成功落实反洗钱监控系统的最佳实践

在“大数据”时代，自动化监控在反洗钱领域是大势所趋。尽管在打击犯罪分子方面，技术可能永远也无法完全取代人工，但考虑到金融机构为此需要处理的信息量，自动化监控系统已成为“以资金为线索”侦查犯罪分子的过程中必不可少的工具。这些系统可将原始数据转换成直观易懂的可视化信息（如报告、图表、警报等），让人一目了然，有助于整合当前的监管要求、变化、预期等，通过处理相关信息来监控原本无法观测的复杂洗钱机制，并借助自动化降低“合规成本”。

金融机构在落实反洗钱 / 反恐融资系统时，无不面临着各种各样的问题。这类落实项目的复杂程度取决于多种因素，包括需监控的客户数量、交易量、产品及服务（类别及复杂程度）、客户地域分组、业务条线数量等。本文将简要介绍落实反洗钱监控系统的最佳实践和典型误区，希望能为您顺利实施该系统提供帮助。

选择最合适的系统供应商

目前，市面上的金融犯罪、风险、合规解决方案供应商屈指可数。其中，仅有一部分供应商能提供完整的反洗钱套件（包括案例管理、监视名单过滤、交易监控、“了解您的客户”、报告），其余仅能提供部分专业工具。在联系供应商前，您的机构必须先考虑自身业务需求，开展市场调研。挑选解决方案前，您还可联系其他金融机构的同行，了解他们采用的监控系统。如果没有此类联系人（强烈建议您与同行建立这种业务关系），您可向咨询公司求助，咨询公司将根据行业标准研究结果，为您提供建议。

启动反洗钱系统落实项目之初，您的机构就应咨询重要员工，例如领域专家、管理人员、合规专员等，并邀请这些人参与挑选最适合机构的解决方案。敲定监控解决方案后，您必须与供应商协商签订一份可靠的合同，从而确保在系统落实过程中出现问题（必会出现问题）时，供应商必须提供全力支持。这是落实反洗钱 / 反恐融资监控系统过程中的一项重要内容，可确保项目不超支，如期交付。

合理的预算

着手实施如此浩大的项目前，必须事先取得高级管理层的支持。尽管反洗钱 / 反恐融资事务目前已经积累了一定的关注，但您还是需要制定具有说服力的商业提案，以确保高级管理层批准对该项目（或一系列项目）的巨额投资。您必须评估项目范围，确保整个项目资金充足。必须注意的是，您还应考虑系统开始运行后的维护成本。此外，确保自己已全面考虑其他杂项，包括基础设施维护费、许可费、系统升级和补丁支出，以及负责处理警报、提供技术支持、定期校准和优化模型人员的雇佣成本。您不仅要获得系统落地所需的预算，还要获得保障系统长期顺利运行所需的各类资源。

可靠的项目团队

项目主办人员全权负责提供项目落实所需的额外资源，也负责确保资金到位。主办人员需要高级管理层的支持，以及用于

解决项目实施过程中出现的任何问题的工具。实施反洗钱监控系统时，一个常见的问题是低估主办人员需为系统落实项目投入的时间（一般为工作总时长的 15% 至 25%，具体时长取决于项目规模）。如果主办人员没有时间投入落实反洗钱 / 反恐融资监控系统这样的大项目，那么这个项目必败无疑。

在这个项目中，产品所有方也发挥着重要作用。他们必须了解监管规定，明确机构需求，才能提供恰当的解决方案。他们必须与主办人员保持顺畅沟通，以便有效履行自己的职责。他们不仅代表终端用户并负责确认项目交付完成，还是项目主办人员的代表。产品所有方必须时刻积极响应项目团队的需求。

对项目成功起关键作用的人员包括：程序员、质量保证分析师、功能分析师、业务分析师、领域专家、解决方案架构师、IT 及项目经理、变更管理顾问、首席反洗钱官等。

外部专家

聘用外部专家的初期成本看似很高，但从长远角度看，实际上非常划算。如果您聘请的专家对您所购买的系统有着全面的了解，且有过类似项目经验，您将享受到诸多优势。经验丰富的集成专家熟知落实监控系统时的常见误区，也清楚如何避免。落实反洗钱 / 反恐融资监控系统是一个复杂的项目，为确保成功，您必须选择合适的人员。许多监控系统供应商不具备帮助客户落实自身反洗钱系统的专业知识，这一点可能会让人感到意外。供应商仅关注产品开发和营销，基本不配备能帮助客户落实产品的相应专家。

外部公司也能为您及时提供落实项目所需的资源（包括必要经验和技能）。不过，由于反洗钱监控系统落实多为短期项目，仅持续几个月，您对于外部专家的需求也仅限于这个期间。这段服务期内，外部专家还可应要求为您提供员工培训。一旦您的内部人员掌握相关技能，他们就能在系统落实后，负责保障新系统顺利运作。

请注意，某些外部“专家”可能名不副实，建议您随时开展尽职调查，找您信赖的人推荐可靠人选。

规划

我们往往会低估规划的重要性。在可行性研究阶段，必须对即将开展的工作进行详细的评估。实施项目时，时间安排如果过紧，项目团队可能会面临过大压力；如果项目预算金额太保守，您在项目过程中需要停下来筹措更多资金（或等待资金到位），项目就可能中途搁浅。这些问题都会导致项目无法如期交付，进而迫使您缩小项目规模。此外，如果您所在的金融机构没有遵循监管规定，您还要与监管机构达成妥协。切记，宁可超额完成任务，也不宜夸下海口后食言。

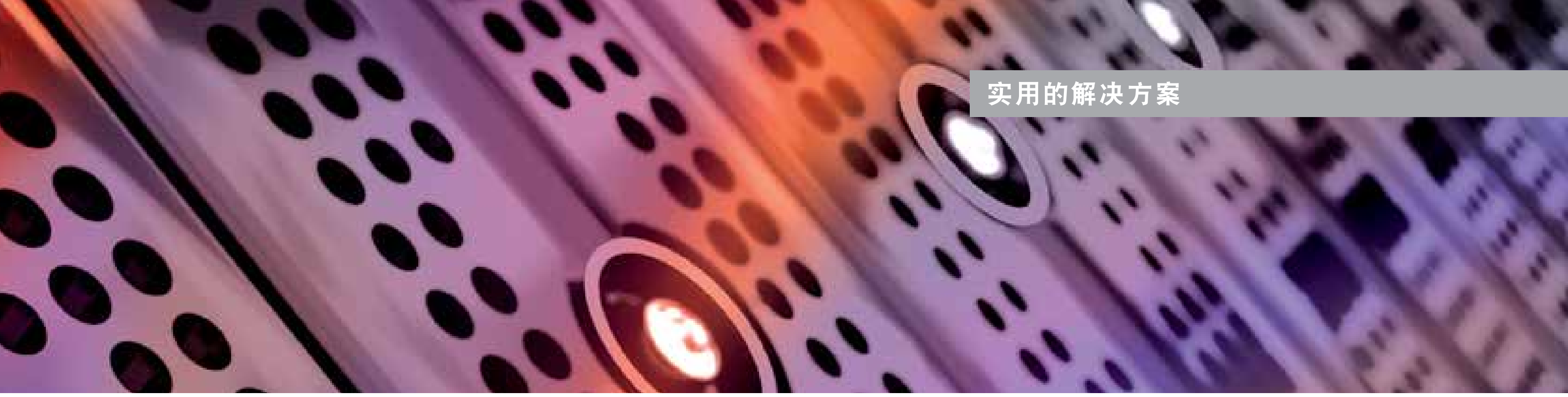
安排好各监控模块的落实顺序非常关键，如果您有多个业务条线，您还要确定各业务条线的落实顺序。制定项目时间表时，您必须从多个角度考虑项目的长远影响。建议您将整个项目分成多个便于管理的小项目，根据过往案例，这种做法非常有必要。

数据质量

反洗钱 / 反恐融资监控系统通过多种模块处理大量数据，其中，有些模块的使用频率较高，例如交易监控模块。多数金融机构服务于数百万客户，每天需处理上亿条交易。这些交易需要经过 ETL 流程（提取、转换、上传），将数据导入您的监控系统。不过，在启动侦测模型前，您必须先进行数据质量评估，确定数据是否可靠，以便侦测模型有效发挥作用。无法完成风险管理、生成有效警报的模型不具实用意义。正如人们所说，金融机构的好坏取决于其数据。

此外，侦查工具和模型在处理数据时必须保持数据完好无损，且完整无漏，这一点也至关重要。您必须采取严密的控制措施来监控 ETL 流程，以便确保数据完好地从源系统传送到监控系统，最后生成警报。监管机构和大多数内部审计员将要求金融机构证明自己采取了有效的控制措施。

近年来，越来越多的金融机构在高级管理层中增设首席数据官一职，这一现象在欧洲最普遍，目前美国也开始效仿。遗憾的是，除欧美外，大多数国家都未兴起这股浪潮。首席数据官的关键职责包括：



监管机构数据质量，负责为任何与数据有关的问题提供数据映射、质量评估和行动方案。

“风险为本”方法

选择和制定侦查模型时，必须采取“风险为本”方法。考虑您提供的产品与服务，您的分销渠道，以及客户分类。您必须事先了解机构的业务活动存在哪些风险，才能采取适当的侦查模型和规则，切实改善监控框架，充分保护机构。

模型风险治理

侦查模型存在固有风险，只有适当管理这类模型，才能缓释风险。一些模型能解决您的风险，满足业务需求，但也有一些模型存在根本性设计缺陷，甚至包括知名供应商的产品。模型风险治理框架中最重要的因素包括：模型库存、模型的开发、实施和应用、模型的验证、校准与优化、治理以及其他因素。

归档

为确保交付的产品符合业务和监管要求，在整个项目落实过程中，您必须登记业务需求和解决方案。此举还可记录您在此过程中做过的决策及相关理由。每个企业都存在人员流动现象，当您需要联系当初负责落实监控系统的项目团队时，当初的团队可能已经无法为您提供支持服务。如果系统需要升级或补丁，或团队对流程产生疑问，此时，了解过往决策及其考量至关重要。此外，监管机构要求金融机构必须保留此类记录，以便供审计员和稽查员过目。

自定义系统

您应当避免的一个常见误区是对监控系统进行自定义设置。当然，系统设置无可避免，但改变源代码会带来极大风险。尽管一些供应商可能会同意您修改源代码，但我们强烈建议您不要更改您的监控解决方案，而应在使用时遵照其最初设计。如果您使用的是多个模块构成的组合解决方案，更改设置产生的风险将大大增加。自定义通常会产生不兼容问题，导致软件更新更加复杂，系统出问题时供应商的技术支持团队可能束手无策，进而影响您的预算和交付。我们再次强调，请尽可能避免自定义设置。

变更管理计划

您需要为使用监控系统的团队实施变更管理计划。向这些团队提供新系统培训也是监控系统落实项目的一部分。由于新系统将自动完成以前由员工开展的工作，这类变化会带来新的难题，在过渡阶段尤其常见。有效的变更管理计划包括以下步骤：明确变更事项，实施沟通计划，为变更做准备，实施变更。变更管理计划的首要目标是充分落实新的监控解决方案，为金融机构创造更多价值。

内部控制团队与监管机构

新的反洗钱 / 反恐融资监控系统不仅会影响监控团队，也将影响内部控制及审计团队。内部审计职能部门必须熟悉新系统的结构、最新流程、程序、政策和控制措施等。内部控制及审计团队必须把握过渡时期，根据新系统调整自己的工作方式。

此外，您开展任何重大项目时，尤其是落实合规系统，必须告知相关监管机构，以证明您已尽最大努力遵守现有监管要求。监管机构还希望高级管理层全力支持这类项目，批准项目预算。切记，监管机构在评估金融机构的残余风险、开展准确审计时，必须了解该机构采取的控制措施和系统。最佳做法是时刻保持操作透明。

结语

每个机构、每个落实项目面临的难题各不相同，没有哪种秘诀能顺利解决一切反洗钱 / 反恐融资监控系统落实项目的问题。不过，本文介绍的各种实践可助您避免陷入同样的误区，犯同样的错误，从长期角度看，这将为您节省时间和成本。

Dominic Hurtubise，CAMS，CFE，
ACAMS 蒙特利尔分会联合主席；
反洗钱项目及业务情报部门主管，
加拿大蒙特利尔，
dominic.hurtubise@desjardins.com

BEST PRACTICES TO SUCCESSFULLY IMPLEMENT AN AML MONITORING SYSTEM

In the era of "big data," automated surveillance in our field of expertise has become inevitable. Although technology may never be able to completely replace humans when it comes to fighting the bad guys, the volume of information financial institutions need to process in order to do so, makes it impossible to ''follow the money" and identify criminals without automated surveillance systems. These systems help transform raw data into visual and intuitive information (reports, graphics, alerts, etc.) that can be more easily processed by the human eye, aid the integration of ongoing regulatory requirements, changes and expectations, allow for the handling of information required to monitor complex money laundering schemes that could otherwise not be monitored, and finally, help reduce the "cost of compliance" through automation.

All financial institutions face their share of challenges when implementing an anti-money laundering and counter-terrorist financing (AML/CTF) system. There are a number of factors that affect the complexity of this type of project, such as the number of customers to monitor, transactional volumes, product and service offering (range and complexity), geographic segmentation of clients, number of business lines, etc. This article provides a brief summary of best practices—as well as pitfalls to avoid—to set you on the road to success.

Choosing the best system supplier for your institution

There are only a handful of providers of financial crime, risk and compliance solutions on the market. While some of them offer complete AML suites (case management, watchlist filtering, transaction monitoring, know your customer, reporting), others will be able to provide only a portion of what you need. Your organization must consider its business needs and conduct its own market research before calling suppliers to the table. You should not be afraid to call your peers at other financial institutions and ask questions about their surveillance systems before you choose which solution you will implement. If you do not have such contacts (establishing such business relationships is strongly recommended), consulting firms may offer a system recommendation, based on a study of industry norms.

Key employees, such as subject-matter experts, management staff and compliance officers, must be consulted at the beginning of the initiative and be involved in the discussion as to which solution is the best fit for your financial institution. Once the decision has been made, it is crucial that a solid contract be negotiated with the supplier in order to ensure its full support when times get tough (which they will) during the implementation. This will be a key factor in your AML/CTF monitoring system implementation and it will ensure that budgets and timelines are respected.

An appropriate budget

Before undertaking a project of this scale, senior management's support is required. While AML/CTF may currently find itself under the spotlight, a solid business case is still required to ensure that senior management signoff on a project (or a series of projects) has substantial investment. Evaluate the scope of the project to ensure you have sufficient funding to complete the initiative. You should not forget to consider the cost of maintaining the system once it is up and running. Ensure that you do not overlook issues such as infrastructure maintenance fees, licensing fees, system updates and patches, as well as the cost associated with hiring employees to process alerts, provide technical support and calibrate and optimize models on an ongoing basis. While obtaining the budget required to implement the system is important, the resources needed to keep the system running smoothly in the long term, should be considered a priority.

A solid project team

The project sponsor is ultimately accountable for any additional resources the implementation project may require, and is responsible for securing the funds needed to go forward. Sponsors need the support of senior management and the tools required to resolve any issues that may arise during the course of the project. A common mistake is to underestimate the time a sponsor needs to focus on their projects (between 15 to 25 percent of their total work time, depending on the size of the project). You are setting yourself up for failure if your sponsor does not have the time they need to focus on the implementation of something as large as an AML/CTF monitoring system.

The product owner also plays a major role in this type of project. They need to know the regulatory requirements and understand the organization's needs, in order to provide appropriate solutions. The product owner needs to have an open line of communication with the project sponsor in order to effectively carry out their mandate. Not only do they represent the end user and approve deliverables, but they also act as the project sponsor's representative on the ground. The product owner has to be available, tactful and attentive to the project team's needs.

Programmers, quality assurance analysts, functional analysts, business analysts, subject-matter experts, solution architects, IT and project managers, change management advisors, the chief AML officer and so on, are all playing a key role in the success of this type of implementation project.

External experts

The expense of hiring external experts may initially seem high, but will prove to be economical in the long run. There are numerous advantages to hiring someone who knows the system you have purchased inside and out, and who has worked on similar projects in the past. An experienced integrator knows the potential pitfalls of implementing a monitoring system and how to sidestep them. Implementing an AML/CTF monitoring system is a complex project, and in order to be successful you need the right people on the task. It may come as a surprise that many monitoring systems suppliers do not have the expertise to help their clients implement their AML solution. Suppliers focus on developing and marketing their products; they rarely have the right experts available to help clients implement them.

External firms can also help provide resources (with the necessary experience and skillsets) rapidly to complete your project. These types of initiatives are typically short-term, usually taking place over the period of a few months. This means that you will require their help for only a brief period. If asked, a team of external experts will also train your employees while they are helping you deliver the project. Once your internal resources have been trained, they may assume the responsibility of ensuring that the new system runs smoothly post-implementation.

Be aware that some external "experts" may not quite live up to their self-appointed title. Conducting thorough due diligence and seeking references is always recommended.

Planning

We tend to underestimate the importance of planning. A detailed assessment of the work to be undertaken must be conducted during the feasibility phase. An overly aggressive schedule can place undue pressure on the project team. A conservative budget could bring the entire project to a standstill should you be required to ask for (and wait for the arrival of) more money, as a consequence. Each of these scenarios may lead to delays and consequently force you to reduce the scope of the project. Furthermore, should your financial institution be non-compliant with regulations, you may need to reach an agreement with your regulator. Remember that it is always better to over deliver than to overpromise!

It is crucial that you set up an implementation sequencing of the various monitoring modules. You should decide the order in which the different modules will be implemented and with which business line to start (assuming you have more than one). You need to consider the long-term implications of the project from all angles while drawing up your project timeline. Segmentation of the project into smaller, more manageable units is recommended and may, in any case, prove to be essential.

Data quality

AML/CTF monitoring systems deal large amounts of data, with particular modules, such as transaction monitoring, using more than others. Most financial institutions have millions of clients and process hundreds of millions of transactions on a daily basis. These transactions follow the ETL process (extract, transform and load) to feed data into your surveillance system. However, prior to implementing a detection model, you must conduct a data quality assessment. This allows you to determine if the data is reliable enough for the model to prove efficient. A model that does not meet your business needs in terms of risk management and does not create useful alerts, serves no purpose. As they say, you are only as good as your data.

It is also important that detection tools and models preserve integrity (no data is corrupted) and integrality (no data is lost) during processing. You need to have tight controls in place to monitor the ETL process so that data is transferred from the source systems to the monitoring system and then to alerts, properly. Regulators and most internal auditors will require evidence that effective controls are in place.

Over the past few years, it has become commonplace (primarily in Europe—although the U.S. is following suit) to

appoint a member of senior management to the role of chief data officer (CDO). Unfortunately, this new trend has not successfully spread to most countries. The CDO plays a pivotal role: overseeing the quality of the organization's data and is responsible for data mapping, quality assessments and action plans undertaken to solve any data-related issues.

Risk-based approach

Detection models must be chosen and set up based on a risk-based approach. Consider the products and services you offer, your distribution channels, as well as the breakdown of your customer segments. You need to know the risks related to your institution's business activities, in order to implement the detection models and rules that will tangibly benefit your monitoring framework and provide sufficient protection for the organization.

Model risk governance

Detection models have inherent risks that may only be mitigated by appropriately managing them. Some models will cover your risks and business needs, but others may have fundamental design flaws—even those created (out of the box) by reputable suppliers. The most important components of a model risk governance framework include, but are not limited to, inventory of models, the development, implementation and use of those models, model validation, calibration and optimization, and governance.

Documentation

To ensure that the delivered product is in line with business and regulatory requirements, you need to document your business needs and solutions throughout the course of the project. Doing this also means that you will have a record of all the decisions that were made and why. All companies experience staff movements over the years and it is possible that the project team will no longer be around when you need it. When there are system updates and patches, or when teams begin to question their processes, it is important that people can understand the reasoning behind past decisions. What is more, regulators require that this type of record be kept and presented to auditors and inspectors.

System customization

A common pitfall, which should be avoided, is customizing your monitoring system. Of course, configurations are unavoidable; but you are taking a huge risk if you make changes to the source code. While some suppliers may agree to make such changes, it is strongly recommended that you do not attempt to adapt the solution to what you believe it should do, but rather use it as intended. The risk increases significantly if you are implementing a solution with multiple modules that work together. Customization often leads to compatibility issues, complicate the installation of software updates and limit what the supplier's technical support teams can do when there is a problem, which in turn may have an impact on your budget and deadlines. This cannot be stressed enough; customization should be avoided at all costs.

Change management plan

You need to implement a change management plan for the teams who will be using the monitoring system. Training on the new system for these teams is an integral part of the implementation project. The new system will perform certain tasks that were previously performed by people. This kind of change comes with its own set of challenges, especially during the transition period. A sound change-management plan will include the following steps: identify what will change, put a communication plan in place, prepare the change and effect the change. The main objective of this change management plan will be to maximize the adoption of the solution that brings added value to your financial institution.

Internal controls and regulators

A new AML/CTF monitoring system does not only affect monitoring teams, but it also has an impact on internal controls and audit teams. The internal audit functions need to be familiar with the new system structure, updated processes, procedures, policies and control measures, etc. The transition period gives internal controls and audit teams the time they need to adapt their work methods to the new system.

You also need to keep regulators informed of any major initiatives underway, especially if you are implementing a system for compliance purposes. You must demonstrate to regulators that all efforts are being made to comply with current requirements. Regulators will also want to see that senior management fully supports the project and has approved the budget for the implementation project to go forward. Keep in mind that for regulators to assess the residual risk and conduct an accurate audit of the organization, they need to be familiar with the controls and systems in place. It is best to remain transparent at all times.

Conclusion

Every organization and every implementation project has its own unique set of challenges. There is no magic formula to successfully implement an AML/CTF monitoring system. However, the practices covered in this article will help you avoid some of the pitfalls and common mistakes, which will help you save time and money in the long run.

Dominic Hurtubise, CAMS, CFE,
ACAMS Montreal Chapter co-chair;
director for AML Projects and Business Intelligence, Montreal, Canada,
dominic.hurtubise@desjardins.com