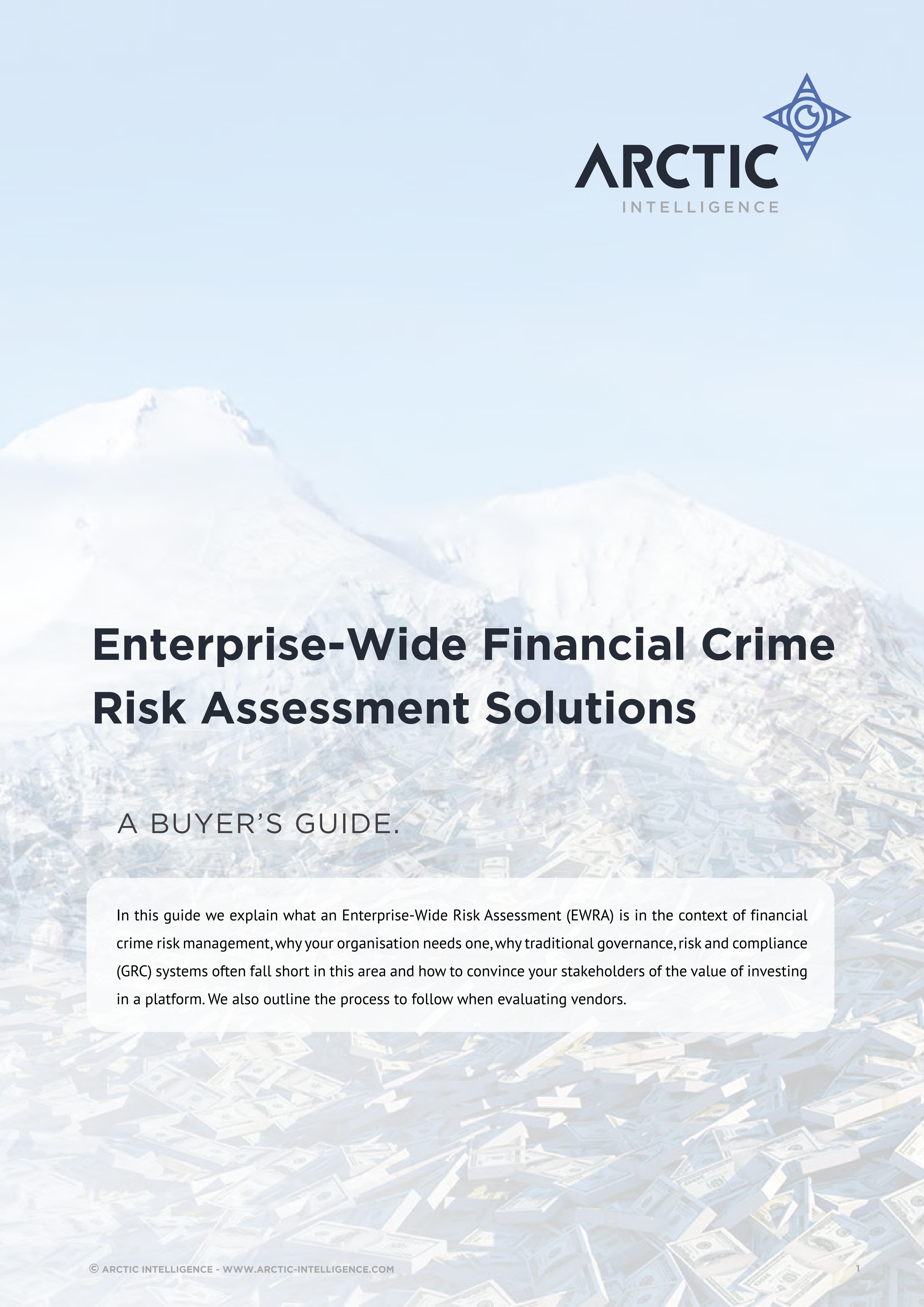


ARCTIC
INTELLIGENCE

Enterprise-Wide Financial Crime Risk Assessment Solutions

A BUYER'S GUIDE.

In this guide we explain what an Enterprise-Wide Risk Assessment (EWRA) is in the context of financial crime risk management, why your organisation needs one, why traditional governance, risk and compliance (GRC) systems often fall short in this area and how to convince your stakeholders of the value of investing in a platform. We also outline the process to follow when evaluating vendors.

WHAT'S INSIDE THIS BUYER'S GUIDE

1. Executive Summary

1.1. What is Enterprise Risk Management and why is it important?

The term Enterprise Risk Management (ERM) is used to describe the way that risks are managed across an entire organisation. It is more important than ever for organisations to balance achieving their objectives with effective risk management in a continually evolving risk and threat landscape. Risk management is not a static activity - new risks are constantly emerging, the nature of existing risks are changing, and the global regulatory landscape is becoming increasingly complex and difficult for most organisations to keep pace with.

Organisations themselves are like living organisms that evolve constantly. Whether this involves launching new products, entering new industry sectors or geographic markets, pursuing new customer segments or growing organically or through acquisition, things do not sit still and organisations need the right systems and processes to help them cope.

1.2. What risks are considered in an Enterprise Risk Management system?

The diagram below shows the types of risks that are typically considered in an Enterprise Risk Management system.

Enterprise risk

Strategic risks

- Business viability risk
- Climate risk
- Commercial risk
- Corporate transaction risk
- Geographic risk
- Intellectual property protection risk
- Key human resource risk
- Leadership risk
- Market entry risk
- Mitigation risk
- Partnership risk
- Product and market fit risk
- Product viability risk
- Reputational risk
- Resource risk
- Investor risk

Financial risks

- Access to capital risk
- Bad debtor risk
- Cash management risk
- Commodity risk
- Currency risk
- Debt financing risk
- Enterprise valuation risk
- Financial liability risk
- Financial management risk
- Financial modeling risk
- Financial viability risk
- Funding risk
- Interest rate risk
- Liquid asset risk
- Loan repayment risk
- Revenue management risk
- Tax event risk

Operational risks

- Business operations risk
- Business outsourcing risk
- Culture risk
- Distribution risk
- Employee risk
- Environment risk
- Human error risk
- Employee/industrial relations risk
- Information security (cyber) risk
- Information technology risk
- Intellectual property risk
- Employee retention risk
- Leadership risk
- Legal risk
- Occupational health and safety (OH&S) risk
- Project execution risk
- Record keeping risk
- Supply chain risk
- Bad weather event risk

Regulatory risks

- Bribery and corruption risk
- Fraudulent activity risk
- Illicit trafficking risk
- Money laundering and terrorism financing risk
- Sanctions risk

Arctic Intelligence has developed Enterprise Risk Models covering all Strategic, Financial, Operational and Regulatory Risks. Our main focus is on the essential requirements of Financial Crime; specifically the Enterprise-Wide Risk Assessment[1] (EWRA), which is a mandatory requirement that any regulated business must conduct and maintain to assess their money laundering and terrorism financing risks.

[1] In some countries the Enterprise-Wide Risk Assessment is also known as Business-Wide Risk Assessment, or BWRA. These terms are commonly used interchangeably. In this document we will use Enterprise-Wide Risk Assessment or EWRA.

Other Financial Crime Risks that we focus on are Fraud, Sanctions, Bribery and Corruption and Illicit Trafficking of arms, drugs, wildlife and people, which have unique considerations in the broader context of Enterprise Risk Management.

Section 2 of this document discusses the constantly changing risk and threat landscape that makes it more important than ever for organisations to take a joined-up approach to Enterprise Risk Management in an interconnected and evolving environment.

1.3. Evaluating Enterprise-Wide Risk Assessment (EWRA) solutions

Enterprise-Wide Risk Assessment (EWRA) solutions must contain all of the features and functionality organisations expect of an Enterprise Risk Management (ERM) / Governance, Risk and Compliance (GRC) solution. Additionally, there are specific elements of EWRA solutions that are required that are more sophisticated than traditional ERM/GRC solutions, and it is important to know the differences.

When organisations are evaluating ERM/GRC/EWRA systems, they must clearly define their functional and technical requirements of a solution to narrow the focus in an often-crowded field. EWRA solutions are new and emerging and go above and beyond traditional GRC systems, so it is important to articulate the questions to put to vendors to ensure your organisation achieves the right result when selecting a vendor to work with.

Section 3 of this document outlines the key considerations that organisations should factor into the EWRA vendor selection process and provides some practical questions to seek answers to.

1.4. Building a business case and demonstrating value

Business users of EWRA solutions often reside in the risk and compliance teams, and they are often won over long before an organisation adopts a solution. These individuals and teams need to champion both the functionality and benefits of a particular solution to a diverse set of stakeholders involved in influencing or making the ultimate vendor selection decision.

Section 4 of this document outlines how to build a business case that demonstrates the value that an EWRA solution would bring to the organisation.

2. About this Buyer's Guide

2.1. What is the purpose of this Buyer's Guide?

The purpose of this Buyer's Guide is to outline the key requirements and considerations that must be evaluated when making investment decisions to licence a risk management platform. It also provides a framework for building a business case that can demonstrate sufficient value to executive decision-makers and influencers, so they can make a considered purchasing decision.

2.2. What are some of today's challenges?

The pace of change for risk and compliance teams is overwhelming for many companies. Every day there are new laws and regulations, changes to existing laws, and consultation papers going out around potential future changes to laws! And of course, organisations are not just subject to a single set of laws and regulations, but often many different laws, such as privacy, employment, capital adequacy, cybersecurity, financial crime and many more.

Once you add an international perspective, where all these laws are replicated in different countries (which are often very different) and throw into the mix both heavy penalties for companies and personal consequences for individuals for non-compliance in the form of senior management accountability regimes, combined with historical under-investment in risk management solutions, is it any wonder that most risk and compliance managers are highly stressed?

2.3. Why are manual approaches no longer effective at managing risks?

In a fast-paced and constantly changing risk, threat and regulatory environment, where the penalties and consequences of compliance failures can be counted in the hundreds of millions or billions, organisations need to invest in managing their risks efficiently and effectively.

Every day, we have discussions with risk managers in banks, non-bank financial institutions, gaming businesses and other sectors, who are attempting to run financial crime risk assessments using spreadsheets that are rarely touched or improved for decades or longer, which is no longer fit for purpose or what financial crime regulators expect.

2.4. What is covered in this Buyer's Guide?

The following few sections of this Buyer's Guide cover the following topics:

- Financial Crime Risk Management overview
- Ten key challenges typically faced conducting Enterprise-Wide Risk Assessments (EWRA)
- The key considerations when assessing GRC/EWRA vendors
- Building a business case and demonstrating value
- Supporting documents to share with your stakeholders.

3. Financial Crime Risk Management Overview

3.1. What is financial crime risk management and why is it important?

Financial crimes like money laundering, terrorism financing, bribery and corruption, fraud, cybercrime, tax evasion and the illicit trafficking of drugs, arms, wildlife and people generate billions in profits every year for organised criminal networks and cause incalculable social harm to many.

Millions of businesses[2] operating in the financial services, gaming and wagering, gatekeeper professions and high-value dealer sectors must comply with money laundering and terrorism financing (ML/TF) laws.

In addition, these businesses, as well as millions of other businesses[3] operate in sectors that - while they are not subject to ML/TF laws - are subject to further financial crime risks such as fraud, bribery and corruption, sanctions, tax evasion and the illicit trafficking of arms, drugs, wildlife and people.

3.2. What is the risk-based approach to financial crime risk management?

The risk-based approach (RBA) is key in preventing money laundering and terrorism financing. It is a principle that financial institutions, gaming and wagering businesses, gatekeeper professions and other regulated entities use to identify, assess, mitigate and manage the ML/TF risks associated with their customers, products, services, channels, business, transactions and geographic footprint.

The risk-based approach involves identifying and assessing the risk associated with a particular customer or transaction and then applying appropriate measures to mitigate that risk. Financial institutions must take a proportionate, risk-based approach to anti-money laundering (AML) and counter-terrorist financing (CTF) measures.

For example, a high-risk customer or transaction may require more extensive due diligence and monitoring than a low-risk one. This approach helps to ensure that AML/CTF measures are focused on the areas where the risk of money laundering or terrorist financing is highest, rather than applying a one-size-fits-all approach.

The risk-based approach is now a widely accepted standard in AML/CTF regulations. It is recommended by international organisations such as the Financial Action Task Force (FATF) and the Wolfsberg Group, an association of global banks which develops frameworks and guidance for the management of financial crime risks.

The risk-based approach presents challenges to many regulated businesses, who lack the internal capacity or capability to design, build and implement enterprise-wide money laundering and terrorism financing risk assessments. This is at the heart of the problem that Arctic Intelligence solves.

[2] Appendix 1 lists the industry sectors that are subject to money laundering and terrorism financing laws.

[3] Appendix 2 lists the industry sectors that are impacted by other financial crimes.

3.3. What is an EWRA for financial crime?

An Enterprise-Wide[4] Risk Assessment (EWRA) for money laundering and terrorism financing is a process that regulated businesses undertake to identify and assess their organisation's risks and vulnerabilities to being exploited by organised criminal networks or terrorist groups, when laundering the proceeds of crime or funding terrorist acts.

The EWRA is a mandatory, ongoing requirement that compels every regulated business to consider their money laundering and terrorism financing risks based on the:

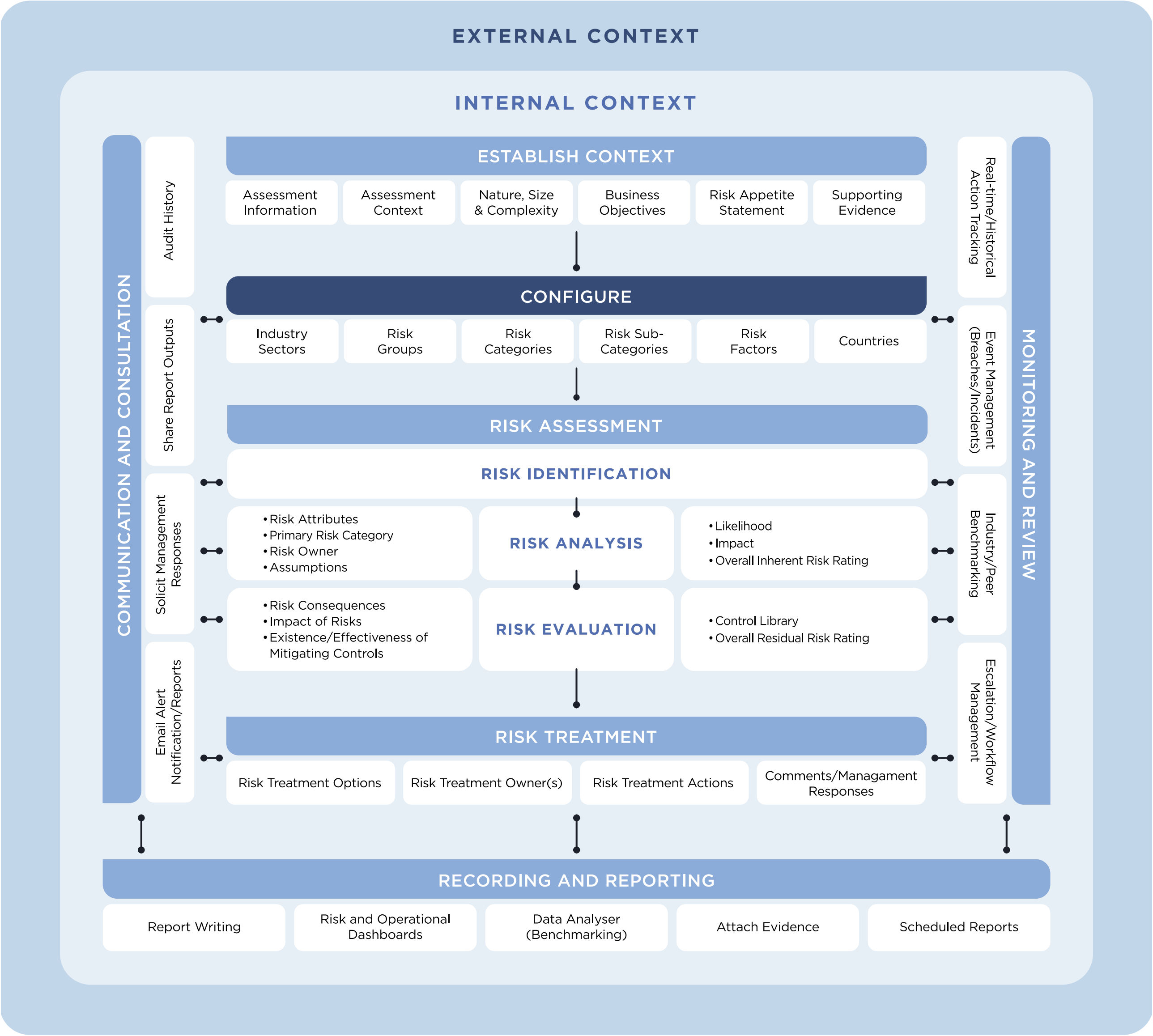
- Nature, size and complexity of their organisation
- Internal and external operating environment that their organisation operates in
- Nature and types of customers that their organisation deals with
- Nature and characteristics of the products and services that are offered to customers
- Distribution channels that are used to offer products and services to customers
- Operating risks of their business (i.e., employee risk, outsourcing risk etc.)
- Geographic risk exposures that their organisation faces.

Once the organisation has identified the risk indicators to consider, they must assess the likelihood and impact of these risks occurring and then design, implement and maintain controls appropriate and proportionate to the identified risks. These risks should be either mitigated or managed in line with the organisation's risk appetite statement.

[4] This is also often referred to as a business-wide risk assessment (BRA), for example in the UK, or institutional-wide risk assessment elsewhere.

3.4. What are the typical steps when conducting EWRAs?

The diagram below highlights the steps that are usually taken when conducting Enterprise-Wide Risk Assessments.



- **Establish context** - involves understanding the risk appetite of the Board and Senior Executives to money laundering and terrorism, as well as the organisation's nature, size and complexity. This step is also important for defining the risk management methodology used and the scope of the assessment(s) to be undertaken.
- **Configuration** - involves agreeing on the risk methodology, defining the risk model (i.e., risk groups, categories, factors, indicators and answer sets), weighting the risk model (optional), defining country risk inputs, defining control categories, controls and control tests, and setting user access controls and role-based permissions.
- **Risk identification** - involves identifying the risk groups, risk categories, risk factors and risk indicators that will be analysed and evaluated in the 'risk model' to assess the inherent risks during the risk assessment(s).
- **Risk analysis** - involves assessing the likelihood and impact of particular risks occurring and the inherent risks across the defined 'risk model'.

- **Risk evaluation** - involves evaluating the design and effectiveness of any systems, policies, and procedural controls implemented to mitigate and manage the identified inherent risks.

- **Risk treatment** - involves identifying opportunities to strengthen the control framework to reduce the overall residual risk, which is the remaining risk after controls have been applied. Risks can be managed and/or mitigated in different ways, including avoiding the risk by ceasing the activity or implementing more comprehensive mitigating controls.

- **Risk acceptance** – ultimately, any residual risks that have been managed and/or mitigated as far as the organisation can, must be accepted. However, if residual risks are outside of the organisation's stated risk appetite, further action is required to be taken.

- **Recording and reporting** - involves monitoring for changes in the risk and threat landscape, for example, regulatory changes and criminal activity changes, as well as the internal business environment, such as changes to the customer, product, channel or geographic risk profile. These 'event-based' and 'time-based' triggers, will determine when the risk assessment must be repeated.

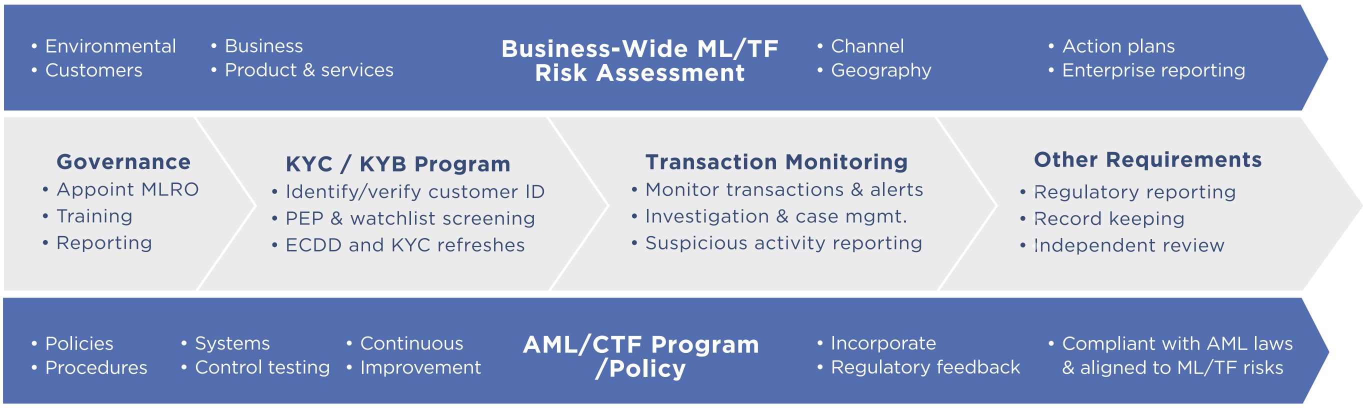
- **Monitoring and review** - involves assessing changes to risks and controls over time, assessment/business-unit risk comparisons and benchmarking, assessing velocity at addressing issues, actions, findings and compliance breaches and documenting suggested improvements to be made when conducting EWRAs in the future.

- **Communication and consultation** - involves communicating the outputs of the risk assessment to key stakeholders by outlining the key findings of the risk assessment, the areas where control effectiveness needs to be improved and the main observations, findings and recommendations.

3.5. Why is the EWRA important and foundational for AML/CTF Programs?

The Enterprise-Wide Money Laundering and Terrorism Financing Risk Assessment is at the heart of any AML/CTF Program because, unless an organisation has a clear understanding of the risks and vulnerabilities that it typically faces from organised criminal networks or terrorist groups in laundering the proceeds of crime or funding terrorism, it is highly likely that the controls to mitigate and manage these risks might be inappropriate.

The diagram below shows how the EWRA is integral to the design, implementation and maintenance of a high-performing AML/CTF compliance program and the main components of the legal requirements that each regulated business is expected to meet.



Business-Wide ML/TF Risk Assessment

- Environmental
- Customers
- Business
- Product & services
- Channel
- Geography
- Action plans
- Enterprise reporting

Governance

- Appoint MLRO
- Training
- Reporting

KYC / KYB Program

- Identify/verify customer ID
- PEP & watchlist screening
- ECDD and KYC refreshes

Transaction Monitoring

- Monitor transactions & alerts
- Investigation & case mgmt.
- Suspicious activity reporting

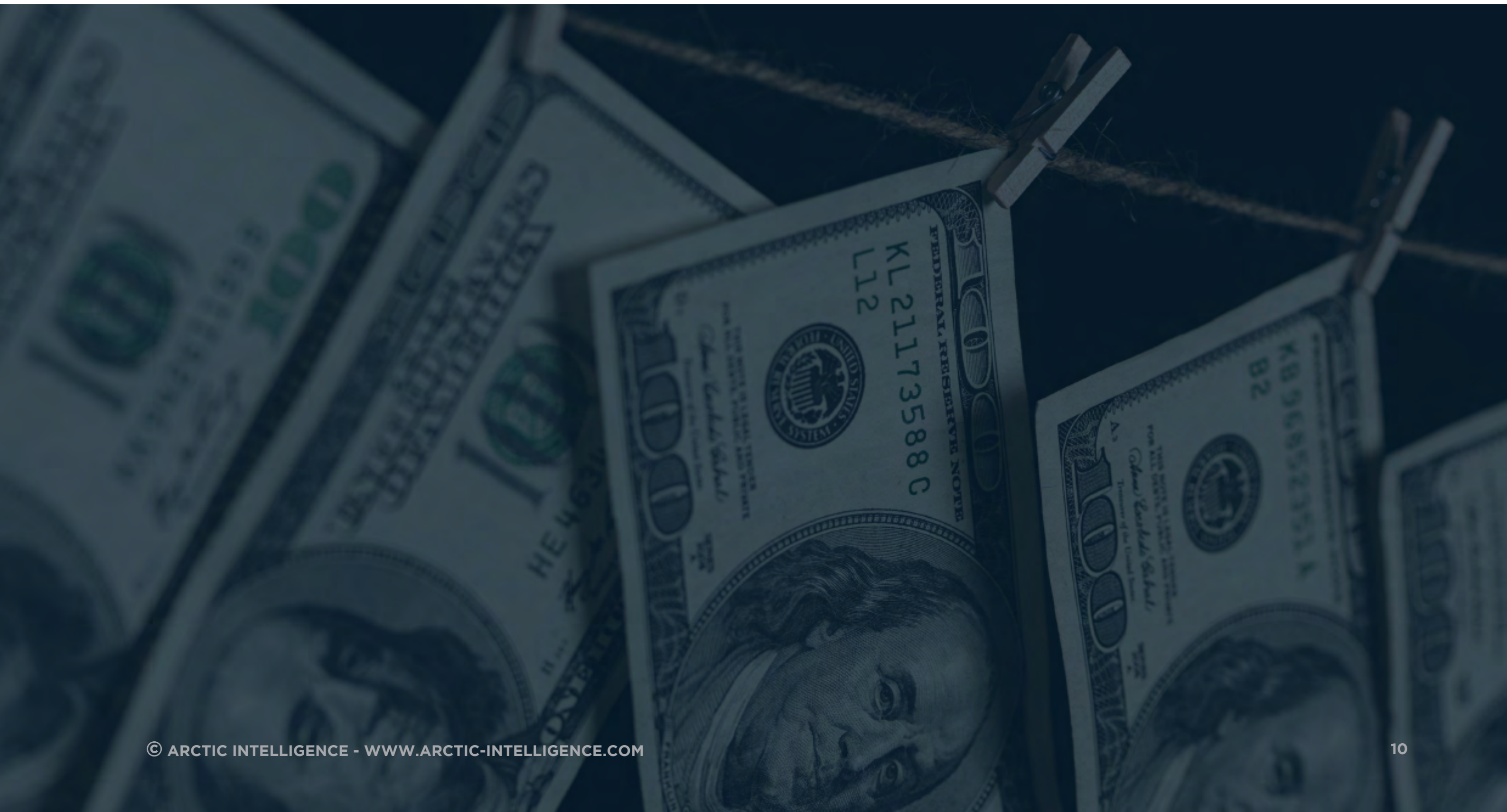
Other Requirements

- Regulatory reporting
- Record keeping
- Independent review

AML/CTF Program /Policy

- Policies
- Procedures
- Systems
- Control testing
- Continuous
- Improvement
- Incorporate
- Regulatory feedback
- Compliant with AML laws & aligned to ML/TF risks

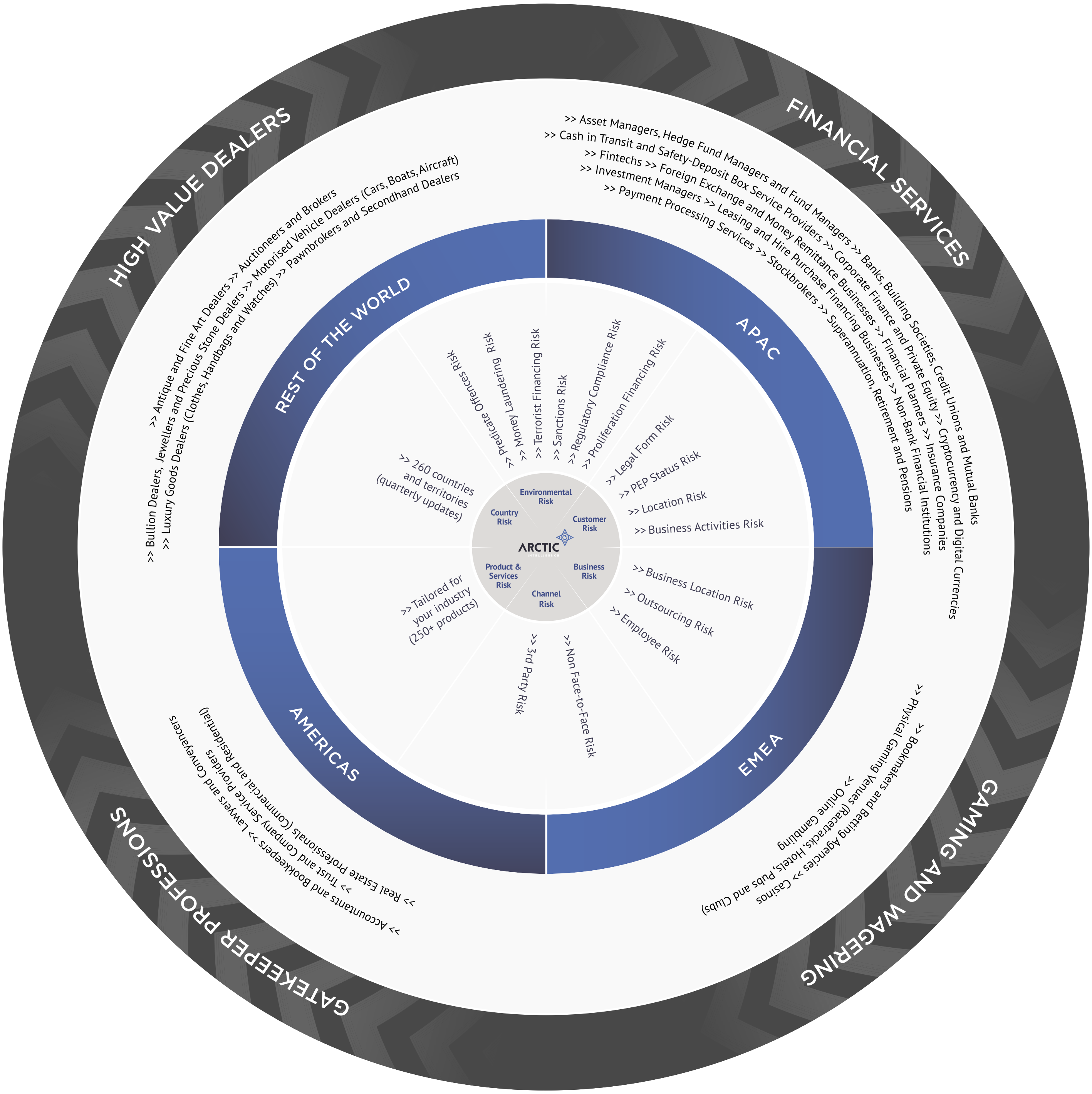
Like building a house, the EWRA is the foundation of any AML/CTF program and must be executed in an explainable, logical and defensible manner, so the systems, procedures and controls that are implemented are both appropriate and proportionate to the identified risks.



3.6. What risks should be considered in EWRAs when assessing ML/TF risks?

The regulatory guidance for what should be considered by regulated entities when conducting EWRA's for money laundering can be quite limited and does not explain how each of the risk areas should be considered both individually and in the context of each other.

The diagram below highlights some of the considerations that buyers of EWRA solutions should expect to see regarding the risk model libraries to determine whether they are sufficiently comprehensive to complete a financial crime financing risk assessment.

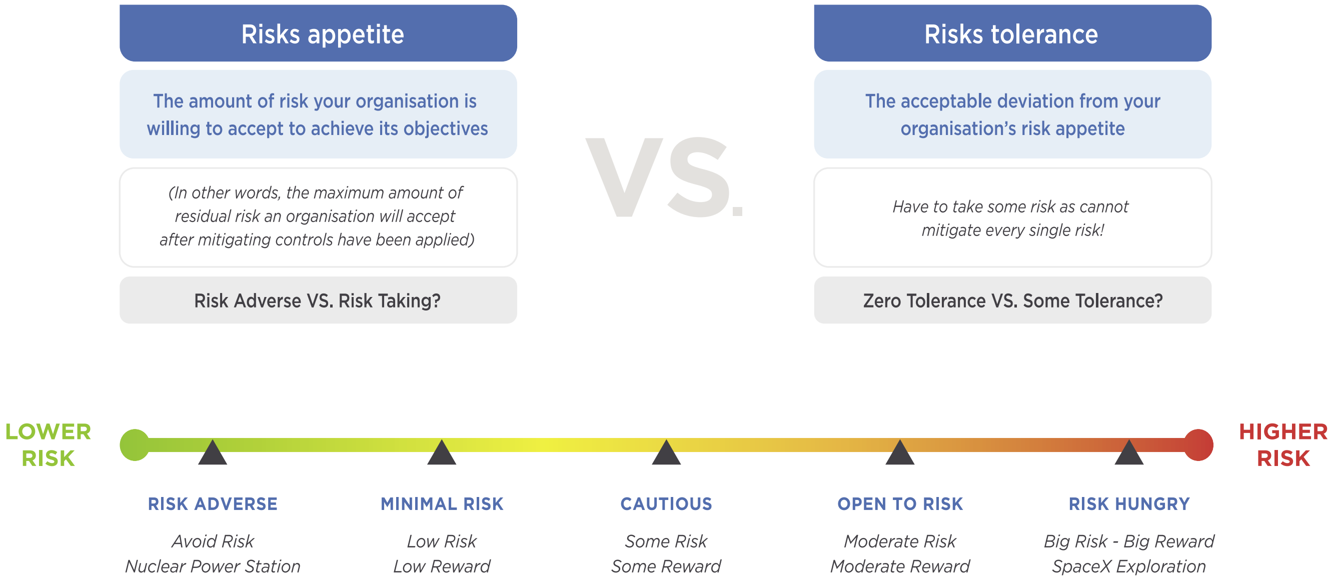

HIGH VALUE DEALERS
>> Antique and Fine Art Dealers >> Auctioneers and Brokers
>> Bullion Dealers, Jewellers and Precious Stone Dealers >> Motorised Vehicle Dealers (Cars, Boats, Aircraft)
>> Luxury Goods Dealers (Clothes, Handbags and Watches) >> Pawnbrokers and Secondhand Dealers
FINANCIAL SERVICES
>> Asset Managers, Hedge Fund Managers and Fund Managers >> Banks, Building Societies, Credit Unions and Mutual Banks
>> Cash in Transit and Safety-Deposit Box Service Providers >> Corporate Finance and Private Equity >> Cryptocurrency and Digital Currencies
>> Fintechs >> Foreign Exchange and Money Remittance Businesses >> Financial Planners >> Insurance Companies
>> Investment Managers >> Leasing and Hire Purchase Financing Businesses >> Non-Bank Financial Institutions
>> Payment Processing Services >> Stockbrokers >> Superannuation, Retirement and Pensions
GAMING AND WAGERING
>> Bookmakers and Betting Agencies >> Casinos
>> Physical Gaming Venues (Racetracks, Hotels, Pubs and Clubs)
>> Online Gambling
GATEKEEPER PROFESSIONS
>> Real Estate Professionals (Commercial and Residential)
>> Trust and Company Service Providers
>> Accountants and Bookkeepers >> Lawyers and Conveyancers
REST OF THE WORLD
APAC
EMEA
AMERICAS
>> Predicate Offences Risk
>> Money Laundering Risk
>> Terrorist Financing Risk
>> Sanctions Risk
>> Regulatory Compliance Risk
>> Proliferation Financing Risk
>> Legal Form Risk
>> PEP Status Risk
>> Location Risk
>> Business Activities Risk
>> Business Location Risk
>> Outsourcing Risk
>> Employee Risk
>> Non Face-to-Face Risk
>> 3rd Party Risk
>> 260 countries and territories (quarterly updates)
>> Tailored for your industry (250+ products)
Environmental Risk
Customer Risk
Business Risk
Channel Risk
Product & Services Risk
Country Risk
ARCTIC INTELLIGENCE

3.7. What are some of the challenges typically faced in conducting EWRA’s?

Challenge 1: Defining risk appetite and risk tolerance

Understanding your organisation’s risk appetite and risk tolerance is essential in helping you design a control framework that is appropriate and proportionate to risks within this context. The Board decides the nature and extent of the significant risks the organisation is willing to embrace to achieve its objectives.

The diagram below introduces these concepts and provides an example.



Risks appetite

The amount of risk your organisation is willing to accept to achieve its objectives

(In other words, the maximum amount of residual risk an organisation will accept after mitigating controls have been applied)

Risk Adverse VS. Risk Taking?

VS.

Risks tolerance

The acceptable deviation from your organisation’s risk appetite

Have to take some risk as cannot mitigate every single risk!

Zero Tolerance VS. Some Tolerance?

LOWER RISK

HIGHER RISK

RISK ADVERSE

Avoid Risk
Nuclear Power Station

MINIMAL RISK

Low Risk
Low Reward

CAUTIOUS

Some Risk
Some Reward

OPEN TO RISK

Moderate Risk
Moderate Reward

RISK HUNGRY

Big Risk - Big Reward
SpaceX Exploration

Challenge 2: Defining what methodology to use

One of the most important things when deciding on the methodology is the risk management framework to use in respect of inherent and residual risk matrices.

The types of things you must decide when defining what methodology to use are:

- The rating scale for assessing risk, for example, low, medium or high or alternatively, a more granular scale, such as very low, low, moderate, high, very high and extreme
- The rating scale and definitions for assessing the likelihood of a risk occurring, for example, rare, unlikely, moderately likely, likely, highly likely, guaranteed or similar scale
- The rating scale and definitions for assessing the impact of a risk were it to occur, for example, no impact, negligible, very low, low, moderate, high, very high or catastrophic or similar scale
- The rating scale and definitions for assessing the effectiveness of controls, for example, not tested, poor/ineffective/weak/needs improvement, moderately effective, effective/meets expectations, strong/highly effective or similar scale
- The inherent risk rating matrix, for example what the inherent risk ratings of different combinations of likelihood and impact are, for example, highly likely and very high impact etc.
- The residual risk rating matrix, for example, a high inherent risk that has strong/highly effective controls may reduce the residual risk rating to medium or low.

There is no right or wrong approach – it is a matter of preference, but it is important to be able to explain and defend the logic used and, in our experience, having a more granular risk rating methodology provides greater flexibility.

Challenge 3: Assessing the nature, size and complexity of the organisation

Risk assessments must be appropriate and proportionate to the organisation's nature, size and complexity - but what does this mean in practical terms?

Below are some questions you can ask to understand this better for your organisation:

Nature of the business	Size of the business	Complexity of the business
What does the business do?	What is the size of the customer base?	How many products/services are offered?
How does it make money?	How much revenue is earned annually?	What is the nature of products/services?
What products and services are offered?	How much staff does the business employ?	How many and what channels are used?
What types of customers does it serve?	How many customers are served?	How many countries does it operate in?
What customer segments does it serve?	How many offices/branches are there?	How regulated is the business?
How are customers acquired?		What is the ownership structure?
What countries does it operate in?		What is the governance structure?

Smaller, more manageable organisations are typically less risky than larger, more complex organisations due to there being more potential points of failure and operational risks resulting from managing a more complex organisation.

Challenge 4: Adopting subjective, objective or hybrid risk indicators

Risk assessments that take a subjective approach rely on individuals to judge the likelihood and impact of risks occurring, as well as the design and operational effectiveness of controls. This is often criticised due to the individual bias that may be introduced.

Risk Assessments that take an objective approach and are more data-driven, whilst less subjective, are often criticised for being too black and white. They could miss subtle qualitative elements or be challenged in accessing the data needed in a timely and accurate manner.

Our view is that a hybrid approach that mixes qualitative and quantitative elements to the risk assessment is best - but what is the approach you will take?

Subjective approach	Objective approach	Hybrid approach
Is question-driven and relies upon An individual judment of:	**Is data-driven and relies upon the organisation's data mastery:**	**Is both question-driven (qualitative) & data-driven (quantitative)**
The likelihood of a risk occurring?	What data inputs do I need?	Qualitative inputs to risk combined with quantitative data inputs can often lead to a more robust outcome
The impact of a risk occurring?	Is data all in one place or distributed?	
What the inherent risk of this is?	Is data standardised, clean & accurate?	
How effective controls are at reducing risk?	How will I extract/load/transform data?	
What the residual risk is?	How will I apply risk decisioning to data?	

Challenge 5: Deciding what risk groups, categories, factors and indicators to use

One of the most important decisions to make is what risk groups, categories, factors and indicators to use. In our experience, organisations often do not give this enough thought, which results in a flawed approach to enterprise-wide money laundering and terrorism financing risk assessments.

You must decide the level of granularity that is appropriate and proportionate to your organisation's risk management framework. However, if you are a complex organisation that has multiple products, channels, customer types, and geographic risk exposures, it will be expected that you have a good understanding of what risks might be relevant for your organisation to consider in the scope of the assessment.

The diagram below shows some examples of the risk groups and risk categories that could be considered:

Environmental risks

Assess the organisations vulnerability to:

Predicate Offences - deceptive crimes, illicit trafficking, personal crimes, property crimes.

Money Laundering - higher risks associated with - business operations, channels, customer transactions, customers, products and services.

Terrorism Financing - higher customer risk and customer transaction risks.

Financial Sanctions - higher customer risk and customer transaction risks.

Regulatory Compliance Risks - governance, and oversight, program alignment to risk, program non-compliance and reporting.

Customer risks

Assess the organisations vulnerability to:

Customer Types - segmentation of customer base - individuals, private companies, public companies, offshore companies, trusts, partnerships including extent UBO's known.

Customer PEP Status - number of customers that are foreign or domestic PEPs and categories of PEPs.

Customer Location Risk - segmentation of customers by location/geography.

Customer Business Risk - segmentation of customers by industry sector/occupation.

Customer Source of Wealth - segmentation of customers where this information is known, unknown or vague.

Business risks

Assess the organisations vulnerability to:

Business Location - extent of business operations that are carried out overseas (and which countries and which operations).

Outsourcing Risk - extent to which third parties are used to perform AML controls on your organisation's behalf, the nature of outsourced controls, the extent of controls over outsourced controls.

Employee Risks - number of employees, proportion that are customer-facing, proportion in key risk roles, proportion that have been background screened and extent of background screening, proportion having adverse screening results, functions performed, etc.

Channel risks

Assess the organisations vulnerability to:

Non-face-to-face channels - the extent to which customers are met face to face during on-boarding or when servicing their accounts.

Methods of interacting with customers - what methods are used, somewhat anonymous (e.g., internet, social media, SMS) or less anonymous (e.g., branch, post office, video conferencing, telephones, etc.)

Use of third parties - the extent to which third parties are used as channels (e.g., introducing brokers, sales agents, intermediaries) and the locations of any of these channels.

Product & services risks

Assess the organisations vulnerability to:

Product and services - extent to which different products and services are offered (250+ Financial Services Products).

Attributes of products and services that make them more attractive to money launderers - for example, transfer of funds into and out of accounts through multiple methods, by unrelated third-parties, using remote access methods, from/to foreign jurisdictions, value/transaction limits, acceptance of cash or cash equivalents, cooling off periods, etc.

Extensiveness of use - what proportion of customers use the product or service, what proportion of revenues are attributable, whether any transaction monitoring controls or suspicious matters related to different types of products, etc.

Country risks

Assess the organisations vulnerability to:

Methodology - there is no universal standard for country risk and is geo-political, but there are numerous recognised sources such as Targeted Financial Sanctions (UN), FATF AML Concerns, High Risk and Other Monitored Jurisdictions, Terrorism Vulnerability (US Department) Illicit Durg Vulnerability (US International Narcotics Strategy Control Report), Corruption Vulnerability (Transparency International Corruption Perceptions Index), Financial Secrecy (Index), Kimberly Process (Conflict Diamonds, etc.) and FATF Members/observer Lists (and extent of compliance).

Frequency - each of these is published at different times of the year and uses different rating scales, so agreeing to a process and frequency of updates (and reflection through the ML/TF risk assessment can be a challenge!

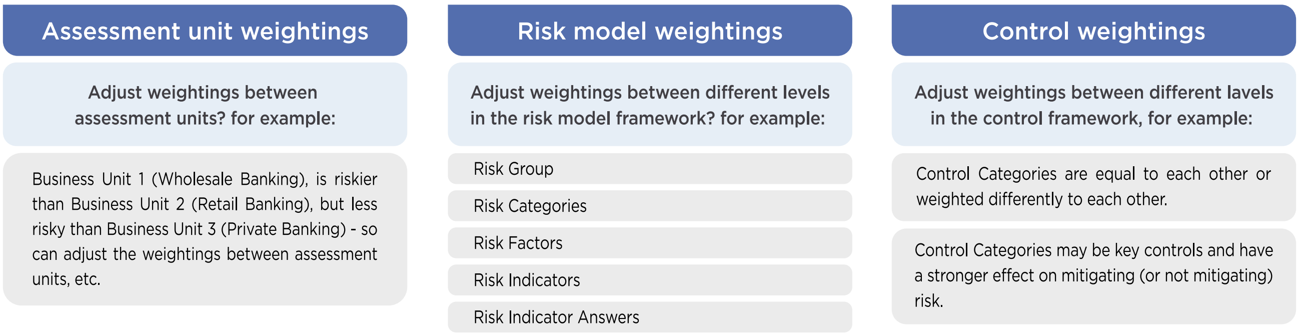
Challenge 6: Deciding whether to introduce proportionality (weighting) or not

The level of sophistication your organisation decides to use could range from treating all risks equally to applying a level of proportionality, which reflects that some risks (and controls) are more important than others and should therefore play a more important role in the risk assessment.

In more sophisticated risk assessment methodologies, weighting can be considered in three areas:

- **Assessment Unit Weightings** - meaning treating one assessment unit (i.e., country, operating group, business unit or product etc.) as more or less important than another
- **Risk Model Weightings** - meaning that certain risk groups, risk categories, risk factors or risk indicators are considered to be more or less important than others
- **Control Weightings** - meaning that some controls should be considered as more important (also referred to as key controls) and play a greater role in reducing residual risks.

The diagram below explains these concepts and is something you should consider and expect in any well-designed Enterprise-Wide Risk Management solution.



Assessment unit weightings

Adjust weightings between assessment units? for example:

Business Unit 1 (Wholesale Banking), is riskier than Business Unit 2 (Retail Banking), but less risky than Business Unit 3 (Private Banking) - so can adjust the weightings between assessment units, etc.

Risk model weightings

Adjust weightings between different levels in the risk model framework? for example:

Risk Group

Risk Categories

Risk Factors

Risk Indicators

Risk Indicator Answers

Control weightings

Adjust weightings between different lavels in the control framework, for example:

Control Categories are equal to each other or weighted differently to each other.

Control Categories may be key controls and have a stronger effect on mitigating (or not mitigating) risk.

Challenge 7: Assessing the design and operational effectiveness of controls

An important element of any Enterprise-Wide Risk Assessment is the assessment of controls to determine whether they are effective in mitigating, managing and ultimately reducing the residual risk.

Controls effectiveness is usually considered from the following perspectives: the first is **control design**, meaning whether the control is present in the first place and, if so, whether it is fit for purpose and secondly **operational effectiveness**, meaning whether a control has actually been implemented and, if so, if it is operationally effective in mitigating the risk of the control for which it was designed, to ultimately form a view on the overall effectiveness of that control.

Another consideration is the type of control that are appropriate to manage risks. There are typically three types of controls:

- **Preventative controls** – controls designed to deter or prevent risks
- **Corrective controls** – controls designed to address breaches/incidents
- **Detective controls** – controls designed to see whether a risk has occurred.

The existence and effectiveness of controls have the effect of reducing residual risks.

Challenge 8: Assessing how all risks link together in the risk assessment

Assessing different risk groups, for example, environmental, business, customer, product and service, and channel and geographic, independently and in isolation won't provide a meaningful result. That's because each of these risks are interconnected and being able to design and implement a risk model that considers combinations of these risks is more likely to be a defensible approach.

An example of this, is to understand how a higher-risk customer that has access to higher-risk products and services and is transacting through higher-risk channels and jurisdictions, should be treated from a risk assessment perspective.

Another important element to consider is how your organisation maps the risks and controls together in an assessment. This is particularly complicated when these relationships are many-to-many between risks and controls, and many-to-many between controls and risks, so you should understand how any Enterprise-Wide Risk Assessment solution supports this complexity.

Challenge 9: Deciding whether to adopt spreadsheet or system-based approaches

As a RegTech vendor, we know we are biased, but we're convinced that manual Excel and Word approaches have significant limitations in conducting EWRAs. The diagram below summarises what we see as the biggest limitations of Excel and Word-based approaches (this was based on a blog[5] we wrote five years ago and is even more relevant today).

Spreadsheet based approach	System based approach
Cost effective - spreadsheets are free (but you'll pay in other ways!)	**Some cost involved** - but very modest compared to benefits
No/Limited Audit Trail - No field level validation or date/time stamping	**Full Audit Trail** - field level comments, track reviewers/approvers real-time
Spreadsheet break and are error prone - no testing to validate logic	**Full testing** - systems are subject to rigorous UAT, Regression & PVT
No live saving - if your file is corrupted you will lose work	**Cloud-based** - 99.98% uptime and fully backed up forever
No version controls - how do you ensure the assessment is the latest?	**Full version controls** - ensures full change control on content/versions
No user access controls - very limited password protection only	**Full user access controls** - set permissions to system access/functions
No uploading documents - cannot upload evidence (e.g. control tests)	**Full upload** - upload risks, controls & control testing evidence/findings
Excel has only basic graphics - need to plug-in to reporting tools	**In-build analytics** - real-time analytics across multiple assessment units
Less efficient - sending/receiving across the organisation is slow	**Highly efficient** - hundreds of users can interact on the platform real-time
No report writing - results need to be written up separately	**Full report writing** - auto generated reports and add commentary easily
No guidance notes - no tooltips, help centres or other support	**Fully supported** - tooltips, help centre, video tutorial, in app=support
Hard to maintain - no "push through" of changes of audit trail of these	**Easy to maintain** - update/push throughcontent and functional changes

[5] https://arctic-intelligence.com/insights/blog/is-excel-really-fit-for-purpose-for-running-risk-and-compliance-assessments

Challenge 10: Maintaining the risk assessment and ensuring it remains up-to-date

The only certainty in risk and compliance management is that organisations are in a constant state of flux. So, with things changing constantly, how do you keep up-to-date?

Regulators expect that Enterprise-Wide Risk Assessments are not static and that they are maintained over time in response to internal and external changes. Most forward-thinking organisations implement both time-based and/or event-based triggers to determine when a refresh of the risk assessment is conducted. Have you determined exactly what would trigger this in your organisation?

The table that follows summarises some of the event-based triggers:

External events		Internal events
Regulatory events	Other events	
Enforcement activity targeted at certain sectors or activities - could these risks occur in your business?	Changes in the geo-political landscape making a country higher-risk than before.	External (or internal) independent review highlighting deficiencies in the ML/TF risk assessment.
Changes in AML/CTF regulations or rules - how do they impact your organisation?	Changes in various published country risk rankings (i.e., transparency international).	Review of ML/TF risk assessment prior to annual compliance reports being filed with the regulator.
Changes in guidance and risk typologies - has your ML/TF risk assessment considered this?	Increased media scrutiny on certain companies, industries or activities.	Organisation is launching or has launched new products and/or services, which pose new ML/TF risks.
Consultation papers about proposed regulatory changes - what would be the impact on your business if these laws are enacted?	Changes in the threat landscape as criminals find more innovative ways to launder criminal proceeds.	Organisation is targeting new customer segments, expanding into new geographic markets or generally changing its business.
International guidance issued by the FATF, the Wolfsberg Group, the Egmont Group highlighting trends and risk-related guidance.	Emerging technologies that could pose new threats to your organisation, such as criminal use of Artificial Intelligence.	Merger and acquisitions activity (i.e., divestments, acquisitions) bringing together businesses with different risks and approaches.
Publishing of National Risk Assessments highlighting threats at national, industry, product or activity level.	Collaboration through public and private partnerships that could present opportunities to update ML/TF risks and controls.	Change in Board and/or Senior Management, with a greater focus on risk appetite and management.
Release of federal, state or local crime statistics relevant to your industry and operations.	Investigations by journalists or law enforcement into organised criminal activity that is related to your organisation's operations.	Appointment of a new AML/CTF Compliance Officer/MLRO looking to make changes to the ML/TF risk assessment and AML Program.
Criminal or civil prosecutions or other enforcement action (i.e. enforceable undertaking, regulator appointed independent auditors).	Class actions being filed against organisations for failing to manage or disclose risks.	Appointment of risk, compliance or legal advisors with experience in conducting and updating ML/TF risk assessments.

If organisations have not refreshed their Enterprise-Wide Risk Assessment based on any of the prior event-based triggers within at least the past 12 months, it's time to ask whether the last risk assessment that was completed is an accurate reflection of where the organisation's risk stands today.

Also, it is important to understand how your organisation is 'horizon scanning' across the regulatory landscape for new and emerging risks and threats, as well as changes in rules, regulations and risks, in each of the countries the business operates in, to ensure that your approach to risk management remains current.

3.8 How do technology-enabled solutions help overcome these challenges?

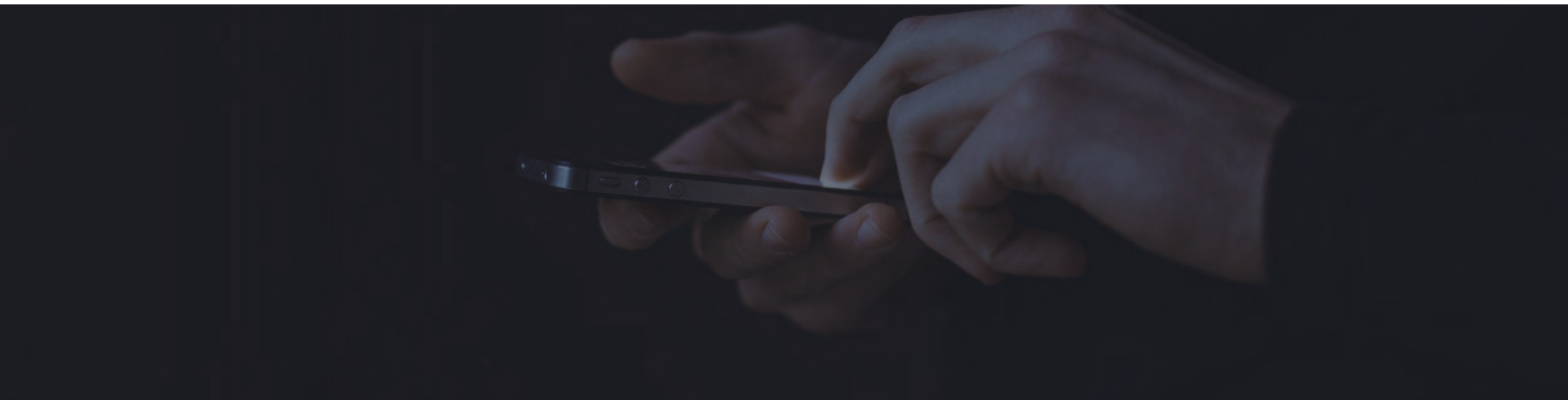
In the previous section, we covered many of the challenges faced by organisations when designing, implementing and maintaining Enterprise-Wide Risk Assessments. In this section, we highlight some of the key benefits that regulatory technology (RegTech) can deliver to improve the execution of risk management across your organisation.

As we have seen, financial crime risks and threats are constantly evolving and regulatory expectations are increasing along with new laws and regulations, as well as new guidance on risk typologies at a national and international level. This makes these challenges feel overwhelming to most organisations.

The emergence of RegTech solutions and the increasing willingness of organisations to adopt new and emerging technologies has resulted in new ways to strengthen your organisation's defences against financial crime in a fast-changing and interconnected environment.

Traditionally, enterprise risks have been managed in silos with different functions across the three lines of defence, for example, the first-line (i.e., sales, operations and customer support), second-line (legal, risk and compliance) and third-line (internal audit, external auditors, consultants and advisers) all having a role to play in identifying, assessing and managing risk.

Across these parts of an organisation, there is also a need to manage a diverse range of risks such as strategic, financial, operational, and regulatory risks, which are constantly changing. This means it is more important than ever to be able to assess and view risks at an enterprise level to understand the current risks and threats in a timely manner in order to be able to inform strategic and tactical decision-making.



The table below summarises some of the key benefits that Enterprise-Wide Risk Assessment technology can deliver for your organisation.

Theme	Benefits
Efficiency	• Complete risk assessments in days or weeks, not months or quarters • Reduce the time to gather data, assess risk and summarise results • Huge reduction in data aggregation and reporting - make better decisions, faster • Access all relevant data to any assessment in one place - no searching for files, no version control issues and remain organised for regulatory visits • Clearly document follow-up actions and receive email alert notifications to update
Quality	• Major improvements in quality - follow a methodical process, with a full audit trail over key decisions made and date/time stamped by who completed the activity • Gain deep insights into risk and control assessments through dashboard reports • Improve record keeping by producing supporting evidence instantly to regulators on demand • Ensures that the risk assessment process is easy to follow, is repeatable and standardised • Produces clear, accurate and timely reports and actionable insights to support decisions
Support	• Applications are subject to far more rigorous testing than formulas in Excel • Application support is provided - email/phone and self-service help centre support • Updates on regulatory changes, country and other risk and control models • Reduce reliance on expensive consultants and become more self-sufficient • Easy deployment of technology solutions in shared or private cloud environments

Technology has an increasingly important role to play in a fast-moving risk, threat and regulatory environment and will act as an enabler for smarter, faster and more evidence-based decision-making.

At the heart of many major compliance failings is often ineffective risk management systems, procedures and controls that are not interconnected, accurate or timely and have resulted in some spectacular failures.

Investing in the right risk management technology platforms is often a big step for many organisations and many legacy GRC systems have simply not kept pace and many are no longer fit for purpose to support critical risk management processes. It might be time to consider what you are looking for to manage your risk function efficiently and effectively.

The question organisations need to ask themselves is not 'can I afford to?', but 'can I afford not to?' This is the subject of the next section of this Buyer's Guide, where we will explore the key considerations when making any investment into risk management technology.

4. What are the key considerations when assessing vendors?

This section of the Buyer's Guide will cover how to determine your requirements and evaluate existing or new vendors GRC/EWRA Solutions, including the key considerations you should discuss with your vendors.

We will cover:

- The importance of clearly documenting your functional, technical and support requirements
- The key differences between generic GRC platforms and EWRA platforms (which can perform all the functions of a GRC platform and much more)
- The general considerations in relation to solution design, implementation and maintenance
- The core functionality that you should expect to see in any GRC/EWRA platform
- The key workflows involved in performing EWRAs, key considerations and why they matter.

4.1. What exactly is it that you want and need?

'So tell me what you want, what you really, really want' is a phrase just as relevant to 90's girl bands as it is to selecting a risk management solution that not only meets your current needs but is future-proofed against changing needs, many of which you have no idea about yet.

Ultimately, the answer to this question lies in being able to have open, honest and transparent conversations within your teams and with your senior stakeholders to honestly reflect on whether the current systems (including the myriad of spreadsheets used for financial crime risk assessments) are serving you well.

This means you'll need to critically examine your existing systems to work out what you do and don't like. In addition, you should determine the core features and functionality that you need to do your job, but which might be missing in your current systems. Then, you'll need to and together a functional requirements checklist of key considerations and rate these as 'must have' or 'nice to have' - and only then start shopping!

4.2. Governance, Risk and Compliance (GRC) vs. EWRA Solutions

If you already have a GRC system, you should ask yourself if it can really do what you need it to for conducting financial crime risk assessments.

Many of our larger clients already have an Enterprise Risk Management (ERM) platform that they use to manage business risks, such as Strategic, Operational, Financial and Regulatory risks. Whilst these systems have merit as repositories for storing libraries of risks and controls, they often fall short in providing an end-to-end auditable workflow for conducting enterprise-wide money laundering and terrorism financing risk assessments.

At Arctic Intelligence, our Risk Assessment Platform can act as a generic Governance, Risk and Compliance (GRC) system but it is also sophisticated enough to be highly configurable in key areas, which most GRC solutions simply cannot do.

For example, every business is different and adopting different methodologies for assessing inherent and residual risks is often very different. Most GRC systems have been built around fixed, rather than flexible and fully configurable risk methodologies, that allow full tailoring of the inherent and residual risk definitions, scores and matrix values, as well as the values and logic for assessing the control design and operational effectiveness of controls.

Another key limitation our clients point out with their existing GRC systems is that they are not designed to execute an EWRA where complex enterprises may have to conduct 50 to 100 assessments across different geographic regions, operating groups, business units, and product or functional lines. They also must complete these assessments inside the platform and automatically aggregate the inherent risks, control effectiveness ratings and residual risks in real-time across the enterprise. Our Risk Assessment Platform does this with ease.

4.3. What is the core functionality that you should expect to see?

In most GRC/EWRA platforms there are a number of key workflows performed and which, from a vendor selection perspective must be understood. This includes the key considerations to evaluate and the reasons that these considerations matter in your evaluation of vendors.

The key workflows include:

- Initial configuration and setup
- Context setting and supporting documents
- User permissions and workflow
- Assessing inherent risks
- Assessing control effectiveness
- Calculating residual risks
- Dashboard and analytics
- Automation and data-driven elements
- Audit trail and management actions
- Report writing and record-keeping
- Other workflows.

The rest of this section should be treated as a reference guide and not all of these workflows may be relevant to your organisation or use case. But, where relevant, it is designed to give you pointers on which questions to ask your vendors.

4.4. Key workflows in the Enterprise-Wide Risk Assessment process

This section of the document considers some of the key workflows that you should consider when determining your business requirements and the important and differentiating functionality that you should expect to see in any flexible GRC/EWRA platform.

4.4.1. Initial configuration and setup

The initial configuration and setup refers to the flexibility of the platform in setting up the system to do exactly what you need it to do, along with some of the key considerations and why they matter.

Key considerations	Why does this matter?
Is the risk assessment methodology flexible to support any risk management framework?	No two organisations have exactly the same risk assessment methodology, meaning the way in which inherent risks (likelihood x impact), as well as control effectiveness ratings and residual risk ratings are defined and described and assessed, for example, the underlying matrices (i.e., 3x3, 4x4, 5x5, 6x6) can be very different. A platform with a single methodology or rigid methodology that is not able to be tailored is very restrictive, particularly if assessing different risk domains in different ways. You should ask if your vendor allows you to tailor their platform to your risk methodology, rather than you having to tailor your risk methodology to the platform.
Can I create my own risk models or any risk domain I choose?	GRC/EWRA platforms that have a 'hard-wired', (meaning pre-defined) list of risk groups, risk categories, risk factors and risk indicators, run the risk of regulators criticising your organisation for operating a risk assessment that is not tailored specifically enough for your business. This is particularly true for larger, more complex and systemically important organisations. You should ask your vendor to confirm if they have content modules they licence and maintain and whether you can build your own bespoke risk models with any risk indicators and any risk hierarchy you like. This is critically important for maintaining a flexible risk management framework.
Can I apply risk weightings to every level of my risk models?	Not all risks are treated equally, so a GRC/EWRA platform needs to be able to apply both proportionate (equal) and disproportionate (unequal) weightings within the risk model and ideally at every level within the model, for example, between risk groups, risk categories, risk factors and risk indicators. GRC/EWRA platforms that treat risks equally without any sophistication for allowing risk weightings are not fit for purpose and should be avoided, so ask your vendor this.

Can I define my own qualitative and quantitative answer sets?	Having the flexibility to assign qualitative, quantitative or a mixture of both answer sets across risk indicators is important. Being able to create these bespoke and align back to the methodology is important. For example, in some scenarios, an answer of 'Yes', could be positive and in other scenarios 'Yes', could be a negative response, so your solution needs to be flexible enough for you to define answer sets and assign values.
Can I import or feed my control libraries into the platform?	A key part of any GRC/EWRA platform is the ability to assess the design and operational effectiveness of controls. It is important to be able to create, import or integrate to a controls library containing the names of controls, the type of control (i.e., preventative, detective), the types of control tests to be performed and the types of evidence to be performed.
Can I assign weightings to controls?	Similar to risks, not all controls are equally effective at mitigating risks. Some controls might be key controls and a greater importance can be applied to these through weighting, so any GRC/EWRA platform that does not facilitate this is also not fit for purpose.
Can I apply any logic to control design and operational effectiveness testing?	Assessing the design and operational effectiveness of controls is important in determining residual risk, but there should be an ability to limit the overall control effectiveness rating of controls, for example, if the design is assessed as poor and the performance of the control is assessed as fair, there should be the ability to apply some logic that prevents a user from selecting an overall control effectiveness of excellent/highly effective controls, as this would be in contrast to the assessment. Smart GRC/EWRA platforms have the ability to configure and modify this logic in an assessment.
Can I create user roles in the platform and assign permissions to users?	The ability to create user roles of your choosing, rather than predefined roles, and then assign granular permissions about what that user can and cannot view, edit or access is important. For example, some users should be prohibited from seeing other risk assessments created by others, while some users may be able to review but not approve controls, apply overrides or any other function. You should ask your vendor how user access controls work and the level of flexibility this has to enable or disable features and functionality based on role-based permissions.
What other settings can I configure?	Most sophisticated GRC/EWRA platforms have a range of other configuration settings, too lengthy to name individually here but could include: • Ability to import and maintain country risks • Ability to assign users to an account • Email notifications • Report output configurations • Ability to integrate to third-party systems via SSO.

4.4.2. Context Setting and Supporting Documents

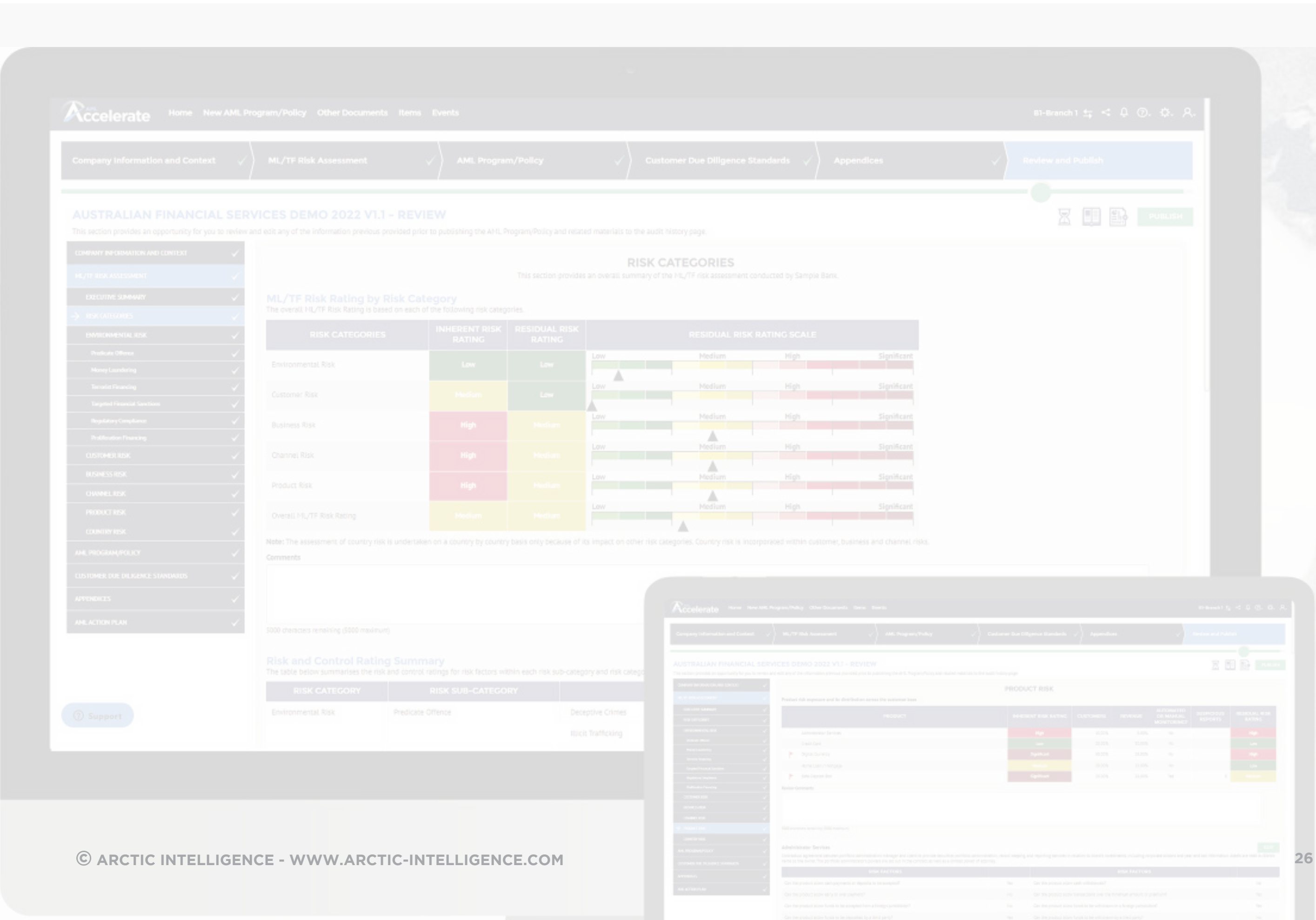
The context setting and supporting documents refer to the ability of the platform to allow users to define the nature, size and complexity of the assessment and allow uploading of supporting documents.

Key considerations	Why does this matter?
Can I provide context behind the nature, size and complexity of the assessment I am conducting?	Regulators expect you to be able to clearly define the nature, size and complexity of the business, so they are able to assess if mitigating controls are both appropriate and proportionate to the identified risks in the context of this. Being able to record this is important.
Can I upload documents to the assessment?	Being able to upload, store and retrieve completed supporting documents, as well as published outputs is important for record keeping purposes. Often, independent reviews or regulatory visits happen months (or years) after the risk assessment period, and it is important to demonstrate what was completed at the time.
How does the organisational context information I enter inform the risk assessment process?	As part of the context, the platform should capture information about the size of the business (i.e., by revenue, employees, customers, transactions etc.), nature of the business (i.e., what products and services are offered, what channels are used, what customers are supported, and the countries exposed to). In respect of country risk exposure, it is important to be able to create a country risk rating matrix based on sound logic and data sources and include this in the assessment in various ways, for example, countries where you have employees, customers, business partners/suppliers, business operations etc.

4.4.3. User permissions and workflow

The user permissions and workflow refers to the flexibility of the platform to assign risks or controls to different levels of user (i.e., reviewer, approver) and track the audit trail through the workflow.

Key considerations	Why does this matter?
Can I create roles in the platform and assign permissions to each of these roles?	Tailoring roles to suit your organisation rather than be limited to a set of pre-defined roles offers more flexibility.
Can I assign different activities to different people (i.e., reviewer, approver and signoff)?	Being able to assign risks or controls for assessments to different users is more efficient and auditable.
Can I view the status of the activities of each user (i.e., not started, awaiting approval, approved)?	Being able to see the status of risks or controls as they move through the workflow makes it easily visible to all.
Does the system provide a field level audit trail of risks and controls, as they move through workflow?	Seeing what the status is, any comments, attachments and actions/issues helps evidence the process.
Is the audit trail of workflow statuses exportable?	Being able to export the outputs of the workflow audit trail to csv allows this to be provided to auditors easily.
Does the system provide a way of tracking the status of workflow items needing to be actioned?	Maintaining a list of open and closed issues/actions helps to manage enterprise risk management.



4.4.4. Assessing Inherent Risks

Assessing inherent risks is a critical element to any GRC/EWRA platform and ensuring that the assessment is explainable and defendable is a very important element to get right.

Key considerations	Why does this matter?
Does the platform allow users to define their own risks to assess?	Being able to specifically tailor the risk groups, categories, factors and indicators, as well as answer types and weightings is important to demonstrate that this was purposefully designed for your organisation.
Does the platform allow traditional methods of inherent risk assessment?	Traditional approaches to risk management like to see the likelihood and impact of risks being assessed.
Does the platform have any logic to allow the inherent risk to be automatically calculated?	Modern approaches to risk management can automatically calculate inherent risks based on an aggregation across a range of risk indicators derived from the answer set(s) and weighting of risk indicators.
Does the platform allow users to weight risks against each other?	Not all risks are the same, so being able to apply weighting to risks is important in making this distinction.
Does the platform allow users to add comments and add links or attachments to support risk decisions?	Mapping risks to controls (and vice-versa) is important to explain the lineage, meaning linking the risk indicator to the control or controls that help mitigate that risk.
Does the platform allow users to map risks to a control library?	Maintaining a list of open and closed issues/actions helps to manage enterprise risk management.
Does the platform allow users to add any actions or issues when assessing inherent risks?	During the assessment it may become obvious that there is a gap or opportunity for improvement and having the ability to attach actions will help improve.
Does the platform summarise inherent risks at each level in the hierarchy and provide an overall status?	Understanding the inherent risks for each risk indicator and also across multiple risk indicators provides a clearer picture of the risks assessment.

4.4.5. Assessing Control Effectiveness

Assessing the control design, meaning whether a control is present and fit for purpose, or assessing the operational effectiveness of a control, meaning whether the control is operating as intended is a key element of the risk assessment process.

Key considerations	Why does this matter?
Does the system allow users to change the rating scales for assessing control effectiveness?	Every organisation may view control effectiveness ratings differently and should be able to define the rating scale that is most suitable to their risk management framework, rather than having to conform to a predefined set of values defined by a vendor.
Does the system allow users to apply any logic to the way in which overall effectiveness is calculated?	Preventing users from providing contradictory control effectiveness ratings is more efficient than having to review ratings after they have been applied, so logic can be applied to prevent these mismatches to save time. For example, if a user has selected 'Poor' for control design and 'Fair' for control performance, the overall effectiveness should be prevented from being set as 'Excellent/Highly Effective', as this would be contradictory.
Does the system allow users to map controls back to the risks the control is designed to mitigate?	Being able to map the controls that are relevant to the risks they are attempting to mitigate (as well as being able to map controls back to risk) provides more explainable and defendable outputs and allows the risks and control connectivities to be easily identified and managed. For example, if one control is mapped against multiple risks and if the control is determined to be only moderately effective, then if enhanced it could improve the management of multiple risks.
Does the system allow controls to be flagged as key controls and weighted to signify their importance?	Similar to risks not always being equal in importance, the same can be applied to controls, as some controls play a more meaningful role in reducing risks and should be able to be recognised as such. For example, a key control flag or a control weighting can be applied to indicate the relative importance of controls.
Does the system allow users to conduct control tests and attach evidence used to test their effectiveness?	Being able to evidence control testing has taken place and to recall the types of tests that were performed, the evidence gathered, as well as the sample files tested is an important element in demonstrable control testing.
Does the system allow users to add comments to support control testing or views on effectiveness?	Adding comments to substantiate control testing and control effectiveness is a minimum requirement.
Does the platform summarise control effectiveness and provide an overall status?	Platforms should aggregate controls against many risk indicators to give a summarised view of effectiveness.

4.4.6. Calculating Residual Risks

The calculation of residual risks as a result of assessing the control effectiveness of inherent risks will determine the residual risk ratings and allow decisions to be made as to whether this is in line with the risk appetite statement.

Key considerations	Why does this matter?
Does the system automatically calculate residual risks based on the risk methodology in the platform?	Platforms should be able to be configured, have the ability to weight risks and controls and be able to handle the automatic calculation of risks at every level in the model, for example: Calculating residual risk rating across risk indicators • Aggregating risk indicators up to a risk factor level • Aggregating risk factors to a risk category level • Aggregating risk categories to a risk group level • Aggregating across risk groups at an Assessment Unit level • Aggregating across multiple Assessment Units at an enterprise level.
Does the system apply any logic to allow for overrides to be applied?	There may be valid reasons for risk overrides to be applied, for example, first-line managers (i.e., business users) on risks and control effectiveness may differ significantly to the perspectives of second-line managers (i.e., risk and compliance), with the latter having discretion to apply overrides and comment on the reasons why these have been applied.
Does the system provide clear traceability on how the methodology works and how calculations are made?	Ultimately, risk management accountability rests with the regulated entity and not with the vendor, so platforms cannot be a black box. This means the way in which calculations are made, impact of weighting of risks and controls, post-assessment overrides and other features must be able to be clearly visible and understood by some (but maybe not all) platform users.
Does the system allow users to add comments to support views on the residual risk rating assessment?	Allowing users to apply comments, for example, on the outputs of the risk and controls assessment and add commentary such as whether the risks are in-line or outside of risk appetite is important information to capture when conducting assessments.
Does the platform summarise residual risks and provide an overall status?	In most risk assessments there could be hundreds of individual risk indicators, with aggregation back up to risk factors, then risk categories, then risk groups, then the assessment unit and ultimately assessment (enterprise). It is important for a platform to be able to summarise and display this at every level.

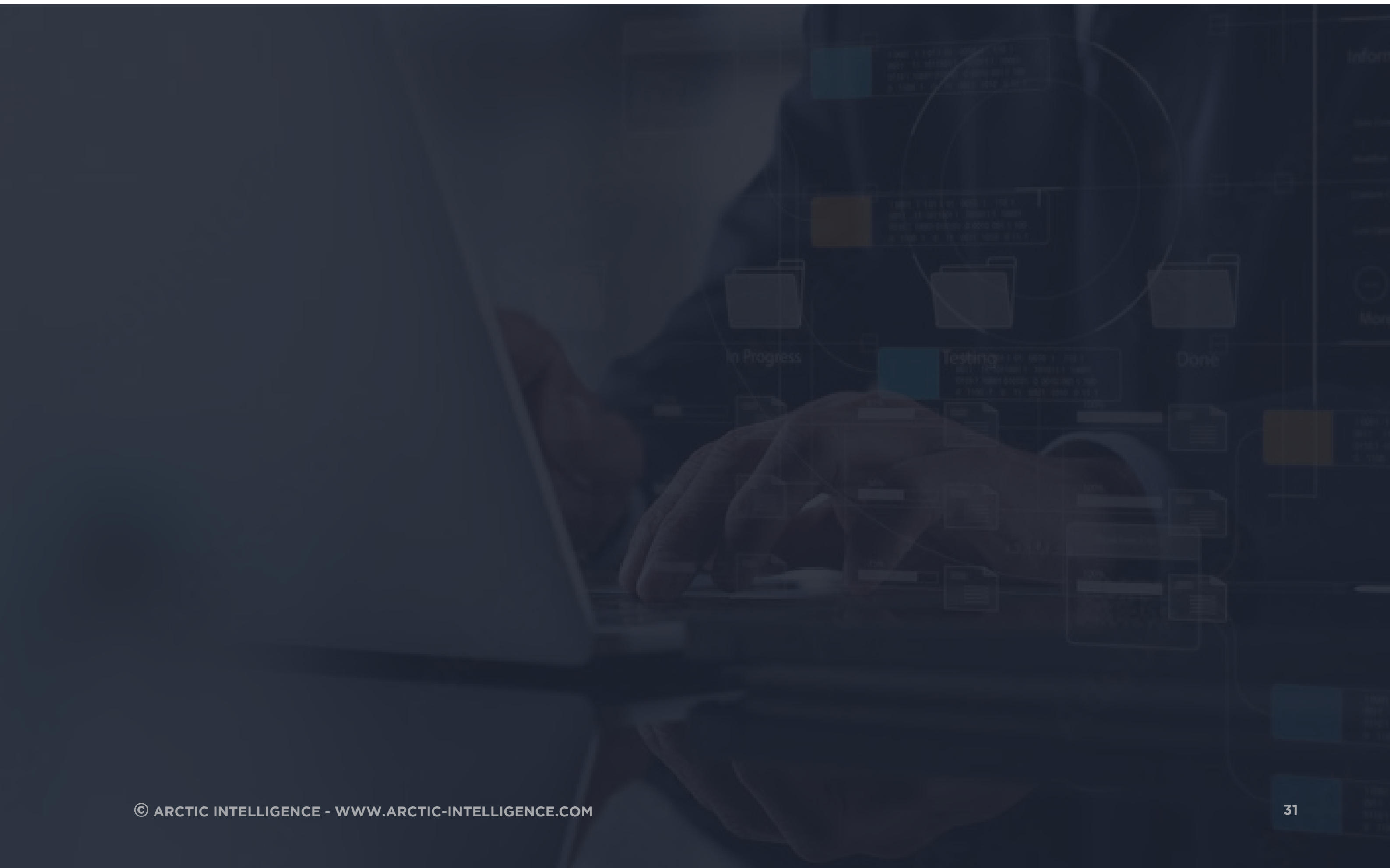
4.4.7. Dashboards and Analytics

Key considerations	Why does this matter?
Does the system generate dashboards at both assessment and assessment unit level?	Being able to view real-time dashboards at both the assessment unit level and aggregated to the assessment (enterprise) level is an important component of staying across the risk assessments, especially if they are fully drillable into any aspect of the risk assessment at a click of a button.
What dashboards are available at the assessment unit level?	At a minimum you should expect to see an assessment unit dashboard containing a status of risks assessed and not assessed, as well as the aggregate inherent risk rating by rating status, control effectiveness ratings by rating status and residual risk rating by rating status, which should be drillable to the risk indicator and control level.
What dashboards are available at the assessment level?	Gathering and analysing risk assessment data is often a major challenge noted and a material limitation of Excel is crunching multiple assessment unit inputs and creating an enterprise report. So, at a minimum, you should seek a solution that has an aggregation across all underlying assessment units (i.e., business unit, country, product or other measures) into an assessment (enterprise) level report with a comparative benchmark of inherent risk ratings, control effectiveness ratings and residual risk ratings.
Does the system generate dashboard reports on issues and actions?	Tracking remedial actions, issues and other items (i.e., findings, observations, recommendations etc.) is important to log in a centralised place against different assessments and to be able to track on a dashboard the progress that is being made in closing out those actions.
Can I configure the dashboards to suit my reporting needs?	Being able to decide what reports are shown within a dashboard is helpful in providing you with exactly the information that you are seeking.

ARCTIC
AML Enterprise-Wide Risk Assessment - UK - Leeds - Business Unit 5

4.4.8. Automation and Data-driven Elements

Key considerations	Why does this matter?
Does the platform have any data ingestion capabilities?	Forward-thinking organisations are trying to mature towards more quantitative (data-driven) rather than more qualitative (question-driven) approaches to Enterprise-Wide Risk Assessments, to reduce the reliance on subjective judgement calls. The ability to be able to ingest data either via a data upload or via an API call is an important step to maturing towards this (but data acquisition is just one part of this).
Does the platform have any automation of risk assessments based on consumed data?	Once data is capable of being able to be ingested into the GRC/EWRA platform, the next challenge is to be able to 'Push' this data into a risk assessment model (that contains all the risk indicators), so the ingested data ultimately drives the model.
What methods of data ingestion are available?	Being able to ingest data both via an upload process, for example through a CSV file import and/or via an API process, is an important mechanism, as this determines the amount of manual intervention required.
Does the platform have the ability to ingest major data sets?	Being able to consume either structured or unstructured data into the platform is important, but not as important as being able to clearly identify the risk indicators that your organisation wants to assess and then match the data elements required to drive the risk indicator.



4.4.9. Audit Trail and Management Actions

Key considerations	Why does this matter?
Is there an audit trail of workflow activities?	Being able to explain and defend the risk decisions is a critical element when performing Enterprise-Wide Risk Assessments. It is often very challenging using Excel to see what actions were taken or decisions made, so this is a critical element to consider.
What information is recorded in the audit trail?	The details that most regulators are interested in is who conducted the assessment/made the decision, what was assessed or decided, who was involved in reviewing and approving and what was the date/time stamp of when this action was performed.
Is the audit trail date and timestamped?	This provides transparency of the control process surrounding the risk assessment and allows a full timeline to be constructed, if required in future.
Is the audit trail exportable into PDF, CSV or XLS?	Exporting data is important for sharing with others.
How is the audit trail displayed on the platform?	The audit trail must be easy to view and accessible on many different elements across the entire platform.
Is it possible to set up email alert notifications when actions are falling due or overdue?	Being able to stay up to date with open or overdue actions is important and having email alert notifications reduces the chance that things will get missed as a result of a user not logging into the platform to check.
Are there dashboard reports available over management actions?	Dashboards on management actions are important to understand current status by priority, type, owner etc. so they can be managed in a timely manner.

4.4.10. Report Writing and Record-keeping

Key considerations	Why does this matter?
Are comments that are made during the assessment included as part of the report?	Having the ability to make comments during the assessment, rather than having to re-key in data into a report, will save time and effort.
What types of reports can be produced from the system?	Having the option to produce Word and PDF reports within the platform gives the choice of having a work in progress report and a locked down version of the report when the report is 'published'.
Does the system allow users to customise report content that is displayed or rendered on the report?	Being able to enable or disable the sections of the reports that are displayed is important when showing the report to different audiences who may have different levels of interest in different information.
Are reports available at both the Assessment and Assessment Unit levels?	Being able to see reports at both an assessment level, with all underlying risk assessment data, as well as an assessment (enterprise) level is important in being able to look at risk from a micro and macro perspective.

4.5. Buyer’s Checklist

The Buyer’s Checklist described in the table below is not intended to be exhaustive but contains other questions that you should think about asking any vendor that you are considering working with:

Key considerations	
Platform considerations	
Is the platform sufficiently flexible and configurable to support multiple risk assessment scenarios?	
Does the platform allow modification of the underlying risk methodology, or is it pre-defined/fixed?	
How flexible is the platform in configuring the risk assessment to any risk management framework?	
Does the platform allow users to build or import their own risk modules and control libraries?	
Does the platform have a detailed and fully auditable user workflow and audit trail?	
Does the platform allow users to apply weighting to risks, controls and assessment units?	
Does the platform allow users to upload supporting evidence as links and/or attachments?	
Does the platform allow users to set up and execute Enterprise-Wide Risk assessment?	
How easy is it to ‘Copy Over’ risk and controls from previous risk assessments?	
Does the platform contain dashboard reports and other analytic insights generated in the process?	
Does the platform provide the ability to automatically write and publish reports in the platform?	
Does the platform allow users to add and track actions, issues, breaches and incidents?	
Does the platform aggregate the risk assessment results across multiple assessment units?	
Does the platform contain user access controls to set permissions for different types of users?	
How easy is it to invite users to the platform and how quickly can they get started assessing risks?	
How easy is it to set up risk assessments for different assessment units (i.e., countries, operating groups, business units?)	
Content considerations	
Does the vendor have expert built and maintained content that is available (for free or to purchase)?	
What are the vendor risk and control libraries available and how frequently are they maintained?	
Does the platform allow the import of risks and controls into the platform?	
How easy is it to manage intellectual property developed by the client within the platform?	
Does the vendor manage country risk and if so what is the methodology and update cycle?	
How often is the content updated and what support is available on an ongoing basis?	
How flexible is the platform in setting up content (i.e., licensing expert content or importing own)?	
Hosting considerations	
Can the platform be multi-tenant hosted (i.e., multiple companies use the same platform)?	
Can the platform be single tenant hosted (i.e., single instance of the platform)?	
Can the platform be deployed on-premise and what is involved on both sides?	

Does the vendor provide any assurances in respect of platform availability if the vendor hosts?	
If vendor hosted, which countries is the platform hosted in and is there any flexibility to change this?	

Information security management

Does the vendor perform regular external security assessments (e.g., application and network penetration testing)? If so, how often, and is there evidence of issues being found and addressed?	
Does the vendor have security incident response policies and procedures to manage web security incidents such as data breaches, website defacement, phishing, and DOS attacks?	
Has the vendor had any significant outages in the hosting service in the last two years?	
Has the vendor had any security breaches or incidents in the last two years?	
Does the vendor have an information security program in place that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorised access, disclosure, alteration, and destruction?	
Is the vendor ISO27001 certified (or equivalent (i.e. SOC II) and is the certificate current?	
Does the vendor have a documented and implemented business continuity methodology in place to ensure all business continuity & disaster recovery plans are consistent in addressing priorities for testing, maintenance, and information security requirements?	
Does the vendor have reliance on any third parties to deliver and maintain the platforms?	
Does the vendor maintain policies and procedures that relate to information security management?	

Commercial considerations

Does the vendor offer annual software licences or are software licences in perpetuity?	
Does the vendor charge additional fees for additional users and if so, what is the per user fee?	
Does the vendor provide discounts for multi-year agreements / upfront payments?	
Does the vendor have clauses in its contracts to limit the amount licence fees can be increased?	
Does the vendor charge additional fees for training and support and, if so, what are these?	
Does the vendor charge initial implementation fees and annoying upgrade fees?	
Does the vendor licence content modules separately to software licence fees?	

Pre-sales support

Is the vendor willing to engage in a proof of concept, proof of value or pilot stage before purchasing?	
Is the vendor willing to spend time understanding ‘as is’ processes to see how to support ‘to be’?	
Is the vendor willing to provide testimonials in the same region, country, sector or peers?	

Post sales support

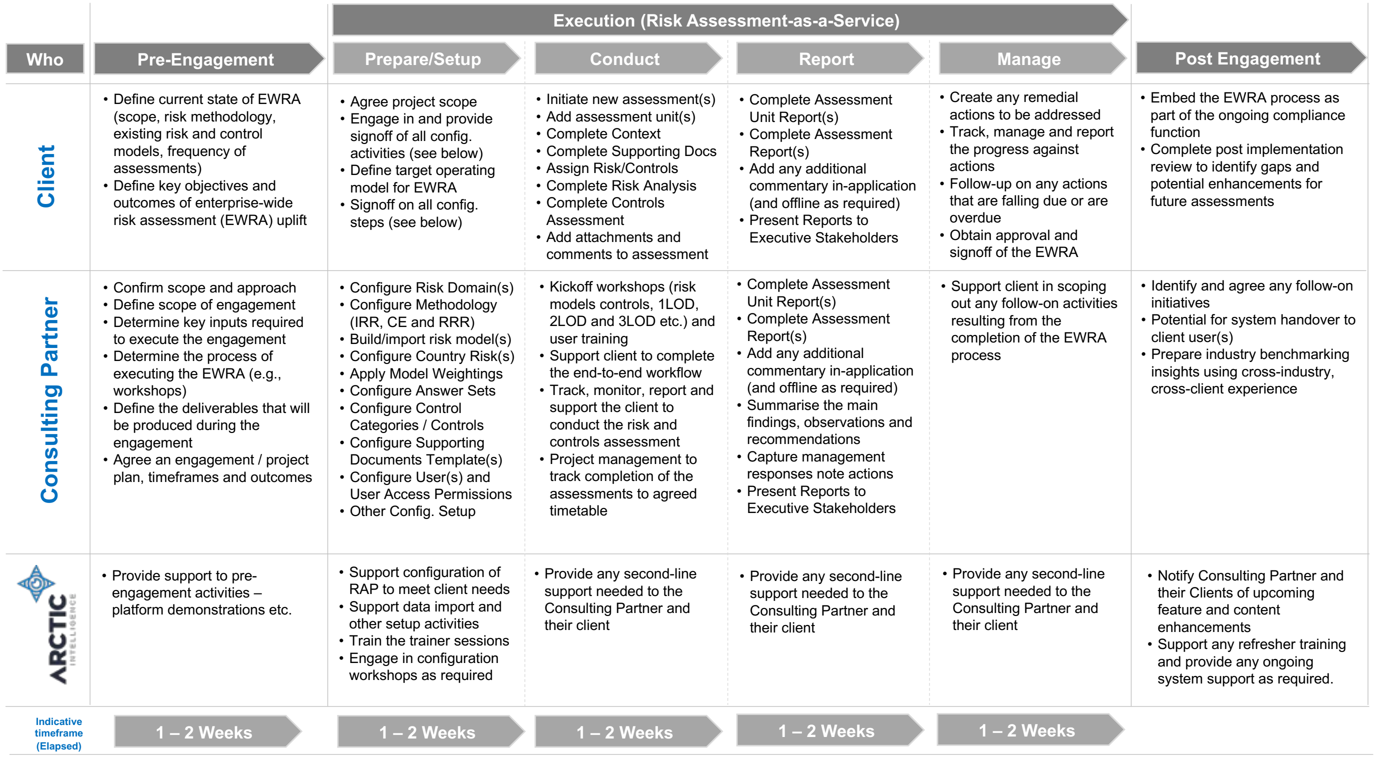
What methods does the vendor use to provide support to its clients (i.e., phone, email, webform)?	
What are the vendor's support hours and how are tickets logged/responded to outside these hours?	
Does the vendor provide onboarding training, refresher training and ad-hoc training as required?	
Does the vendor have a self-service help centre with videos, FAQs and other materials?	

Post sales support (cont.)	
Does the vendor have any in-application tutorials to be able to submit tickets with the platform?	
Does the vendor provide professional services support to provide additional consulting if required?	

Future roadmap and thought leadership	
Does the vendor run any user focus groups to gather feedback on future requirements?	
Does the vendor publish a product roadmap and engage in client consultation about priorities?	
Does the vendor's future product roadmap align to the same vision as your organisation?	
How often is the software updated with bug fixes, new features and improvements?	

Implementation considerations*	
Does the vendor provide initial setup and implementation support, and if so, describe the process?	
What level of training and support does your organisation require and can the vendor support this?	
Are the steps in the implementation process well-articulated and understood, including roles?	
Does the vendor have the resources to support an implementation project?	
Does the vendor work with implementation partners that can support delivery of the project?	

* As an example, Arctic Intelligence has a clearly defined pre-engagement, execution and post engagement process outlining the steps involved and the typical roles and responsibilities[6].



		Execution (Risk Assessment-as-a-Service)				
Who	**Pre-Engagement**	**Prepare/Setup**	**Conduct**	**Report**	**Manage**	**Post Engagement**
Client	• Define current state of EWRA (scope, risk methodology, existing risk and control models, frequency of assessments) • Define key objectives and outcomes of enterprise-wide risk assessment (EWRA) uplift	• Agree project scope • Engage in and provide signoff of all config. activities (see below) • Define target operating model for EWRA • Signoff on all config. steps (see below)	• Initiate new assessment(s) • Add assessment unit(s) • Complete Context • Complete Supporting Docs • Assign Risk/Controls • Complete Risk Analysis • Complete Controls Assessment • Add attachments and comments to assessment	• Complete Assessment Unit Report(s) • Complete Assessment Report(s) • Add any additional commentary in-application (and offline as required) • Present Reports to Executive Stakeholders	• Create any remedial actions to be addressed • Track, manage and report the progress against actions • Follow-up on any actions that are falling due or are overdue • Obtain approval and signoff of the EWRA	• Embed the EWRA process as part of the ongoing compliance function • Complete post implementation review to identify gaps and potential enhancements for future assessments
Consulting Partner	• Confirm scope and approach • Define scope of engagement • Determine key inputs required to execute the engagement • Determine the process of executing the EWRA (e.g., workshops) • Define the deliverables that will be produced during the engagement • Agree an engagement / project plan, timeframes and outcomes	• Configure Risk Domain(s) • Configure Methodology (IRR, CE and RRR) • Build/import risk model(s) • Configure Country Risk(s) • Apply Model Weightings • Configure Answer Sets • Configure Control Categories / Controls • Configure Supporting Documents Template(s) • Configure User(s) and User Access Permissions • Other Config. Setup	• Kickoff workshops (risk models controls, 1LOD, 2LOD and 3LOD etc.) and user training • Support client to complete the end-to-end workflow • Track, monitor, report and support the client to conduct the risk and controls assessment • Project management to track completion of the assessments to agreed timetable	• Complete Assessment Unit Report(s) • Complete Assessment Report(s) • Add any additional commentary in-application (and offline as required) • Summarise the main findings, observations and recommendations • Capture management responses note actions • Present Reports to Executive Stakeholders	• Support client in scoping out any follow-on activities resulting from the completion of the EWRA process	• Identify and agree any follow-on initiatives • Potential for system handover to client user(s) • Prepare industry benchmarking insights using cross-industry, cross-client experience
ARCTIC INTELLIGENCE	• Provide support to pre-engagement activities – platform demonstrations etc.	• Support configuration of RAP to meet client needs • Support data import and other setup activities • Train the trainer sessions • Engage in configuration workshops as required	• Provide any second-line support needed to the Consulting Partner and their client	• Provide any second-line support needed to the Consulting Partner and their client	• Provide any second-line support needed to the Consulting Partner and their client	• Notify Consulting Partner and their Clients of upcoming feature and content enhancements • Support any refresher training and provide any ongoing system support as required.
Indicative timeframe (Elapsed)	1 – 2 Weeks	1 – 2 Weeks	1 – 2 Weeks	1 – 2 Weeks	1 – 2 Weeks	

[6] Where no consulting partners are involved, we train our clients to perform and can support directly through advisory services.

5. How to build a business case and demonstrate value

5.1. What stage of the buyer lifecycle are you?

Whether you are even ready to create a business case really depends on your stage of the buying lifecycle. These are typically broken down into one of the following stages with corresponding activities:

Buying stage	Typical activities
Awareness	• The organisation recognises that it has a problem/pain points and needs a solution • The solution options are unclear (i.e., buy, build, partner or carry on) • There are stakeholders expressing interest in seeing what solutions are available
Market Research	• The organisation is conducting a broad market scan into possible solutions • The organisation is gathering information, requesting demos and drawing up a list • Initial meetings have been held with initial vendors to assess problem solving fit
Solution Evaluation	• Organisation has agreed a scope, budget, timeframe and objectives of a solution • Organisation has agreed vendor selection criteria (i.e., business/technical requirements, budget requirements and support requirements etc.) • Organisation is actively engaged in demos, proof of concepts/pilots etc. • Organisation has commenced vendor due diligence on shortlisted vendors • Organisation has considered pricing/budget and is gathering stakeholder support
Negotiation	• Organisation is reviewing the terms of any commercial agreements (i.e., master services agreements, statements of work and licensing agreements) • Organisation is actively negotiating over key commercial terms in the agreement • Organisation is discussing post-contract on-boarding, training and kick-off activities
Implementation	• Organisation has agreed contract terms and has started to engage with the vendor on account setup, user onboarding, training and configuration setup • Organisation has agreed a project plan, key deliverables and milestones.

Based on the table above you should ask yourself and your peers these questions:

- Do we know the problem we are trying to solve and what are the best options in solving this?
- Do we understand who the main reputable solution providers are and what they offer?
- Do we have stakeholder support to start investigating possible solutions?
- Do we have a budget approved, or will this require an out-of-budget cycle approval?

In most organisations, depending on the level of investment required, there may be no formal business case requirement, or it may be extensive, requiring approval and endorsement from many stakeholder groups. It is important to understand this at the outset, to ensure you can provide what is required to navigate the buyer journey in your organisation.

5.2. What is the buyer journey in your organisation?

In our experience, many regulated entities operate on the basis that manual spreadsheets for conducting enterprise-wide money laundering and terrorism financing risk assessments are fit for purpose and they may not be actively looking to improve how this is managed. This often changes, usually after a regulatory inspection or independent audit highlighting deficiencies in risk assessments, or internally through changes in leadership or a desire to improve things. This leads to initial support to look at solutions that can improve how risk assessments are managed.

Once there is a recognition of a need to invest in a solution, one of the first steps that should be taken is to identify who the key people are to be involved in or influence the decision-making process. It is important to canvas opinions from all stakeholders to understand their perspectives and pain-points so you can start building up and prioritising the key requirements.

To help this process, we have summarised the key stakeholders and their typical roles, which obviously varies by organisation to organisation but is important to understand at the outset:

Role	System User	Decision maker	Power to Veto
Business User (1st Line)	◑	◑	○
Risk and Compliance (2nd line)	●	●	○
Head of Risk and Compliance (2nd Line)	●	●	◑
Chief Risk Officer (2nd Line)	◔	●	●
Internal Audit (3rd Line)	◔	◔	◔
Chief Audit Officer (3rd Line)	◔	◔	◔
Technology	○	◔	●
Finance	○	◔	●
Procurement	○	◔	●
CEO, Board and Senior Executives	◔	◕	●

○ NO INVOLVEMENT

◔ MINOR INVOLVEMENT

◑ PARTIAL INVOLVEMENT

◕ EXTENSIVE INVOLVEMENT

● FULL INVOLVEMENT

5.3. Understanding stakeholder pain points and pain relievers is important

Once you have a clear understanding of who is involved in the buying process it is important to arrange information gathering sessions with each of these stakeholder groups, either collectively in workshops or individually, with the objective of identifying the key pain points that need to be solved from their perspective, the relative importance and priority of their requirements and any other material factors that could influence their decision-making, such as preferences or bias.

An effective way of doing this is to design and issue a survey, followed by stakeholder workshops to listen to what stakeholders have to say about the audit, risk and compliance challenges that they face every day and those that are either quick wins or higher priority to address.

The common challenges we hear from our clients and prospective clients include the:

- Time that it takes to gather the data inputs required to complete the assessment
- Availability of data inputs is hard to extract from upstream systems
- Time spent preparing to rollout the risk assessment across the enterprise
- Elapsed time assessing inherent risks and evaluating control effectiveness
- Efforts involved in aggregating data across multiple parts of the enterprise
- Time spent writing reports of findings and presenting these to stakeholders
- Ability to record actions and issues and track completion over time.

A helpful resource you might want to consider downloading is our Annual AML Benchmarking Report which contains common pain points. Do any of these resonate with your stakeholders?

For conversation starters, look back at the key workflows when completing the Enterprise-Wide Risk Assessments section for key considerations your stakeholders may be interested in exploring.

Also, some of the heavy lifting may have already been done to highlight these pain points and any of the following could be leveraged to help articulate these, for example:

- Has there been any material incidents that highlight ineffective risk management controls?
- Have regulators provided feedback into the effectiveness of risk management processes?
- Have regulators documented actions they expect to be taken to improve risk management?
- Has the board or senior management asked questions you are unable to answer?
- Has there been an independent review of risk management practices that has found gaps?
- Has there been any remediation or change management projects to uplift risk management?

5.4. Try and quantify and qualify the impact of these pain points

Once you have identified the pain points from key stakeholders it is important to try and quantify these in terms of key metrics, as well as qualify these with anecdotes from conversations in order to bring some tangible meaning to the problem that needs to be solved.

In terms of quantifying pain points a few questions to ask might include how many hours:

- Does it take to prepare the methodology and agree on the risk factors?
- Are spent gathering the necessary information and data that will be assessed?
- Are you spending identifying and assessing risks across the enterprise?
- Are spent assessing the design and operational effectiveness of controls?
- Are taken clarifying answers, writing reports and retesting risks and controls?
- Are spent overall on Enterprise-Wide Risk Assessments?

In terms of qualifying pain points a few questions to ask might include:

- What are the top 3 biggest challenges you face conducting risk assessments?
- What are the 3 biggest improvements that could be made to help you do your job?
- Do you believe there are benefits in using technology to conduct risk assessments?
- What specific features would you like to see in a solution and what are the benefits?

And don't forget to gather the anecdotes as there are often hidden frustrations in these quotes, such as:

- "I am worried that when regulators come to examine our risk assessment I won't be able to explain it"
- "It is taking us way too long to complete our risk assessments - by the time it's done they are out of date"
- "I am not sure what risk factors we need to consider or how to assess if our controls are effective"
- "I feel like I am spending most of my time gathering information and administering the process rather than understanding and managing my risks".

A combination of hard-hitting evidence combined with softer quotes and anecdotes from people are powerful inputs when building business cases and helps bring clarity to the pain points so that you can speak to vendors about how their solutions can specifically address these points.

5.5. What are the key elements to cover when writing a compelling business case?

So, you have found a solution that solves your problem and provides you and your team with the capabilities you need to perform your role but whether you can convince other stakeholders, (particularly those who hold the purse strings) to invest in a solution depends on the strength of the business case.

The table following summarises the key elements of writing a compelling business case:

Key element	Key points to cover
Define the problem or opportunity that the software solution will solve for	Start by clearly defining the problem or opportunity that the software purchase is meant to address. Identify the pain points, inefficiencies, or missed opportunities that the organisation is experiencing by not having the software solution. This will help ensure that everyone understands what you are trying to achieve.
Define the objectives, scope, approach and deliverables	Provide some background context by describing the current situation and the problem that you are seeking to solve, then define the business objectives and the features, functions and requirements that are in-scope, out-of-scope or where the scope is to be clarified. Outline the approach and deliverables of the project.
Analyse the risks of implementing or not implementing the software	Identify the risks associated with the proposed software purchase, such as the risk of the software not meeting the organisation's requirements, the risk of disruption to current processes, or the risk of the software being too complex to use and then develop strategies to mitigate these risks.
Conduct a cost-benefit analysis of investing in a software solution	Estimate the costs and benefits of the proposed software purchase. Consider factors such as the cost of the software, installation and training, ongoing maintenance and support, the potential return on investment.
Focus on the benefits	When building your business case, emphasise the benefits that will result from adopting the software solution and be specific about the financial benefits, such as time or cost savings, reduced risk exposures or other benefits, such as being able to standardise processes and improve the quality and auditability of risk assessments.
Provide evidence, examples and case studies	Back up your claims with evidence such as data, statistics, or case studies. This will help build credibility and increase the likelihood that your proposal will be accepted by key stakeholders. Seek out customer references about their experiences.
Develop a timeline and a project plan	Create a timeline for the software purchase, including time to complete vendor due diligence and the procurement process, user onboarding, installation, configuration, and training. Ensure that the timeline is realistic, achievable and clearly communicated, as well as managed, if certain stages are taking too long.
Consider the impact on stakeholders and socialise with them to build support	Identify the stakeholders who will be affected by the software purchase, such as employees from across the first-line (business), second-line (risk and compliance) and third-line (internal audit), management, executives and consultants. Consider how the software will impact their work and develop a plan for managing the transition to a new software solution. Engage key stakeholders early on in the process and get their buy-in. This will help build support for your proposal and increase the likelihood that it will be accepted.
Tailor your approach to different stakeholders	Tailor your approach to your audience. For example, if you are presenting to a finance team, emphasise the financial benefits or cost savings, if you are presenting to an executive team, focus on the benefits of risk reduction.
End with a call to action	End your business case with a clear call to action. This could be a request for approval or a request for further discussion. This will help ensure that everyone understands what is expected of them and what the next steps are.

5.6. Refining and submitting the business case

Once you've drafted the business case and have a better understanding of pain points stakeholders have and a clearer understanding of their priorities, it is important to re-engage with key stakeholders to 'playback' what you have found and heard, either informally in one-on-one sessions, or through more formal channels.

If possible, it is always a good idea to understand who the supporters are and who is yet to be convinced of the merits of making an investment. It is worth circulating earlier draft versions of the business case for feedback, ensure that the benefits are articulated as well as they can be and that any feedback raised can be answered to address any concerns in advance of any formal submission or decision.

In many organisations there is not a single decision-maker to convince and decisions are made 'by committee', which has advantages and disadvantages. Additionally, the decision-maker(s) may request further information to be included or clarified before re-presenting the business case for final approval.

Generally, investing the time in building a compelling business case that has examined all of the pain points and benefits, both quantitative and qualitative, with well-articulated and argued points of view supporting the decision should make it easier for decision-makers to understand the benefits and achieve sign-off on the business case. This time investment spent upfront engaging with stakeholders is rarely wasted and will prepare you for the next stage in engaging vendors in evaluating their solutions against your requirements, or even engaging in a more formal request for proposal (RFP) process.

It is worth thinking about a back-up plan if a business case is not approved and what can be done to strengthen the business case to make it compelling enough to convince stakeholders in the future.

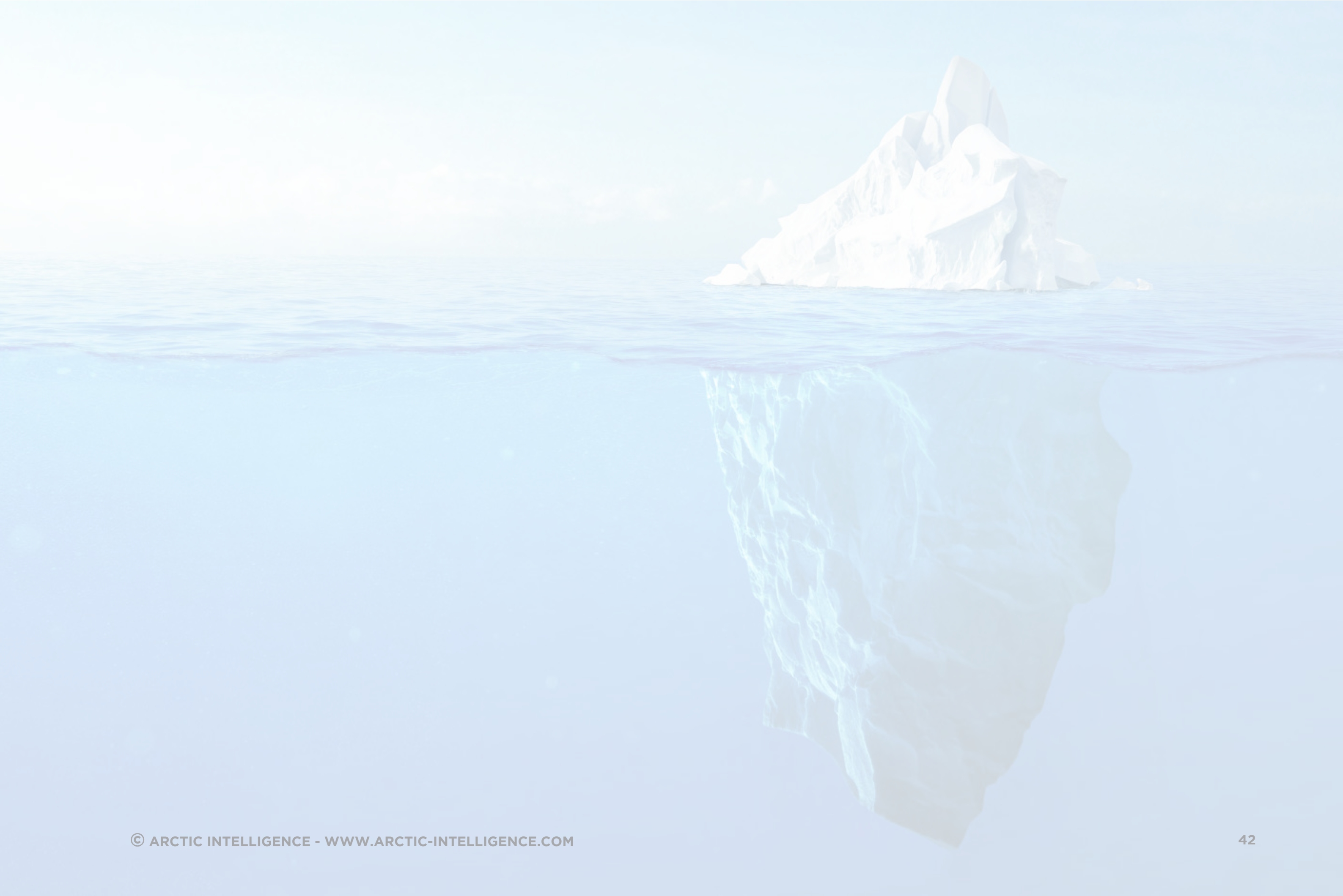
5.7. Cost and savings estimator

Demonstrating the benefits is not always clear cut, as they sometimes come as hard-hitting quantifiable time savings, but more often than not they are less tangible, such as improving risk management culture, reducing workload and stress on employees, being more organised when regulators visit or approach risk management in a more methodical way.

However, for those stakeholders that are only considering quantitative benefits, we have built a cost and savings estimator that tries to break down the amount of combined human time that is spent conducting Enterprise-Wide Risk Assessments from all stakeholders involved in the process. This is further broken down into each of the main workflows of the assessment, with the ability to model different anticipated percentage time savings at each stage by using a technology solution to support the process.

The cost and savings estimator is designed as one input into a business case but it should be presented alongside qualitative, less tangible benefits too

Access the Cost and Savings Estimator HERE



6. About Arctic Intelligence

6.1. Company overview

Arctic Intelligence is a multi-award winning, RegTech firm that specialises in audit, risk and compliance software related to financial crime compliance and risk management.

6.2. Our solutions

Arctic has developed three leading cloud-based software solutions that leverage technology to re-engineer the way in which major financial institutions and other regulated businesses manage their financial crime risks.

AML ACCELERATE

AML Accelerate is a cloud-based guided risk assessment solution for assessing money laundering and terrorism financing risks and developing AML/CTF Programs/ Policies.

AML Accelerate has been tailored to over 30 different financial and non-financial services industries, as well as over 30 different countries.
This platform has been designed by experts to support regulated entities of all sizes, sectors and geographies in understanding ML/TF risk and demonstrating compliance.

PLAY VIDEO DEMO

VISIT WEBSITE

DOWNLOAD BROCHURE

RISK ASSESSMENT

The Risk Assessment Platform is a cloud-based highly flexible & configurable Enterprise-Wide Risk and control assessment solution.

The platform can be used by smaller reporting entities out-of-the-box with standard risk and control libraries for various financial crime risks or can be configured by larger organisations to suit any enterprise risk management framework and methodology.

The platform contains in-built workflows, audit trail and real-time enterprise analytics and insights.

PLAY VIDEO DEMO

VISIT WEBSITE

DOWNLOAD BROCHURE

HEALTHCHECK

The Health Check Platform is a cloud-based platform designed to help regulated businesses (and their professional advisers) to assess the design and operational effectiveness of compliance programs, by mapping policies/ procedures to compliance obligations; performing control testing; documenting key observations / recommendations in reports and using data analytics to derive actionable business intelligence on compliance data.

There are two Health Check Platform modules - AML Health Check and Anti-Bribery Health Check.

PLAY VIDEO DEMO

VISIT WEBSITE

DOWNLOAD BROCHURE

Our Risk Assessment Platform contains various financial crime risk models and control libraries for a range of risk disciplines including; money laundering and terrorism financing, anti-bribery and corruption, sanctions, fraud, modern slavery, human trafficking, correspondent banking and wildlife trafficking.

REQUEST A DEMO

6.2.1. AML Accelerate Platform

6.2.2. Risk Assessment Platform

6.2.3. Health Check Platform

REQUEST A DEMO

6.3. Our credentials

Arctic Intelligence continues to be recognised for our innovative approach to enterprise-wide financial crime risk assessments.

2022

2021 and 2022

2019 and 2020

2022

6.4. Our clients and what they say about us

Arctic Intelligence has helped hundreds of clients in 20 industry sectors and 12 countries. Here are some of the organisations we have helped in the banking and financial services sector.

APAC		EMEA		AMERICAS	
BOQ	SUNCORP	Bank of India	African Bank	FirstOntario CREDIT UNION	Credit Unions OF ALBERTA
credit unionsa	BIBD	ARBUTHNOT LATHAM Bankers since 1833	HERMES INVESTMENT MANAGEMENT	VISION CREDIT UNION We see banking differently.	bow valley credit union
Beyond Bank AUSTRALIA	Qudos Bank	SBI	JUPITER	Prospera CREDIT UNION	1st Choice Savings and Credit Union Ltd.
MOVE BANK	imb bank	unionbank	SKIPTON BUILDING SOCIETY Since 1853		
Bendigo Bank	Defence Bank	Federated Hermes	BANCO VALOR		
Great Southern Bank	Heritage Bank People first	paragon	Ford | Ford Credit		
NEWCASTLE PERMANENT	Unity Bank				
Police Credit Union Better Banking	p&n bank				
Australian Unity	regional australia bank				
Australian Military Bank	BELL POTTER				
PARRA LEAGUES	GOLD BULLION AUSTRALIA				
THE WESTS GROUP Australia	FLIGHT CENTRE TRAVEL GROUP				
People's Choice Banking for life	me				

The Arctic Intelligence platform enables the reporting entity to establish a robust risk assessment that is the cornerstone of any AML/CTF Program. The platform provides a cloud-based auditable repository of documents and risk assessments, the system is independently maintained and updated, using empirical evidence to help support the risk outcomes. Arctic's team of professionals have deep, long-term experience in financial crime risk and compliance, they provide great service and timely advice.

AML/CTF Manager – Suncorp

SUNCORP CASE STUDY

OTHER CASE STUDIES

6.5. Some of the benefits delivered to our clients

Our solutions are transforming the financial crime risk assessment process by replacing spreadsheets with real-time reporting, and enabling more frequent reviews in response to global regulator expectations.

Here some benefits:

- Auditability
- Reliability
- Efficiency
- Time & Cost Savings
- Enterprise Analytics
- Standardisation
- Repeatability
- Configurability
- Explainability
- Flexibility
- Self-Sufficiency
- Peace of Mind
- Workflow Management
- Records Management
- Support

REQUEST A DEMO

APPENDICES

APPENDICES

Appendix 1 - Industry sectors subject to ML/TF laws

Financial services

- Asset Managers, Hedge Fund Managers, and Fund Managers
- Banks, Building Societies, Credit Unions, and Mutual Banks
- Cash in Transit and Safety-Deposit Box Service Providers
- Corporate Finance and Private Equity
- Cryptocurrency and Digital Currencies
- Fintechs
- Foreign Exchange and Money Remittance Businesses (MSBs)
- Financial Planners
- Insurance Companies
- Investment Managers
- Leasing and Hire Purchase Financing Businesses
- Non-Bank Financial Institutions
- Payment Processing Services
- Stockbrokers
- Superannuation, Retirement, and Pensions

Other Industry Sectors

- Gaming and Wagering
  - Bookmakers and Betting Agencies
  - Casinos
  - Physical Gaming Venues (Racetracks, Hotels, Pubs and Clubs)
  - Online Gambling
- Gatekeeper Professions
  - Accountants and Bookkeepers
  - Lawyers and Conveyancers
  - Trust and Company Service Providers
  - Real Estate Professionals (Commercial and Residential)
- Dealers in High-Value Goods
  - Antique and Fine Art Dealers
  - Auctioneers and Brokers
  - Bullion Dealers, Jewellers, and Precious Metal and Stone Dealers
  - Motorised Vehicle Dealers (Cars, Boats, Aircraft)
  - Luxury Goods Dealers (Clothes, Handbags and Watches)
  - Pawnbrokers and Secondhand Dealers
- Other Sectors
  - Non-profit organisations, including charities and religious organisations
  - Marijuana related businesses

For more information on what products and services are offered within each of these industry sectors, what money laundering and terrorism financing risks these businesses might typically face and the steps that they can take to mitigate and manage these risks please visit our website.

VISIT WEBSITE

Appendix 2 - Industry sectors impacted by other financial crime risks

Major corporates in the following sectors are exposed to fraud, bribery and corruption and other financial crime risks

- Agriculture/Agribusiness
- Automotive
- Arms, Defence and Military
- Banking and Financial Services
- Biotechnology
- Building and Construction
- Chemicals and Plastics
- Civil Aerospace
- Consumer Services
- Education
- Electronic and Electrical
- Fisheries and Forestry
- General Industries
- Global Hotel Chains
- Government
- Heavy Manufacturing
- Industrial Engineering
- Industrial Metals
- Information and Communications
- Information Technology
- Light Manufacturing
- Mining
- Oil and Gas
- Oil Equipment and Services
- Pharmaceuticals and Healthcare
- Power Generation/Transmission
- Printing and Publishing
- Professional Services
- Public Works Contracts
- Real Estate and Property
- Retail
- Legal and Business Services
- Support Services
- Telecommunications
- Textiles, Clothing and Footwear
- Transportation and Storage
- Utilities
- Waste Management

ARCTIC
INTELLIGENCE

REQUEST A DEMO

APAC

Arctic Intelligence Head Office
Level 4, 11-17 York Street,
Sydney, NSW 2000, Australia

Call us on your local number:

Australia	+61 (0) 2 8001 6433
Hong Kong	+852 (0) 8197 4022
New Zealand	+64 (0) 9889 3324
Singapore	+65 6817 8650

EMEA

United Kingdom +44 20 8157 0122

AMERICAS

USA +1 646 475 3718
Canada +1 613 5188002

GLOBAL

support@arctic-intelligence.com

The information in this Buyer's Guide and website is for general informational purposes only. Arctic Intelligence makes no representation or warranty, express or implied. Your use of the Buyer's Guide and website is solely at your own risk. This Buyer's Guide and website may contain links to third party content, which we do not warrant, endorse, or assume liability for. Arctic Intelligence makes no representation and assumes no responsibility for the accuracy of information contained on, or available through, this Buyer's Guide and website, or its suitability for any purpose, and such information is subject to change without notice. You are encouraged to confirm any information obtained from or through this Buyer's Guide and website with other sources, and review all information independently. Arctic Intelligence does not recommend or endorse any specific products, processes, opinions, or other information that may be mentioned in this Buyer's Guide and website.