Compliance Improvement Review

Introduction

1. I have been asked by the Home Secretary to review compliance risk management in MI5[1]. The objective is to strengthen governance and the transparent management of non-operational risk, in the light of compliance issues being identified in certain IT environments, in particular the [*Technology Environment*]. The Terms of Reference for this review are attached at **Annex 2**.

2. The report sets out what happened, why it happened, and what should be done to improve risk management in the future. Its content draws on the work of a combined Home Office/MI5 review team and a range of discussions with key personnel.

3. I am grateful for the team's hard work to complete the report promptly. I also appreciate the frank and constructive input of colleagues across MI5, the Home Office and the Investigatory Powers Commissioner's Office. The conclusions of the report and the recommendations for action are made on my personal responsibility.

Context

4. The period between 2009 and 2019 was one of profound change for MI5. Three trends are worth highlighting.

[1] There are two elements to this. First, the role of the Secretary of State in accepting, before warrants are approved, the basis upon which information obtained under warrant would be managed once acquired. Second, the legal requirements or safeguards related to warranted data. More detail is available at **Annex 1**.

5. First, the national security threat has evolved, often rapidly. Securing the Olympics, the Woolwich attack in 2013, the rise of ISIL, terrorist attacks in the UK in 2017, the Salisbury incident in 2018 and a persistent threat from Northern Ireland related terrorism are just the most high profile examples. As an illustration, Figure 1 shows the numbers of priority international counter- terrorism (ICT) investigations and leads MI5 has responded to since 2016:

[REDACTED]

6. Second, there has been a huge increase in the volume, complexity and importance of data, which has had important implications for how MI5 operates. [REDACTED].

[REDACTED]

7. Third, the legal environment has become more exacting. The IPA introduced new oversight for MI5's activities and judicial review of its warrantry applications. MI5, together with GCHQ and SIS, also now face far greater levels of legal challenge to their activities than they have in the past.

The [*Technology Environment*]

8. [*MI5 uses different technology environments. One of these technology environments will be referred to as "the Technology Environment" or TE. This TE holds data including warranted data*].

How MI5 Defines Compliance

9. Since the formation of its legal compliance department in around 2017, MI5 has generally used the term 'compliance' to mean compliance with the law, in particular with regard to information handling in accordance with the IPA and RIPA. In that context, 'compliance risk' is used to mean the risk that MI5 might not be complying with the law. Where MI5 find evidence that they are not complying with the law, this would be usually be described as 'non-compliance' or 'unlawfulness' rather than 'compliance risk'.

10. Such cases would not be categorised as RED risks but would instead be 'issues', or 'errors' that would be reported to the Commissioner. RED risks in the context

of compliance risk might mean it is judged likely that issues or errors will be uncovered (and when found reported and remedied as quickly as possible), or it might mean that there is insufficient understanding of whether MI5 is complying with the law and more assurance was needed (and it is not known whether subsequent investigations might any unlawfulness or non-compliance).

11. Where 'compliance' is used in documents prior to 2017, it might be being used in a number of ways to mean compliance with security or other internal MI5 policies. 'Non-compliance' in this context would not necessarily be non-compliance with the law or unlawfulness. This more consistent use of the term was one of recommendations implemented following the January 2016 compliance report.

Review of Events

[*A period of time prior to establishment of the TE working group in 2010*]

12. The decision to create the [*TE*] was made in [REDACTED]. It was intended to replace [*networks*], which were responsible for the [*processing*] of data from what would today be described as [*a type of warranted data*].

13. Work to build the [*TE*] started in [REDACTED]. It was originally intended to service [*a number of*] technical users (with the capacity to service [*more*] clients or terminals), with [*a number of*] technical administrators. In common with its predecessors, it was built with shared network storage (this functionality was later referred to as 'fileshares'), [REDACTED]. Additional storage was to be added as required, for example to accommodate additional users. The [*TE*] was intended to [REDACTED] [*process warranted data*]. According to an early accreditation document ([*date*]), the [*TE*]'s principal functions were [*processing and managing*] on [*warranted data*] and [REDACTED][2].

14. [*An MI5 programme*] began considering how MI5 should approach compliance requirements as part of its work to improve MI5's ability to [*use a type of data*]. [*The programme*] paper dated [*2010*] identified [*an area*], enforcing data retention policies, the retrievability of data for disclosure requirements, and [*another area*] as early compliance priorities. The same paper also identified the need to 'proactively involve key stakeholders, namely [*the information management team*][3] and legal advisors in solution design and implementation'[4].

15. [REDACTED]

16. [*The TE working group*] was established in [*2010*] to focus on [*risks and controls*], although the terms of reference do not include legal compliance[5]. This group's composition reflected its key task; it was chaired by [*technical engineers*] and [*included others*].

---

[2] [REDACTED]
[3] [REDACTED]
[4] [REDACTED],
[5] [REDACTED]

17. [*In 2010*] [*a Deputy Director*][6] issued a paper to [*a Director*][7] entitled 'Recent Compliance Failures in [*a department*]'[8]. It focused on issues related to data collection and authorisation, rather than how data should be handled once obtained. However, it did raise a number of issues relevant to the handling of data including:

    i. Inconsistent staff perceptions of the importance of compliance;
    ii. Increasing levels of automation and removing the scope for human intervention;
    iii. Failure to consider the implications for compliance [*with new types of data*];
    iv. Imperfect processes to cope with systems that are still under development;
    v. A tendency to view compliance in the context of historic errors; and
    vi. An imperfect understanding of how systems work on the part of senior managers coupled with an imperfect understanding of compliance requirements and how to address them on the part of working-level staff.

18. The MI5 Management Board[9] meeting [*in 2010*] considered the organisation's corporate risk register. The register included a risk relating to "Information Management" that was rated AMBER. The paper highlighted the establishment of a programme to ensure information availability, and reduce the risks of "intelligence failure and compliance failure"[10].

19. The [*TE*] was granted an interim accreditation as a [*system that holds restricted information*] [*in 2010*][11]. The accreditation process identified a number of 'HIGH' rated risks. These included the lack of [REDACTED] and policies mandating how the [*TE*] was to be utilised, managed and supported. A plan to resolve these issues by [*a date*] was mentioned in the post accreditation [*register of residual risks*] [12].

---

[6] [REDACTED]
[7] [REDACTED]
[8] [REDACTED]
[9] [REDACTED]
[10] [REDACTED]
[11] [REDACTED]
[12] [REDACTED]

20. [*In 2010*] a [*digital*] programme discussion paper identified a number of controls required in respect of legal compliance obligations, including on the 'storing, securing, and destroying of data' and 'viewing of data'[13].

21. [*In*] 2010 [*a department's*] [*compliance group*] had its first meeting. The group considered a number of tasks to improve compliance with MI5's statutory obligations in respect of information management, including all systems being built [REDACTED] being checked for compliance by MI5 legal advisors, and an audit of existing systems[14].

2011

22. [REDACTED].

23. In [*2011*] [*a department's*] Compliance Group issued a report entitled 'Audits and Investigations into [*a team's*] Compliance incidents of summer 2010 and emerging conclusions and recommendations'[15]. It assessed [*a number of systems*] for the [*data usage*] against compliance requirements, including access control and data retention and deletion, assigning a RED-AMBER-GREEN (RAG) status in each case. This report made a number of recommendations, including:

    i. A compulsory job objective and mandatory compliance training for all [*team*] Staff;
    ii. Prioritisation of any software engineering work that addressed compliance issues; and
    iii. Implementation of retention policies on all systems that contained relevant data.

    Some of these recommendations, including drafting an appropriate job objective and arranging training for [*team*][16] staff, had been implemented by the time that the report was issued. However, assessment of the [*TE fileshares*]' (later known as the

[13] [REDACTED]
[14] [REDACTED]
[15] [REDACTED]
[16] [REDACTED]

'fileshares') appears to have been incomplete at the time of the final report; supporting documentation indicated its RAG status was still to be determined.

24. [REDACTED].

2012

25. Re-accreditation of the [*TE*] as a [*restricted*] system occurred throughout 2012. It was eventually granted in similar terms to the original 2010 accreditation, which noted 'HIGH' risks as a result of [REDACTED] as well as various other risks including [REDACTED][17].

26. In [*2012*] MI5 issued the first iteration of the [*team*] Data Retention Policy. The policy identified legal obligations with respect to the retention and deletion of different data obtained under:

- Regulation of Investigatory Powers Act 2000 (RIPA) interception warrants and [*warranted data*] authorisations; and
- Intelligence Services Act 1994 (ISA) [*warranted data*]

These obligations were expressed in general terms, rather than with reference to individual systems, and as such the policy applied to both data held within the [*TE*] and to data held elsewhere. The policy required [*regular users*] to 'conduct regular checks of any areas you are responsible for [REDACTED]'[18]. It is unclear how users were informed of this policy.

27. A security audit of the [*TE*] was commissioned in [*2012*] following the [REDACTED]. The review focused on [*a particular type of risks*], but also covered user security practices[19]. The Review was complete [*in 2012*]. It highlighted [*a number of*] key risks:

[REDACTED]

[17] [REDACTED]
[18] [REDACTED]
[19] [REDACTED]

[REDACTED]. It is unclear from available documents what steps were taken to implement these recommendations.

28. In [*2012*] the general [*team*] Data Retention Policy was superseded by a system-specific data retention policy[20]. The new policy outlined retention periods for data stored within specific systems on the [*TE*] and elsewhere, including systems for the [*processing of data*]. It also identified the '[*risk*]' arising from [*a type of data*] stored in [*areas*]. The new policy recommended that, as a mitigation, 'structures and processes must be put in place to ensure all this data is accounted for and can be routinely deleted in line with policy'. [REDACTED].

2013

29. [*In 2013*] the MI5 Management Board discussed, among other things, a paper entitled [REDACTED]. The paper focused on [*areas other than legal compliance*]. It identified the following root causes of MI5's information management risks:

i. Information management was not given a high enough priority by MI5;
ii. Information policy, guidance and standards were inadequate, absent or not followed;
iii. Information-related knowledge development activity was not sufficient;
iv. Ownership of the information environment (including systems) was fragmented and unclear;
v. Technologies were designed without taking information management requirements into account; and
vi. [*A particular capability*] was not sufficient.

The minutes of this meeting show that the Board agreed a strategic commitment to resolve the information challenges, and that work should proceed to scope and define the elements of the new [*information management programme*].

2014

[20] [REDACTED]

30. Throughout 2014 [REDACTED]. This was [*an important milestone*]. It was by now clear that, owing to the need to [*process data, MI5 required another TE*].

31. The [*TE*] was re-accredited as a [*restricted*] system for a second time in [*2014*]. [*A number of risks were noted*][21].

32. A new iteration of the [*team*] Data Retention Policy was issued [*in 2014*][22]. This version was the first since [*2012*] not to include language pertaining to [*a risk*] [REDACTED]. It is unclear why this text was not included.

33. [*An MI5 report*], prepared for MI5's Management Board, recorded two corporate risks relevant to MI5's compliance with its statutory obligations. [*Risk 1*] that '[REDACTED]', is rated [*AMBER*]. [*Risk 2*], '[REDACTED]' was a new risk that had not yet been fully assessed. A historic view of risks from 2014- present can be found at **Annex 3**.

34. [*The second MI5 report*] recorded that [*Risk 1*] remained AMBER, and that [*Risk 2*] remained a new risk yet to be rated.

35. The first major compliance issue with the [*TE*] [*had first been identified in 2014*]. [REDACTED]. Subsequent internal reviews identified three major causes:

    i. [*A failure to create a type of record on another TE*];
    ii. A failure to apply review, retention and disposal (RRD) policy to the repository of data on the [*TE*]; and
    iii. A failure to understand what data was held on the [*TE*].

    The reviews framed ii. and iii. as risks relating to [REDACTED], but not in terms of MI5's compliance with its statutory obligations.

2015

36. [*In 2015*] the MI5 Management Board met to discuss the [*third MI5 report*]. [*Risk 1*] remained [*AMBER*]. The commentary on this risk stated 'a major Service wide e-

[21] [REDACTED]
[22] [REDACTED]

learning package on information management has been launched with good uptake overall… there [was] a growing issue…[REDACTED]… The absence of formal, comprehensive and effective RRD policy at the relevant time [REDACTED] led to a failure to [REDACTED]. This [REDACTED] underlines the depth and complexity of the problems being addressed by [*the Information, Security, Compliance, and Strategic Policy department*]. Steps [were] being taken to address the immediate causes'[23]. [*Risk 2*] was rated for the first time; scored AMBER.

37. [*In 2015 a particular platform was deployed on the TE*].

38. [*A further MI5 report*] was issued [*in*] 2015[24] and discussed by MI5's Management Board [around the same time]. [*Risk 1*][25] was rated AMBER. [REDACTED]. [*Work*] to focus renewed effort on building a complete picture of MI5's information holdings in the [*information register*] initially focused on [*one of the department's TE*] where the risk was deemed to be most severe… The increasing scope of published RIPA handling arrangements and the consequent need to examine practice, report errors, etc. raises a risk that bad practice is uncovered of which we were previously unaware. Oversight bodies are pressing for broader and deeper insights into MI5's information processes, at a time of continuous change in [*work*]. Keeping pace with this is [*difficult for information specialist staff*] and negatively impacts on the risk trajectory.' [*Risk 2*][26] was also rated [*AMBER*].

39. At its meeting [*in 2015*] the MI5 Executive Board discussed, among other things, the issue of compliance. [*It was reported*] that 'the Board agreed that MI5 [was] at a compliance watershed and a structured approach would be needed to address this…ensuring statutory compliance was the priority together with Retention, Review and Disposal. External developments (especially the IPT[27]) were likely to mean… internal policies had to have greater force. Compliance was recognised as a subset of a wider 'professionalism' agenda but… the watershed required a sharper more focused response…[*the director general of strategy*] agreed to report

[23] [REDACTED]
[24] [REDACTED]
[25] [*Risk 1*]: [REDACTED]
[26] [*Risk 2*]: [REDACTED]
[27] The Investigatory Powers Tribunal

back to the [Executive Board] in the autumn with a plan on compliance initially focusing on statutory obligations. The Board agreed that this work should be resourced at a senior level'[28].

40. [*A further report produced in 2015*] was discussed by MI5's Management Board at [*a meeting*]. [*It was reported*] that the Board agreed to combine [*Risks 1 and 2*] into a new corporate risk ([*Risk 3*]) focusing on compliance; '[*There is a risk that [REDACTED] MI5 is held to be failing to comply with its statutory obligations attracting adverse criticism or rulings from the IPT and/or oversight bodies (current or future) leading to substantial legal and/or reputational damage*]'. [*The director general of strategy*] was assigned ownership of this new risk.

41. [*A platform was rolled out to TE users in 2015*].

42. [*In 2015*] the MI5 Management Board discussed the IP Bill and a review of legal risks, as well as a forward look, a sub-committees update, and [*reviews*]. [*It was reported*] that the 'DG concluded by summarising that the IP Bill was an opportunity to put [MI5's] powers on an updated, transparent and robust legal footing (although noting it was important that any new mechanisms still enabled [MI5] to carry out [its] operations at speed and scale)'[29].[REDACTED]

43. [REDACTED]. [*Information and technical specialist staff*] were commissioned to map the data held in the [*TE*] for inclusion in a new MI5 [*information register*].[30] [*Work started with the TE*]. Recommendations were made to put in place processes to ensure the [*risk*] from MI5's handling of new warranted material did not increase, but to accept the existing level of risk for material already on the [*TE*].

44. The MI5 Management Board met [*in*] 2015. Among other things it considered [*a performance report*] and compliance issues. The Report recorded that [*Risks 1 and 2*][3132] remain rated AMBER. [*Risk 3*] (MI5 is held to be failing to comply with its

[28] [REDACTED]
[29] [REDACTED]
[30] [REDACTED]
[31] [*Risk 2*]: [REDACTED]
[32] [REDACTED]

statutory obligations leading to substantial legal/reputational damage) is included on the register for the first time, but not scored.

45. At [a] meeting [in] 2015 the MI5 Executive Board had a further discussion of compliance issues. [It is reported] that [the director general of strategy] updated the board, noting that a compliance review had been commissioned to understand the scale of MI5's compliance task and to propose a plan. The Board was due to discuss the findings of the review at [a meeting in 2016][33].

2016

46. [In] 2016 [the legal department] issued a report[34] for MI5's Management Board on the legal compliance risks facing MI5[35]. [It highlighted:]

i. Continued RRD risks in relation to some [TE] systems;
ii. [The risk relating to data in the TE]
iii. New Investigatory Powers Commissioner oversight and the likelihood that 'scrutiny of MI5 [was] likely to concentrate on the handling of the product from warrants and authorisations.'

The report considered a range of policy, process and IT systems, [REDACTED]. It concluded that 'Post Bill [IPA], if MI5 is seen to be less than exacting in its approach to compliance… we will face calls for our powers to be curbed and oversight to be further increased.'

47. The MI5 Management Board considered the legal compliance report at its meeting [in] 2016, and responded by [MI5 created a compliance programme]. At the same [time] the board also considered [a further report]. [Risks 1 and 2][36,37] remained at

[33] [REDACTED]
[34] This report is legally privileged material and MI5 has waived privilege for the purposes of the Compliance Improvement Review only; the report or reference to its contents may not be disclosed further without MI5's prior agreement
[35] [REDACTED]
[36] [REDACTED]
[37] [REDACTED]

[REDACTED]. [*It was*] recorded that [REDACTED] [*Risk 3*] [would] be completed [*at a time*].

48. [*In 2016 the first elements of a platform were rolled out to the TE*].

49. The MI5 Management Board met [*in*] 2016 and considered, among other things, [*a performance report*][38]. [*Risks 1 and 2*] [39][40] continued to be rated AMBER. The new [*Risk 3*] [41] was rated for the first time, and scored at [*RED*]. Ownership of this risk was given to [*the director of the legal department*] whilst work to agree where MI5's refocused compliance effort would be located was completed.

50. [REDACTED]

51. [*A compliance programme*] meeting was held [*in*] 2016. It agreed two outcomes[42]:

i. By the implementation date [*sometime in 2017*] to have delivered the changes required for MI5 to operate compliantly and effectively under the Investigatory Powers Act, whilst maintaining the confidence of our oversight bodies; and

ii. To have implemented the [*compliance review*] recommendations agreed by MB [Management Board], and by [*a time in 2017/2018*] to have established MI5's new compliance function (to at least [*a %*] capacity), along with a [*longer-term plan*] to ensure MI5 is fully equipped to demonstrate legal compliance with the IP Act.

The [*programme*] also expressed its ambition to 'maintain focus on the legacy compliance risks, implementing at least those aspects of the [*compliance recommendations*] that could impact the IPC's willingness to approve warrants and authorisations'[43]. The programme itself was split into three [*areas*]:

[38] [REDACTED]
[39] See Footnote 32
[40] [REDACTED]
[41] [*Risk 3*]: [REDACTED]
[42] [REDACTED]
[43] ibid

i. IP Bill implementation – deliver changes required for MI5 to operate compliantly and effectively under the new Investigatory Powers Bill;

ii. [*Compliance plan*] – implementation of a range of measures to address recommendations made by the recent [*compliance review*] (cited in [*a recent compliance report*]); and

iii. [*Compliance in the future*] – the establishment of a new central legal compliance function to ensure we [MI5] understand and bear down on our core function national security compliance risks.

52. During this meeting the [*compliance programme*] Board also considered some of the specific challenges it faced. [*19% of the*] recommendations in the [*compliance review*] had already been delivered. Delivery of the remaining [*recommendations*] constituted the work plan for the [*compliance plan*] above. Points [*recorded*] included[44]:

i. It was noted that the amount of work and immovable deadline for implementation of the IP Bill might require moving at least some of the responsibility for delivering the [*compliance plan*] outside of the [*compliance programme*];

ii. In delivering the [*compliance plan*], priority was to be given to those recommendations most likely to affect the Judicial Commissioners' willingness to approve authorisations; and

iii. The recommendations were split into themes, including one theme of [REDACTED], which was rated a RED[45] risk and under which [*a number of*] recommendations sat, including for example some that related to [*a system on the platform*]. Each of these recommendations was considered an individual task. The only recommendation relating to the [*TE*] as a whole was to consider the viability of implementing a deletion function across it. This recommendation sat under the '[REDACTED] theme, which was rated as an AMBER risk, rather than under [REDACTED].

[44] [REDACTED]
[45] [REDACTED]

53. [*In 2016 another system went on to the TE*].

54. [REDACTED]

55. [REDACTED][46]

56. [REDACTED]

57. In [*2016*] [*an MI5 senior manager*] reviewed the key risks and issues relating to the [*TE*]. In [*2016*] this review reported three key findings[47]:

    i. [REDACTED]
    ii. There was a high likelihood of relevant material not being discovered, or being discovered when it should have been deleted, in a disclosure exercise; and
    iii. [REDACTED]

58. [*A report in*] 2016/17 recorded [*Risk 3*] [48] as [*a RED risk*] on MI5's corporate risk register[49].

59. [*In*] 2016 the [*Home Office*] summarised MI5's [*latest report*] in a submission to the Home Secretary. The submission did not mention the RED rated [*risk*] on MI5's compliance with its statutory obligations.

60. [*A further report*] was issued [*in*] 2016. The report stated that [*Risk 3*] [50] continued to be rated [*RED*]. [REDACTED]

---

[46] [REDACTED]
[47] [REDACTED]
[48] [*Risk 3*]: [REDACTED]
[49] [REDACTED]
[50] [*Risk 3*]: [REDACTED]

61. The Home Office-MI5 Quarterly Review meeting took place [*in*] 2016, chaired by the Home Office Director for National Security. The meeting was not recorded, which was normal practice [*at this time*].

62. [REDACTED].

63. [*In*] 2016 MI5's Executive Board discussed the progress of the [*compliance*] programme. [*It is recorded*] that [*a significant percentage*] of the recommendations of [*a 2016 compliance review*] had been delivered, albeit the 'easier' [*percentage*]. Work had begun to establish MI5's compliance function, and a small team was due to be in place by the end of the financial year. Full compliance with the IPA was noted as a priority. The Board also endorsed efforts under the [*compliance*] programme to support the new Investigatory Powers Commissioner with briefings about MI5 and how it operates, to provide essential context for the Commissioner in their new role[51].

64. [*In*] 2016 a submission from the [*Home Office*] to the Home Secretary reported that 'MI5's corporate risk register flags that MI5… [might not be] compliant with the relevant legislation with regards to information handling. MI5 [had] currently classified this as a [*RED risk*]. This is a [*risk*] for MI5 and in response it has created a new [*department*] ([*the Information, Security, Compliance, and Strategic Policy department*]) that will lead on a whole range of measures including staff training, file reviews, and new IT processes in order to improve legislative compliance'[52].

2017

65. The MI5 Management Board met [*in*] 2017. It discussed [*a review*]. The [*report*] stated that [*Risk 3*][53] remained [*RED*], and was predicted to do so for [*a period of time*]. [REDACTED].

66. [*On the same date*], the Management Board held an 'informal' discussion on compliance. [*It is recorded that the*] discussion focused on RRD policy and its

---

[51] -[REDACTED]
[52] [REDACTED]
[53] [*Risk 3*]: [REDACTED]

implications for compliance[54]. The Board concluded that MI5's approach to legal compliance ought to be aligned with the changes it made to its systems and processes to comply with the requirements of the forthcoming Investigatory Powers Bill. The Director General also asked [*the director general of strategy*] to review MI5's senior management structures to ensure that legal compliance risks were appropriately and adequately owned.

67. The MI5 Executive Board met [*again in 2017*], and also discussed [*a report*].

68. The Executive Board met again [*in*] 2017. It discussed, among other things, the [*compliance programme*]. [*It is recorded*] that [*a significant percentage*] of the recommendations of the [*compliance review*] had been implemented, but the remainder included [*challenges*]. The [*TE*] was one of [*the*] systems rated RED on compliance by the review. [REDACTED][55].

69. [REDACTED]

70. In parallel, the [*TE*] was again reaccredited [*as a restricted system*] in [*2017*][56]. Risks highlighted in granting this re-accreditation included:

    i. [REDACTED];
    ii. [REDACTED];
    iii. [REDACTED];
    iv. [REDACTED]; and
    v. [REDACTED]

71. Accreditation was granted on an interim basis for 12 months and on the condition that a programme of [*improvements*] be put in place. The paper recommending this decision to MI5's [*senior information risk owner, the director general of strategy*] stated that the 'significant risk around the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements... [an incomplete

[54] [REDACTED]
[55] [REDACTED]
[56] [REDACTED]

understanding of material held on the [*TE*]] prevents us from implementing an appropriate deletion policy including for categories of data where there are strict legal requirements such as [*warranted*] material… [concluding that] there is also a compliance risk in that MI5 would currently be unable to give sufficient assurance externally that we are handling information in accordance with current legislation'[57].

72. [REDACTED]

73. [*In*] 2017 [*the Home Office*] summarised [*a*] Home Office - MI5 Quarterly Performance Review [*from*] 2016/17 ([REDACTED]) in a submission to the Home Secretary. The submission recorded the [*risk*] reported in MI5's corporate risk register that MI5 may not be 'compliant with its statutory obligations'[58]. This submission additionally reports a conversation between [*the Home Office*] and [*MI5's Information, Security, Compliance and Strategic Policy department*] officials about MI5's approach to managing this risk; 'it seems clear MI5 takes this risk seriously and is seeking to address it comprehensively; it aims to reduce the risk to the next category (orange-high) by [*sometime in 2017/2018*]'[59].

74. [*In*] 2017 MI5 established the [*TE Programme*] to address a range of [*things*] in the [*TE*]. The Programme was overseen by the [*TE steering group*], chaired by [*a deputy director*] [60] and included representation from business users, technologists, and security assurance and compliance experts. The responsibilities of the steering group included:

    i. Being accountable for the [*TE*], with collective accountability for delivery of the [*TE Programme*];
    ii. Prioritisation and decision making in relation to the [*TE*], including resolution of resource conflicts between [*the TE Programme*] and other programmes; and
    iii. Ensuring appropriate stakeholder management.

[57] [REDACTED]
[58] [REDACTED]
[59] ibid
[60] [REDACTED]

75. [*In*] 2017 [REDACTED] early priorities for the [*TE Programme*] included:

    i. A clean up of inactive user accounts;
    ii. Further analysis of [*higher user*] access; and
    iii. [REDACTED]

76. [REDACTED]

77. [REDACTED]

78. The MI5 Executive Board met on [*in*] 2017. Discussion topics included [*a report*] and the [*compliance programme*]. [REDACTED]. [*A significant percentage*] of the recommendations of the [*2016 legal compliance report*] had been implemented, and RRD policy was highlighted [REDACTED][61].

79. [REDACTED]

80. [*A report*] was issued [*in*] 2017. It reported that [*Risk 3*] [62] remained [*RED*]. The report also forecasted that [*Risk 3*] would remain [*RED at the (then) current time*].

81. [*In*] 2017, [*a*] paper setting out guidance on legal compliance principles for the [*TE*] stated that the most significant legal compliance risks relating to the [*TE*] included:

    i. RRD policies, including consistency with policies in other systems outside the [*TE*] and the existence of a [REDACTED] capability to enforce the policies;
    ii. [REDACTED];
    iii. Application of the [*legal safeguards*]; and
    iv. Future risks arising from [*different types of data*].

    It recommended that these risks should be mitigated through:

[61] [REDACTED]
[62] [*Risk 3*: [REDACTED]

i. Confirmation that ownership of identification and mitigation of compliance risks sat with the [*TE Programme*], in consultation with [*the compliance team*] [63] and [*the legal department*];

ii. A series of workshops for the [*TE Programme*] to systematically identify and assess legal compliance risks, involving [*the compliance team*], [*the information team*], [*the legal department*] and users of the [*TE*];

iii. Prioritising [*TE*] risks alongside MI5's wider legal compliance risks; and

iv. The [*TE Programme*] agreeing (with [*the compliance team and legal department*]) and overseeing a programme of work to address these risks.

82. Two versions of this paper (para 81) exist. One version contains two additional paragraphs. These state that MI5 must comply with legal requirements on the acquisition, storage, examination and protection of material [REDACTED] throughout the lifecycle of that material, including through the application of RRD policies. Further, that 'technical systems and processes that manage material [REDACTED] [...] must enable users to comply with the law, and be able to demonstrate legal compliance'[64].

83. A [*document*] dated [*in*] 2017, considered possible work relating to the [*TE Programme*] information storage clean-up process[65]. It noted the [REDACTED] within the [*TE*]. [REDACTED] and a risk that "any audit of the [*TE*] by the Investigatory Powers Commissioner could lead to a negative impact on MI5's [*ability to operate*]." It recommended that responsibility for identifying relevant data repositories, and putting in place processes for decommissioning or ensuring they are appropriately managed, be given to team leaders in relevant business units. [REDACTED].

84. A paper [*in*] 2017 stated that the [*TE Programme*] had identified a number of further priorities, including[66]:

---

[63] MI5's new compliance function
[64] [REDACTED]
[65] [REDACTED]
[66] [REDACTED]

i. Cleaning up [*a number*] of [*data repositories*] in [*the TE*]', noting that this data was '[REDACTED]'; and

ii. [REDACTED]

85. The MI5 Executive Board discussed the Quarterly Review process at its meeting [*in*] 2017. The Board concluded that the process sighted Ministers on MI5's work and internal oversight[67].

86. [*In*] 2017, the [*compliance programme*] Board agreed to transfer to the [*TE steering group*] responsibility for the development of a tool (or tools) [*relating to deletion of material*]. There were two principal reasons for doing this. First, it established clearer accountability [REDACTED]. Second, specific [*department*] resources had already been allocated to managing the [*TE*]'s [REDACTED] and legal compliance challenges. [REDACTED].

87. [*In*] 2017 the MI5 Management Board reviewed [*a report*]. It recorded that [*Risk 3*][68] remained RED. [REDACTED].[69]

88. [REDACTED]

89. The OSCT-MI5 Quarterly Review meeting held [*in*] 2017 considered [*one of MI5's performance reports*]. [*It*] was reported by MI5 that its Board had recently concluded that the ambition to [*reduce the risk by a time*] had been too optimistic[70]. [REDACTED].

90. [*In*] 2017, in a submission to the Home Secretary, [*the Home Office*] summarised the MI5 Quarterly Performance Review for [*a quarter*]. The submission noted that [REDACTED]. The submission additionally noted that 'There are [*2 very high risks*] [on MI5's corporate risk register]. [*It included*] compliance with statutory obligations. This [was] a longstanding risk that MI5 [was] placing significant effort into

[67] [REDACTED]
[68] [*Risk 3*]: [REDACTED]
[69] [REDACTED]
[70] [REDACTED]

managing. [*The timeframe by which MI5 believes it will be able to reduce this particular risk had slipped. Another risk had now turned RED*].[71].

91. On 27 October 2017 [*the senior manager*] of the [*TE Programme*], issued an internal note to [*directors*] that identified a number of compliance risks[72]. These included [REDACTED], inconsistent and incomplete RRD policies, [REDACTED] this paper made the following recommendations:

    i. That MI5 make a decision about where ownership of compliance in the [*TE*] should sit [REDACTED];
    ii. That MI5 develop 'a new plan that prioritises hard on the top compliance risks and sets out a realistic target state' [REDACTED];
    iii. [REDACTED]; and
    iv. That MI5 consider how to balance investment [*between compliance/capability*].

92. The MI5 Executive Board met [*in*] 2017. It discussed the [*compliance programme*]. [*The*] discussion focused on the IPA commencement process and MI5 readiness, including a programme of [*mandatory legalities overview training*] for staff that was due to commence in [*2018*][73].

93. At its meeting [*in*] 2017 the MI5 Management Board discussed [*a review*]. [*A report*] recorded that [*Risk 3*][74] remains RED [REDACTED]. Of the [*risks*] on the register, [*Risk 3*] was [REDACTED].

94. The next Home Office-MI5 Quarterly Review meeting took place [*in*] 2017, and considered [*a quarter*]. The compliance risk was discussed further. [*It was reported*] that MI5 reported that [*the RED rating*] reflected the [*challenge*] of how to ensure current systems are in a compliant state, and ensuring that where systems are not compliant, there is resource to acquire new systems which are'. [*It was also recorded that*] 'MI5 were also aware of the step up in oversight that will be coming

---

[71] [REDACTED]
[72] [REDACTED]
[73] [REDACTED]
[74] [*Risk 3*]: [REDACTED]

in with the new Investigatory Powers Commissioner' and that 'On the [*compliance*] programme, MI5 explained that [REDACTED]. The long-term risks are essentially around legacy systems… MI5 hoped to get [*a better rating*] on compliance by [*next year*]'. The meeting was chaired by the Director General OSCT. Senior attendance from MI5 included [*the director general of strategy*].

95. [*In*] 2017 the [*TE Programme*] provided an update on its work to MI5's [*security and information committee*], chaired by [*the director general of strategy*]. It stated that progress had been made on work relating to account management [REDACTED]. Finally, the paper noted the 'significant information and legal compliance risks' on the [*TE*], and that [*the information management team*] would now coordinate work on [*TE*] compliance.

2018

96. [*In*] 2018 the MI5 Management Board discussed compliance risk. Incomplete and inconsistent RRD policies and [REDACTED] were identified as key issues.

97. The MI5 Executive Board met [*in*] 2018 and discussed the [*compliance programme*]. The minutes show discussion focused on the [*mandatory legal overview*] training programme [REDACTED].

98. The MI5 Management Board met [*in*] 2018. It discussed [*a review*]. [*A report*] recorded that [*Risk 3*][75] remained RED [REDACTED].

99. [REDACTED].

100. [REDACTED].

101. The Home Office – MI5 Quarterly Review meeting occurred [*in*] 2018. It considered MI5 performance during [*a quarter*]. No discussion of compliance issues was [*recorded*].

[75] [*Risk 3*]: [REDACTED]

102. [*In*] 2018 the [*TE Programme*] had established a programme consisting of work to [REDACTED] compliance and culture in relation to the [*TE*]. [REDACTED].[76]

103. The interim accreditation of the [*TE*] was extended for a further 12 months in [*2018*]. The paper that recommended this decision set out progress made against the [REDACTED] under the [*TE Programme*], and restated the legal compliance risks in similar terms to the previous year (para 69). The paper also highlighted a specific strand of work to address the compliance risks being implemented under the auspices of the [*TE steering group*]. This included a commitment to 'create a single view of prioritised compliance risks in [*TE*]' in FY 2018/19[77].

104. Also in [*2018*], MI5 established the [*TE improvement programme*]. It was intended to address a range of [REDACTED] and compliance related issues. The latter included developing an understanding of the data and information holdings on the [*TE*] and implementing the necessary steps to remove or reduce duplication, [REDACTED], and ensure that MI5 can demonstrate broader compliance (such as RRD and deletion policies).

105. [REDACTED].

106. [*In*] 2018 [*the director of the information, security, compliance, and strategic policy department*] wrote to the Home Office Director for National Security confirming that MI5 would be ready on [*a date in*] 2018 to commence relevant [*provisions of the IPA*]. A series of caveats are listed, relating in part to the readiness of the Investigatory Powers Commissioner's Office to assume its functions. Whilst noting that MI5's declaration of readiness did not mean the commencement would be risk free, the letter does not mention the 'RED' rated legal compliance risk on MI5's corporate risk register, or more specific compliance challenges associated with the [*TE*].

107. [REDACTED]

---

[76] [REDACTED]
[77] [REDACTED]

108. At its meeting [*in*] 2018 the cross Whitehall IPA implementation Board, chaired by [*a member of the H.O.*], decided to proceed with commencement of the Act[78]. The minutes do not record discussion of the risk that MI5 may not be compliant with its statutory obligations. The minutes record MI5 representation at the meeting, but that [*the information policy deputy director/director of the information, security, compliance, and strategic policy department*] was not present.

109. The MI5 Management Board discussed [*a report*] and its meeting [*in*] 2018. The report stated that the compliance risk, [*Risk 3*]79, remained [*RED and was forecast to remain so into 2018/2019*].

110. [*In*] 2018 [*the Home Office*] summarised MI5 governance, budget and oversight issues in a submission to [*the*] Home Secretary. This submission was intended as a general overview. It highlighted the Home Secretary's accountability to Parliament for MI5's activities and set out how oversight has worked in practice. [REDACTED]. Finally, this submission also sets out the new arrangements governing the Investigatory Powers Commissioner's role in MI5 oversight and warrantry approvals, expected to come into force on 27 June 2018. The submission does not refer to ongoing MI5 business, risk registers or governance and does not mention concerns about MI5's compliance with its statutory obligations in general, or specific risks associated with the [*TE*].

111. An OSCT-MI5 Quarterly Review meeting took place [*in*] 2018, and considered MI5 performance during [*a quarter*]. [*It is recorded that there was*] a discussion of the compliance risk during which 'MI5 stated that it… was still on track to be rated at AMBER. A pathway to get to yellow was also in development, which would probably involve [*an uplift*]. More broadly, MI5 felt that it would be useful to brief the Investigatory Powers Commissioner about this work on this [*specific*] risk to ensure he is up to date with progress'[80]. The meeting was chaired by the Director General, OSCT. Senior MI5 representation included [*the director general of strategy and the deputy director general*].

---

[78] [REDACTED]
[79] [*Risk 3*]: [REDACTED]
[80] [REDACTED]

112. [*In*] 2018 [*the Home Office*] recommended to the Home Secretary that he agree MI5's high level standard handling arrangements for material gathered through [REDACTED][81]. The submission stated that '[REDACTED]'[82]. It concludes 'we [*the Home Office*] are satisfied that the proposed new arrangements are satisfactory. They are comparable with existing arrangements under RIPA which you have approved previously. Over the coming months in discussion with MI5 we will look to expand and strengthen these.' The submission did not mention RED legal compliance risk on MI5's corporate risk register, or any specific compliance concerns related to the [*TE*].

113. [REDACTED].

114. [*In*] 2018 [*the deputy director of the information, security, compliance and strategic policy department*] wrote to the Home Office Director for National Security to confirm MI5's readiness [REDACTED]. Whilst noting that its declaration of readiness did not mean [*it*] would be risk free, the letter did not mention the RED rated legal compliance risk on MI5's corporate risk register, or more specific compliance challenges associated with the [*TE*].

115. [*In*] 2018 the Home Office Director for National Security recommended that the Security Minister and the Home Secretary agree [REDACTED][83]. The submission did not mention the RED rated legal compliance risk on MI5's corporate risk register, or specific concerns related to compliance of the [*TE*].

116. [*In*] 2018 [*the Home Office*] submitted to the Home Secretary on the highlights from [*a*] meeting (para 110)[84]. The submission stated that there was 'one [*corporate risk rated higher than others*] for MI5 [*at this time*]. This relates to compliance with statutory obligations. The RED rating reflects the [*challenge*] of how to ensure that

[81] [REDACTED]
[82] [REDACTED]
[83] [REDACTED]
[84] [REDACTED]

MI5 systems facilitate the organisation's compliance with its legal and other obligations. This was RED earlier and is a [*risk*] that MI5 is placing [*effort*] into managing. In [*a*] meeting, MI5 stated that it was implementing the recommendations from the Compliance Board and was on track for this risk to reach AMBER. OSCT will continue to monitor MI5's progress on compliance.'

117. The MI5 Management Board discussed [*a report*] at [*a*] meeting [*in*] 2018. In this report [*Risk 3*] was rated at AMBER. The register contained [*one risk rated RED (from AMBER previously)*][85].

118. [*Paragraph about risks identified*][8687]

i. [REDACTED]
ii. [REDACTED]

[*The register*] identified legal and information risks arising from:

i. Lack of corporate knowledge about what data was held in the [*TE*];
ii. Systems not handling data in accordance with legal obligations;
iii. [REDACTED]; and
iv. [REDACTED].

The presentation also highlighted the [*pool of risk*]' that arose from [REDACTED]'. Contributory factors included [REDACTED], RRD and [REDACTED]. The paper stated that the information policy team ([REDACTED]) assess that 'the legal compliance risks concerning the application of appropriate RRD [REDACTED] of [*a type of*] material are RED which could lead to successful [Investigatory Powers Tribunal] challenges, loss of confidence of Ministers [Judicial Commissioners] and consequently restrictions in warrants or reputational damage'.

119. A range of mitigations were proposed. These included the [REDACTED], and a two-strand approach to addressing [REDACTED] compliance risks associated with the [*TE*]. First, continuing to deliver tactical mitigations to these risks through the

[85] [REDACTED]
[86] [REDACTED]
[87] [REDACTED]

[*TE Programme*]. Second, delivering longer-term, sustained change though the [*Improvement*] programme. Prioritisation of the former was delegated to the [*security and information deputy directors' group*], chaired by [*the director of the information, security, compliance, and strategic policy department*].

120. [*In*] 2018 the MI5 Executive Board had a '*teach-in*' on the [*TE*] and the various [REDACTED] compliance challenges it presented. The [*presentation*] used at this session stated that 'systems [were] not handling data in accordance with [MI5's] legal obligations… [REDACTED], either through a lack awareness of what their obligations are, or [REDACTED]… [and] data continues to be held for longer than is necessary and proportionate and in places it cannot be accounted for'[88]. Key [*TE*] challenges included:

    i. [REDACTED];
    ii. That the [*TE*] did not have an owner or a strategy to guide decision making;
    iii. [REDACTED];
    iv. [REDACTED];
    v. [REDACTED]; and
    vi. That there was a lack of automated RRD processes.

121. The OSCT-MI5 Quarterly Review meeting to consider MI5 performance [REDACTED] took place [*in*] 2018. The minutes record that 'MI5 had not briefed the Investigatory Powers Commissioner about [*a RED risk*] on compliance in its corporate risk register. However, this risk had moved to [*AMBER earlier than expected*] and MI5 assessed that it was no longer necessary to brief the Investigatory Powers Commission on this risk. [*MI5 would need to think about whether to brief the IPC on the new RED risk*][89]. The minutes record no further detail. The meeting was chaired by the Director General OSCT. Senior MI5 representation included [*the director general of strategy*].

122. [*In autumn*] 2018 [*the director of the information, security, compliance, and strategic policy department*] orally briefed the Home Office Director for National

[88] [REDACTED]
[89] [REDACTED]

Security on the [*TE*] compliance and other challenges, and agreed to brief the relevant Home Office Deputy Director in detail.

123. [*In*] 2018 the MI5 Executive Board discussed a paper setting out the challenges associated with the [*TE*], focusing on the [*Improvement*] programme [REDACTED]. [*It was reported*] that[90]:

i. '[REDACTED] that MI5 is unable to provide robust assurances to its oversight bodies that data held in the [*TE*] cannot be accessed unlawfully. The risk is that the Investigatory Powers Commissioner may be unwilling to authorise further warrants until this is rectified [REDACTED]';

ii. 'Effective review, retention and deletion (RRD) has not been implemented across all data stores in the [*TE*], potentially including warranted material, and therefore there [was] a risk that elements of it [were] non-compliant. There [was] a risk that lack of effective RRD policy could lead to successful [Investigatory Powers Tribunal] challenges, loss of confidence of Ministers/Judicial Commissioners and consequently restrictions in warrants or reputational damage. In order to mitigate these risks, we anticipate that MI5 will want to pre-emptively brief oversight bodies on these [[*TE*] issues] challenges and our plans to address them'

At this meeting, the Board agreed the expansion and continued funding of the [*Improvement*] programme, which had estimated costs of [REDACTED]. More precise funding and timelines were to be agreed through MI5's wider portfolio build process.

124. The MI5 Management Board met [*in*] 2018. It discussed the performance report for [*a quarter*]. The Corporate Risk Register recorded that [*Risk 3*][91] remained [*AMBER. Another risk remained RED*].

[90] [REDACTED]
[91] [*Risk 3*]: [REDACTED]

125. The OSCT-MI5 Quarterly Review meeting to consider MI5 performance for the second quarter of 2018/19 took place [*in*] 2018[92]. No discussion of legal compliance issues is recorded. [*It is recorded that the question of whether to brief the IPC on the RED risk was still under discussion, MI5 were confident there was no need to brief the Home Secretary about risks at this stage*][93]. In addition [*it is recorded that there was a discussion*] about [REDACTED] The board [was] still looking for [*funding for*] [REDACTED] [*TE*] remediation work [REDACTED]]'[94].

126. [*In*] 2018 [*the information policy deputy director*] issued a [*document*] for [*the director of the information, security, compliance and strategic policy department, and the technology and innovation department*] that recommended briefing the Home Office and the Investigatory Powers Commissioner on the range of issues MI5 faced in relation to the [*TE*] as soon as possible, despite the fact that MI5's knowledge of the compliance issue was not yet complete.

127. [*In*] 2018 the Director General MI5 wrote to the Home Secretary following the cancellation of their meeting to discuss key developments over the previous quarter and MI5 performance. The letter suggested [*topics*] to discuss once the meeting could be rearranged including [*topics*], but not MI5's ongoing concerns about legal compliance and specific issues related to the [*TE*].

128. [*In*] 2018 the [*security and information deputy directors*] group met to discuss progress with [*TE*] remediation work. Although a range of activities had been completed [REDACTED][95].

129. At the same meeting (para 127), the [*security and information deputy directors*] group also considered a proposal on [*further remediation work*][96]. The group agreed to establish [*a governance group*] to oversee [*a*] process [*of review*] [REDACTED].

---

[92] [REDACTED]
[93] [REDACTED]
[94] ibid
[95] [REDACTED]
[96] [REDACTED]

2019

130. The MI5 [*security and information committee*] met [*in*] 2019. It noted that a formal decision would soon be required on [*a risk*]. This decision would 'enable communications with the Investigatory Powers Commissioner (IPC) on how this issue will be handled against legal obligations', and 'options will be mature enough for decision in [*a number of weeks*], with IPC notification soon after'. It was decided to return to this topic at an extraordinary [*security and information committee*] meeting to be held [*shortly after*].

131. The MI5 Executive Board met [*in*] 2019. It discussed progress on implementing the [*Improvement*] programme, including on improvement of the [REDACTED] compliance profile of the [*TE*][97].

132. [*In*] 2019, during a regular catch up with the Chief Executive of the IPCO, [*director and deputy director of legal compliance*] said that MI5 would most likely need to brief the Investigatory Powers Commissioner on a 'legacy IT issue' in the near future.

133. [*In*] 2019 the [*security and information committee*] agreed that [REDACTED] and that immediate action was required to improve compliance where possible. The papers that supported this meeting noted that MI5 'intended to brief the [Investigatory Powers Commissioner]... as soon as possible as [MI5] was likely to be criticised for the delay in informing him'[98].

134. [*In*] January the Director General MI5 authorised the briefing of the Investigatory Powers Commissioner on issues relating to the [*TE*]. The meeting was arranged for [*shortly after*].

135. In parallel, MI5 was considering internally whether there were implications for warrantry applications of the planned briefing on the [*TE*] for the Investigatory Powers Commissioner.

---

[97] '[REDACTED]

[98] [REDACTED]

136. At its meeting [*in*] 2019 the MI5 Management Board discussed Strategic Risk. [*It is recorded*] that the Board accepted a proposal to replace its [*corporate risk register*] with a [*different, new risk register*], to be used for the first time in [*a report*]. The Board agreed the Directors General should become the primary owners of [*the*] risks, with Directors leadings on specific sub-risks[99].

137. [*In*] 2019 [*the deputy director general*] MI5 wrote to the Investigatory Powers Commissioner and the Director General OSCT summarising a recent MI5 review of the impact on MI5's work of the transition of warrantry arrangements to the IPA[100]. It reports benefits to MI5 including an improved ability to robustly defend its actions in court and a strengthened compliance culture owing to the [*compliance programme*]. The letter did not refer to the ongoing compliance risk or specific compliance concerns related to the [*TE*].

138. [*In*] 2019 the Deputy Director then covering the Home Office's National Security Unit was given an oral outline brief of the issues MI5 faced in relation to the [*TE*].

139. [*In 2019*], during a regular monthly meeting, the Chief Executive of the IPCO was given a fuller oral briefing of the compliance and other issues MI5 faced with the [*TE*]. The Deputy Director then covering the Home Office National Security Unit was briefed in similar terms later the same day.

140. [*In*] 2019 [*the director of information, security, compliance, and strategic policy*] wrote to the Home Office Director for National Security[101]. The letter informed the Director for National Security that MI5 intended to brief the Investigatory Powers Commissioner on challenges in maintaining assurance in terms of legal compliance [REDACTED] in regard to the [*TE*]. It listed four specific concerns:

i. [*relating to data within the TE*];
ii. [REDACTED];
iii. [REDACTED]; and
iv. Inconsistent application of Review, Retention and Disposal (RRD) policies.

---

[99] [REDACTED]
[100] [REDACTED]
[101] [REDACTED]

141. [*In 2019, the Home Office*] informed the Home Secretary of MI5's intention to brief the Investigatory Powers Commissioner on issues related to the [*TE*][102]. The submission summarised the four issues highlighted above (para 139) and recommended supporting the briefing.

142. On 27 February 2019, MI5 briefed the Investigatory Powers Commissioner on compliance and other challenges pertaining to the [*TE*]. At the Investigatory Powers Commissioner's request, the content of this briefing is set out in writing in a letter from [*the director of information, security, compliance, and strategic policy*] to the Investigatory Powers Commissioner on 11 March 2019.

143. [*In*] 2019 the MI5 Management Board discussed [*a report*]. This was the first [*report*] to use the [*new risk register*]. The compliance risks are recorded under [*Risk 4*][103] and [*Risk 5*][104]. Both were rated [*AMBER*].

144. Between 18 and 22 March 2019 Inspectors from the Investigatory Powers Commissioner's Office conducted an inspection of the [*TE*].

145. [*Later in March*] 2019 the Director General OSCT wrote to the Home Secretary ahead of the latter's forthcoming meeting with the Director General MI5. The letter suggested that the meeting could cover [*a number of*] issues, one of which being the [*TE*]. It explained the [*TE*] 'poses difficult questions around MI5's compliance with the Investigatory Powers Act'[105].

146. [*In*] 2019 the Home Secretary was updated on the [*TE*] problems by [*the Home Office*][106]. The submission recommended that the Home Secretary agree to continue considering MI5 warrant applications.

147. On [*29 March (referred to in the report as 27 March due to a presumed typographical error)*] 2019 the Investigatory Powers Commissioner's Office (IPCO)

---

[102] [REDACTED]
[103] [*Risk 4*]: [REDACTED]
[104] [*Risk 5*]: [REDACTED]
[105] [REDACTED]
[106] [REDACTED]

issued version 2 (of 2) of the report of its inspection of the systems and processes within the [*TE*], conducted [*in*] 2019. Six key findings were reported:

i. [REDACTED];
ii. [REDACTED];
iii. [REDACTED];
iv. MI5 had a manual process in place for deleting material subject to legal professional privilege (LPP material) from its systems, but was [REDACTED];
v. [REDACTED]; and
vi. That by [*January 2018*] if not earlier, MI5 had a clear view of some of the compliance risks around the [*TE*], to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in the [*TE*]. The risks were also sufficiently clear that they should have been communicated to the Investigatory Powers Commissioner.

148. [*In the first quarter of*] 2019 MI5 responded to a series of technical questions raised by IPCO in respect of MI5's proposed mitigations (set out in a new Annex H to MI5's standard Handling Arrangements) earlier that day and following its 18-22 March inspection.

149. Also [*in the first quarter of*] 2019 [*the Home Office*] recommended that the Home Secretary continue to consider and, as appropriate, approve MI5 warrant applications, noting also the risk that the applications could be refused by IPCO.

150. [*In the first quarter of*] 2019 the Director General MI5 wrote to the Home Secretary to provide an update on [REDACTED] compliance [REDACTED] challenges relating to the [*TE*][107]. The letter states that the 'compliance risks identified are largely associated with our [MI5's] ability to [REDACTED] warranted data.' The letter also describes [REDACTED] and key mitigations, including the [*Improvement*] programme. The letter also states that 'MI5 has been aware of [*risks*] relating to the [*TE*] for a number of years… and MI5 has a deep commitment

[107] Letter from the Director General MI5 to the Home Secretary

to meeting our compliance obligations… there should be no sense that we treat compliance with anything less than the greatest priority and it is a matter of profound regret that these issues were not identified and fully addressed sooner.'

151. On 5 April 2019 the Investigatory Powers Commissioner issued his first decision on the [*TE*] issue and compliance with the IPA[108]. The decision states 'MI5's retention of warranted material in [*TE*] cannot be shown to have been held lawfully and the failure to report these matters timeously to IPCO is a matter of grave concern which I will be addressing separately. The critical question, however, on this application is whether the data to be covered… will be appropriately safeguarded. On the basis of the mitigations set out… combined with the answers to the questions I have received, subject to certain critical caveats, I am satisfied that MI5 have the capability henceforth to handle warranted data in a way which is compliant with the IPA'.

[108] [REDACTED]

ANNEX 1: Relevant provisions in legislation which govern compliance for warranted data

Upon the commencement of the relevant warrant provisions of the Investigatory Powers Act on 31 May 2018, the Secretary of State must consider, before issuing a warrant, that satisfactory arrangements are in force in relation to the warrant, setting out safeguards for the retention and disclosure of material obtained under the warrant. Those arrangements are set out in the Act, and include aspects such as:

- Limiting the number of persons who can access warranted material
- The extent to which any of the material is disclosed or made available
- The extent to which any of the material is copied and number of copies made/ held
- The period of retention based on necessity (in support of the grounds set out in the warrant) and in support of the requesting agency performing its statutory function
- Material being stored in a secure manner

The Act however is quiet on how these constraints should be met. Further guidance on dissemination, storage, copying and destruction of [*warranted material*] is contained in the [*relevant IPA code of practice*], but again the precise details of how those requirements are met is left to the particular warrant requesting agency's internal arrangements, to be approved by the relevant Secretary of State.

- MI5 submitted these handling arrangements to the Home Secretary for approval for each type of warranted product under the Investigatory Powers Act[109]
- Combined Targeted Interception and Equipment Interference Handling Arrangements[110]

[109] [REDACTED]

[110] MI5 handling Arrangements for material obtained under interception warrants and equipment inference warrants under sections 19, 21, 102, 103, 138 and 178 of the IPA, dated July 2018, submitted to Home Secretary for approval on 13-June-2018

- Bulk Personal Data Handling Arrangements[111]
- Bulk Communications Data Handling Arrangements[112]

[REDACTED]

Where a public authority has internal arrangements and policies in place, general public law principles require it to comply with those policies. [REDACTED]

[111] MI5 Handling Arrangements for material retained under bulk personal dataset warrants issued under sections 204 and 205 of IPA dated July 2018, submitted to Home Secretary for approval

[112] MI5 Handling Arrangements for CD acquired under bulk acquisition warrants issued under S158 of IPA dated July 2018, submitted to Home Secretary for approval

Annex 2: Terms of Reference for the Compliance Improvement Review of MI5

Review into the circumstances surrounding the compliance risk management and reporting of the MI5 '[TE]' issue and the potential need for remedies to address any identified governance weaknesses, including implications for the management of non-operational risk and compliance

Aim

1. To provide an independent assessment of how the compliance issue linked to the '[TE]' IT environment arose; assess how MI5 identified and responded to the issue, including disclosure to the Home Secretary and Investigatory Powers Commissioner (IPC); provide assurance that, in light of this episode, MI5 have in place appropriate governance and non-operational risk management procedures; to surface any lessons; and to make recommendations for the future.

Objectives

2. The review should address the following objectives:

Objective 1: To identify when and how the [TE] compliance issue arose, and what the root causes of it were, how MI5 identified, handled and reported their compliance concerns, what factors led to the timeline for notifying the Home Secretary and the IPC, and whether notification was done as quickly as it should have been.

Specific questions to answer should include:

i. What were the root causes of the issues with the [TE] which led to the risk of non-compliance?
ii. How and why did this happen?
iii. When was it recognised that there might be a potential risk to MI5's compliance with the IP Act? What were the layers of accountability and responsibility for compliance and informing the IPC?
iv. What was MI5's response to the problems once identified from initial identification of a potential issue through to reporting to the Home Secretary and the IPC? Were the Home Secretary and the IPC notified as quickly as they should have been, and, if not, what caused this?

Objective 2: In light of the [TE] compliance issue, to identify whether MI5's governance, compliance arrangements and broader approach to non-operational risk management are sufficient.

Specific questions to answer should include:

i. In light of the [TE] compliance issue, what, if any, changes are required to MI5's compliance arrangements?
ii. How are major non-operational risks spotted and flagged within MI5?
    - Where does accountability sit at each level within the organisation?
    - How are risks and mitigations decided upon and reviewed in their implementation and effect?
iii. What role does organisational culture play?

iv. How does MI5 balance its management of operational risks against its management of major non-operational risks, including compliance?

Objective 3: To identify lessons to be learned for the future and provide recommendations for the future on governance, compliance arrangements and approach to non-operational risk management.

Timing

3. The review and reports should be completed by the end of July 2019.

Outputs

4. The Independent Reviewer will provide a full analysis of the issues and a final report that addresses the objectives at paragraph 2 to the Home Secretary. This will be copied to [REDACTED]

5. The Independent Reviewer should be mindful that there may be a requirement to produce an unclassified summary of their final report for publication, should the Home Secretary decide that is appropriate.

Approach and conduct of the review

6. This report is not seeking to attribute individual blame but to identify remedies for any systemic problems with non-operational risk management and compliance.

7. The independent reviewer will lead the review supported by appropriate staff from the Home Office, MI5, other agencies and the National Security Secretariat.

8. The independent reviewer will chair a steering board that will meet [*regularly*] during the review period. The composition of this board will include [REDACTED].

9. The independent reviewer will be given full access to all relevant documents [REDACTED], and will be able to engage as they see necessary with relevant officials in MI5 and Whitehall Departments as well as IPCO.

10. The review will, of course, take account of the existing statutory framework that governs MI5, including their responsibility for implementing any recommendations arising.

[REDACTED]

Glossary

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
EB	Executive Board
[REDACTED]	[REDACTED]
Fileshare	Functionality on [*TE*]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
ICT	International Counter Terrorism
[REDACTED]	[REDACTED]
IPA or IP Act	Investigatory Powers Act 2016. This provides MI5 with the powers, upon approval of a warrant approved by the Secretary of State and IPCO, to undertake interception, equipment interference, acquire bulk communications data and bulk personal datasets. It also provides for the new oversight regime of the IPC, new safeguards for warranted data and the new "double lock"/ independent approval under IPCO and OCDA (for non- warranted CD)
IPC/ IPCO	Investigatory Powers Commissioner/ Investigatory Powers Commissioner's Office. This replaced 3 RIPA commissioners in September 2017 under the IP Act for the oversight and compliance of that same Act. In May 2017 onwards, IPA warrantry was considered by the Commissioner and his Judicial Commissioners by virtue of a Judicial Review of the decision made by the Secretary of State to approve that warrant. This is known as the Double-Lock
IPT	Investigatory Powers Tribunal. This independent Judicial panel investigates complaints made in regard to the use of powers under RIPA and any conduct undertaken by the three security and intelligence agencies
[REDACTED]	[REDACTED]
ISA	Intelligence Services Act 1994. This Act provides MI5 with the powers, upon approval of a warrant approved by the Secretary of State, to interfere with property
[REDACTED]	[REDACTED]
Judicial Commissioners	Senior independent Judges who work to the IPC to "double-lock" the UK's warrantry under the IP Act

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
MB	MI5's Management Board
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
OSCT	Home Office, Office for Security and Counter Terrorism
[REDACTED]	[REDACTED]
RIPA	Regulation of Investigatory Powers Act 2000. Act which provides MI5 the powers, upon approval of a warrant by the Secretary of State, to intercept communications and undertake intrusive surveillance. It also provides the powers to acquire communications data, undertake directed surveillance and make use of covert human intelligence sources through an Authority. RIPA, for interception warrantry and communications data acquisition was repealed and replaced by the IPA. It also provides for the RIPA oversight Commissioners and handling arrangements for warranted data
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
RRD	Review, Retention and Disposal (Deletion in some contexts)
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]