INDEPENDENT VERIFICATION OF THE COMPLIANCE IMPROVEMENT REVIEW

COMPLIANCE IMPROVEMENT REVIEW 2019

In May 2019, the then Home Secretary established an independent review to consider what could be learned after MI5 identified compliance risks within certain technology environments. Sir Martin Donnelly conducted this Compliance Improvement Review (CIR), the summary section of which and the recommendations were published in July 2019.

While recognizing that "*MI5 is a consistently high performing organisation",* whose staff have "*a deep seated commitment to respect and work within the law",* Sir Martin concluded that "*poor management of legal compliance within the IT environment posed risks for the continued effective operation of the organisation"* and that there had been *"limited communication with the Home Office about the extent of the compliance problem".*

Sir Martin's review identified 3 areas where improvements could be made:

- Improvements to support an effective compliance culture across MI5 (recommendations 1-5);
- Improvements to ensure more effective sharing of information between MI5 and the Home Office to identify emerging issues (recommendations 6-9);
- Improvements to ensure increased legal input to the MI5 Management Board and ensure closer joint working between MI5 and Home Office legal advisers (recommendations 10-14).

Sir Martin set a deadline of June 2020 for completion of the change programme to deliver the first 5 recommendations and a deadline of the end of 2019 for delivery of the first part of recommendation 9 (increase in staff resources in the Office of Security and Counter Terrorism in the Home Office). The remaining recommendations did not have specified deadlines.

Additionally, in the concluding section of his report, Sir Martin outlined the commitment needed across MI5 to achieve a sustained improvement in compliance. He noted that "*MI5 must ensure that all its data can be shown to be held in accordance with legal compliance requirements by June 2020."* This has come to be known as the "Summary Action" and has been treated by MI5 and the Home Office as a de facto recommendation.

COMPLIANCE IMPROVEMENT PROGRAMME

The then Home Secretary received the CIR in late June 2019. MI5 established the Compliance Improvement Programme (CIP) in July 2019, to implement the CIR recommendations. The programme was split into 2 phases, the first to deliver the CIR recommendations by June 2020 and – recognising the need for continuing commitment to legal compliance as identified by Sir Martin – the second (to run until the end of 2020) focused on embedding longer term legal compliance change. A significant programme team was established to take the work forward.

RELATED WORK

The significant risks which had led to the commissioning of the CIR were subject to an urgent inspection by the Investigatory Powers Commissioners' Office (IPCO) in March 2019. MI5 initiated a major programme of remediation work in response. IPCO undertook further inspections to review the progress of these mitigations. In his Annual Report for 2019, the Investigatory Powers Commissioner said: "*we are confident that MI5's internal review of safeguards, initiated following their realisation of the severity of this issue, will identify any substantial vulnerabilities in their data handling model*"

THE IMPACT OF COVID 19

The CIP initially set a deadline of June 2020 for all 14 recommendations and the Summary Action. However, the scale and complexity of the work involved, meant that it was quickly apparent that all the work required could not be completed within that deadline.

Covid 19 restrictions have also very significantly delayed delivery of the recommendations, given the requirement for much of the work to be done within highly secure premises.

INDEPENDENT VERIFICATION

Recommendation 5 of the CIR stated that "*the satisfactory delivery of this change programme should be independently verified by the end of June 2020".* The Home Secretary announced in July 2020 that this independent verification exercise would have to be postponed due to the impacts of Covid 19.

I was therefore appointed by the Home Secretary in December 2020 to conduct the verification exercise by the end of January 2021.

OVERARCHING ASSESSMENT OF PROGRESS

A huge amount of work has been done through the CIP and the remediation work. Not all Sir Martin's recommendations have yet been fully implemented, but significant, measurable progress is evident. MI5 have used the CIR to make fundamental changes across the whole organisation and develop a new legal compliance operating model intended to cope with future changes in technology and data.

Sir Martin noted that the effectiveness of his recommendations depended on "*MI5's leadership delivering the lasting change in organisational culture which will ensure that, when such issues arise in the future, they are handled as a management priority and properly resourced. Individual improvements, while needed, will not be sufficient without a sustained focus on compliance."* I have therefore sought to test, not just delivery of the 14 recommendations, but more broadly how far improvement is visible in 3 areas, both now and for the future:

- MI5 confidence (and therefore that of IPCO and Home Office Ministers) that all its data holdings are and remain **legally compliant** in an evolving technology environment;
- Legal compliance is seen as **integral to the core operational mission** across MI5 and is clearly prioritized by the top leadership, from the Director General downwards;

- **Transparency and collaborative problem solving** with the Home Office and IPCO in relation to potential legal compliance risks as soon as they are identified.

ARE MI5'S DATA HOLDINGS NOW LEGALLY COMPLIANT?

MI5 has reviewed its data holdings to identify relevant systems and infrastructure storage assets, assess the legal compliance risk for each and develop mitigations for identified risks. Implementation of those mitigations continue.

While there is more still to be done, the broader changes that MI5 has made to strengthen its legal compliance risk management processes, instil a culture of individual accountability for legal compliance risk and ensure that compliance is built in to new products should give Ministers greater confidence that new risks will be identified early and addressed promptly.

IS LEGAL COMPLIANCE SEEN AS INTEGRAL TO THE CORE MISSION AND PRIORITIZED BY TOP LEADERSHIP?

Legal compliance is now an organisational priority for MI5 and an important element of its strategy. There is no doubt that the Director General and his top team see compliance within the regulatory framework as an essential part of delivering operational effect.

There is new governance to oversee compliance and security risks and resourcing for compliance work has been significantly increased. More than 80% of staff in scope have completed mandatory training, despite covid restrictions. The staff I spoke to across the organisation had done the mandatory training for their roles, demonstrated a high level of awareness of their individual accountability for legal compliance and were able to describe a variety of guardrails, processes and assurance mechanisms.

However, organisational culture change is always slow and needs persistent leadership attention to succeed. The top leadership team should continue to communicate that operational success requires legal compliance and that demonstrating compliance is essential to MI5 maintaining the trust of the public and of Ministers. They will also need to ensure they have the right management information to monitor the impact of the changes which have been made.

IS THERE TRANSPARENCY AND COLLABORATIVE PROBLEM SOLVING BETWEEN MI5 AND THE HOME OFFICE?

The creation of the Ministerial Assurance Group has been an important step forward, with much greater information sharing and more effective challenge. However, continuing effort and collaboration will be needed to build and sustain this new relationship of openness and constructive challenge, particularly between the two legal teams.

DOES MI5 NOW HAVE AN EFFECTIVE COMPLIANCE FRAMEWORK THAT WILL SERVE IT WELL IN FUTURE?

MI5 has introduced new policy, processes and training to ensure that legal compliance is "built in" to new product development. More broadly, it has introduced a new compliance operating model for the whole organisation. However, the changes that have been implemented are still very new and the transition to the new operating model will not be completed until the 3rd quarter of 2021. Covid restrictions have meant that new policies and processes have not yet been extensively tested.

MI5's data holdings are constantly changing. New legal compliance risks will continue to emerge. What matters is a compliance framework that can spot, assess and mitigate those risks early. The new operating model is an excellent start, but it will need continuing resource and senior management attention to properly embed it.

MI5's leadership recognise the continuing challenge and are committed to ensuring the organisation maintains the momentum it has established. A successor programme to the CIP will take forward further work, overseen by the new governance. Ministers will wish to continue to test progress through the Ministerial Assurance Group, while IPCO's next inspection will also test the effectiveness of the new assurance arrangements.

PROGRESS AGAINST INDIVIDUAL RECOMMENDATIONS

I looked in detail at the work that had been done to deliver the individual recommendations and Summary Action to assess the extent to which they have been implemented. Broadly:

- recommendations 1, 5, 6, 8, 9 and 10 have been fully implemented (although work continues to refine and expand the training programme rolled out under recommendation 1). Monitoring of completion rates for mandatory training should continue;
- recommendation 14 has been fully implemented, but will not be concluded until the review of the IP Act;
- the intent of recommendation 7 has been addressed by alternative means;
- Good progress has been made to implement recommendations 2, 3, 4 and 11, but further work is needed to fully roll out and test new policies and to reduce reliance on manual processes. The new compliance operating model remains very new and will need time to embed;
- further work is needed to extend the collaboration envisaged in recommendations 12 and 13;
- extensive review and mitigation work has been undertaken – and continues - to deliver the Summary Action, with effort prioritised accord to risk.