AI & Partners

EU AI Act

RegTech Adoption Practice Guide: Governance, Risk and Compliance (GRC)

Version 1.0

Last Updated: 14 December 2023

Disclaimer

Regtech Adoption Practice Guide is a publication published by AI & Partners B.V. (AI & P). It should be noted that the sole purpose of this publication is to provide firms with information on the latest regulatory technology (Regtech) developments in regards to the European Union Artificial Intelligence Act (EU AI Act). AI & P outlines its use cases, solutions and/or implementation guidance alongside this adoption practice guide.

AI & Partners

Amsterdam - London - Singapore

Contents

1. Introduction

1.1 Background

The value of RegTech across industries is coming to the fore in Europe and globally, offering clear benefits to firms[1], customers, investors, regulators and other stakeholders. In December 2023, the European Commission provided political approval for the European Union ("EU") artificial intelligence ("AI") Act (the "EU AI Act" or "Act") to set down rules for AI use, development and/or deployment for firms with a presence in Europe. The use of regulatory Technology ("RegTech") - the use of technologies that enhance efficiency and/ or the effectiveness of risk management and regulatory compliance – presents opportunities to unlock significant benefits for in-scope entities to achieve regulatory excellence.

If the key barriers to adoption can be overcome, then RegTech adoption and the realisation of these significant benefits can be accelerated.

As an initial document, this RegTech Adoption Practice Guide (the "Guide") builds on market sentiment around EU AI Act compliance – and wider market research - to include possible industry challenges, guidance on implementation and examples of what can be done to successfully to overcome adoption barriers. The Guide enhances the sharing of experience related to RegTech implementation across different regulatory regimes, such as the General Data Protection Regulation ("GDPR"), which will help further drive RegTech adoption in Europe.

Regtech solutions have emerged to improve the effectiveness and efficiency of risk management and compliance activities through harnessing new technologies such as Cloud, AI, and Blockchain. The Guide focuses on "Governance, Risk and Compliance" (GRC) Regtech solutions with respect to the EU AI Act, a large number of which can potentially 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 firms to seek to implement GRC RegTech solutions.

1.2 Purpose

The purpose of this Guide is to provide an overview of EU AI Act GRC RegTech solutions, outline the potential challenges regarding EU AI Act GRC solutions adoption, and share information on how firms can address the challenges to successfully adopt EU AI Act GRC Regtech solutions in their organisations. This Guide follows the outline below:

1 Explain how EU AI Act RegTech solutions can be used to support GRC

- Outline the key challenges that firms are currently facing in relation to GRC
- Illustrate the benefits of leveraging EU AI Act RegTech solutions to manage GRC
- Describe key risks/considerations when adopting EU AI Act GRC solutions

[1] This firm generally refers to users, providers, deployers, authorised representatives, importers, distributors, product manufacturers, and operators of AI systems. To this end, firms interacting with 'high-risk' AI systems are the primary focus of the Guide.

2 Provide practical implementation guidance to firms on the adoption of EU AI Act GRC Regtech solutions

- Outline the key components of EU AI Act GRC Regtech implementation, including the types and methods of EU AI Act GRC Regtech solution implementation
- Provide insights on what can be done to achieve successful EU AI Act Regtech adoption

3 Share use cases on the adoption of EU AI Act Regtech solutions to manage GRC

- Describe the likely GRC challenges faced by a firm and how the EU AI Act Regtech solution can help to resolve these challenges
- Outline possible key learnings from successful GRC EU AI Act Regtech implementation, from both the firm and the EU AI Act Regtech provider's perspectives

2. 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 regulated firms, such as developers or deployers of high-risk AI systems, given increasing regulatory scrutiny and complex compliance requirements under the EU AI Act. Widely publicised regulatory breach cases for similar regulations, such as the GDPR, and the corresponding regulators' attention place a significant demand on firms to demonstrate whether appropriate controls have been established to meet relevant regulatory obligations.

The key GRC challenges that firms currently face are:

Escalating cost of compliance

- Increasing EU AI Act regulatory requirements are only being addressed through manual processes that are not scalable, efficient or effective

- To keep EU AI Act regulatory obligations registers up-to-date, firms often need to establish operations, compliance and technology teams to perform regular scanning and monitoring of stakeholders' 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 EU AI Act 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.

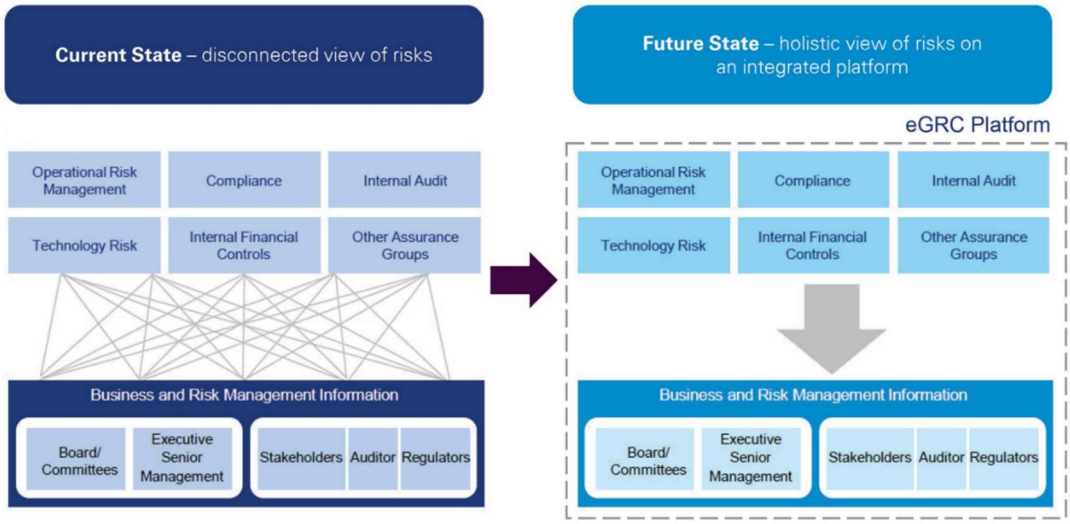
2.2 How can GRC EU AI Act RegTech Solutions Help?

2.2.1 Electronic-GRC

An electronic-GRC ("e-GRC") platform is an integrated technology platform that captures a holistic view of EU AI Act 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 shown in **Figure 1**, many organisations have a disconnected view of enterprise and business unit ai risks whereby these are handled independently of each other and via different channels of communication. An e-GRC 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 e-GRC platform[2]



[2] Sourced from the Hong Kong Monetary Authority (HKMA) paper, accessible at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210927e1a1.pdf (last accessed 1st September 2023)

The key benefits of using an e-GRC platform for EU AI Act compliance 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 e-GRC 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.

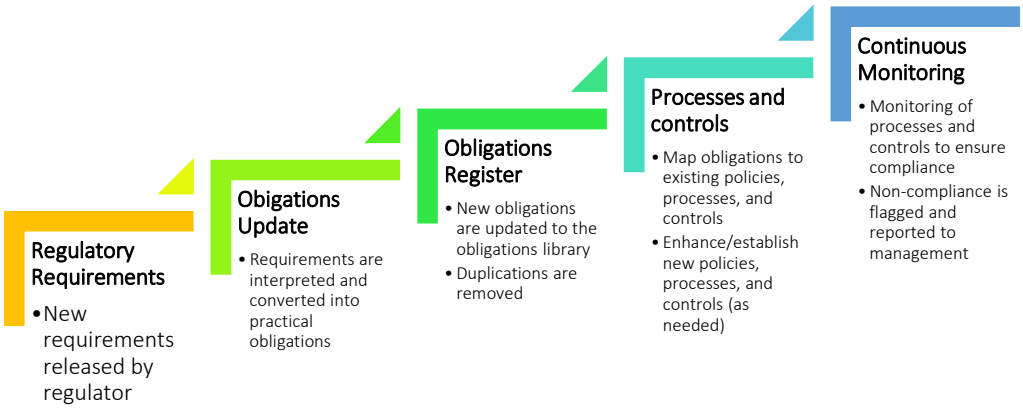
- **Reduces costs**: Checklists and templates standardise communication and action. Automation standardises and facilitates monitoring and testing of controls and processes across the three lines of defence. Cost reduction can be achieved via reduction in bespoke processes and documentation through controls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

Regtech opportunities can provide immediate benefits for firms, 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.

Figure 2: Regulatory Compliance Lifecycle



To achieve compliance with EU AI Act regulatory obligations, a firm needs to first understand the relevant regulatory obligations across different business units in their organisation. Relevant requirements need to be ingested on both a periodic and ad-hoc 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 firm 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 both deliver and monitor compliance through exception reporting or dashboards showing the current state of risks and compliance with regulatory obligations. A breakdown in any of these elements may lead to regulatory compliance failure.

2.3 Key Considerations when adopting EU AI Act GRC RegTech Solutions

As GRC EU AI Act RegTech solutions provide firms with efficient platforms for managing aggregated risk and compliance, it is crucial for firms 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 firms should consider when adopting GRC EU AI Act RegTech solutions:

- Vision and planning: Successful GRC EU AI Act 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 EU AI Act 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 EU AI Act RegTech solutions implementation. For people, this could include hiring GRC EU AI Act 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 firms operating in Europe, as they may be subject to existing European regulations such as the General Data Protection Regulation ("GDPR").

3. Implementation Guidance

GRC EU AI Act 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 EU AI Act RegTech adoption, firms 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 EU AI Act RegTech implementation. This section is not an exhaustive guide. Rather, it provides suggestions on what can be done to successfully implement GRC RegTech solutions.

3.1 Define State of Maturity and the GRC Vision

For firms seeking to adopt GRC EU AI Act 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

European-focused firms are at different stages of their GRC journey. Below we outline the common stages of EU AI Act RegTech adoption based on observations from similar European regulatory regimes.

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. risk management, control testing).
- Limited data exchange processes (e.g. a firm may have an off-the-shelf auto-feed for EU AI Act regulatory requirements, but it is not linked to the GRC platform).

Stage 3: Characterised by adoption of EU AI Act 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 EU AI Act 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:

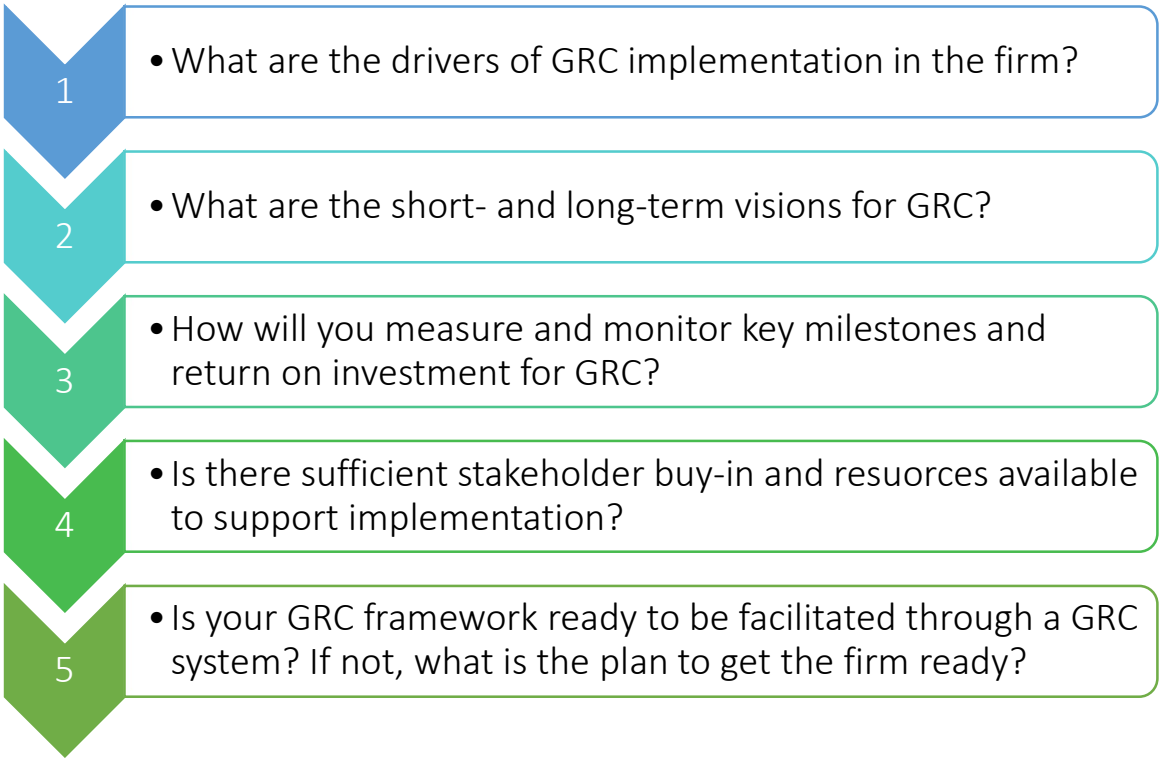
- Business can make decisions rapidly to respond to events and meet regulatory requirements using real-time data.
- Integrated systems with built-in approval and escalation processes.
- Data follows the Extract, Load, Transform ("ELT") process for seamless data exchange between systems and allows for big data analytics via data lake.
- Organisations can view their GRC obligations at an enterprise level.
- GRC EU AI Act 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 firm'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 a firm's GRC vision



3.2 Understanding your GRC Needs

Based on the firm's maturity assessment and GRC vision, the firm can determine the size and scale of their GRC transformation. e-GRC platforms are largely componentbased, utilising a modular approach to build a holistic platform. For smaller-sized firms 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 firms featuring multiple siloed business units, an integrated e-GRC platform can be adopted to manage the firm's overall GRC. e-GRC 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. 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.

- 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.

- 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 e-GRC platform modules above, with most firms focussing on “risk and control management” and “regulatory obligations management”.

3.3 Procuring Suitable GRC Solutions

A firm 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 EU AI Act 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 firm'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 EU AI Act RegTech solutions. The use of Artificial Intelligence, including machine learning, and other predictive analysis can help firms to identify new risks in regulatory changes, as well as irregularities in the GRC framework. Firms should also seek long-term commitment from solution providers that would help them envision their GRC roadmap and continue to support beyond deployment.

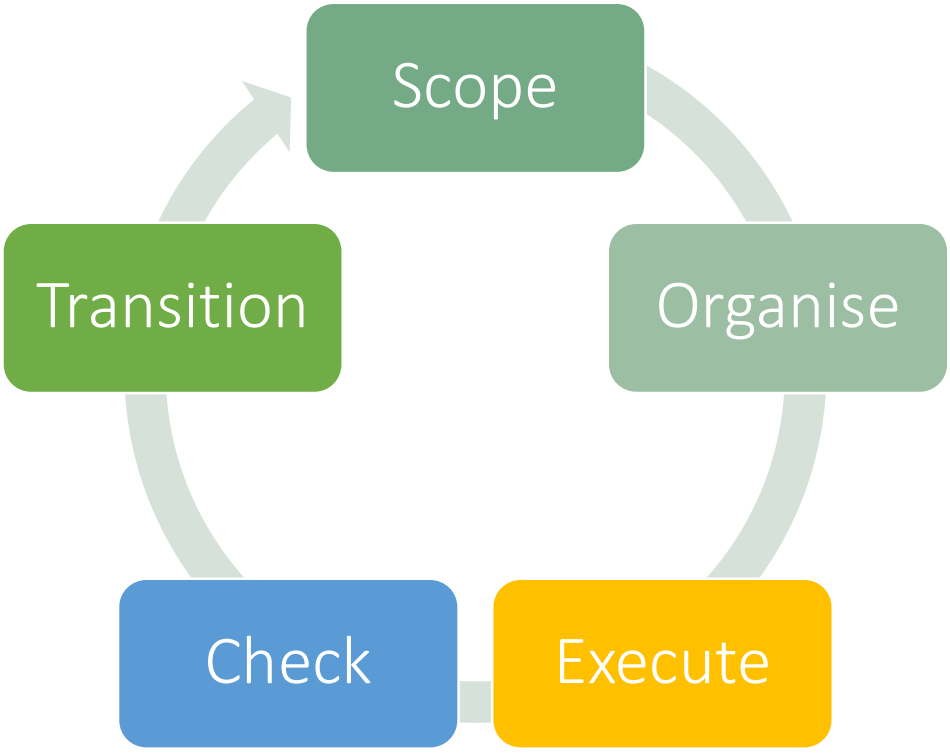
3.4 e-GRC Project Implementation

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). 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 Lifecyle



Scope

- Perform initial high-level planning
- Obtain sponsor buy-in
- Define the GRC transformation vision and initiate the project

Organise

- Estimate costs, plan schedule, conduct workshops and define scope
- Establish a number of governance processes (e.g. IT Change Control)

Execute

- Build, test and release per plan
- Keep control on change requests

Check

- Monitor the progress, scope, time, cost, quality, risks, and issues continuously

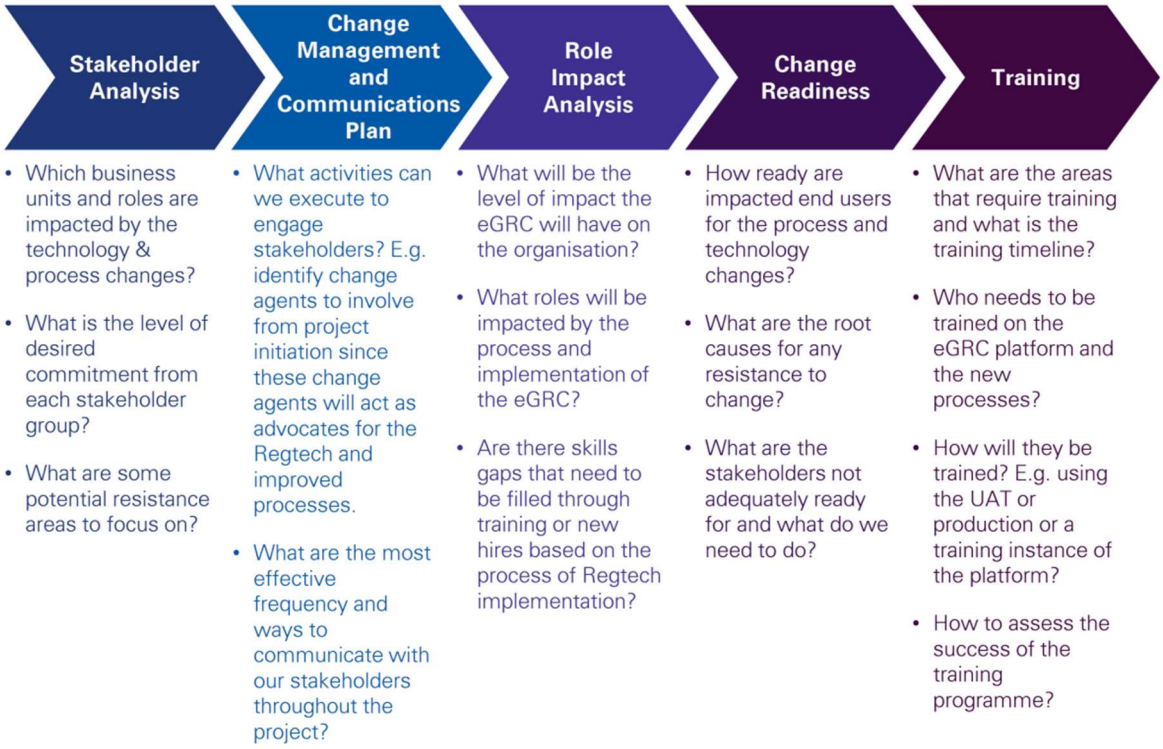
Transition

- Conduct necessary training
- Manage people and process changes

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 EU AI Act 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[2]



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 EU AI Act RegTech solution (e.g. adjusting processes to ensure data is captured digitally for integration with the new system). The implementation of GRC EU AI Act 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.

4. RegTech Use Case

AI System Identification and Risk Classification Tool

Challenge

In navigating the regulatory landscape of the EU AI Act, firms encounter several challenges.

- Accurate identification of AI systems and their associated risks stands out as a primary concern. The diverse nature of AI applications within organizations often leads to a lack of standardized approaches for risk classification.
- Firms struggle to keep pace with evolving regulatory frameworks, making it challenging to ensure compliance.
- Additionally, the dynamic nature of AI technologies poses difficulties in implementing consistent risk management practices.
- Transparency in AI operations, a crucial aspect of the EU AI Act, is another challenge, as firms find it complex to provide clear insights into the decision-making processes of their AI systems.

Challenge

When engaging Orthrus, firms adopt a strategic approach to overcome these challenges.

- The onboarding process involves a comprehensive evaluation of the firm's existing AI infrastructure.
- The provider collaborates closely with the firm to customize Orthrus according to specific risk parameters and regulatory requirements.
- This collaborative approach ensures that the tool seamlessly integrates into the firm's existing compliance framework. Regular training sessions and workshops are conducted to familiarize the firm's staff with Orthrus functionalities, facilitating a smooth transition.
- Continuous communication channels are established to address evolving regulatory nuances, enabling Orthrus to adapt proactively to changing compliance requirements.

Key Learnings

Using Orthrus yields several key learnings for firms.

- Firstly, the tool significantly enhances operational efficiency in compliance procedures related to AI systems.
- Its robust risk classification capabilities empower firms to identify and address potential compliance issues promptly.

- Continuous monitoring provided by Orthrus enables real-time adjustments to risk management strategies, ensuring ongoing compliance.

- The adaptability of Orthrus to dynamic regulatory changes is a crucial advantage, as firms learn to navigate evolving legal landscapes confidently.

- Furthermore, the tool's contribution to transparency not only aids in meeting regulatory obligations but also fosters trust among stakeholders.

- Ultimately, firms using Orthrus gain a comprehensive understanding of their AI risk landscape, leading to improved compliance and governance practices.