Regulatory technology implementation guide

Jersey Financial Services Commission

Contents

RT ASSOCIATES

This document was written in conjunction with **RT Associates**

Introduction

Our **financial crime and regulatory technology guide**, published in January 2024, described RegTech as a technology that helps firms meet their regulatory requirements. Implementation of any technology that affects a core business process for financial institutions should be subject to a risk assessment to understand the impact of the technology on service delivery.

Purpose of the document

This document is designed to highlight some of the considerations when procuring and implementing a RegTech solution. It also covers the sequential steps of RegTech implementation, from initial scoping to post-implementation review.

This document is not intended as a comprehensive manual for experienced change managers or programme managers, but rather as a guide for business managers to navigate through the process.

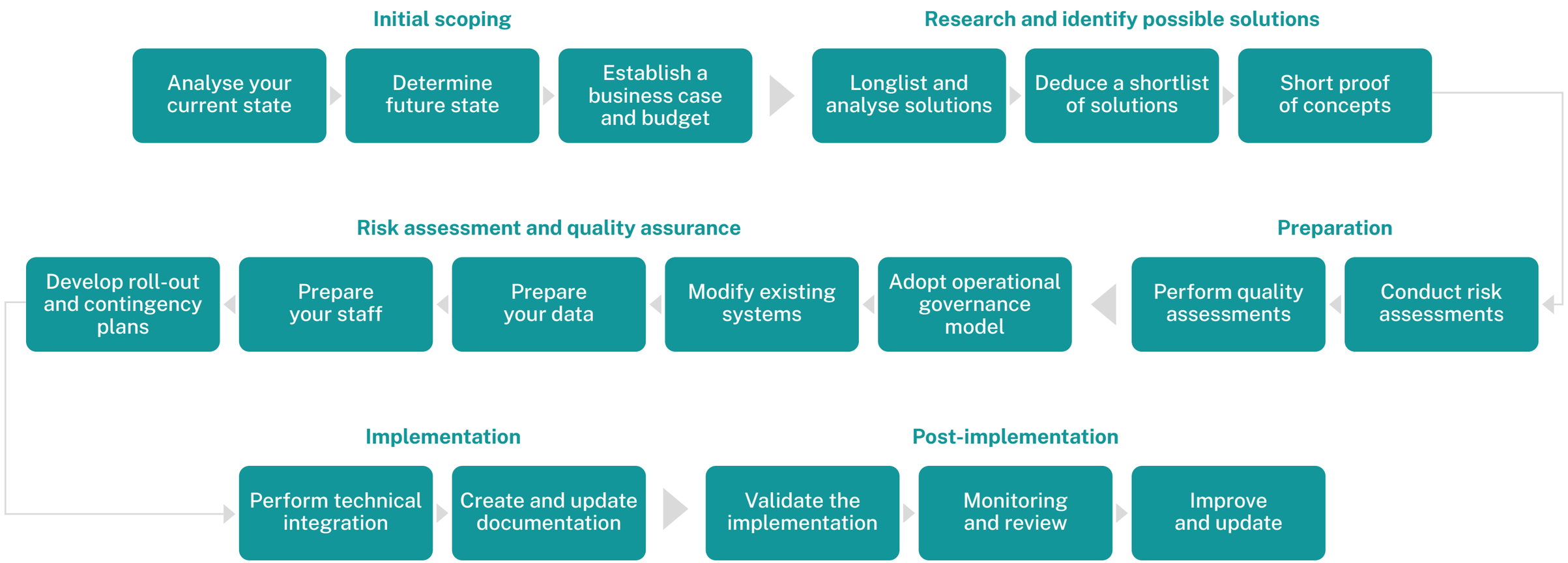
Adopting a RegTech solution

Overview

To start, this section lays out suggested steps that firms should take when adopting RegTech effectively and responsibly. Since each firm's circumstances and needs differ, and there is variation in the products that are best suited, these suggestions are good practice only and should not be treated as prescriptive, necessarily sufficient, or exhaustive. This section then sets out risks to be aware of from the outset.

Overview cont.

Indicative flowchart for firms to consider when adopting a RegTech solution



Suggested steps

Below are some suggested steps of how supervised persons might approach the adoption of a RegTech solution. We've identified six high level stages:

1. initial scoping
2. research and identify viable solutions
3. risk assessment and quality assurance
4. preparation
5. implementation
6. post-implementation

This guide does not cover many of the standard steps followed in change management projects but does provide detail of the most important considerations for firms adopting RegTech in Jersey.

Initial scoping

While most firms are familiar with this foundational change management stage, the outlined steps emphasise the significance of culture, regulatory foresight, and transparency in preparing for RegTech adoption.

Analyse your current state

- **Identify your compliance challenges** by determining whether there are gaps, inefficiencies, or both, as this will change the specification of your solutions.
- **Assess your organisation's technological maturity** - evaluate your organisation's ability to integrate the new technology, with a particular focus on your compliance department. This process should inform the scale and complexity of any RegTech solution.

Key consideration: the technology culture of your company, and compliance department, should be considered when assessing your technological maturity. A chosen technical solution may fail if it isn't a good fit with your people.

Determine your preferred future state

Key consideration: stay informed about ongoing or upcoming regulatory changes in Jersey. Engage with us to understand any consultations, or directives that may impact your technology and compliance strategy.

Establish a business case and budget

- **Quantify the indirect costs and benefits of RegTech** which include all the implementation costs, staff training and ongoing maintenance. The benefits of adopting RegTech are the potential revenue protection from reputational damage, and operational efficiencies that free up resources for further compliance and innovation initiatives.
- **Be comprehensive and transparent in documentation** by clearly outlining the decision-making processes, justifications, and expected outcomes to allow for easy review and verification. Considering potential challenges and outlining strategies to adapt and overcome them will ensure resilience.

Research and identify possible solutions

While this stage is often standardised through procurement processes, it is crucial to differentiate between on and off-island RegTech providers and to be aware of any discrepancies between a firm's marketing and its actual capabilities.

Long-list and analyse potential solutions

- **Map out each solution's range of financial crime capabilities** by using the financial crime regulatory technology guide as an aid to evaluate what each solution is offering.
- **Assess in-house capabilities** - are the available solutions more effective than what could be built in-house? The buy/build/partner question is one that should arise before committing to buying in a solution. Encouraging the adoption of RegTech does not necessarily mean recommending a third party if your in-house technical resource is more efficient.

Key consideration: evaluate the advantages and challenges of choosing technology providers based on their location. Investigate their coverage and specialisation in Jersey regulations, business challenges and regional considerations, such as local data sharing regulations and the region's track-record in cybersecurity.

Create a shortlist of solutions

- **Look closely at each solution's ongoing regulatory coverage** as this will determine if they are designed to address imminent regulatory changes in Jersey. If not, ascertain whether the vendor commits to timely regulatory updates.
- **Take responsibility for due diligence** as while peer recommendations can offer valuable insight, each firm's regulatory challenges make it paramount that you conduct your own due diligence. Evaluate the suitability and strengths of potential vendors, either independently by using guides like this, or with the assistance of external experts.

Consider running short proofs of concept or proofs of value.

Key consideration: vendors can sometimes overestimate their capabilities, so it is important to scrutinise. Allow the time to perform proofs of concept or proofs of value to validate if the solution delivers on its promises.

Risk assessment and quality assurance

RegTech implementation carries unique risks compared to other tech initiatives, especially when entrusting technology with financial crime compliance. This section highlights the importance of transparency as a means of measuring quality and refers to the specific risks to be aware of when adopting a RegTech solution.

Conduct thorough risk assessments

- **Map the risks of each solution to your organisation** to ensure you have comprehensively assessed the risks associated with RegTech identified in the AML/CFT/CPF Handbook and financial crime regulatory technology guide and to confirm that the risks align with your firm's defined risk appetite for each category.
- **Map the customer journey within the software to your own processes** to be sure there are no gaps between what the software does and your proposed process.

Key consideration: the new solution may add value across the entire process, but it may exclude a key process step for your organisation.

Ensure you identify any gaps and mitigate those through configuration changes or additional manual steps if necessary.

Perform a rigorous quality assurance exercise

- **Scrutinise data sources** where relevant to confirm that the solution uses high-quality data from trustworthy sources that are acceptable in a regulatory context. This includes in the context of KYC/CDD and ECDD.
- **Assess the solution's technical foundation** by evaluating the integrity of the system's technology stack, and its security, latency, and load times, ensuring they meet the demands of your specific financial crime compliance process.

Key consideration: the solution's outputs and decision-making processes should be clear and easy for a non-technical audience to understand. They should offer ample documentation to facilitate audits.

Preparation

While firms typically have tech teams skilled in adapting systems for general technology change, RegTech adoption demands special attention. It is essential to focus on the operational and governance models that facilitate tech-driven compliance and to clearly convey any changes in staff responsibilities.

Adapt your operational and governance models

› **Review your current operational processes and governance policies** to make sure they align with and allow the new RegTech solution's functionality. Additionally, account for the second-order impacts of any changes made, confirming that other compliance operations can continue without disruption or contradiction.

Modify your existing systems and data

› **Evaluate the data attributes and sources required by the new solution** to identify and onboard any additional data sources needed and focus on data quality and compatibility, including the frequency and format of data to and from the new solution. If you are involving third parties for data processing or storage, confirm their Jersey-specific data protection or GDPR compliance and cyber security credentials.

› **Establish a data governance framework** to define roles and responsibilities for data ownership, access control and data maintenance.

› **Implement data security measures** as this will make sure that appropriate security protocols are in place to protect sensitive data during migration and in the new system.

Key consideration: RegTech solutions may use an Application Programming Interface (API) in deploying their solutions. Verify the compatibility of your current systems, including existing firewalls and any other connectivity concerns.

Prepare your staff

› **Identify skillsets and expertise needed across departments** by developing role-specific training to equip staff with the knowledge and skills to implement, use, maintain and monitor the solution, which includes compliance staff who may have had little exposure to certain technologies. It is also important to make IT and development teams aware of the business context to avoid subtle errors in implementation or maintenance that could hinder compliance.

Key consideration: RegTech is often capable of automating certain tasks. Where this is the case, make clear to the people formerly responsible what their new role in the process will be - this encourages staff buy-in and aids a smoother transition to the new solution.

Develop rollout and contingency plans

› **Design a phased rollout strategy that allows continuous compliance**. Consider the impact of technology and process changeovers on your ability to fulfil regulatory requirements on a continuous basis, and on the welfare of your customers.

Key consideration: regulated entities are encouraged to reach out to the Innovation Hub to discuss their plans to implement RegTech, as this will help ensure regulatory alignment and the use of best practice.

Implementation

While technical integrations are typically routine for firms, the stakes of regulatory compliance elevate their importance. This section underscores the necessity of incorporating strong validation and error handling from the outset and maintaining clear documentation to demonstrate due diligence.

Manage technical integration with other systems

› **Scalability checks** for regulatory data can come in high volumes. Ensure that the integration process tests the RegTech ability to handle large data sets without performance degradation.

Key consideration: firms should prioritise robust validation mechanisms within their technical integration, including real-time system monitoring and comprehensive error handling processes. Furthermore, staff should receive clear notifications for any data mismatches, or other process failures, and maintain written records to ensure non-technical staff are able to investigate in more detail.

Create and update documentation

› **Compliance documentation** should be updated to reflect how the integrated RegTech solution complies with all necessary regulations, including data privacy and protection laws.

Post-implementation

Many firms face challenges during this phase. It is critical that firms recognise that technology transformation has not finished once the solution is implemented – in fact, it has only just started. After initial setup and tests, firms should prioritise continuous testing and monitoring, to ensure they're able to continuously adapt.

Validate the implementation

› **Test compliance** by conducting a phase of intensive monitoring in the live environment, confirming compliance and measuring efficiency. Take note of the edge cases that you come across during this phase and remain alert to to any that do not appear.

Monitoring and reviews

› **Define key performance indicators (KPIs)** to capture success with respect to your specific financial crime use case and compliance process. Automate your report generation where possible to reduce operational burdens.

Key consideration: as financial crime regulations, typologies and behaviours change over time, the functioning of your compliance systems will be more prone to error. If you identify errors in your compliance systems, this should trigger a root cause analysis with a detailed examination of your systems, processes, and measures.

Improve and update

› **Collaborate with the solution provider** if a third -party technology is being used. Ensure your agreement includes provisions for regular system enhancements that cater to evolving needs and the dynamic regulatory landscape.

Key consideration: a disconnect can often emerge between senior stakeholders driving technology adoption and the compliance staff using it daily. To prevent friction, underutilisation of the new system, and inefficiencies, encourage an open feedback loop by providing insights from those who use the technology daily. This will provide important direction for improvements and updates to bridge this gap.

Risks

There are many risks associated with outsourcing technology, and regulatory or compliance contexts only add to those risks. When considering whether to adopt a RegTech solution, it is therefore important to also consider the following:

Compliance risk

Compliance risk revolves around the question of whether the product will be successful in helping your firm meet its compliance obligations. In the case of financial crime, firms should ensure that the solutions they evaluate comply with Jersey's regulatory framework, such as the AML/CFT/CPF Handbook. You should consider the JFSC's updated Outsourcing Policy and determine whether the solution you select requires you to notify the JFSC. You may also need to consider requirements under other jurisdictions in which you operate.

It is also crucial to consider whether the product might expose your firm to other compliance risks. For instance, data privacy could become a concern if your firm needs to share sensitive data with the RegTech vendor. As a supervised person holding personal data, it is your responsibility to ensure that all uses of that data are compliant with requirements under the Data Protection (Jersey) Law, 2018.

IT risk

IT risk relates to the potential for the technology to expose or cause any limitations or deficiencies in your current IT infrastructure. For example, the solution might require computational resources beyond what your current infrastructure can provide.

Cybersecurity risk is a significant component of IT risk. The adoption of a RegTech solution could potentially expose your firm to cyber threats like hacking, viruses, and other online attacks. These could compromise the RegTech solution and, by extension, your firm's broader IT infrastructure.

Operational risk

Process, policy and control changes introduced to facilitate and implement the solution could cause risks to the functioning of other processes. For instance, the introduction of the solution might introduce new dependencies within your firm that could put critical activities at risk in the event of a technical failure.

Obsolescence risk

Obsolescence risk refers to the risk that the technology of the RegTech solution may become outdated over time. This could necessitate costly and time-consuming upgrades or even a complete replacement of the solution. When adopting a RegTech solution, it is important to consider the vendor's willingness and ability to maintain and update their technology to mitigate this risk.

Vendor risk

Vendor risk pertains to the potential that the RegTech provider may not be able to deliver on its commitments due to financial instability, changes in business strategy, or other issues. It is crucial to assess the vendor's stability and track-record before adopting their solution.

A specific aspect of vendor risk is concentration risk. If your firm relies on a single RegTech vendor for multiple regulatory compliance tasks, there is a risk of significant disruption if the company or their solutions fail. Diversifying your RegTech solutions across multiple vendors can help mitigate this risk.

About the JFSC Innovation Hub

The Innovation Hub provides a collaborative environment for FinTech/ RegTech start-ups, supervised persons, global regulators, and standard-setting bodies to work together to develop and launch new products and services that meet evolving industry requirements.

The Innovation Hub also encourages the adoption of technology in the financial services industry by:

- providing help for innovative businesses to understand how the regulatory framework applies to them and their proposed products and services
- listening to and engaging with industry, considering relevant policy where appropriate to foster the development of innovative products or services
- working closely with key stakeholders, including the Government of Jersey, industry bodies, and international standard setters to ensure that Jersey is well placed to respond quickly to new innovations in financial services

When considering, developing or implementing innovations such as RegTech, firms are encouraged to reach out to us at **innovate@jerseyfsc.org**.

Appendices

Appendix A - **AML/CFT/CPF Handbook**
Appendix B - **RegTech guide – Fincrime**

Jersey Financial Services Commission
14-18 Castle St, St Helier
Jersey JE4 8TP

www.jerseyfsc.org