banks become increasingly digital, it is important to implement strong cybersecurity controls to protect banks from cyberattacks. With the successful launch of the Cybersecurity Fortification Initiative 2.0 in 2020[3], many banks have identified security control enhancement opportunities that could be fulfilled by implementing Cyber Risk Management Regtech solutions, or are considering upgrading existing solutions.

1.2 Purpose

The purpose of this Guide is to provide an overview of Cyber Risk Management Regtech solutions, outline the common challenges observed regarding Cyber Risk Management solution adoption, and share information on how others have addressed the challenges to successfully adopt Cyber Risk Management Regtech solutions in their organisations. This Guide follows the outline below:

1 **Explain how Regtech solutions can be used to address cyber risk**

- Outline the key challenges that Hong Kong-based banks are currently facing in relation to cyber risk management
- Illustrate the benefits of Regtech solutions to manage cyber risk
- Describe the key risks/considerations when adopting Regtech solutions for cyber risk

2 **Provide practical implementation guidance to banks on the adoption of Cyber Risk Management Regtech solutions**

- Outline the key considerations to Cyber Risk Management Regtech implementation
- Provide insights on what others have done to achieve successful Regtech adoption

3 **Share use cases on the adoption of Regtech solutions to manage cyber risk**

- Describe the cyber risk challenges faced by banks and how the Regtech solution helped to resolve these challenges
- Outline the key learnings from successful Cyber Risk Management Regtech implementation, from both the bank and/or the Regtech provider's perspectives

[3] Cybersecurity Fortification Initiative 2.0, HKMA (November 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1.pdf

02 Cyber Risk Management

Banks are increasingly leveraging technology to drive business growth and enhance operational efficiency. Traditionally, operational requirements have been fulfilled by on-premises systems, deployed locally on a bank's own computing infrastructure. The acceleration of technology development is driving the incorporation of established and/ or emerging technologies (e.g. Cloud) into banks' business and operating models. Benefits include service flexibility, enhanced customer experience, and the ability to efficiently manage risk and compliance.

As organisations begin to adopt new technologies and new practices in their business operations, cyber risk has become an increasingly relevant concern faced by banks, as they collect and possess substantial amounts of confidential financial information and sensitive personal information, etc. This is due to the potential financial gains that perpetrators can obtain from a successful exploitation. However, beyond financial impacts, cyber incidents could also lead to reputational damage and business interruptions, which could greatly impact public trust and confidence towards the banking industry.

2.1 Key challenges

The key cyber risk challenges that banks currently face are:

Difficulties in keeping pace with rapidly changing cyber risk

- With the introduction of more customer service channels and digital services (e.g. mobile banking) empowered by different technologies including artificial intelligence, Cloud, 5G, Internet of Things, etc., the attack surface has increased substantially and there are more opportunities for hackers to attack.

- Accelerated development lifecycles increase the potential threat of releasing new digital services with unresolved vulnerabilities. Tight development schedules may also create difficulties for organisations to properly assess cyber risk comprehensively.

Increased usage of third-party services and open-source components

- Banks have become increasingly reliant on third-party services due to their frictionless application and services. Without proper scrutiny, there is potential for hackers to leverage vulnerabilities or control deficiencies to attack banks' systems and infrastructure.

- Additionally, as third-party components or services may be open-source, hackers might be able to understand their implementation and use it to their advantage when they plan to attack banks' systems.

Ineffective cybersecurity awareness programme

- The human factor often represents the "weakest link" in cybersecurity and human error or carelessness is often attributed as the top vulnerability for a cyberattack. Insider threat also has a much higher impact given employees can easily access valuable confidential information and have system privileges.

- As hackers opt for increasingly sophisticated and elaborate attack scenarios, the identification and awareness of such situations may pose a challenge to the untrained and unsuspecting employee. The awareness training may not be frequent enough to draw employee attention to the latest phishing or social engineering tricks.

- Lack of awareness in cybersecurity-related matters among members of the Board or related committees could also add to the risk faced by their respective organisations. Cyber risks arising from adoption of new technologies are often underestimated. Providing regular updates on cyber risk and cybersecurity awareness programme will help improve awareness among senior members.

Limited customer awareness

- Despite ongoing efforts to educate and alert the general public on the prevalence and dangers of fraudulent messages (e.g. phishing emails and other scams), hackers' attack methods are becoming increasingly sophisticated and therefore customers are still falling prey to these attacks.

2.2 How can Cyber Risk Management Regtech solutions help?

Below are some key areas where banks will benefit from adopting Cyber Risk Management Regtech solutions:

- **Early identification of potential cyber attack attempts:** User entity and behaviour analytics solutions learn behaviour patterns of the end user at a granular level and use this as an anchor to determine what is considered as "normal" behaviour. This then helps banks to detect novel attacks and insider threats. These solutions can be integrated with a company's security monitoring systems and notify security teams through immediate alerts once uncommon behaviour is detected. The correlation of attack patterns from other resources (e.g. network firewall) can then be aggregated to enable more precise detection of attack patterns.

- **Prioritise vulnerability remediation:** Banks need to conduct vulnerability scans more frequently across different infrastructure and remediate the findings from the scan result in a timely manner. Vulnerability management solutions help banks prioritise vulnerability remediation by taking into consideration multiple sources of intelligence and severity. Banks can utilise multiple vulnerability scanning tools to identify vulnerabilities in their IT environment across operating systems, applications, databases and networking devices. Banks have to develop configuration and patch management plans to address these security defects. Given the volume of vulnerabilities and the number of machines to rectify, a vulnerability management solution can support banks with automating vulnerability management process, determining impact and remediation priorities, and assigning respective findings automatically to a corresponding service owner and tracking the remediation actions.

- **Respond to cyber attack:** Organisations are using security information and event management (SIEM) solutions that leverages Artificial Intelligence and Machine Learning to automatically identify and take action to neutralise **cyber attacks**. This allows a security team to proactively update the rules, and detect and prevent a similar kind of attack. Also banks can subscribe to third-party threat intelligence feeds to get the latest information on attacks including zero-day attacks. These solutions automatically generate incident reports and each task that requires action is

assigned to the responsible team member. This also helps banks to prioritise incidents based on risk and urgency levels so that the security team can respond accordingly. Furthermore, breach response analysis is created to capture all relevant information for forensic analysis. This helps conduct root cause analysis in the environment and identify controls gaps, and implement the respective controls to mitigate the risks.

- **Cyber risk assessment:** As discussed in a previous Regtech Adoption Practice Guide Issue #3 on Governance, Risk and Compliance (GRC)[4], GRC Regtech solutions can enhance risk assessment and data collection process, help banks meet their compliance obligation and demonstrate the compliance status.

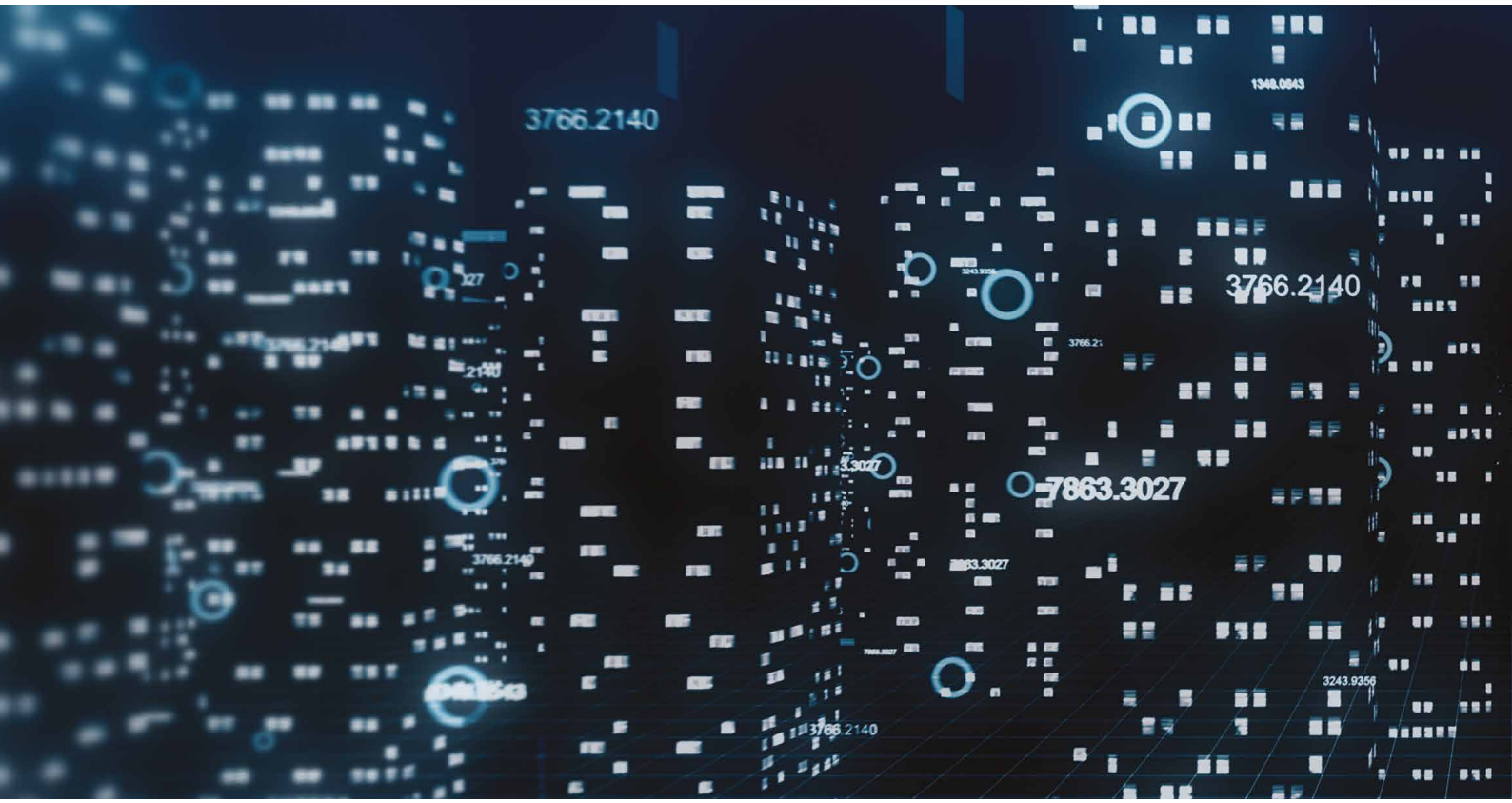
- **Data protection:** Data loss prevention (DLP) solutions assist banks in securing business sensitive data and intellectual property from accidental or malicious breaches by preventing and detecting the transmission of sensitive information. DLP provides visibility and control over data regardless of whether it is stored in a laptop/desktop, in transit over the enterprise network, residing in storage systems, or sent to Cloud services. DLP promotes regulatory compliance and business risk reduction through policy enforcement. Meanwhile, a Cloud Access Security Broker (CASB)[5] is a Cloud security control that allows banks to extend their security policies to Cloud services so that they remain in control of information being stored in Cloud services and can implement consistent preventive and detective controls across various type of cloud services provided by different solution providers.

2.3 Key considerations when adopting Cyber Risk Management Regtech solutions

As banks undergo digital transformation journeys and develop multi-layer defence strategies, it is crucial for banks to ensure that Cyber Risk Management Regtech solutions can work together with existing technology and security architecture of a bank. Determining what, how and when to implement are major considerations. Without proper planning, the risk of failure remains high, and may even compromise the security posture of the organisation.

[4] Regtech Adoption Practice Guide Issue #3: Governance, Risk and Compliance, HKMA (September 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210927e1a1.pdf

[5] CASB is a Cloud-based or on-premises software or hardware that serve as an intermediary between users and Cloud services to enforce security policies on access to Cloud services



Below are some key factors that banks should consider when adopting Cyber Risk Management Regtech solutions.

- **Cybersecurity programme and roadmap:** without a holistic cybersecurity programme, management might take a more conservative approach in addressing individual security issues by upgrading existing security infrastructure only. It may be difficult to justify the adoption of a Cyber Risk Management Regtech solution, which would be able to provide a holistic security benefit across various security issues. It is also worth planning ahead for the adoption in the security roadmap, allowing the security architecture team sufficient time to research and evaluate solutions.

- **Cost and benefit analysis:** While the adoption of new Cyber Risk Management Regtech solutions may be considered as an additional cost, the benefit of adoption should be thoughtfully justified across various factors. These would include a reduction of effort in cyber incident handling and security operation, lower cost in maintaining traditional security appliances, and the reduction of attrition in security teams.

- **Compatibility with legacy systems and integration with existing security solutions:** Many banks still possess legacy systems that are tightly coupled to existing infrastructure and are difficult to change. While some Cyber Risk Management Regtech solutions may not be designed to work with those technologies, a bank should still consider the benefit a solution may have in protecting other systems, as well as the bank's digitalisation roadmap in upgrading the legacy systems. Meanwhile, security solutions seldom function by themselves and often require integrations with other security solutions. Banks should consider how a Regtech solution can work together with existing solutions, automate controls by system integrations and reduce the reliance on manual security operation.

- **People and processes:** In addition to technology considerations, people and processes should also be reviewed to ensure successful Cyber Risk Management Regtech solutions implementation. For people, this could include training the existing security operation team to configure and use the solutions and support the operational processes. For processes, this could include implementing processes to respond to alerts from the solutions, and setting up review procedures to ensure the solutions are working as intended to prevent or detect security events.

03 Implementation guidance

Banks generally have a cybersecurity framework in place which covers people, processes and technology, and a system acquisition and development lifecycle to manage the technology solution implementation process. This section does not intend to provide an exhaustive guide to implementation of a Cyber Risk Management Regtech solution. Instead, it outlines specific implementation considerations.

3.1 Formulate a cross-functional implementation team

Cyber risk is a business issue and the implementation team should consist of individuals from different functional areas, such as IT security, enterprise architect, IT operations, infrastructure, technology risk and compliance, and relevant stakeholders from the business units. Having involvement from a representative of each function from the beginning can ensure that a chosen solution will bring the best possible benefits to the bank as a whole.

The following are guidelines that should be adopted when selecting members to form a cross-functional team

1. A Cyber Risk Management Regtech solution commonly provides security benefits at endpoint, network, application, database and storage which may be managed by different teams within a bank. Banks should consider individuals from these respective functions. The respective functional team can provide the factors that need to be taken into consideration when choosing a solution that benefits the bank and addresses the risks.

2. For solutions that collect or process personal information, the bank's designated officer should be consulted and the privacy impact assessment process should be followed to ensure that personal data processing activities are in compliance with privacy regulations and expectations from the data subjects.

3. For solutions that protect the bank against insider threats, business heads may be included if the solution will help monitor and evaluate employee behaviour. The business heads can help evaluate the solution and also formulate the operation process required to follow up on investigations if there are alerts generated from the solution. For example, there might be configurations required in the solution that can notify the business heads or line management of the suspicious activities.

3.2 Business case analysis

Before banks evaluate a particular solution, the bank should analyse the business case with the following questions:

- What are the drivers for implementing a particular solution?
- What are the relevant risks and issues that could be addressed by the solution?
- Are there other beneficial outcomes of the solution, e.g. reduce operation overhead and manual activities?
- Which part of operation/which department would benefit the most from Regtech adoption?
- Does the bank have buy-in from the stakeholders?
- How will the bank use the solution?

3.3 Vendor evaluation

There are many different solutions provided by various types of vendors. It is common for banks to adopt external solutions to build a comprehensive security architecture. When ready to adopt a Cyber Risk Management Regtech solution, a bank should evaluate the solutions available in the market and perform due diligence on the tools and vendors to choose the most suitable solution.

Some of the key criteria to be considered when choosing a Regtech solution are the skillset required, as well as capabilities and ongoing support of the Regtech solution providers.

1. Banks can refer to industry analyst reports to understand the security solutions available for specific use cases and understand the leaders and new players in the market specific to the region. These reports cover information about the vendors, services offered and their capabilities in this space, which can help shortlist a few vendors.

2. There are Regtech solutions available in the market which might not be listed in analyst reports. Banks can utilise vendor evaluation questionnaires to assess the capabilities of those vendors against a set of criteria which include financial stability of the vendor, any named customers for reference, product features etc.

3. As security solutions usually work best when they integrate well with existing IT infrastructure and other security tools, the bank should evaluate whether the solution can protect a relevant type of IT assets of the bank and also provide integration with other security tools (e.g. threat intelligence platform, privileged access management solution, SIEM, IT service management, etc.) The solution should provide API capability to integrate with the respective target platforms or if required there should be an option to customise the solution for integration.

4. The cyber threat landscape is evolving every day and the solution should be able to be updated to address emerging threat. The ability and mechanism to update the solution should be considered.

5. For Cyber Risk Management Regtech solutions, the bank should assess the ability of the solution provider to continuously improve the product, and adapt to the continually changing regulations and technological environment. The solution vendor should be asked to demonstrate their ability with historical version enhancements and a product enhancement roadmap.

The following are some other criteria to evaluate vendors' capabilities:

- Products or services – Their technical capability and product maturity in this space
- Financial – The financial health of a company, number of customers and indicator of business success (e.g. increase in number of customers or geographical presence)
- Pricing – Pricing options and flexibility
- Customer experience – Quality of the service experience
- Operations – Ability to meet commitments and service level agreements

3.4 Proof of concept testing

It is essential to test the solutions to evaluate whether the solutions achieve their security objective. The bank may also discover additional functionalities and benefits in this process.

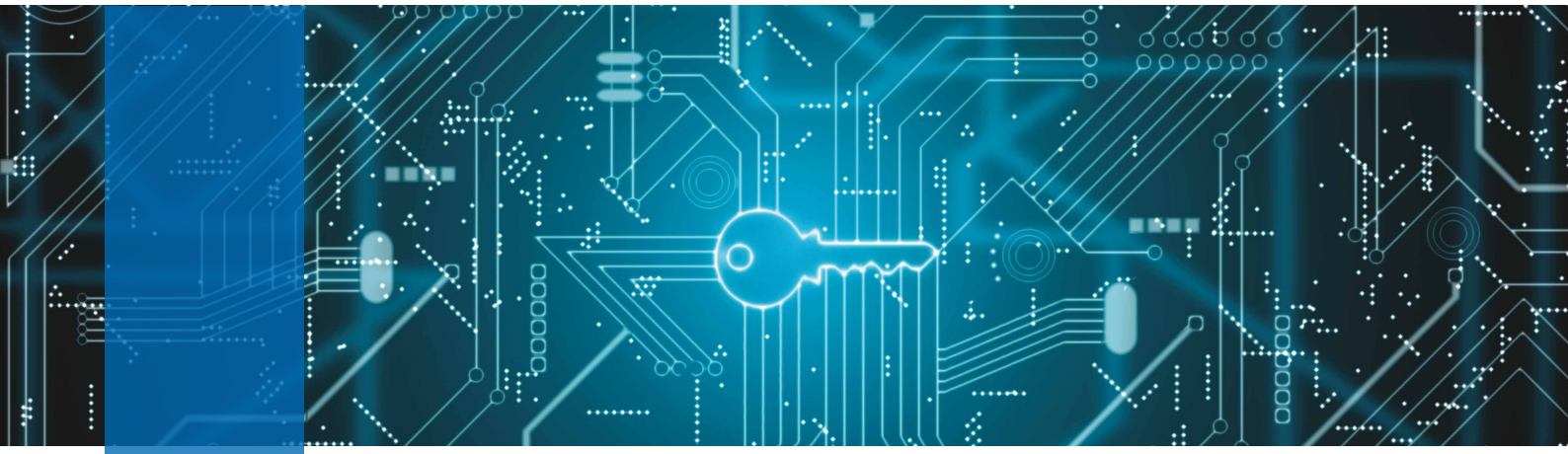
When testing a Cyber Risk Management Regtech solution, a sufficient testing period should be negotiated with the solution provider to demonstrate the security benefits. It is especially relevant for solutions that use machine learning and require the development of a normal baseline situation, which is then used to send alerts if it detects any changes to the baseline as a result of new threats.

The bank should develop a testing approach with various user test cases and define the expected outcome. This will help the bank assess the effectiveness of the solution against various scenarios. When the bank executes the use cases and analyses the outcome, it should review the findings and the rate of false positives, which would require further calibration of the system.

3.5 Ongoing measures

Security operation processes should be updated with the steps required to operate the solution, including the security alerts generated from the new solution.

Banks should also incorporate a regular review of the solution into the bank's regular configuration review exercise, to review the appropriateness of current configurations. The ongoing monitoring can also validate accuracy and desirability of the solution outputs.



04 Regtech use cases

4.1 Use Case #1 Securing Containers – Changing landscape of containers

4.1.1 Challenge

Banks continually aim to adopt new technology solutions as part of the business and technology strategies. The agile speed and scalability requirements to deliver innovative products, services and technology applications have driven banks to leverage container technology[6].

Containers have many technology benefits for banks to meet their service requirements, but there are also potential security risks to be addressed. As application development in container environment often includes the use of third-party software that may have vulnerabilities, containers can be susceptible to rogue processes opening the door to unauthorised access to other container images. The container image itself may also include vulnerabilities. Developers may also accidentally bring in additional security issues when implementing containers and using pre-built external open-source codes.

Existing traditional infrastructure security controls in an on-premises environment do not provide an adequate level of protection when used with container technology. There are several challenges that the security team needs to consider, including detecting vulnerabilities at an early stage of the system development lifecycle, implementing a process to scan the container image periodically and also detecting vulnerabilities in the containers post implementation. Developers may also accidentally bring in additional security issues when implementing containers and using pre-built external open-source codes.

Thus banks need to select and deploy security technologies that support the adoption of a containerised environment. These technologies typically provide the following security features: image scanning, runtime security, vulnerability scanning, threat detection, compliance monitoring and incident response.

[6] Container technology is adopted commonly in Cloud computing to package an application and its dependencies into standardised units, which are isolated from other processes, and therefore the application can run more quickly and reliably in different computing environment.

4.1.2 Approach

Stage 1: Identifying requirements

A bank identified that there was a requirement to implement a container security solution to meet their technology requirements. The bank established a project team with members from different functions:

- Infrastructure – responsible for defining the process for deployment of containers
- IT security – responsible for defining the security requirements for the containers
- Risk and compliance – responsible for validating the container security posture in complying with the bank's information security policy
- Application support team – responsible for mitigating the vulnerabilities identified in the container
- Project management – managed the implementation and provide updates to management

Stage 2: Evaluating the vendor

The security team developed a set of security requirements and mapped these against existing solutions in the market. An analyst report was leveraged to shortlist the container security solutions. The bank issued a request for proposal to the vendors, followed by an evaluation of each vendor's response against criteria defined by the bank. A selected container security vendor was then appointed, which conducted a pilot ahead of full implementation.

Stage 3: Pilot and full implementation

The project team set up a testing environment to review the functionality of the container security solution. The set of criteria defined by the bank were evaluated and the outcome was documented. Some of the use cases that were validated as part of the pilot included:

- Security of the container deployment
- Monitoring of container network traffic
- Security of applications within the container
- Detection of vulnerabilities of the containers
- Monitoring of container utilisation
- Integration with existing security monitoring solutions and processes

The use cases' outcomes and the lessons learnt from the pilot implementation were discussed. The lessons learnt were then taken on board for the full implementation.

4.1.3 Key learnings

Establish security operation process for managing containers: Since there were different teams involved in managing the containers, the roles and responsibilities of each team must be defined. The bank established a process with clearly defined RACI (responsible, accountable, consulted, informed) matrix, and discussed and agreed on the responsibilities of the respective teams.

Identify opportunity to automate the vulnerability management process: The container security solution had been integrated with the existing vulnerability management solution, so that the bank could have a holistic view of vulnerabilities in the environment including the containers. Notifications were also automatically sent to respective teams for prioritisation and remediation. This helped the bank monitor, track and remediate the vulnerabilities at an agreed frequency.

Subscribe to new detection capability from a vendor based on threat intelligence: As the threat landscape of container technology is constantly changing, the solution allowed the bank to systematically adopt new detection cases based on new threat intelligence. The solution assessed the compliance status of a container against industry standards and alerts were triggered when there were any deviations from the normal baseline. The alert was relayed by the container security solution to existing security monitoring solution.

4.2 Use Case #2 Implementation of data protection solution against remote working scenario

4.2.1 Challenge

The Covid-19 pandemic has changed the way of working and has required banks to rapidly adapt their working models. The pandemic has also made the job of embedding, monitoring and enforcing data protection controls much

harder both at a technical and governance level. Working from home is getting more common due to the pandemic, and bank staff must access sensitive information to perform their duties remotely.

While banks have implemented controls to mitigate against phishing, malware, and data leakage via public internet at staff's computer, there are challenges to mitigate against unauthorised disclosure of confidential information when staff is not physically present in office premises. There are deterrent controls within an office (e.g. CCTV and presence of other staff). When staff is working from home remotely, the physical environment is not being monitored and that may pose data leakage risks if an unauthorised person tries to use the staff's computer or take a photo of the computer screen.

4.2.2 Approach

A bank implemented a cyber risk management solution to detect a potential data breach event. The solution leveraged emerging technologies including machine learning, facial recognition, object detection, Blockchain and natural language processing to detect malicious user behaviour in front of the computer. The solution utilised the camera of the computer to recognise the facial image of the authorised user. When an unauthorised person tried to use the computer, or when someone tried to capture the screen with a smartphone or camera, the solution will automatically lock down the computer to protect the bank's confidential information. The event records were logged on a Blockchain so the evidence was preserved for further investigation.

The bank had implemented this data protection solution since staff and contractors must access confidential information remotely. The solution deployed a software agent to laptops and monitoring policies were pushed to the laptops for enforcement from a centralised management console. The solution used the laptop camera to detect malicious behaviour and locked down the laptop. An alert was triggered and sent to the management console where the security operation team can further investigate. This helped prevent leakage of confidential information when users are working remotely. By leveraging this AI-powered compliance automation solution, the bank reduced its risk and gained confidence in its remote work program.

The bank conducted the solution by phases based on analyses of the inherent risk profile of the user groups. The devices of contractors and customer-facing staff were covered initially. Change management steps were also introduced to make staff beware of the new security monitoring in place.

4.2.3 Key success factors

Key factors that contribute to the successful implementation of the solution:

- **Define targeted use cases for solid return on investment:** The business case mapped out the priorities regarding data protection. The solution started with monitoring high-risk activities, reducing false positives, and creating more efficient ongoing operation processes.

- **Conduct proof of concept (POC):** The project team agreed on the use cases to be tested and conducted POC to validate the business requirements. In the process, the bank appointed an in-house testing team to work alongside the vendor to provide suggestions to fine-tune the detection criteria and user experience.

- **Configure the solution:** Different institutions have different business and user activities, and thus are different in the criteria needed to detect suspicious activities and threats. The solution was adjusted based on the unique end-user environment and usage by staff members.

- **Ongoing testing:** With the continuous collection of new data from the monitoring process, the solution support team can validate and retrain the model. The team can evaluate and understand the expected data for normal business operations to resolve data issues and conduct more systematic validation checks.

The above-mentioned use cases demonstrated how banks could leverage Regtech solutions to adopt new technology and adapt to ever-changing working environment while managing their cyber risk appetite. In both cases, the Regtech solution was implemented from a functional or risk-based approach with established ongoing operational controls, which contributed to their successful implementation.

A Appendix

A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Paul McSheaffrey, Brian Cheung, Stanley Sum, James O'Callaghan, editor Philip Wiggenraad

A.2 Relevant regulatory requirements and/or guidance

Name	Link
HKMA Supervisory Policy Manual – General Principles for Technology Risk Management (TM-G-1)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf
HKMA Cybersecurity Fortification Initiative 2.0 (CFI)	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1.pdf https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1a1.pdf
HKMA Circular – "Customer Data Protection"	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf