Regtech Adoption Practice Guide

Issue #3: Governance, Risk and Compliance

September 2021

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

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.

Regtech solutions have emerged to improve the effectiveness and efficiency of risk management and compliance activities through harnessing new technologies

[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

such as Cloud, Artificial Intelligence, and Blockchain. The first Guide in this series outlined the benefits of Cloud-based Regtech solutions. The third Guide of the series is on "Governance, Risk and Compliance" (GRC) Regtech solutions, a large number of which utilise Cloud-based platforms. Increased regulatory expectations, coupled with the increasing need for risk and compliance departments to balance costs and effectiveness, are driving a number of banks to seek to implement GRC Regtech solutions or consider upgrading existing solutions.

1.2 Purpose

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

1 **Explain how Regtech solutions can be used to support GRC**

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

2 **Provide practical implementation guidance to banks on the adoption of GRC Regtech solutions**

- Outline the key components of GRC Regtech implementation, including the types and methods of GRC Regtech solution 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 GRC**

- Describe the GRC challenges faced by a bank and how the Regtech solution helped to resolve these challenges
- Outline the key learnings from successful GRC Regtech implementation, from both the bank and the Regtech provider's perspectives

02 Governance, Risk and Compliance

2.1 Key challenges

GRC is a framework of people, processes and technologies to gather and aggregate risk information across an organisation in a manner that focuses management's attention and action in a timely manner.

Successful GRC strategies maximise the effectiveness of an organisation's control framework while driving consistency, transparency and efficiency across the three lines of defence. GRC is an important enterprise-wide responsibility especially for financial institutions, given increasing regulatory scrutiny and complex compliance requirements. Widely publicised regulatory breach cases and the corresponding regulators' attention place a significant demand on organisations to demonstrate whether appropriate controls have been established to meet relevant regulatory obligations.

The key GRC challenges that banks currently face are:

Escalating cost of compliance

- Increasing regulatory requirements are addressed through manual processes that are not scalable, efficient or effective

- To keep obligations registers up-to-date, banks often need to establish operations, compliance and technology teams to perform regular scanning and monitoring of regulators' websites to access published materials and derive regulatory obligations. A manual process is resource intensive and costly to maintain. Processes that involve manually updating a spreadsheet may not be sustainable, complete or accurate.

- The data transformational exercises required to produce aggregated views of compliance across different functions or businesses could be extremely costly and resource intensive.

Lack of business and risk transparency

- There is a need for clear visualisation of risks and insights into different business units and functions, as well as a desire for more timely risk information.

- Compliance efforts could also be duplicated or missing across business units and functions, providing fragmented governance and compliance risk management.

Inadequate risk ownership

- There is a need for better risk culture and risk ownership to improve risk management and compliance across the three lines of defence.

- It is often challenging to identify the right risk owners in an organisation in a timely manner. It may not be practical to track risk and obligation owners using manual processes. The lack of appropriately defined roles and responsibilities will ultimately affect the ability to monitor and address compliance requirements.

Cumbersome and ineffective risk reporting

- Current traditional solutions are unable to efficiently provide data analytics, data visualisation, data insights and business analysis.

- Traditional GRC frameworks do not provide a consolidated view for senior management to assess regulatory requirements compliance, and hinder the ability to spot areas that require management attention or remediation.

- Each business unit may have varying tools and process standards to extract data for compliance assessments. The complexity of siloed data also further complicates the data aggregation and evidence gathering processes as there may be internal data sharing constraints between business units, which may cause inconsistency in documentation.

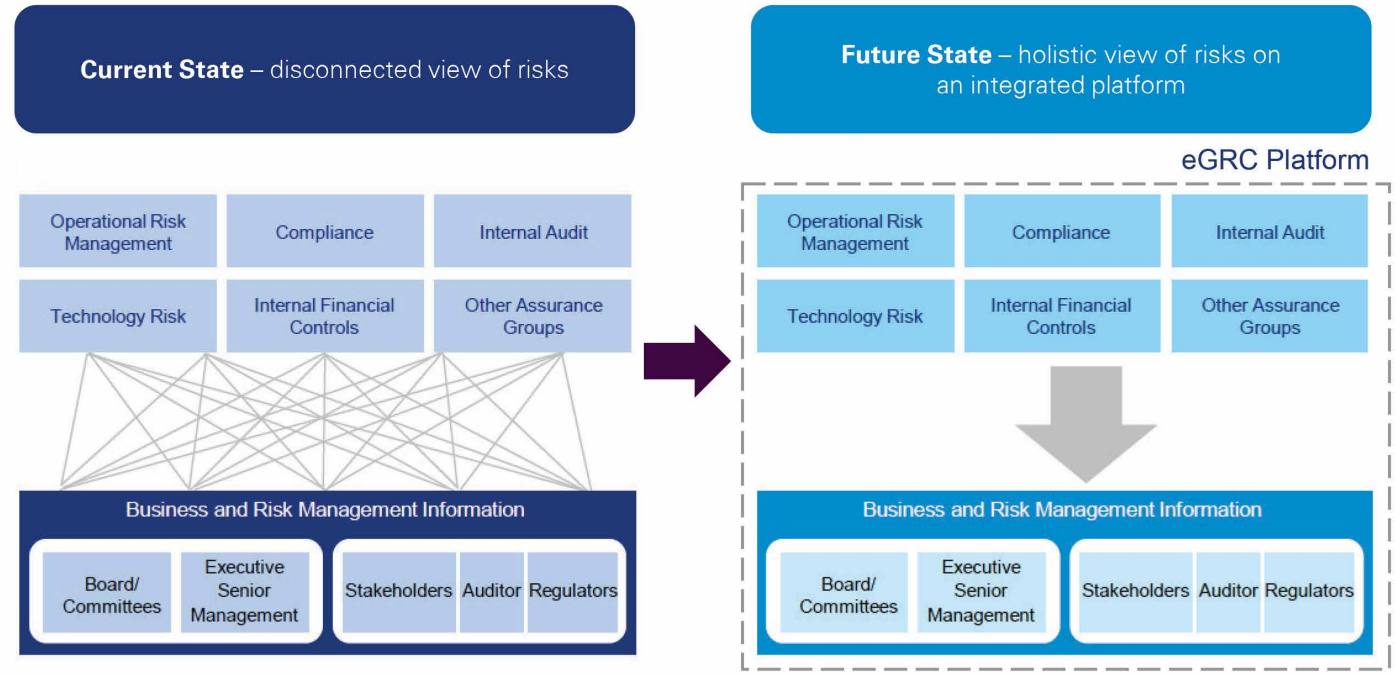
2.2 How can GRC Regtech solutions help?

2.2.1 Electronic-GRC

An electronic-GRC (eGRC) platform is an integrated technology platform that captures a holistic view of regulatory obligations, compliance, events and controls to form a single source of truth. GRC platforms operate across an entity, whether it is a legal entity, business unit or a wider group. A successful GRC platform drives consistency, transparency and efficiency across the three lines of defence in order to maximise the effectiveness of an organisation's control framework.

As illustrated in Figure 1, many organisations have a disconnected view of enterprise and business unit risks whereby these are handled independently of each other and via different channels of communication. An eGRC platform can solve this issue, providing a single source of truth and a reporting channel for all issues relating to GRC across an organisation in a way that prompts management's attention and remediation in a timely manner.

Figure 1: Current and future state of GRC under an eGRC platform



Source: KPMG

The key benefits of using an eGRC platform are:

- **Enhances visibility across the business:** By integrating data into one platform, advanced analytics can be performed to provide senior management with an aggregated dashboard overview of all risks/compliance obligations within the defined entity while tracking the implementation of controls to comply with those obligations.

- **Promotes risk ownership:** Electronic tagging via an eGRC platform solution can map the incoming regulatory obligations to the policies, procedures, controls and owners according to pre-defined business rules. Maker/checker and approval workflow automation eliminates resource-intensive processes such as identifying the right owner, email communications and filing. Automating the push of obligations to the correct process or control owners can also reduce the risk of missing actions.

- **Reduces costs:** Checklists and templates standardise communication and action. Automation standardises and facilitates monitoring and testing of controls and processes across the three lines of defence. Cost reduction can be achieved via reduction in bespoke processes and documentation through controls rationalisation and integration of data sources for analysis and reporting.

- **Improves data and analytics:** A GRC platform consolidates information from across the organisation – including quantitative, qualitative, predictive and historical factors – which can be used for analysis and to provide insights. The platform can produce tailored reports that are customisable and readily available for download and use, and risk dashboards with scenarios and thematic analyses, enabling management to identify and take pre-emptive measures against potential emerging areas of non-compliance.

2.2.2 Horizon scanning and regulatory obligations management

The HKMA's White Paper identified the Regtech opportunities that can provide immediate benefits for financial institutions including regulatory horizon scanning and inventory of compliance obligations for compliance obligations management, which are key components of the regulatory compliance lifecycle (see Figure 2 below). This section mainly introduces readers to regulatory horizon scanning and obligations management. In addition to the aforementioned Regtech application areas, other related risk management Regtech solutions also exist to manage organisational GRC.

Figure 2: Regulatory compliance lifecycle

Source: KPMG

To achieve compliance with regulatory obligations, a bank needs to first understand the relevant regulatory obligations across different business units in their organisation. Relevant requirements need to be ingested on a periodic basis and then interpreted for application to the business. Interpretation largely relies on having the right subject matter experts to provide guidance on the associated risks, impact and ownership. The next step is to ensure appropriate policies and procedures are in place to tackle regulatory compliance, including the design and operation of appropriate controls. Finally, the bank should establish monitoring mechanisms that are aligned with regulations and internal policies. This includes reviewing and testing the controls and processes periodically to provide assurance that they are operating effectively. The use of a technology-enabled solution should then allow senior management to monitor compliance through exception reporting or dashboards showing the current state of compliance with regulatory obligations. A breakdown in any of these elements may lead to regulatory compliance failure.

Approximately one new regulatory alert is generated every nine minutes across the world.[2] Given the increasing volume and complexity of regulatory requirements, it has become difficult to manage regulatory requirements using traditional manual methods. The initial challenge is to capture and identify new regulations. While the major Hong Kong regulators have prescribed ways to push out regulations and announcements (primarily via e-mail or letters), the breadth of regulations can extend to various other regulatory bodies, exchanges, self-regulatory organisations and international standard setters. The format (e.g. supervisory policy manual, Q&A, FAQ, risk event, and enforcement) and level of detail (e.g principle-based, rules-based or best practice) may vary, making it even more difficult to interpret and capture. Standardised machine-readable regulations are still in the development stage at this point in time. There is also increasing concern over management of cross-border regulations and other regulations that a Hong Kong branch or subsidiary may need to follow in their parent jurisdictions, and Hong Kong regulations that an overseas parent bank needs to comply with.

One future development is machine-readable regulations, which are regulations designed for ingestion directly by machines rather than humans.[3] Machine-readable content is not a new concept, although its application to the financial industry is currently limited. Machine-readable regulations would enable regulators to release and update regulations as frequently as required in a machine-readable format, enabling their automatic incorporation to obligations registers and GRC systems, and reducing errors

[2] 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
[3] Regtech in the Smart Banking Era – A Supervisor's Perspective, HKMA, https://www.hkma.gov.hk/eng/news-and-media/speeches/2018/09/20180927-2/

and manual effort. This would, however, increase the importance of Regtech adoption to ensure integration with the machine-readable regulations.

A view into the future: With the advancement of Artificial Intelligence, including Natural Language Processing (NLP), and perhaps the standardisation of regulatory pronouncements, possibly through machine-readable regulations, there could come a day where there is straight-through-processing of new regulations to policies and controls. A newly issued regulation would be pre-tagged for relevance and, via horizon scanning and integration into eGRC, would automatically be fed into a workflow for further human or machine intervention. Artificial Intelligence can create simple language obligations or the system can leverage machine-readable regulations. Existing policies and procedures would be pre-tagged or associated with regulations such that changes to regulations would trigger a need to modify such policies and procedures. Associated controls could be pre-defined and modified by way of a pre-defined control library linked to regulator definitions or expectations. Automated controls testing would be adjusted to reflect updated controls and outputs would automatically feed up to management reports – a utopian control environment.

2.3 Key considerations when adopting GRC Regtech solutions

As GRC Regtech solutions provide financial institutions with efficient platforms for managing aggregated risk and compliance, it is crucial for financial institutions to ensure that the people and processes are also supporting the digital transformation. Determining how and what to implement is also a major consideration. Without proper planning, the risk of failure remains high.

Below are some key factors that financial institutions should consider when adopting GRC Regtech solutions:

- **Vision and planning:** Successful GRC Regtech solutions implementation will require careful planning from the outset to think through all of the components and key activities required. These may include whether or not business processes are ready for automation and the estimated effort and time required for preparation and testing, including standardising current processes

and migration from the existing "fragmented" approach to the consolidated GRC platform. Standardisation, including controls rationalisation and processes improvement, may require substantial effort in order to fit the GRC system to prevent the transfer of bad processes. Challenges with articulating the GRC vision to a GRC vendor during the planning stage may result in scope limitations, budget overruns and implementation delays. It is therefore imperative to complete a comprehensive planning stage before implementing GRC Regtech solutions. Furthermore, planning must take place organisation-wide rather than in silos to reduce the risk of introducing standalone solutions across the organisation that may require additional effort to integrate in the future.

- **The extent of solution customisation:** GRC platforms can vary in cost based on the degree of customisation and features required. The solution scope needs to be properly defined and controlled throughout the project. Changes in requirements and over-customisation will lead to budget overruns and prolonged implementation timelines. Given the rapidly changing technology environment and continuously evolving business and regulatory requirements, the scalability of the solution needs to be considered.

- **People and processes:** In addition to technology considerations, people and processes should also be reviewed to ensure successful GRC Regtech solutions implementation. For people, this could include hiring GRC Regtech solutions experts and training existing employees to use the solutions and support the processes. For processes, this could include adjusting processes to ensure data is captured digitally for integration with GRC systems, and ensuring processes are in place to respond to alerts and prompts from the GRC systems themselves. Regional coordination and consideration are also important, even for smaller local banks operating in Hong Kong, as they may be subject to overseas regulations such as General Data Protection Regulation (GDPR) and Foreign Account Tax Compliance Act (FATCA).

03 Implementation guidance

GRC Regtech solutions can provide many benefits, but the implementation of such large-scale projects must be carefully considered and planned in order for the benefits to be fully realised. As a pre-requisite for Regtech adoption, banks should understand the process of introducing GRC solutions to their organisation, key areas of concern at each stage and how to navigate through them.

This section outlines some key components of GRC Regtech implementation. This section is not an exhaustive guide. Rather, it provides observations on what others have done to successfully implement GRC Regtech solutions.

3.1 Define state of maturity and the GRC vision

For banks seeking to adopt GRC Regtech solutions, the first step is to evaluate the current state of GRC maturity, and then define its overall GRC vision.

3.1.1 Maturity analysis

Hong Kong-based banks are at different stages of their GRC journey. Below we outline the common stages of Regtech adoption based on observations in the banking industry.

Stage 1: Characterised by applying manual processes in fulfilling regulatory compliance obligations and managing the organisation's GRC. Regulatory compliance solutions are implemented solely for the purpose of meeting compliance obligations and are not aligned to business benefits. Some examples include:

- Heavy reliance on manual processes complemented by a spreadsheet to perform data entry, updates and ad hoc analysis.
- Data exchange processes (e.g. document sharing/ emailing) are mostly manual and require extensive human resources.

- Enterprise-wide visualisation is difficult to achieve, and reporting across units varies in quality, depth and consistency.

Stage 2: Characterised by limited use of technology in fulfilling regulatory compliance obligations and managing the organisation's GRC. Regulatory compliance solutions are implemented mostly for meeting compliance obligations with few business benefits. Some examples include:

- Reliance on heavy manual processes complemented by spreadsheet macros or Robotic Process Automation (RPA) to perform data analysis.

- Adoption of some GRC platform modules to manage GRC (e.g. policy management, control testing documentation, and incident management).

- Limited data exchange processes (e.g. a bank may have an off-the-shelf auto-feed for regulatory requirements, but it is not linked to the GRC platform).

Stage 3: Characterised by adoption of Regtech solutions to maintain regulatory compliance obligations and manage GRC. Regulatory compliance brings some business benefits, but they cannot be formally measured/quantified. Some examples include:

- Overall management information (e.g. results of control testing or instances of non-compliance) is technology-enabled, but some manual effort remains.

- Approval processes are system-managed, that is the designated approvers are based on a centrally controlled authorisation matrix.

- Automatic data exchange between systems with limited manual intervention (e.g. direct auto-feed of obligations register into the GRC platform).

- Multiple business units have access to the GRC platform allowing for data interchange with each other, driving consistency.

Stage 4: Characterised by extensive and integrated use of Regtech solutions across multiple business units to manage enterprise regulatory compliance obligations. Risk management and regulatory compliance completely align with business strategy and deliver tangible business benefits, with measurable outcomes and continuous improvements. Some examples include:

- Business can make decisions rapidly to respond to events and meet regulatory requirements using real-time data.

- Integrated systems with built-in approval and escalation processes.

- Data follows the Extract, Load, Transform (ELT) process for seamless data exchange between systems and allows for big data analytics via data lake.

- Organisations can view their GRC obligations at an enterprise level.

- GRC Regtech solutions are used to manage enterprise regulatory compliance obligations and beyond, including third-party risk management, business continuity planning, internal audit, financial controls management, IT governance and model risk.

By assessing their current state of GRC solution maturity, organisations will be able to pinpoint different challenges and respond to regulatory changes. Organisations should continuously assess and improve their GRC framework to achieve greater benefits.

3.1.2 Define the GRC vision

A bank's GRC vision should align with the overall company vision and therefore should involve stakeholders from the C-level executives, business unit leaders and the technology team. The involvement of different stakeholders at this stage helps to provide a holistic assessment of the risks and key objectives across the organisation. In Figure 3 below, some of the key questions that organisations should ask to define their GRC vision are outlined.

Figure 3 – Key questions to define an organisation's GRC vision

To define the GRC vision, the organisation shall be clear on the following:

1	**What are the drivers for GRC implementation in the organisation?**
2	**What are the short and long-term visions for GRC?**
3	**How will you measure and monitor key milestones and return on investment for GRC?**
4	**Is there adequate stakeholder buy-in and resources available to support implementation?**
5	**Is your GRC framework ready to be facilitated through a GRC system? If not, what is the plan to get the organisation ready?**

Source: KPMG

3.2 Understanding your GRC needs

Based on the bank's maturity assessment and GRC vision, the bank can determine the size and scale of their GRC transformation. eGRC platforms are largely component-based, utilising a modular approach to build a holistic platform. For smaller-sized banks facing budget and resource constraints, key risk management and compliance modules can be prioritised (for example "risk and control management", "regulatory obligations management"), with other modules gradually added to the platform via a phased approach. For large-sized banks featuring multiple siloed business units, an integrated eGRC platform can be adopted to manage the bank's overall GRC. eGRC modules can encompass:

- **Risk and control management:** include but not limited to controls definition and reporting. Periodic controls review to foresee/pre-empt risks and prompt necessary actions to manage/mitigate the risks to acceptable levels.
- **Regulatory obligations management:** break down regulations into a catalogue of requirements, business impacts, and actionable tasks.
- **Issue and incident management:** establish standardised processes to identify, investigate, and remediate issues.
- **Policy management:** manage policy creation, approval, communication, refresh, retention, and structured policy adherence across the organisation.
- **Financial controls management:** manage assessments, testing, and certification process to standardise and manage compliance.
- **Business continuity management:** document and manage business continuity and recovery.
- **Third-party/vendor risk management:** assess the risks associated with vendors, and manage third-party risks and compliance.

- **IT risk management:** document governance structure, guiding principles, roles and responsibilities to manage IT risks.

- **Internal controls:** control framework documentation, internal control management, and automation.

- **Internal audit:** integrate self-assessment and assurance programme (e.g. internal audit report and internal audit testing programmes) with the overall GRC platform.

- **Model risk management:** support creation and maintenance of a model inventory including workflow for periodic testing. Provide reporting, tools, and decision support to manage risks associated with the misuse of models involved in decision making.

Most organisations are a long way from implementing all the eGRC platform modules above, with most banks focussing on "risk and control management" and "regulatory obligations management". Some of the areas where Regtech solutions could bring the greatest benefits from the two aforementioned modules are highlighted below. Banks can use the summary below to identify areas of need and assess the potential benefits that a Regtech solution can bring.

- **Data-driven analysis and speed of reporting**

  eGRC platforms have excelled in recent years with the proliferation of more powerful visualisations and analytics, achieved through the consolidation of data obtained through establishing a data lake or system integration such as via Application Programming Interfaces (APIs). Readers can refer to Regtech Adoption Practice Guide Issue #1 on Cloud-based Regtech solutions[4] to see more guidance on system integration via APIs. Once the data "nut" is cracked, the GRC tools could have the ability to provide a powerful feedback loop whereby control results, events and issues can be fed back to different parts of the organisation for thematic analysis and improve risks and controls definitions, control testing protocols and escalations. Advanced visualisations and dashboards help management quickly identify hot spots in the organisation that may require attention and supervision. Data-driven analysis allows for thematic and scenario-based analysis.

- **Controls automation and workflow via RPA**

  RPA can be applied to streamline processes, remove repetitive manual intervention and improve processes such as controls testing. RPA is built to configure rule-based software bots in order to automate business activities. RPA takes over repetitive tasks, reducing the chance of human errors and freeing up manpower for other activities that require higher levels of cognitive ability. Workflow tools can assist in the management of policy and procedure updates, including the update and approval processes as well as the dissemination and attestation of policies and procedures.

- **Horizon scanning**

  Horizon scanning takes on the challenge of sourcing the regulatory requirements and enables end-to-end monitoring of news and regulations to keep entities informed with the latest regulatory developments. News, events and relevant updates related to regulatory changes across the globe can be automatically integrated and curated into topics or themes, which helps organisations track, assess and further process the information into other insightful analysis. Horizon scanning drives periodic assessment of the GRC environment and forces impact assessments to be conducted on existing processes, policies and procedures, reducing risks of non-compliance.

The current functionality of different horizon scanning Regtech solutions includes:

- Uniform Resource Locator (URL) link/repost of regulatory posting, news, events, and fines

- Summary of regulatory requirements (Artificial Intelligence or human-driven)

- Legal/expert interpretation, and definition of obligations

- Tagging of the regulatory requirement to types of business/product/risk taxonomy

- Search function capability – by topic/theme, risk, and jurisdiction

- Calendar functionality – regulatory implementation timelines

[4] Regtech Adoption Practice Guide Issue #1: Cloud-based Regtech solutions, HKMA (June 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2021/20210617e5a1.pdf

- Language translation
- API/integration into eGRC platform

Horizon scanning utilises Artificial Intelligence, including NLP, and auto-tagging to intake requirements from a list of applicable regulators, extract relevant compliance requirements, and automatically tag, for example, to an organisation's policies, risks, controls and specific business units. Horizon scanning enables continuous assessment of changes to regulatory requirements relevant to the business and the resulting impact on existing processes, thus reducing risks of delayed compliance or non-compliance.

- **Regulatory Obligations Register**

  Using horizon scanning to identify a regulatory requirement is only the first step to achieving regulatory compliance. The establishment and maintenance of a regulatory obligations register that ultimately plugs into an eGRC system is critical to achieve regulatory compliance. An obligations register should have the following functionalities:

  – Centralised repository of regulatory requirements including link/copy of pronouncement, summary/ definition of the requirement (i.e. obligation) including expert interpretation, and categorisation of the obligation (e.g. regulator, type of regulation, regulatory theme, and applicability). Absent expert interpretation, it can only be considered a repository of regulatory requirements.

  – Ability to compare and contrast changes in regulations.

  – Mapping of obligations to businesses/products.

  The translation of regulatory requirements to an obligations register at this point, relies largely on human subject matter experts. However, with the expansion of machine-readable regulations (see **section 2.2.2**) and advancements in Artificial Intelligence, including NLP, the future may provide greater standardisation of risk identification and application relevance. Various risk advisory consultants and law firms also currently provide curated summaries, relevant market cases and further categorisation of underlying risks and considerations to improve risk management. Integrated eGRC platforms will have a front-end module to capture regulatory requirements and develop an obligations inventory.

  Some of the key benefits of using an obligations register are summarised below:

  – **Structured and organised:** ability to maintain single source of truth, and enable compliance risk management based on a complete and up-to-date regulatory obligations database. Allows understanding of interdependencies between different regulatory requirements and avoids duplication of – or unnecessary – compliance effort.

  – **Cost-effective:** replaces manual and resource-intensive processes required to search, study, consolidate and map regulatory requirements.

  – **Enables accountability:** clear categorisation of compliance requirements and roles and responsibilities within the business. Once linked to the GRC platform, the actions can then be cascaded to the action owners.

  – **Reportable action:** Regtech solutions often provide a dashboard view on the state of compliance obligations and any changes or updates. Reports can be configured for the varying needs of users and to pinpoint required actions.

  With regulators increasingly focusing on ensuring that banks have a comprehensive view on obligations, the importance of – and requirement for – an obligations register is expected to increase.

3.3 Procuring suitable GRC solutions

A bank should evaluate and align its maturity and GRC vision with the most suitable GRC solutions. The key factors to aid the evaluation are:

Appetite for investment: Depending on the solution, consider whether a phased implementation is preferred or a "Big-bang" transformation.

Expected GRC use case: Consider whether the solution is for a specific business case/process, or enterprise-wide implementation with standardisation across different business units.

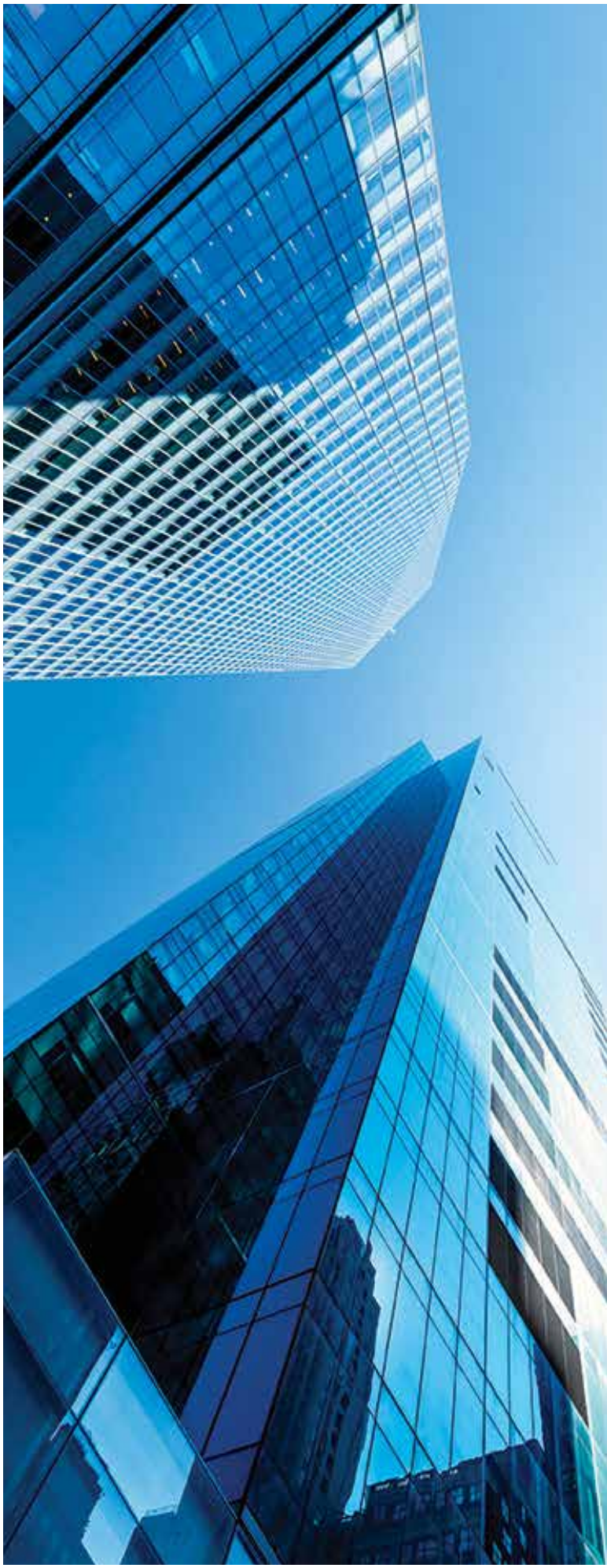
Where information is standardised or processes/risks have uniformity, for example capturing third-party risk information, off-the-shelf GRC Regtech solutions may be suitable. Although business users may initially perceive their processes as unique, it is suggested to conduct workshops in order to understand the processes and whether there is possibility to optimise the process and align with off-the-shelf solutions which may be more cost-effective. It is also helpful to identify business cases where automation can provide a more standardised and efficient approach.

Ability to tailor the GRC solution: Consider whether the solution needs to be fully customised due to unique needs, or if the processes and requirements can be met by an off-the-shelf solution. If there is a need for customisation, establish a prioritisation framework to evaluate system functions and capabilities against the user requirements. It could be advantageous to work with experienced vendors that can support a bank's GRC maturity roadmap by recommending practical and usable customised features with the ability to future-proof and scale up.

Required integration with other systems: Consider whether the solution requires integration with other systems (e.g. enterprise resource planning, human resources, and existing risk management systems), or exists as a standalone system with manual upload of other systems' data.

Resources to support implementation: Consider which part of the solution will be delivered in-house, and assess the level of involvement available/required from business users and IT. Consider if outsourcing to an implementation partner is required.

Future-proofing the solution: Consider choosing solution providers that leverage new technology trends and continuously use the latest trends to improve the Regtech solutions. The use of Artificial Intelligence, including machine learning, and other predictive analysis can help banks to identify new risks in regulatory changes, as well as irregularities in the GRC framework. Banks should also seek long-term commitment from solution providers that would help them envision their GRC roadmap and continue to support beyond deployment.



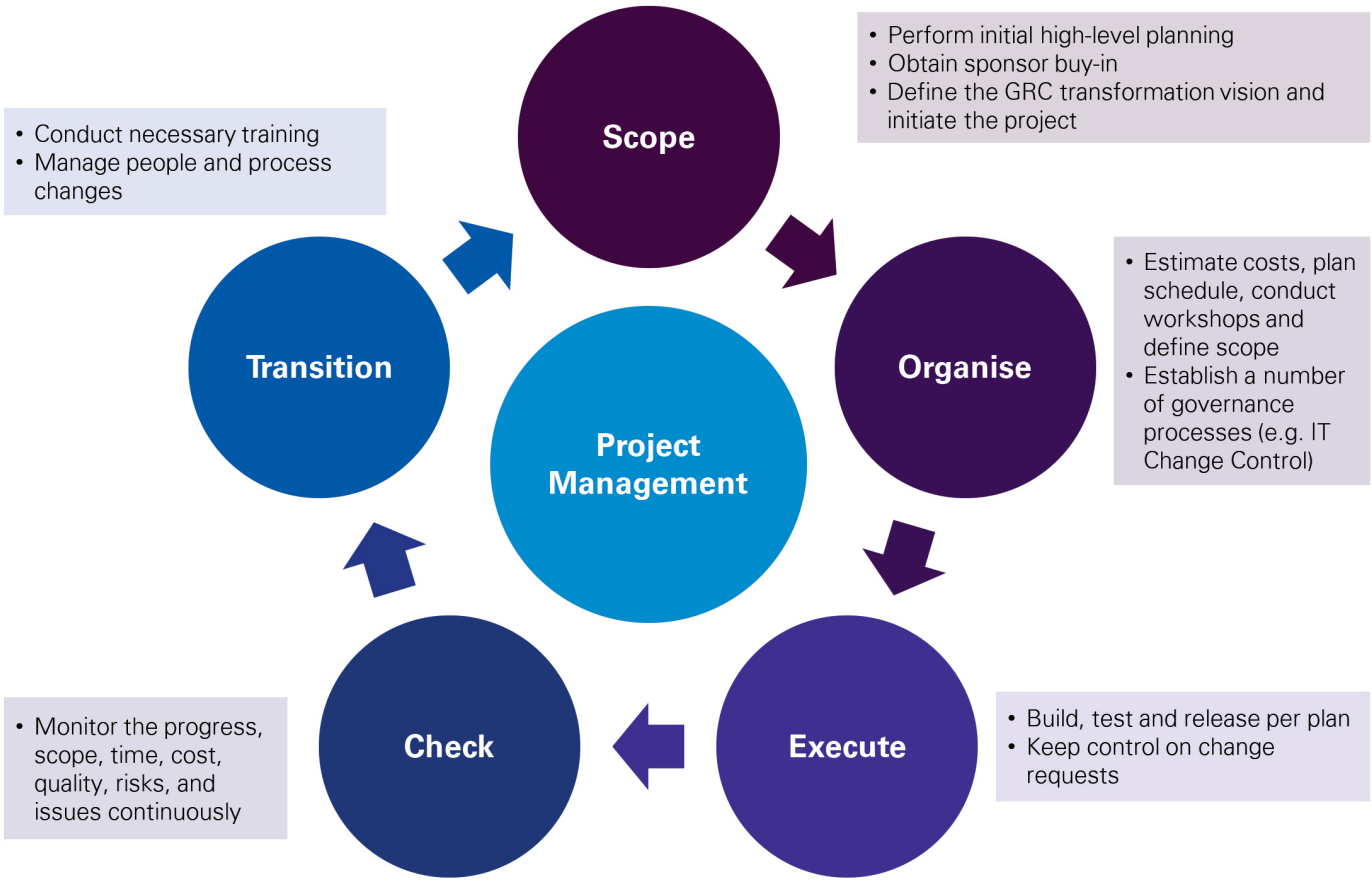
3.4 eGRC project implementation

Project governance and IT change control

Given the size of GRC transformations, it is essential to establish and follow a robust and structured project management framework and governance model. In response to the key considerations outlined in **section 2.3**, robust and strictly followed project management governance enables scope and budget control, which is essential to successful implementation. All five elements of project management (namely scope, organise, execute, check and transition) should cover the entire GRC implementation project lifecycle to guide delivery towards the objective and scope (Figure 4).[5] The project management team is required to oversee and manage the project cost, scope and schedule, facilitate effective dependency and risk management, provide delivery quality assurance as well as manage coordination and communication across different stakeholders.

Implementation of an enterprise-wide GRC platform solution requires input, review and authorisation from various stakeholders across the entity. This inevitably causes requests for customisation, and conflicting requirements and prioritisation. The establishment of proper IT change control procedures enables the identification, tracking evaluation, approval and execution of all change requests. With a structured project management framework in place, the possibility of budget and timeline overruns can be minimised, enabling delivery of the GRC vision.

Figure 4: Sample Project Management lifecycle



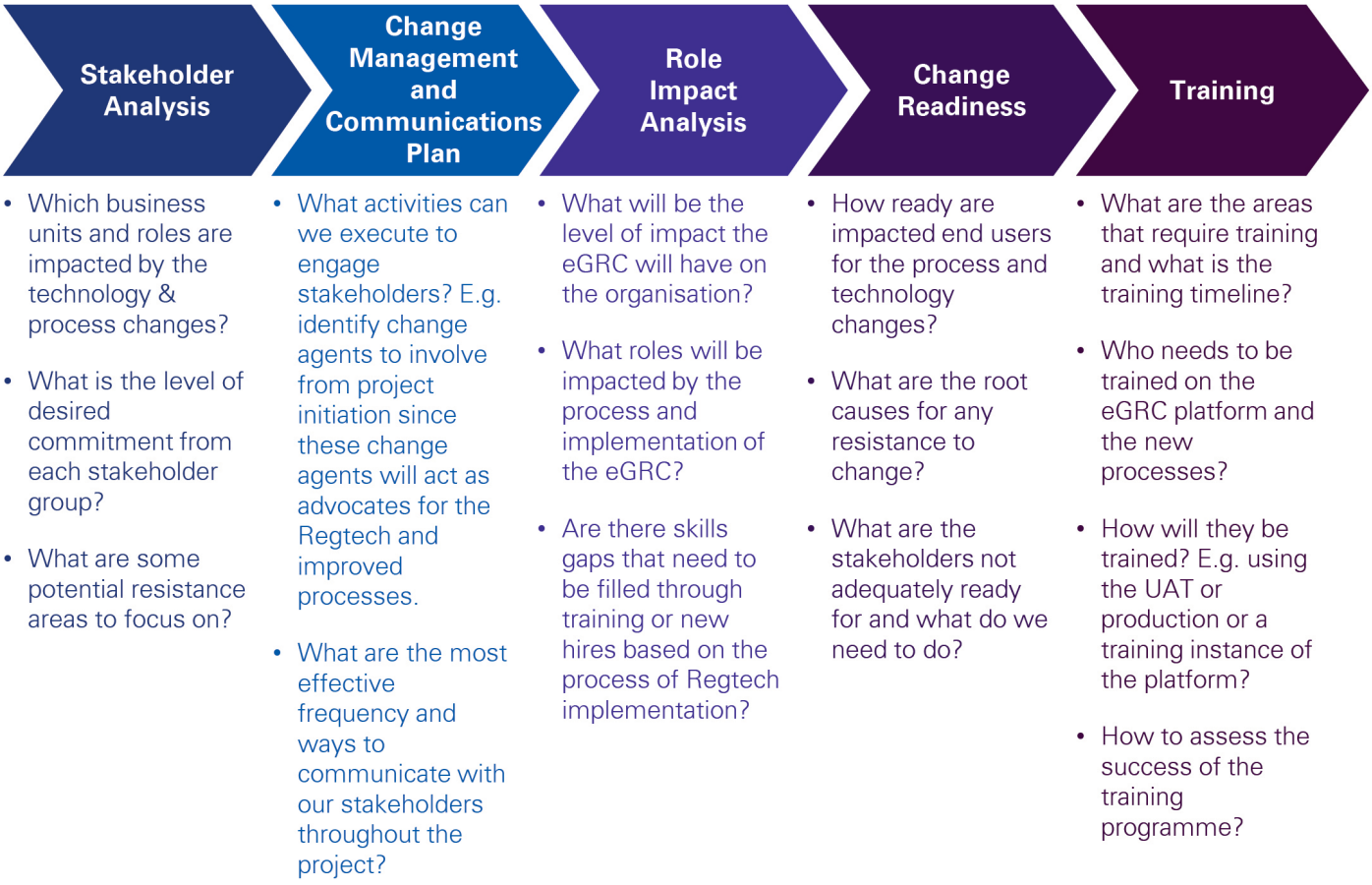
Source: KPMG

[5] What is Project Management?, Project Management Institute, Inc. (n.d.). https://www.pmi.org/about/learn-about-pmi/what-is-project-management

Managing people and process changes

As a GRC transformation programme affects various people and processes across the organisation, **section 2.3** outlined the importance of people and process change to support Regtech implementation. While project management focuses on governing overall project status and progress, change management focuses on the intersection of people and processes to support the deliverable. As various change management activities often happen in parallel throughout the project lifecycle, a detailed change management approach (Figure 5) helps clearly establish the goals of the change initiative, lay down the steps to achieve the goals, and ensure consistency with the overall project plan.

Figure 5: Sample Change Management Framework



Source: KPMG

Adoption of a structured approach provides a smooth transition of individuals, teams and organisations from a current state to a desired future state employing a GRC solution. Following the change management roadmap, processes will be revised to support the new Regtech solution (e.g. adjusting processes to ensure data is captured digitally for integration with the new system). The implementation of GRC Regtech solutions require subject matter experts to provide comprehensive training in relation to the technology itself, application to day-to-day operations and changes in processes.

04 Regtech use cases

4.1 Use Case #1 – Regulatory tracking and obligations management tool

4.1.1 Challenge

As part of its annual audit, a bank received an observation from its external auditors saying that it lacked a comprehensive centralised record of regulations and was unable to demonstrate how it was able to identify relevant rules and regulations and appropriately capture obligations in its policies and procedures.

Similar to this bank, many financial institutions face the following challenges:

- The volume of regulations is large and can be further exacerbated for global banks that may also need to comply with international or head office requirements. Cross-border activity also adds another layer of complexity.
- Manual or static regulation mapping needs to be updated as regulations or business lines change. This is largely unmanageable without technology.
- Regulations require subject matter experts to translate into obligations for an institution to comply with.
- Policies and procedures should be updated on a timely basis and reflect the latest obligations while identifying appropriate controls. Policies and procedures need to be communicated to affected parties with positive attestation.
- Regulatory non-compliance can cause both reputational and financial damage.

4.1.2 Approach

As part of a comprehensive Cloud-based eGRC offering, the bank engaged a Regtech solution provider to provide a regulatory change management tool which features regulatory tracking, obligations management, and policy and procedures workflow and attestation.

The Regtech solution provider, through a partnership with a regulatory horizon scanning data provider, provided access to the latest regulatory changes issued by governments, regulators and other third parties across different jurisdictions. The data provider also prepared curated regulatory summaries along with hyperlinks to the posted regulations. Regulatory summaries were compiled by a team of compliance and legal professionals at the data provider, filtering out extraneous information and forming an initial view which can be further translated into obligations. The data could be ingested into eGRC platforms through APIs, and regulations, risk events, and other information were categorised by product, business function, jurisdiction, and publish date. It also offered customised daily email alerts for subscribed users to facilitate regulation monitoring.

The tool housed the regulations and interpreted obligations, assisting the bank to manage rules and assess the impact. The bank was required to define applicable rule scope, allocate rules to risk topics, update policies and procedures, and assign risk owners and support teams. The regulatory management platform provided a structure and a workflow tool to assist the assessor of impact assessment to determine the risk impact level and steps required to comply with each new/updated regulation. Policies and procedures were also housed within the platform with a workflow overlay to facilitate maker-checker implementation, dissemination, and attestation.

4.1.3 Key learnings

As a result of implementing a comprehensive regulatory change management tool, the bank was able to demonstrate to those charged with governance that regulatory compliance remains consistent with its core values. As the Regtech solution is Cloud-based, implementation does not require significant resources or technical expertise from the bank. However, **adequate planning is required which may take a considerable amount of time** and involves obligations interpretation, risk taxonomy mapping, ownership assignment, and policy and procedures updates.

Also, in this specific case, the bank had to conduct a comprehensive stock-take of relevant requirements using information from the data provider to identify whether the existing regulations inventory was complete. The Regtech solution will allow for easier maintenance on a go-forward basis. However, the look-back was critical to address the auditor's observation and reduce the risk of missing previous regulations.

4.2 Use Case #2 – Implementation of a global GRC platform

4.2.1 Challenge

A financial institution historically managed GRC at the business unit level, resulting in customised processes and use of potentially standalone technology solutions across the company with limited oversight on a holistic basis. Given that certain reportable jurisdictions required the financial institution to maintain all risks and compliance obligations on a centralised platform, the organisation had identified the following challenges with managing GRC under the current model:

- Each business unit had customised processes, requiring translation to report on a holistic level, causing duplication of work and lack of economies of scale.

- The technology, introduced as standalone solutions across different business units, had varying levels of maturity, and lacked an interface with other systems. Multi-sourced information created long lead-times to pull management reports at a consolidated level.

4.2.2 Approach

Phase 0: The bank appointed programme sponsors and established a GRC programme to prepare for the transformation. This phase involved reviewing the company vision, mapping current processes and evaluating current process maturity across all entities. The outcome of phase 0 included defining key drivers of a GRC platform, current state maturity analysis, budget plans and high-level implementation and communications plan to prepare for the transformation.

Phase 1: Defined future operating model and vendor selection. Based on outputs from Phase 0, the programme produced mapping of available solution functionality to business processes that the organisation was required to address. Following the selection and appointment of a GRC platform vendor, the programme performed mapping and documentation of risk owners, and linking of risks to controls. This provided the baseline required for solution implementation.

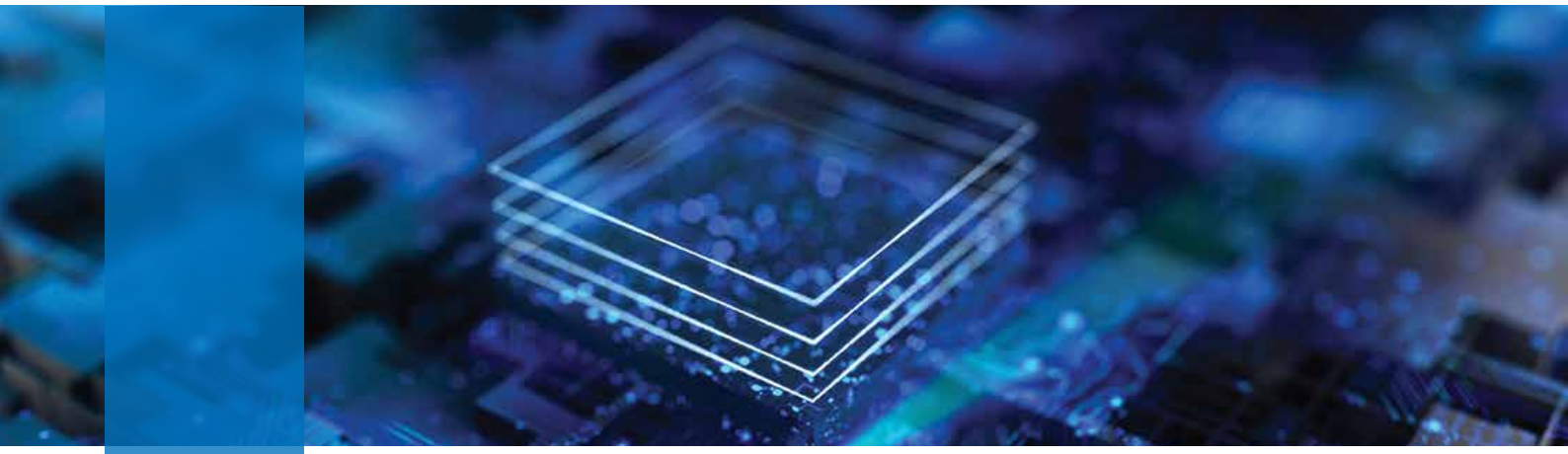
Phase 2: Development, pilot, and full implementation. All business units had to follow the centralised guideline on risk management and governance framework. To prepare for system development and implementation, each business unit had to identify relevant data sources and transform them to the standardised format for migration. Streamlining and standardisation of processes were also required due to the varying levels of maturity across all the business units and operating jurisdictions. Customisation requirements were managed to meet all requirements covering all operating jurisdictions. A prototype was built by the vendor for the pilot jurisdiction. Post user-acceptance testing, the platform was at a standard required for implementation. The lessons learnt from the pilot implementation were applied to the full implementation.

4.2.3 Key learnings

A complete organisation-wide GRC transformation is a large and significant project. The entire organisation needs to be on board with the transformation backed by strong management buy-in. Some of the key learnings obtained from this project are outlined below:

- **Preparation takes time:** due to the varying maturity and processes of each siloed business unit/operating jurisdiction, time and effort are required to define common standards and reach common understanding on the necessary guidelines for all to adhere to. This leads on to allowing enough time to extract, transform and load data for the new system, as well as uplift supporting processes to the required standards.

- **A robust project management framework is required:** The transformation vision and scope need to be clearly defined and agreed upon prior to programme kick-off. A robust project management office with clear IT change management governance is required to prevent scope creep. For a major transformation project involving a large number of stakeholders, scope creep and over-customisation are major risks and can cause project delays. Stakeholders need to understand and agree with the established requirements prioritisation framework to establish a platform that meets the original vision and objectives.



A Appendix

A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Paul McSheaffrey, Jeffrey Hau, Stanley Sum, James O'Callaghan, Angela Zhang, Adam Bobrowski, Phoebe Lee, Kelly, Albert Tan, editor Kanishk Verghese

A.2 List of Hong Kong regulators and key regulatory stakeholders related to the banking sector

- Companies Registry (CR)
- HKSAR Government
- Hong Kong Deposit Protection Board (HKDPB)
- Hong Kong Interbank Clearing Limited (HKICL)
- Hong Kong Monetary Authority (HKMA)
- Hong Kong Stock Exchange (HKEX)
- Independent Commission Against Corruption (ICAC)
- Insurance Authority (IA)
- Mandatory Provident Fund Schemes Authority (MPFA)
- Office of the Privacy Commissioner for Personal Data (PCPD)
- Securities and Futures Commission (SFC)
- Treasury Markets Association (TMA)