NICE
ACTIMIZE

洗錢防制中的人工智慧：改變正在發生

NICE Actimize 洞察報告

Ted Sausen
洗錢防制主題內容專家 | NICE Actimize

Anne Liegel
資深洗錢防制產品行銷經理 | NICE Actimize

作爲在 2020 年及未來洗錢防制環境中提供趨勢和變化的一種手段，NICE Actimize 展開年度行業調查，以更深入地瞭解機器學習 (ML) 和自動化技術對洗錢防制 (AML) 計劃的認知差異。

在這項基於該研究的產業調查中，NICE Actimize 評估了在交易監控方案方面面臨的持續性挑戰，並探討了大量金融服務組織 (FSO) 對洗錢防制計劃的現代化導入機器學習與自動化技術發生改變中的觀點。

調查結果中最明顯的推斷顯示，當代金融犯罪的複雜性和多樣性對洗錢防制解決方案的複雜性造成什麼樣的影響，同時也帶來不停歇的挑戰以維持有效的洗錢防制計劃。風險和合規主管常常無法找到資源來控管工作負載，加上可疑交易警報量持續上升，監管期望繼續加強，這些為他們帶來更多困擾。

全球受訪者來自於多種資產規模的金融服務組織，包括第 1 級銀行、中型銀行以及擁有 100 億美元以下資產的銀行。大多數受訪者都在風險和合規、營運或技術部門中擔任職務，並且對於交易監控具有主要關注領域。

在我們開始之前需要注意的一些重要結果：

- 2019 年，大約一半的受訪者表示警報量和警報品質是其交易監控解決方案中最顯著的挑戰。緊隨其後的是數據完整性問題以及合規性的整體成本。
- 同樣在 2019 年，90% 的受訪者表示他們的系統應該每年調整一到四次。（更頻繁的調整會導致警報量降低並產生相關成本。）
  - 雖然這是一項行業最佳實務，但其中只有一半的受訪組織能夠這樣做，而原因是他們並沒有可用資源（即調查員、技術、其他知識淵博的員工）。
- 確保適當調整客戶產業區隔正在成爲一種受到認可的必要性，因爲「通用」模式並未受到證明具有效果。
  - 就像系統調整，區隔維護的頻率並不總是如期執行。
- 對於人工智慧、機器學習和自動化科技的觀感正逐漸產生變化。由於產業使用情況已開始展現出各種好處，例如偽陽性訊號降低和更佳警報品質等，因此有很多金融服務機構重新評估他們現有的解決方案。
  - 2019 年，有 90% 的受訪者表示他們目前正在進行這些評估。
- 使用現有工具已無法滿足金融服務機構的永續發展需求。員工、資源以及支援預算並未隨工作負載量的軌跡同時發展，甚至在很多情況下都呈現反方向軌跡。現在我們已經進入 2020 年，這項現實正在型塑未來十年內的洗錢防制計畫發展程度。

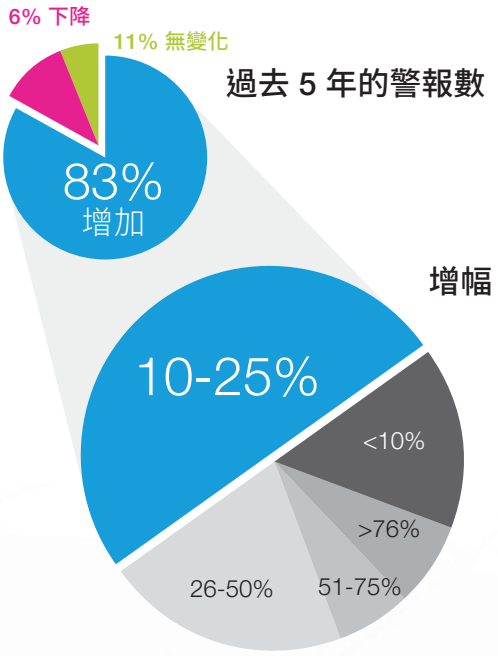
複合交易監控工作負載

不斷演進且變化的威脅與更強大的監管計劃相互結合，因此需要有新的分析數據加入到現有的洗錢防制解決方案中，以解決虛擬貨幣、人口販運或資助恐怖主義等情況。這在我們最新的 2019 年研究中獲得確認，其中一半受訪者表示他們每年都會將這些新分析數據加入到交易監控計劃中。

新分析數據對保護金融服務機構而言至關重要；但是，新資訊的導入將對現有的嚴峻工作負載產生不利影響。2019 年，有 83% 的受訪者表示在過去五年中發現警報量增加。大多數人同時表示，警報數量增加 10-25%，其中部分增幅更高達 75%。

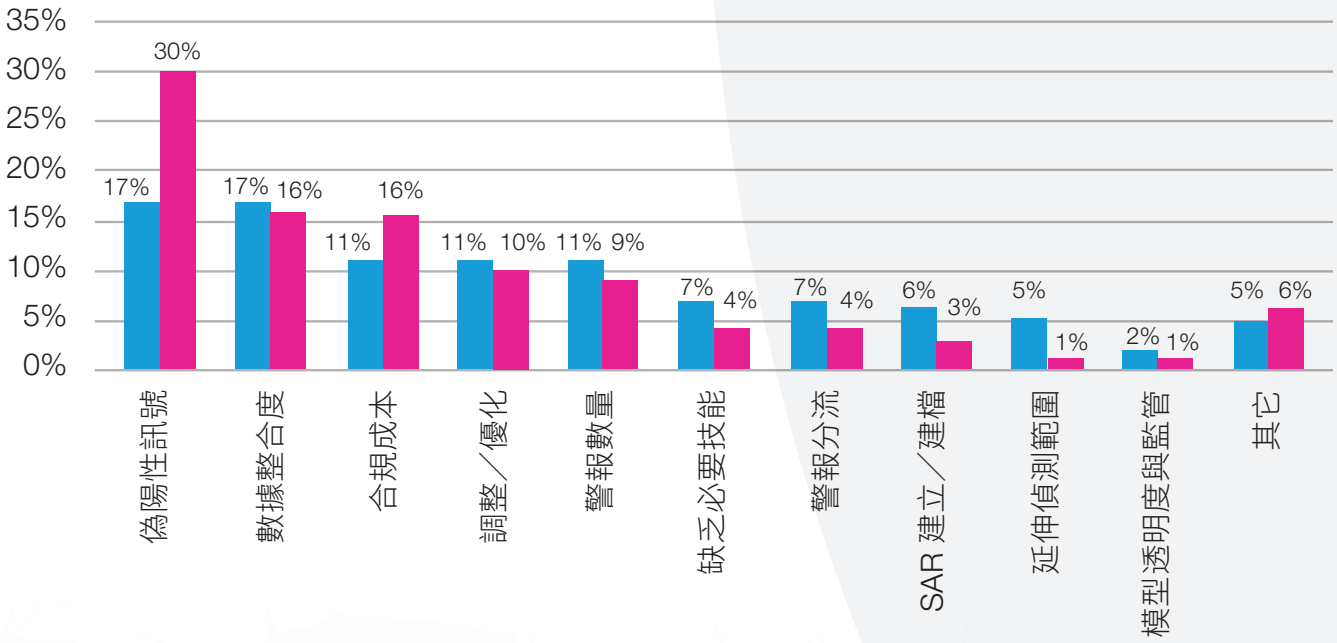
現金交易監控系統中的大多數警報都由偽陽性訊號組成。由於「偽陽性訊號」的定義有不同的意見，因此對於本報告的目的，我們將其定義爲不會導致提交可疑活動報告的任何警報。

偽陽性訊號被稱為是金融服務機構目前面臨到的最重大挑戰。結果顯示，近 95% 的警報係由偽陽性訊號導致，部分金融服務機構表示比例甚至會更高。還需要注意的是，從 2018 年到 2019 年，認為此問題是他們最重大挑戰的人數幾乎翻倍。



為了幫助調查員因應這種挑戰，需要付出相當大的努力。爲了證實此觀點，一家大約有 60,000 名洗錢防制調查員和合規官的大型英國跨國組織表示，他們調查一個低程度的偽陽性訊號通常需花費 5 到 30 分鐘的時間。[1]更複雜的警報可能需要好幾個小時甚至好幾天的時間來解決。這會為分析師、調查員和合規人員帶來壓力，有時還包括客戶經理以及可能需要參與並提供協助的職務。

交易監控計劃中的哪個方面是您所屬部門最重大的挑戰？



2018 年和 2019 年受訪者面臨的最重大挑戰，正是具有說服力的觀察結果。以上圖表顯示出偽陽性訊號增加、工作任務的減少，例如 SAR（可疑活動回報）建立、警報分流、偵測和模型驗證。**此結果顯示，從營運角度來說，組織內的成熟度不斷成長，同時他們擁有正確且到位的人員和流程，但仍然無法減少這些偽陽性警報，這些警報也直接導致了洗錢防制計劃的整體成本增加。**

再加工技術 解決問題

解決高偽陽性率是具有兩個步驟的流程。首先，金融服務機構需要驗證客戶群體是否獲得正確分組。確保適當調整客戶產業區隔具有必要性，因爲「通用」模式並未受到證明具有效果。以兩個加油站為例 — 一個可以作爲加油站搭配附有商用 ATM 的便利商店，而另一個則是加油站和附有私人 ATM 的便利商店，同時內建可用於博奕的遊戲機。雖然他們非常相似，但應該根據情況放入不同的區隔組別進行監控。

正確將客戶群體分組，可將具有類似特質的客戶針對交易行為進行比較。若某些活動超出這些區隔範圍的典型行爲，則會產生警報。在實務中，應每年對這些區隔分類進行檢視。如果可以，更頻繁的檢視是有益的，因爲如有必要，客戶可以根據他們的行爲移動到不同的分類。同時也須謹記，從客戶一開始加入，到與組織發展關係期間，行爲可能會發生變化。區隔分類若未能正確維護，會將活動錯誤貼上異常標籤，因此觸發其他警報。其實真正造成的結果，是根據行爲和風險建立具有常見屬性的高針對性區隔分類。擁有非常類似的同行有助於嚴密地發揮閾值效果。

區隔管理

在 2018 年和 2019 年調查中，對於區隔管理的回答非常相似。大多數組織至少每年檢查一次他們的區隔分類，75% 的組織表示他們在過去兩年內皆執行過檢視。因為過去在一開始就缺乏對區隔的注意，這一點顯示出產業正向前邁出積極的步伐。

解決高偽陽性率的第二步是調整分析模型。調整是最佳化參數和閾值的過程，確保它們適合之前提及的各區隔分類定義。最大的挑戰，是在建立更多區隔分類時如何讓付出的努力獲得加乘的倍數效果。金融服務組織必須確定適當數量的區隔分類以有效監控客戶，而不會導致因調節力道過大而造成無法定期實施的結果。我們強調正確區隔 的重要性，因爲若缺少此要素，便無法爲具有相異活動的客戶進行正確的參數設定。

2019 年的調查對象中有 90% 皆同意應該每年至少進行一次調整，因爲更頻繁的調整會導致警報量降低並產生相關成本。

- 雖然這是行業最佳實務，但其中只有一半的組織有可用的資源來執行調整（即調查員、技術、其他知識淵博的員工）。許多組織都選擇調整其模型的子集合，但這意味著他們無法擁有完全調整的模型。

由於涉及的變量數量，在使用傳統方法時，將無法透過人工來實現這些活動。這就是爲什麼金融服務機構開始從傳統方法中變化方向的原因，轉向探索融合機器學習和叢集技術的方法。

90%

同意每年至少進行一次調整

人工智慧與機器學習：新標準

機器學習和人工智慧與機器學習空間的導入最初面臨不同程度的阻力。分析師、研究者和監管機構習慣於他們能理解的傳統規則式模型，而機器學習卻採用不同的方法。這些模型的輸入和輸出是已知條件，但在這之間進行的流程並不透明也無法被理解。

2018 年，透過機器學習強化對監管機構提供的證明模式是合規團隊的首要問題，第二個問題則是實施這些技術的成本。有趣的是，短短一年後的 2019 年就發生了變化：兩者順序交換，實施成本變成首要考量，並將對監管機構進行的證明放到第二位。根據這些結果和其他產業的觀察，監管接受程度已不再是這麼重要的問題。金融服務機構已經從「謹慎觀察」開始積極追求這些技術，以補足現有的洗錢防制計劃。

這些變化中的氛圍更因多重因素的累積而加快腳步：

- 結果開始變得明顯。開始執行實驗的早期採用者觀察到正面結果。
- 部分供應商對於缺乏透明度的「黑盒子」做出快速因應對策，並製作可解釋的分析以消除任何疑慮。
- 監管機構的支持和鼓勵。

在監管障礙消除後，就會產生一些收穫:

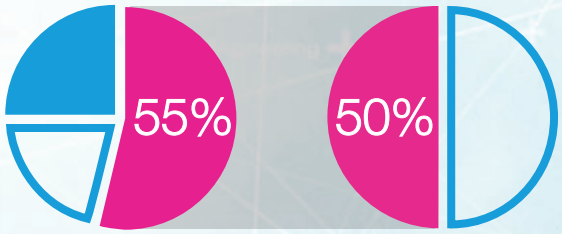
- 如果這些創新技術發現了以前未被其傳統的洗錢防制計畫檢測到的洗錢陰謀，金融服務機構將被授予安全保護，並且不會受到懲罰或罰款。這可以消除組織認爲他們需要執行昂貴的回顧練習而產生的憂心。
- 監管機構不會懲罰選擇不實施創新技術的組織，而這導致一項問題：「那爲什麼要提到這個？」。

2019 年，15% 的受訪者表示他們仍然不認爲機器學習能夠輕鬆遵守法規。從另一系列 問題的回應中可發現，他們實際上相信這些新技術，但是他們的信心卻會在尋找導入新技術的資料科學家這一過程中，發生動搖。這些疑慮通常是由於整合所需的成本、對風險的趨避以及缺乏能夠準確考量投報率的計劃所造成的。

15%

不相信機器學習能夠輕鬆遵守法規

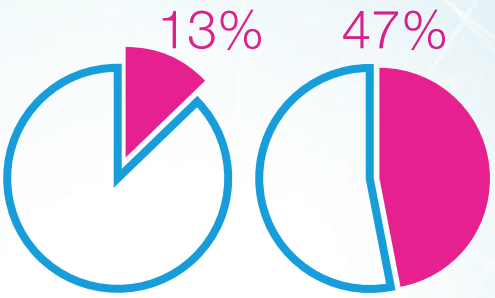
而另一方面，有 25% 的受訪者已經將人工智慧和機器學習技術整合到現有的洗錢防制解決方案中，超過一半的受訪者表示他們正在積極評估。在此數字中，50% 的人特別指出他們希望在明年進行整合。



25% 已經實施人工智慧
55% 正在評估
20% 未評估或規劃

在 55% 正在評估的組織裡，其中有一半計劃在明年內進行整合

在 2018 年和 2019 年調查中，受訪者表示他們運用洗錢防制機器學習的主要業務驅動因素包括異常情況檢測、區隔分類和模型調整（兩者搭配使用）。**我們發現一個有趣的現象，2018 到 2019 年間，「用機器學習進行區隔分類」的業務驅動因素一下子大量攀升，從 13% 一下躍升至 47%。**



以機器學習執行區隔分類

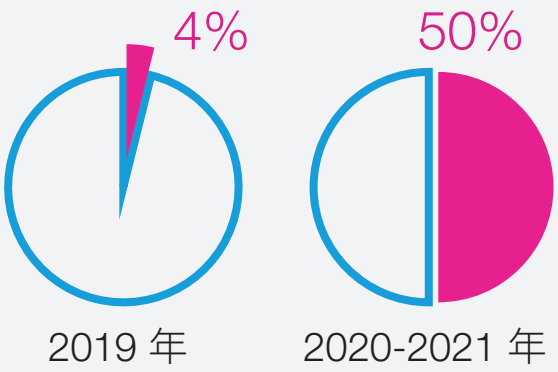
由於大多數組織都趨向發展人工智慧、機器學習和自動化技術，他們在不久的未來將成全新的典範，甚至會成為一項必要條件。

邁向雲端

在洗錢防制計劃中有效實施機器學習意味著對大量數據的高度依賴，這也將帶來一系列需要與需求。為能有效管理此趨勢，許多金融服務機構紛紛尋求雲端解決方案。受訪者指出，尋求雲端的前兩大驅動因素包括可輕鬆與其他技術整合以及其提供的可擴充性。雲端解決方案的其他優勢包括:

- 降低成本（雲端儲存空間與其他硬體）
- 更出色的運算效能選擇，且具有更高靈活度
- 資料科學資源（例如由第三方供應商提供的服務）
- 來自多個組織的數據運用整合情報（同行基準和進階異常檢測）

2019 年僅有 4% 的受訪者表示他們目前正在使用公用雲端洗錢防制軟體和服務，但卻有高達 50% 的受訪者計劃在未來兩年內使用公用雲端。



未來展望

展望 2020 年及未來，業界將加快腳步將洗錢防制計劃的現代化視為首要任務。展示出新技術具備之可量化優勢的案例研究已開始浮現，而尚未擁抱這項轉變的組織將會利用這些案例做為打造自家商業案例的實證，以合理化相關成本開銷。

迄今爲止，從機器學習和人工智慧角度所看到的重點皆放在交易監控相關議題，但我們將開始看到這種情況擴展到過濾和客戶盡職調查的流程中。機器學習將利用結合了交易活動的大量客戶端屬性來深入辨識行為異常，並減少現今許多交易監控系統中存在的「噪音」情況。

需要瞭解瞭解客戶流程中的缺陷將如何對整個瞭解客戶／客戶盡職調查計劃帶來負面影響，同時也會造成其他領域效能下降（如交易監控和監視名單過濾）。使用最新創新技術可實現擴大風險覆蓋範圍，並簡化客戶整體生命週期評估的所有方面 — 意即將瞭解客戶應用程序導入、持續的客戶盡職調查和強化的盡職調查流程等納入考量，打造出整合洗錢防制解決方案。這可以提高營運效率並提供客戶風險的整體觀點，因此金融服務機構可以放心，他們將能隨時掌握最新客戶資訊。在過去數年發展並於 2019 年間形成主流的所有金融犯罪科技主題，將在 2020 年付諸行動。預計有五個關鍵領域將從這些主題中脫穎而出，並且在我們向前邁進的過程中大幅影響金融犯罪和洗錢防制活動:

1. 私人對私人資訊的共享 對環境型金融犯罪
2. 提高的因應
3. 即時洗錢防制監控
4. 品質影響而非數量影響
5. 更加符合標準

有一件事是肯定的 – 金融犯罪將不斷發展，變得越來越複雜。這是您的組織需要贏得的戰爭。NICE Actimize 在此提供幫助並隨時準備好深入瞭解本研究所涵蓋的主題和方法。請隨時與我們聯繫，深入瞭解洗錢防制產業的最新發展和未來展望。

引用

1. McGowan，J.（2018 年）。人工智慧用於減少偽陽性訊號。Celent，3–3。

NICE
ACTIMIZE

關於 NICE Actimize

NICE Actimize 是最大型且範圍最廣泛的金融犯罪、風險與合規解決方案供應商，為區域性及全球性金融機構以及政府監管單位提供服務。NICE Actimize 的專家運用創新科技來揪出金融犯罪，避免詐欺發生並提供監管合規服務，藉以保護機構、捍衛消費者及投資人資產，也因此持續被排名為業界第一。公司提供即時、跨管道的詐欺防制、洗錢防制的偵查以及交易監控解決方案，解決如付款詐欺、網路犯罪、交易監控、市場濫用、客戶盡職調查與內線交易等問題。