



*Regtech Watch is a newsletter published by the Hong Kong Monetary Authority to promote the use of Regtech by the banking industry. It provides information on actual or potential Regtech use cases rolled out or being explored in Hong Kong or elsewhere. The objective is to assist authorized institutions (“AIs”) in adopting innovative technology to enhance their risk management and regulatory compliance.*

## Background

This fourth issue of Regtech Watch focuses on the use of technology in conduct risk management, in particular how Regtech can help banks detect misconduct and monitor conduct and culture within their organisations more efficiently and effectively.

It should be noted that the sole purpose of this newsletter is to provide AIs with information on the latest Regtech developments. The HKMA does not endorse any use cases or solutions described in this newsletter. If an AI intends to adopt a particular solution, it should undertake its own due diligence to ensure that the technology is suitable for its circumstances.

## Regtech in conduct risk management

### Key challenges

Conduct risk is inherently difficult to identify and quantify using traditional risk management processes. For one, misconduct can take numerous forms, ranging from inappropriate employee behaviour that falls short of professional or regulatory expectations, to more serious transgressions that include criminal acts. Furthermore, misconduct can potentially be observed in any part of the organisation, ranging from frontline to back-end operations. Taken together, this wide scope makes misconduct difficult to detect, monitor and mitigate.

---

In general, banks manage conduct risk by implementing surveillance programmes that serve two purposes: (i) monitor employee activities and detect irregular behaviour; and (ii) collect data which can help the bank identify drivers of misconduct. Surveillance of conduct risk is a resource-intensive process, and banks have faced difficulties in making effective use of the data collected via such monitoring. Examples of challenges encountered are detailed below:

- There is a better chance that unusual employee behaviour can be detected in a timely manner if surveillance data are collected from different sources (e.g. email communications, call recordings, access logs for applications or databases storing customer or other confidential information, and leave records) and then amalgamated and considered in aggregate. However, banks that adopt a more conventional approach of review normally consider individual data sets separately, meaning they may miss out on opportunities to “connect the dots” and identify suspicious patterns of behaviour that more holistic analyses would have made evident.
- Another inherent challenge of managing conduct risk is finding ways to handle the unpredictable “human behaviour” aspect of it. Conventional surveillance programmes are often rule-based and rigid, meaning for example, alerts are only generated when generic “trigger” words are identified. This formulaic approach has a number of drawbacks, including that it provides rogue employees the opportunity to “game” the system, or may result in a high number of false positive alerts.

Most of the challenges boil down to a single key issue – how banks can analyse the vast amount of data<sup>1</sup> that flow through different systems within the organisation in order to predict and identify instances of misconduct.

---

<sup>1</sup> These can include both structured and unstructured data, e.g. verbal and written communications, customer complaints, whistleblowing reports, employee surveys, past incidents of conduct failing, disciplinary actions and performance measurement.

---

## **How can Regtech help?**

Against this backdrop, banks are increasingly exploring how Regtech can help address some of the aforementioned challenges. Some have found that artificial intelligence solutions can help aggregate and holistically review a broad set of conduct risk data, and be used to develop surveillance programmes that are more adaptive to different employee behaviours.

## **Regtech use cases**

Various technology solutions aimed at analysing surveillance data have been developed by banks or external vendors. Three use cases observed by the HKMA are summarised below for reference –

---

### **Use case 1 – Automation of call monitoring reviews**

Telemarketing activities involving distribution of financial products to retail customers are a common source of conduct risk for banks. Failure by sales staff to meet the bank’s internal or regulatory requirements, such as misrepresenting key product features or not reading out the risk disclosure statement(s) in full to the client, could trigger customer complaints and give rise to sales misconduct.

Absent the use of more advanced technologies, banks typically rely on the compliance function to manually review call logs and identify isolated instances of non-compliance or inappropriate sales practice. This is resource intensive, and consequently banks can review only a sample of calls and may therefore leave some problematic cases uncovered.

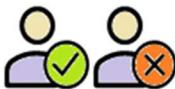
To overcome this constraint, Regtech solutions built upon natural language processing (“NLP”) and machine learning (“ML”) technologies have been developed to monitor sales calls.

One vendor has developed an NLP-enabled application which allows computers to take the place of humans to conduct the first round of call log review, leaving only the more complex or high risk cases to the bank’s compliance or risk management function to follow up. This enables full-scope review of all sales calls, and also the more efficient use of compliance and risk management resources. Riding on its NLP capabilities, the solution can also detect the customer’s emotions (e.g. via monitoring of tone of voice or verbal expressions) and provide the bank with more insights to enhance customer experience. Furthermore, the solution features add-on technologies (such as voice recognition technology) which provide additional functions that human reviewers would not typically be able to deliver. For example, some banks prohibit sales staff from soliciting the same customer more than once. While a human reviewer may not be able to spot this easily, voice recognition technology can help identify participants in a call and ascertain whether the same combination of voices is found in other calls. This way, repeated contact can more easily be uncovered. Finally, the inclusion of ML

technology also means that the system can “learn” and “adapt” as it processes more cases, and become increasingly more accurate over time.

The benefits of technology-enabled solutions relative to the conventional approach are summarised in **Exhibit 1**.

**Exhibit 1: Conventional vs. technology-enabled approach to reviewing call logs**

	 <b>Manual review</b>	 <b>Technology-enabled solution</b>
<b>Review 100% of call logs</b>	<p style="text-align: center;">✘</p> <p style="text-align: center;"><i>(Too time and resource intensive)</i></p>	✔
<b>Availability of staff to handle more complex cases requiring human judgement</b>	<p style="text-align: center;">↓</p> <p style="text-align: center;"><i>(Significant portion of manpower likely occupied by the first round of call reviews)</i></p>	↑
<b>Additional features</b>	N/A	<ul style="list-style-type: none"> <li>• Add-on technologies (e.g. voice recognition) support the detection of certain types of misconduct</li> <li>• Collect insight on the quality of the customer’s experience</li> </ul>

---

## **Use case 2 – Detecting unusual employee behaviour**

As a key element of sound risk culture, banks should set and adhere to professional standards and corporate values that promote ethical and responsible professional behaviour amongst employees. Banks should remain alert to the risk that lone individuals could exhibit undesirable behaviours that result in significant legal and reputational damages to the organisation.

### Surveillance tools for monitoring employee behaviour

Without the support of more advanced technologies, banks mainly monitor employees' conduct through ongoing surveillance of activity logs or records (such as access to emails, customer information databases and application systems) to flag anomalies that may indicate rogue behaviour. However, the more typical approaches for monitoring activity tend to be conducted in silos (e.g. application by application) or respond to rule-based triggers, meaning they often lead to many false positive alerts generated. Moreover, the damage is often already done by the time a red flag is raised (e.g. an alert may only be generated when an email containing the bank's proprietary information is dispatched to an external recipient). This means banks can only react to, rather than pre-empt, incidents of misconduct.

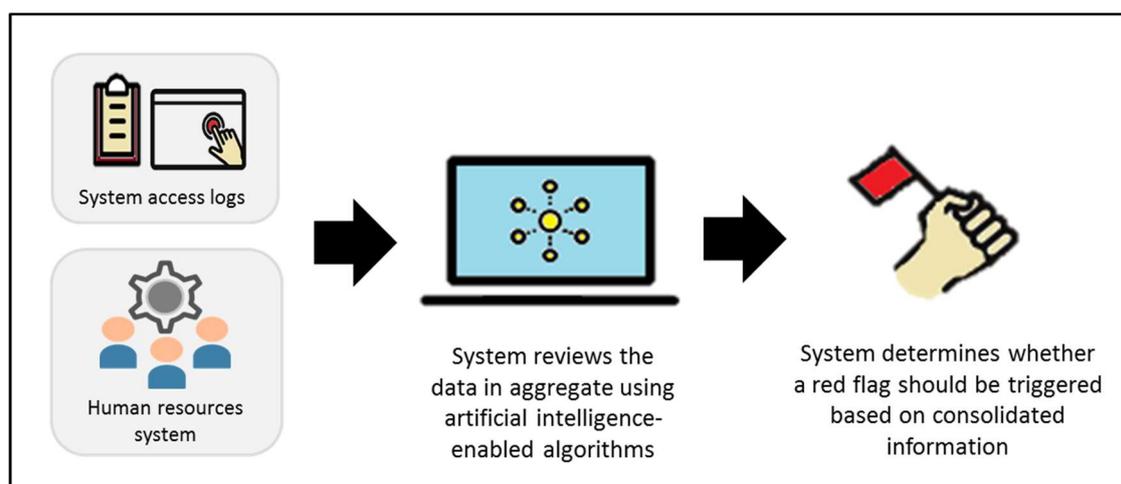
To enable ex-ante detection of unusual employee behaviour, one bank has adopted a system built on artificial intelligence-enabled algorithms to generate a more holistic view of an employee's activities. The system is fed data from a number of sources, including the employee's system access logs, leave record (e.g. whether the employee was on block leave when accessing certain applications and databases) and employment status (e.g. whether the employee has recently tendered resignation). These data points allow the system to take into consideration a fuller spectrum of observations when assessing whether an alert should be triggered.

As with the first use case, ML technology has been used to augment the solution to enable it to continuously learn and improve itself based on past observations. By considering a wider spectrum of data in aggregate, the bank

may also be able to glean insights into what tell-tale signs usually preclude errant behaviour and be able to take appropriate action to close relevant loopholes in advance.

A simple illustration of this process is at [Exhibit 2](#).

### Exhibit 2: Technology-enabled solution for detecting unusual employee behaviour



### Holistic surveillance and conduct risk visualisation tool

Regtech solutions are also available for markets and communication surveillance. Such solutions are increasingly being applied to trading activities and are primarily used to identify regulatory breaches within unstructured data logged via various communication channels, including voice, email, text and chats.

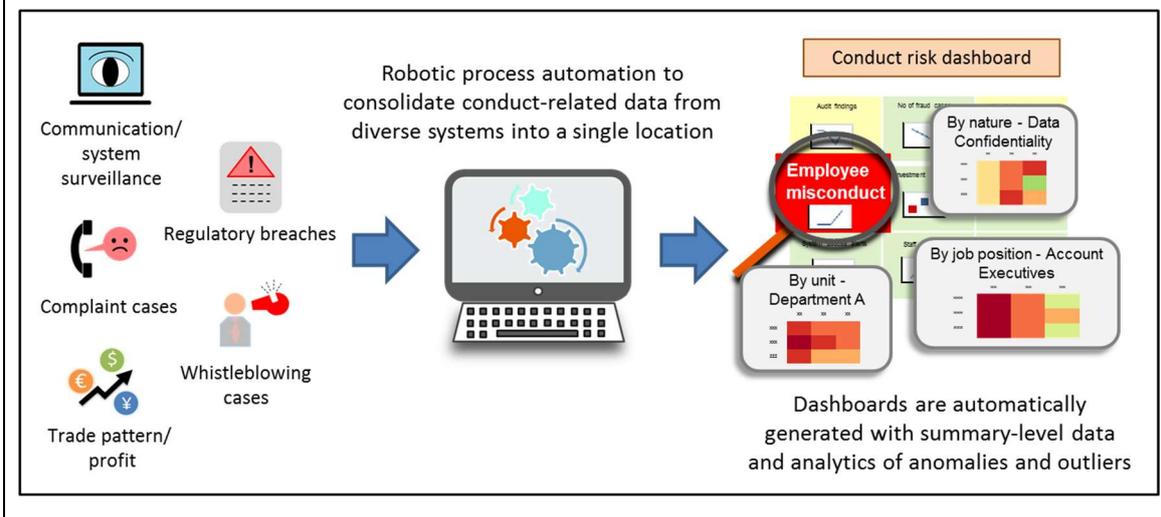
Riding on this, one vendor has offered a “one-stop” suite of solutions to assist financial institutions to holistically monitor and manage conduct risk across the entire institution. Apart from the NLP and ML technologies built in to improve efficiency and effectiveness of conduct surveillance, the add-ons include (i) robotic process automation to extract conduct-related data (such as regulatory breaches, exceptions from communication surveillance, trade pattern and profits, complaints, and whistleblowing cases) from diverse systems and consolidate them in a single location; (ii) anomaly detection

which analyses large data sets and creates benchmark patterns in order to find outliers (i.e. employees acting differently from their “normal” behaviour) and generates risk alerts for further review; and (iii) an integrated case management system to facilitate review and follow up on alerts that are enriched with relevant information, such that manual resources can be deployed to higher risk cases instead.

To enable a bank’s board of directors and senior management to grasp the magnitude and direction of conduct risk, dashboards are automatically generated with summary-level data and analytics are presented in a graphical and easy-to-read format. Conduct risk can then be visualised in a context tailored to the readers’ needs and in multiple dimensions (such as on a global or regional level, on the trend of different types of conduct risk, on which business line or function the risk is coming from).

The above process is summarised in **Exhibit 3** below:

**Exhibit 3: Technology-enabled solution for holistic surveillance and conduct risk data visualisation**



---

### **Use case 3 – Identifying culture and conduct issues through employee exit surveys**

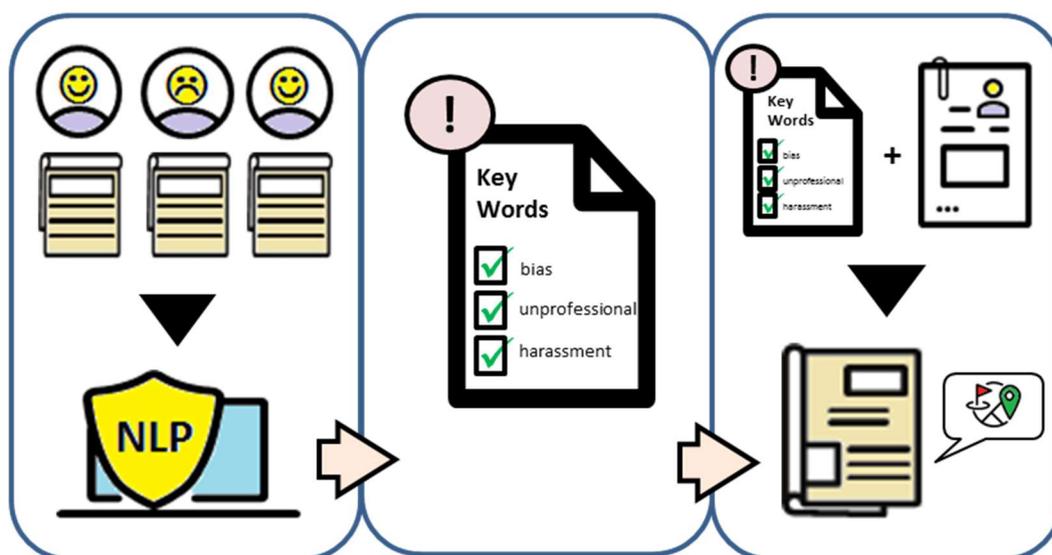
Many banks recognise employee exit surveys as a valuable source of information for identifying potential culture and conduct issues. However, as relevant feedback is provided not only through “close-ended” questions, but also in the form of “free form” text, reviewing such “free form” feedback can be time-consuming and labour-intensive. Following conventional methods, the human resources (“HR”) function usually has to spend significant time manually scanning and cross-checking each form against a list of key words, before even moving to consider whether any investigation is warranted.

To enhance the efficiency of the review process, one bank has made use of a solution built on NLP technology. The solution can take the place of HR function to conduct a first review of the submissions and flag up feedback which contains the identified key words. Apart from speeding up the review process, the NLP solution can contribute to improved accuracy. The NLP solution is able to recognise that different variations of the same base word have the same meaning. For example, “account opening” and “accounts were opened” will all be recognised as a variant of “account open”. This means it will not omit relevant entries simply due to different writing styles, and which human staff may have a chance of overlooking.

Deployment of the NLP solution can help facilitate management to understand and respond to culture and conduct issues identified via the exit surveys. Specifically, the resulting dataset of the NLP review can be aggregated with other contextual data (e.g. data related to the position of the employee submitting it) to generate more detailed and comprehensive reports. These in turn can help inform senior management of the common themes and trends related to conduct or culture identified within different businesses and categories of employees, and allow them to consider more targeted and appropriate follow-up action in a timely manner.

A diagrammatic illustration of this process is at **Exhibit 4**.

Exhibit 4: Technology-enabled solution for the review of exit survey



1. Exit surveys are fed into the NLP-based System
2. The System scans the exit surveys for designated key words and produces a resulting dataset of all flagged feedback
3. The resulting dataset can be merged with contextual data to produce comprehensive insights to inform management and facilitate their formulation of targeted responses

Apart from the above use cases, there are emerging Regtech solutions leveraging predictive linguistic and behavioural analysis of interactions among employees to generate early conduct risk indicators such as increased stress level and risk-taking propensity. Bank management can thus identify root behavioural causes of misconduct more effectively. These solutions aim to help banks manage culture and conduct related risks in a more proactive and forward-looking manner.

This newsletter is benefitted by input and ideas contributed by the following companies:

- DBS Bank (Hong Kong) Limited
- JPMorgan Chase Bank, National Association
- NICE Actimize
- Nova Credit Limited