Assurance

Assessment Notice Audit Process Manual

Document name/title	Assessment Notice Audit Process Manual
Version number	1.2
Status (draft, published or superseded)	Published
Department/Team	Assurance
Relevant or related policies	
Distribution (internal or external)	Internal
Author/Owner (if different name both)	[redacted] (Author) Assurance (Owner)
Approved by	[redacted]
Date of sign off	15/09/2021
Review by	15/09/2022
Security classification	Official

Contents

1.0 Foreword

The implementation of the Data Protection Act 2018 (DPA18) provided the Information Commissioner with the power to conduct compulsory assessments of organisations through the issuing of an Assessment Notice (AN). This process document looks to support the completion of an Assessment Notice audit from referral to end.

Assessment Notices can be issued to organisations where a high risks have been identified with their processing activities or continual non conformance is demonstrated. As a result AN audits are usually referred to Assurance from other areas of the ICO such as complaints or investigations teams.

This process looks at the means by which an AN is referred to Assurance, and the decision making prior to the commencement of an AN. The process for staff referring an investigation to Assurance is documented in the Investigation Manual and should be reviewed in line with this process. Additionally, the conclusions of the AN audit may require enforcement action and therefore will also interact with the Investigation Manual. The Investigation Manual details the ICO's investigative powers and as such sets out high-level information in respect of ANs.

AN audits will have their own requirements based on the information and intelligence gathered prior to a referral and can vary in many aspects including the size and sector of the organisation, the processing activities undertaken and the areas of risk or concern. As a result each AN audit will adopt its own approach to the preparation, resources assigned, reporting, follow-up and output to meet these specific requirements. The process listed does not define a standard approach for all AN audits but highlights the key requirements end to end and aligns with the principles as laid out in the Regulatory Action Policy (RAP), Statutory Guidance (draft) and universal principles of audit. Its purpose is to provide guidance for the decision making that takes place during each engagement and the variable approach. The RAP, Statutory Guidance and Investigations Manual are essential reading for those managing and making decisions as part of the AN audit process. To support this, links to previous examples of audit output have been included as supporting case studies to show variances and examples of previous decision on different approaches used.

Where appropriate the commonality and differences between this audit process and the consensual engagement as well as their implications have been highlighted.

The main audience for this process is Assurance Senior Auditors (SA), Group Managers (GM) and the allocated audit team. However instructions and helpful information has been added for those in the entire resource pool, including internal interested stakeholders, key or senior decision makers and Assurance Team Managers (TM) who will require a degree of detail to support the audit and their people.

This document will be subject to continual review and updates and will be amended accordingly. This will include updates to incorporate future changes to the RAP and as more AN audits are completed which identify where incremental ways to make stages within the process standard.

Back to contents

2.0 Key Stages and Documents

There are 6 key stages in the AN audit process.

Key stages index:

1. Referral to Assurance and the decision making to proceed with an AN, or alternative
2. Preparations and planning to issue AN and ToR
3. Detailed planning and document review
4. Onsite audit, and key messages at open and close
5. Reporting, QA, peer review and business case for next steps (EADN)
6. EADN and potential outcomes

Document Index:

AN template

Terms of Reference (ToR)

Referral template

Enforcement Action Decision Notice (EADN) template

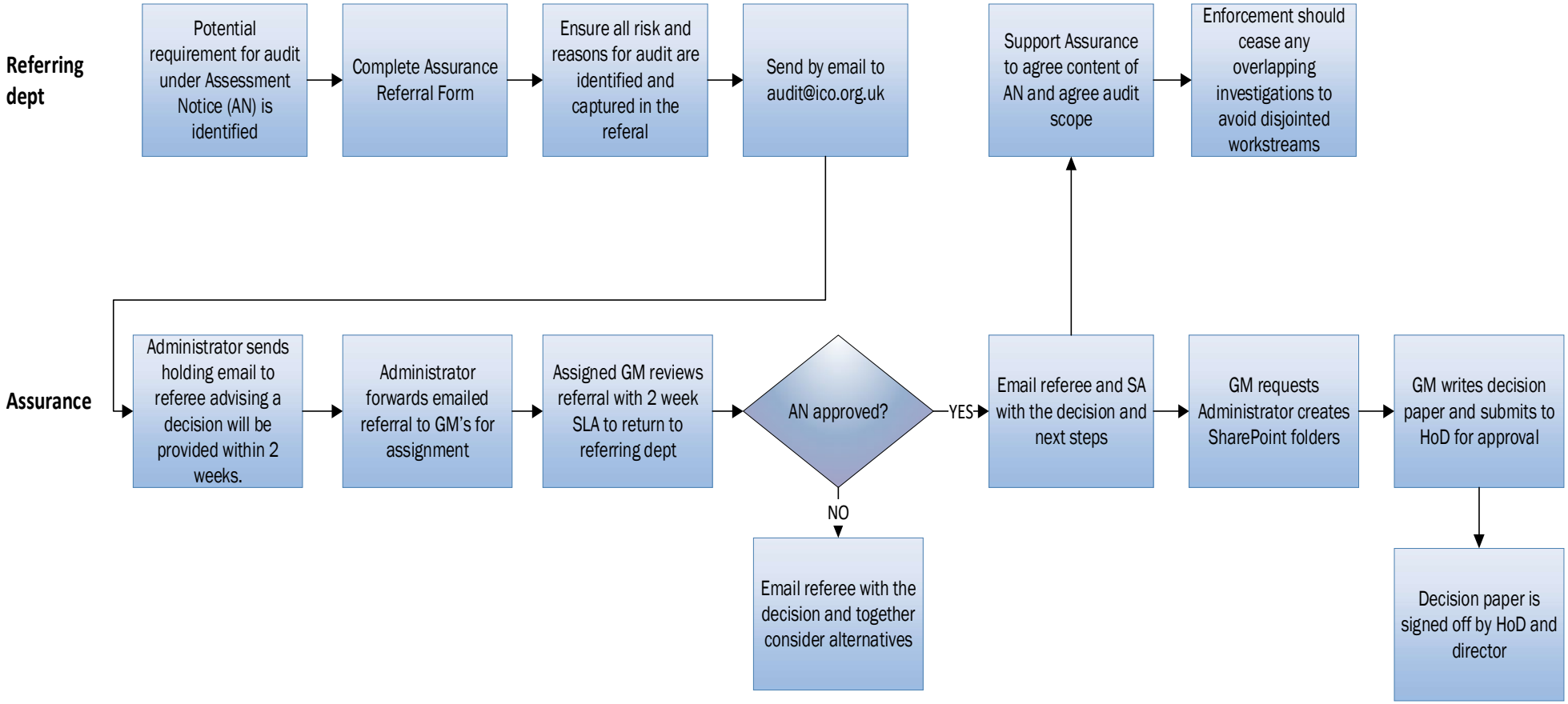
Blank WP template

Blank audit schedule template

Sample voluntary offer letter/redacted case study

3.0 Referral to Assurance (Stage 1)

3.1 Referral to Assurance and the decision making to proceed with an AN, or alternative flowchart



3.2 Referral

Where other internal departments wish to refer an organisation to Assurance for audit, this should be done using the referral template. The referral must contain sufficient information about the high risk areas to be audited and include any current evidence available which warrants the concern and supports the requirement to issue an AN. This will allow Assurance decision makers to make a full assessment and form the basis of the audit scope and AN. It will also provide supporting evidence for the decision to issue an AN should it be appealed by the organisation.

3.3 Assessment of referral

Each referral should be considered on a case by case basis to assess whether it is suitable for an AN audit. The GM must make sure that all the risks are understood, asking for clarity on points where there may be gaps in the written proposal, however extended back and forth between departments should be avoided. It may be necessary to arrange a meeting with the referrer in order to fully understand the reasons for the referral. Any additional information gathered should be recorded as part of the referral and decision making process.

In addition to considering the information and evidence provided in the referral, the RAP and Statutory Guidance should also be consulted to determine whether the intended approach is in line with the ICO's published approach.

Case Study 1
Prior to an organisation's referral to Assurance for audit they had agreed to participate in a consensual audit. However, due to the number of evidenced and identified high risks in their processing activities and volume of data subjects these affected. The decision was made to issue an AN for the audit as this was in line with the requirements of the RAP.

If a decision is made to proceed with an AN audit the reasons should be captured in a decision paper along side any other intel available to support the decision and signed off by the delegated authority (DA) where required.

If risks cannot be identified or suitability for AN audit is insufficient for any reason, this should be captured in the appropriate section of the referral template on it's return to referrer. At this stage alternative options can be considered

with the referrer, including the option to contact the organisation and request a consensual audit. The consensual audit procedure should then be followed.

At this stage it is likely that members of the referring department may request or expect to join the audit. This has advantages but should be managed carefully.

The decision and response should be provided within the 2 week SLA.

Back to contents

4.0 Issuing an AN and ToR (Stage 2)

4.1 Preparation and Planning to issue AN and ToR

AN's can be issued setting out different timescales for compliance with them. Typically they will fall into three categories

- Standard AN. The organisation is required to allow us to undertake an assessment of whether they are compliant with data protection law, on not less than 28 days' notice;
- Urgent AN. The organisation is required to allow us to undertake an assessment of whether they are compliant with data protection law, on not less than seven days' notice;
- No-notice or short notice AN. The organisation is required to allow us to undertake an assessment of whether they are compliant with data protection law, on less than seven days' notice;

When deciding the period for compliance with assessment notices, in particular whether to issue a 'standard', 'urgent', 'no-notice' or 'short-notice' AN, the RAP sets out the key considerations to determine what action is appropriate and proportionate and should be consulted for this process. The outcomes and decisions made during this assessment should be recorded as part of the decision making process.

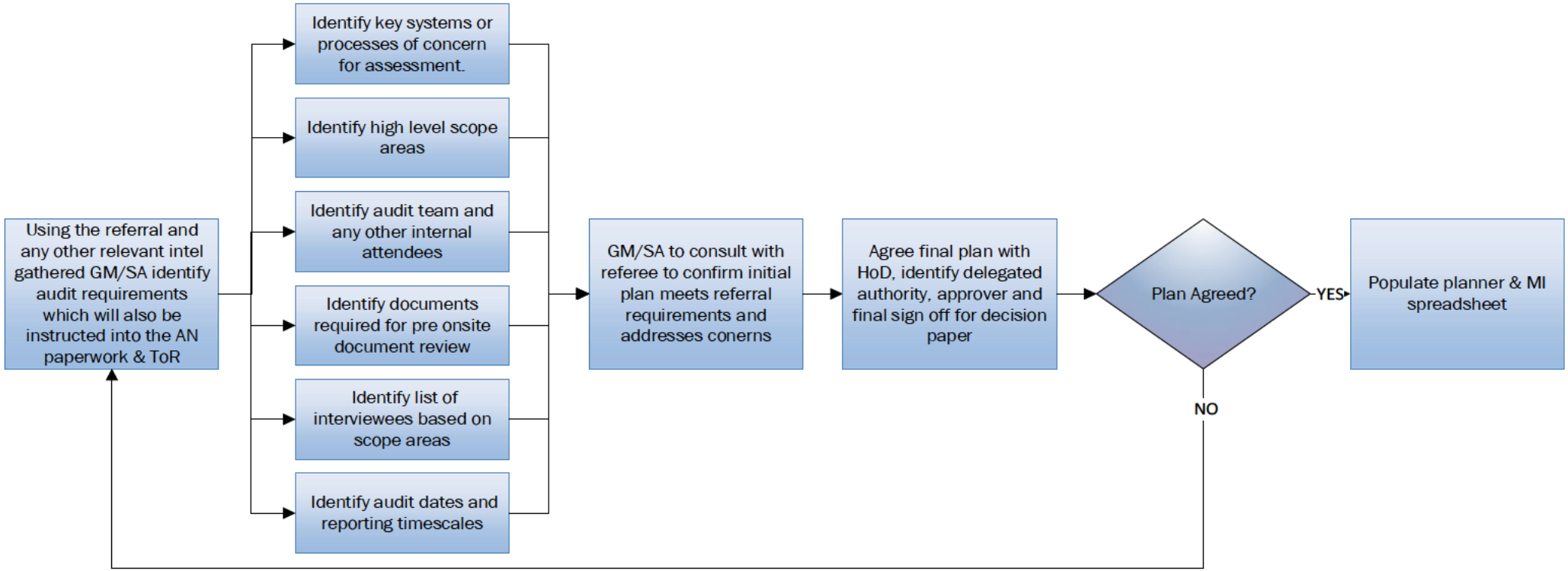
In contrast to the consensual audit process and due to the prescriptive nature of the AN, preliminary planning of the audit is required in order to issue the paperwork: specifically onsite and reporting dates, scope of the assessment, resources to cover scope areas and any documents required etc. The below map tasks (section 4.2) are critical in order to issue the AN and accompanying Terms of Reference (ToR). It is expected that this stage take 7/10 days. More detailed planning takes place once the AN has been issued and the audit is confirmed.

How much time will be required to produce the report will also have to be considered at this stage based on what is known now. This will be written into the ToR and subsequently reflected in the Assurance planner. There is no set timescale for the issuing of reports and this can be determined to suit the requirements of each AN audit considering the size and scope of the audit against the remit of consensual audit timescales.

AN audits represent a good development opportunity for Lead Auditors (LA). However, consideration of an LA's ability to handle highly pressurised environments and their experience of assessing the compliance of complex processing activities should be made, particularly for those participating in an AN audit for the first time. AN audits can result in formal enforcement action therefore the ability to record, evidence, assess and explain non compliance effectively will be a key requirement. This document however, is not a training manual and no substitution for being supported or mentored by the SA and GM through a first compulsory audit.

Back to contents

4.2 Preparation and Planning for issuing Standard AN



A standard AN refers to when the organisation identified gets no less than 28 days notice from issuing the AN to the onsite start of a compulsory audit.

When planning a standard AN, the onsite audit dates must be at least 28 calendar days after the paperwork has been delivered by recorded delivery to the organisation – this is to allow sufficient time for the organisation to exercise their right to appeal the compulsory assessment.

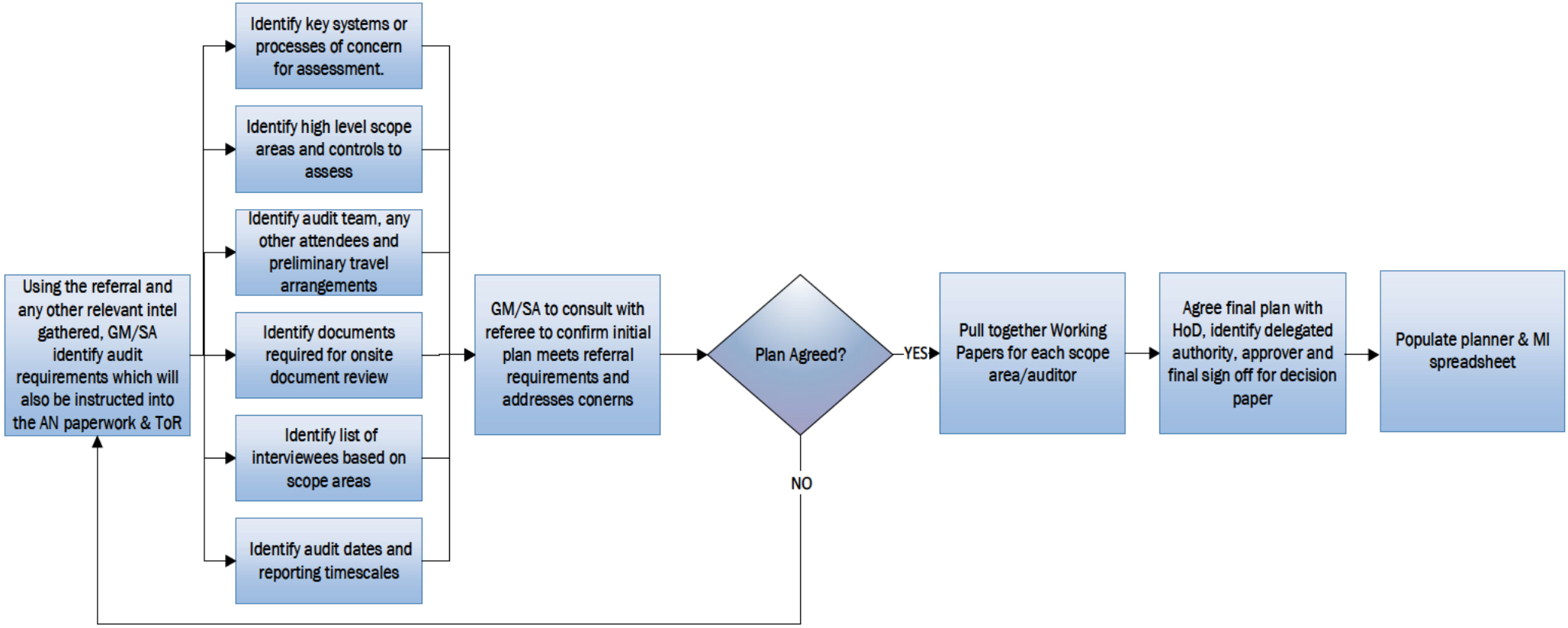
Additionally, any other requirements, such as the submission of pre-audit documentation for review cannot be expected prior to the 28 day deadline for appeal and the planning should take this into consideration. However, occasionally an organisation may respond ahead of the 28 days to say that they will not appeal, and may volunteer the documents requested ahead of the schedule. However this is their choice and we must plan and only expect as per the ToR and AN dates.

Case Study 2
A standard assessment notice was issued to an organisation on Day 1 outlining a requirement to attend their premises 43 days later. The ToR required the organisation to submit all relevant documents on day 29 (the day following the right to appeal expiring). This allowed 14 days for a review of submitted documentation to take place prior to the on-site element of the audit.

Essentially a key factor in preparation for a 28 day AN audit should be how much documentation is required ahead of the audit versus how much can be reviewed during the onsite part. Additionally, as part of the referral process, the referrer may already have provided (or may already have) a list of, or documents already obtained as part of their investigations.

Back to contents

4.3 Preparation and planning for issuing Urgent, Short Notice or No-Notice AN



An urgent AN refers to when the organisation identified gets no less than 7 days notice from issuing the AN to the onsite start of a compulsory audit (AN). A short or no-notice AN refers to when the organisation identified gets less than 7 days notice from issuing the AN to the onsite start of a compulsory audit (AN).

For an urgent AN, the onsite audit dates must be at least 7 calendar days after the paperwork has been delivered by recorded delivery to the organisation – this is to allow sufficient time for the organisation to exercise their right to appeal

the compulsory assessment. Although it is not essential, due to the urgent nature, the expectation is that the onsite visit would begin on day 8 (the day after the 7 day appeal window has elapsed).

When planning a short notice or no-notice AN, the audit dates will predominantly be determined by resources available to carry out the onsite visit within days of the AN being issued. Consideration should be given to including additional time into the assessment timescales on the AN to provide the ability to react to any circumstances which may come to light during the audit and were previously unknown.

Case Study 3

An AN is issued to an organisation requiring them to be available for audit starting 8 days after the AN is issued. The audit team begin the audit at the organisation's head office and during an interview discover that, although governance takes place at head office, a key task that is being assessed is carried out at a different site. In order to complete the audit successfully auditors would need to interview two operational staff and their line manager at the additional site as well as see a demonstration of the system. Due to the distance between sites it is not possible to include it within the current audit plans.

Due to the amount of unknown elements in the planning of the audit, the timescales for assessment in the AN covered a two week period so auditors were able to include this second site visit the following week and within the scope of the assessment notice.

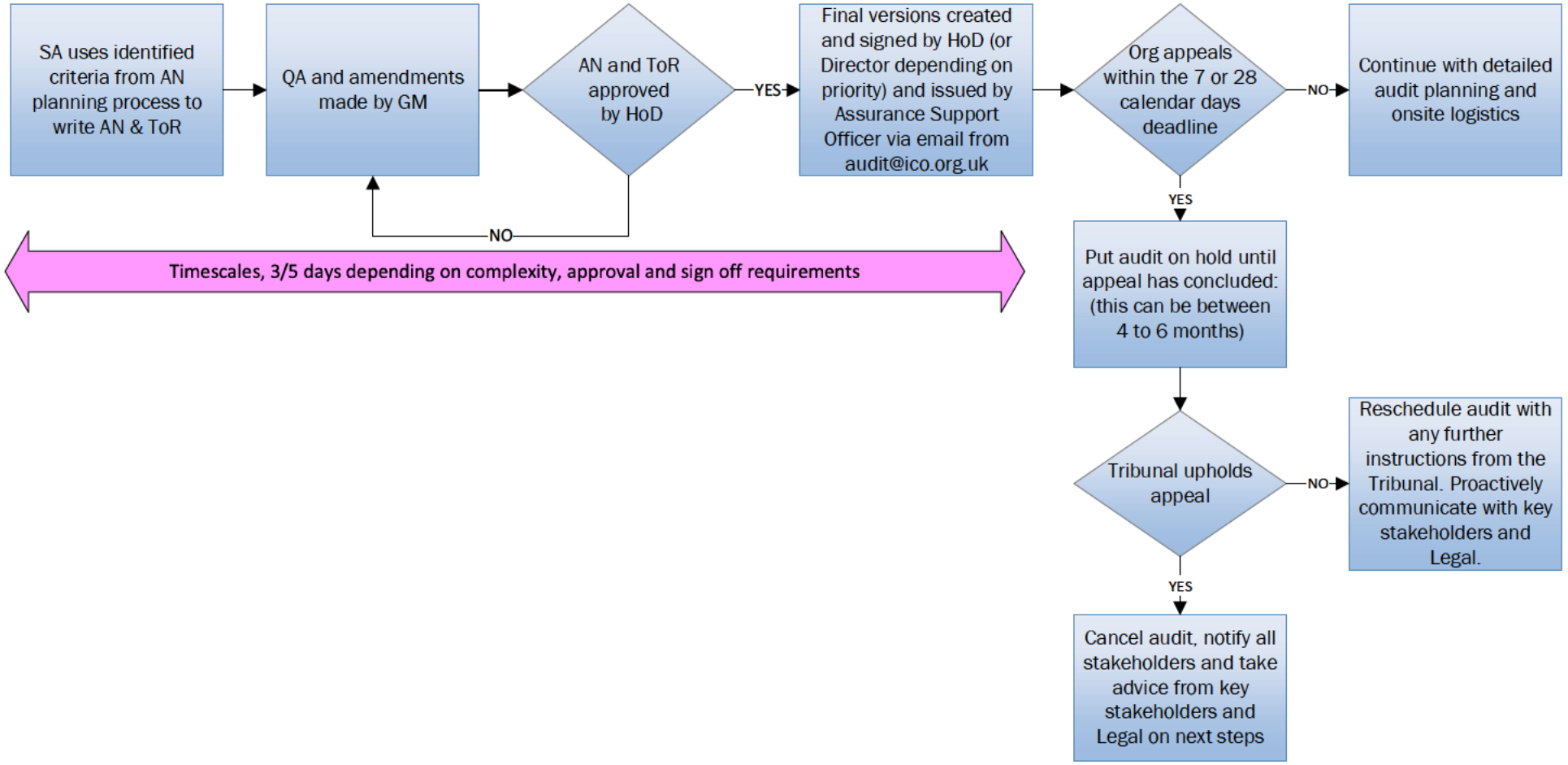
To prepare an urgent, short notice or no-notice AN, as before, requires a degree of preliminary planning. However, the circumstances in which these AN's would be used are for very specific, high risk processing reasons and more suited to a narrow scope. The planning requirements are limited here for example, due to the urgent nature of the AN it may be unrealistic to expect many documents for review or build in additional time to review them, however as with the standard process some documentation may have been made available as part of the referral process or be available on the organisations website. As a result, this map focuses on resources, logistics and getting prepared for the onsite visit. It is estimated this stage to take 7/10 days.

Importantly, a 7 day AN would be driven by unique circumstances and from a senior level decision. Therefore additional advice must be sought from legal when completing the AN as the referring requirements will most likely be exacting and targeted. These will be reflected in expectations set in the AN and there will be additional scrutiny around the sign off of the AN. Sufficient time to allow for the negotiation of final wording and sign off should be included within these timescales.

Urgent, short or no-notice ANs to do not always provide sufficient time to carry out detailed planning once the AN has been issued therefore this part of the process should be done in conjunction with detailed planning (See section 5.0)

Back to contents

4.4 Write and issue the AN and ToR



Each AN and ToR should be completed in accordance with the requirements of the audit on a case by case basis. The AN template should be used when completing an AN and each section completed using the outputs from the previous stages of the process to ensure that the scope and requirements of the AN are supported by identified and evidenced risks and concerns. Organisations have the right to appeal ANs therefore it is critical that the AN is both balanced and proportionate when considering those risks and this can be demonstrated through the decision making process.

An AN is accompanied by the ToR. The ToR serves a similar purpose to the Letter of Engagement used in a consensual audit and provides additional information to the organisation about the audit process. The ToR template should be used and as with the AN template, the outputs from the previous stages of the process should be used to populate the required areas.

It is important to ensure that the AN and ToR include all the timescales, scope areas, documents and access to staff required to complete the requirements of the audit. If they are not all recorded within these documents the organisation can refuse access to any additional elements identified after the notice has been issued. Additionally, as indicated above, the AN and ToR should not include requirements outside of any identified and evidenced risks and concerns with the organisations processing activities as this could add weight to any appeals made.

In terms of issuing the AN to the DC, ensure all prepared documentation are sent to the Assurance Support Officer and subsequently sent from the audit@ico.co.uk inbox. This ensures any response is monitored and not the sole responsibility of an individual, and has a corporate appearance for the initial contact. Later correspondence to complete detailed planning can be completed as usual by individuals in the audit team.

Where the organisation ignores the delivered AN, first ensure the documents were delivered and signed for and the addresses and contacts were correct. If the information was correct then refer to page 11 in the Statutory Guidance and contact LSRE for further advice.

4.5 Appeals

The right to appeal must be included within the AN and as such is set out in the AN template. This includes the timescales for which an organisation can make an appeal to the Tier 1 Tribunal. An organisation has 28 days to appeal a standard AN and 7 days to appeal and urgent AN. Where an urgent AN is issued the organisation has an additional right to challenge the short notice of the AN (in addition to the right to challenge the AN entirely). For no notice AN's refer to the RAP and Statutory Guidance for more information.

Where an appeal is lodged you should refer to Tier 1 Tribunal advice and inform and take advice from the relevant Legal teams within the ICO who will set out the Assurance obligations and responsibilities dependant on the nature of the appeal. At this stage, all documentation including the completed referral form along with any additional risk assessment and decision making that led to the issuing of the AN should be collated and available for review by legal teams.

Where an appeal against the AN has been rejected by the Tier 1 Tribunal, work should begin to rebook and reschedule the original audit. The original reasons for the AN should be reviewed to determine if, after the appeal, the original components are the same however, these considerations should be made against the reasons and decision making that resulted in the original AN. If any additional factors or risks have come to light since the original AN was issued then legal advice should be sought as to what is subsequently included in any revisions.

Following the review, the planning stage should be revisited to determine new timescales for onsite visit, reporting timelines and document submission where relevant. Once determined these should be updated in a new version of the AN and ToR and issued to the organisation.

The decision by the tribunal maybe to reject the overall challenge to the AN but uphold part of the appeal resulting in changes to the audit scope and therefore an amended AN. In this instance the original decision paper should be reviewed and repeated to give an audit trail of any amends, changes in risk and decisions made following the Tier 1 Tribunal decision. In practical terms this will most likely involve removing sections from the original AN rather than adding new requirements

for audit in. It is therefore important to ensure that all stakeholders are informed of any proposed changes to the AN and audit ahead of re-issue.

Whether an appeal is rejected or partially upheld, a new AN and ToR should be completed and issued quickly after the tribunal decision to avoid any further delays to the audit. Unnecessary delays can undermine the requirement for an AN therefore if necessary it should be prioritised over BAU audits which are already arranged and can be postponed to a later date.

Where the Tier 1 Tribunal upholds the appeal in full, we cannot proceed with the planned audit. In this event it is important to make sure that all stakeholders, particularly those who may not have direct knowledge of the Tribunal decision are informed. In these circumstances alternative options should be considered which may be (but not limited to):

- another AN based on new information and risks identified,
- an offer by the organisation to complete a consensual audit or,
- cancel all audit activity,
- move the investigation back into the referring department.

Where an appeal is upheld then a lessons learned exercise should also be carried out to understand the reasons for the successful appeal and assist in developing and strengthening the AN process.

4.6 Communicating with Stakeholders

It is critical and expected that all stakeholders at all levels are kept informed of the preparations, planning, changes, decisions, timescales, aims and goals. Regular meetings throughout the audit to communicate key information and evolving expectations are good practice, especially if the audit is large and fluid – as is often the nature of these engagements.

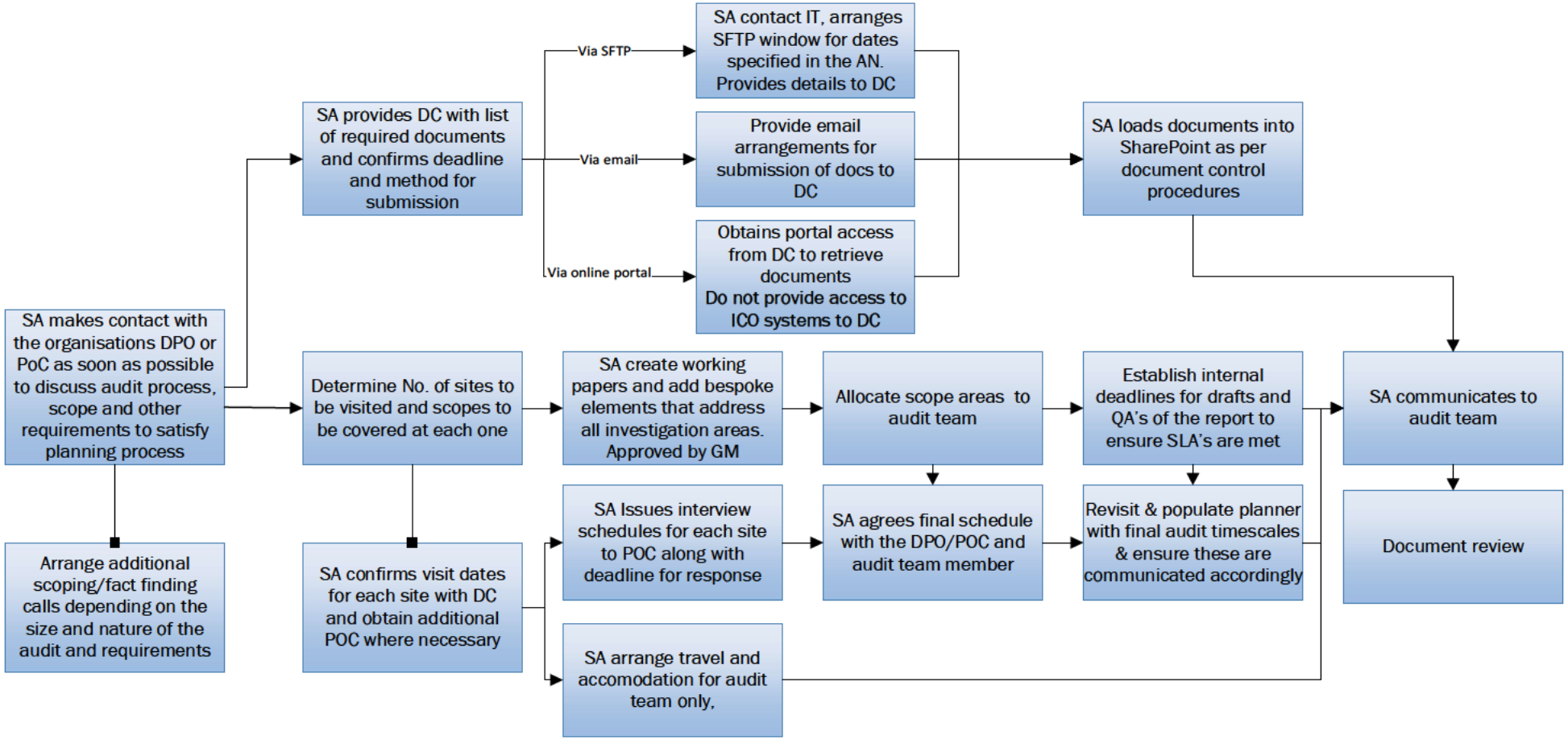
Your stakeholder group is often wide and may have different information/communication requirements. As an example, it may be that you split regular update or project meetings into an operational meeting that includes the full audit team as

well as any policy and experts contributing to the audit, a planning update meeting for TM's and GM's where their staff are participating and then a senior level update for the high level messages and decisions. This makes good use of resources and the messages communicated therein at the right level. Additionally it allows all stakeholders to ask questions and fully understand how they can best support the overall engagement. Members of the referring department should also be kept up to date with regular communications as they may also be able to provide additional support or feedback based on their ongoing knowledge of the organisation.

Back to contents

5.0 Detailed Planning and Document Review (Stage 3)

5.1 Detailed planning and document review flowchart



Much of the audit planning has already taken place in order to issue an AN and ToR and whilst not identical, the run up to the onsite element of the audit is similar to the consensual audit process. However, routine/essential tasks should be completed being mindful of the prescriptive nature of the AN and the high risk nature of the organisations' processing that has been identified.

The requirements now are to obtain as much information from the documents supplied and/or the organisation in order to fine tune the working papers and logistical arrangements. However this may not be possible depending on the type of AN issued. Overall an agile approach should be adopted as the planning will be specific to the requirements of each individual audit which can vary considerably in terms of size and scope.

5.2 Detailed planning for a Standard AN audit

The standard AN process should provide sufficient time for more detailed planning to take place following confirmation from an organisation that they will not be appealing the AN or after the expiry of the appeal window.

During the available time, and at the earliest opportunity, the SA should contact the organisation and arrange a meeting to discuss the audit. The objectives of this meeting include:

- to enhance the SA's understanding of the organisations processing, relevant to the AN and proposed audit scopes,
- to focus the working papers by adding/removing relevant controls within the scope of the AN,
- to identify relevant interviewees and develop the interview schedule,
- to identify whether more than one site needs visiting during the audit,
- to identify any additional documents that are required for review,
- to enhance the organisations understanding of the audit and audit process,
- any intended publication following the audit, such as the executive summary.

This will allow the SA to develop a more detailed plan for the audit and set the expectations of the organisation and what is required of them to assist with developing the logistical arrangements, interview schedules and document submissions. It may be that more than one meeting is necessary.

The SA should also ensure that as plans are developed, relevant stakeholders and the audit team are kept updated. Any proposed or amended plans should be provided to the GM/DA for review and approval. Once approved, the SA will be responsible for making the necessary travel and accommodation arrangements for the audit team.

At this stage it is also worth considering the impact of multiple line of enquiry on an organisation from the ICO. For example, where an organisation is referred to Assurance as a result of ongoing investigations, they may already be responding to requests for information from the investigating team. Requiring them to simultaneously provide large amounts of documentation for review prior to an audit may be problematic or not even possible dependant on their available resources. In these circumstances the audit requirements should take priority as these are restricted by the timescales set out in the AN. It may be necessary to request that the investigating team put their casework and any ongoing requests on hold during the audit to allow the organisation to commit their resources to responding to the requirements of the AN.

5.2 Detailed planning for Urgent, Short Notice and No-Notice ANs

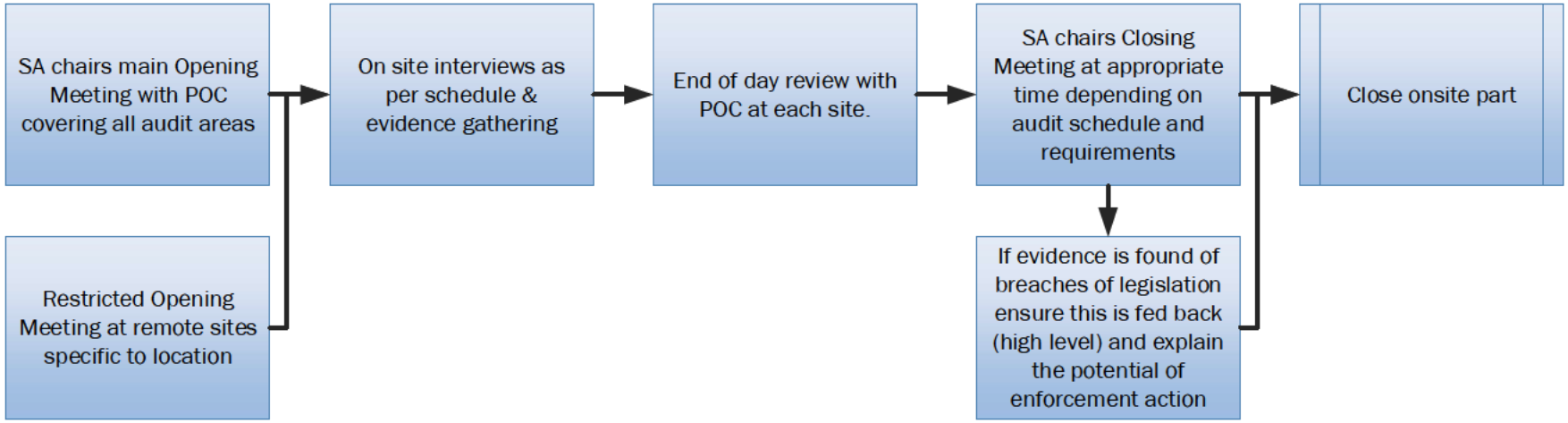
The shorter timescales between the issuing of an urgent, short notice or no-notice AN and the onsite element of the audit makes it more difficult for detailed planning or a document review to take place. Much of the information and planning for these ANs would have been gathered and put in place prior to it being issued.

Where possible SAs should make every effort to arrange a pre onsite meeting with the organisation, as above, to gather as much information as possible although it may not be possible to put a complete logistical plan in place. In these circumstances some of this planning, such as finalising the interview schedule or obtaining documents will have to take place during the onsite visit.

Back to contents

6.0 Onsite/Remote Audit (Stage 4)

6.1 Onsite/ remote audit flowchart



The onsite audit will follow a similar process to a consensual audit, but being mindful of the risk identified to warrant auditing under an AN. Additionally, and considering the amount of time available to carry out detailed planning prior to the visit, it may be necessary to continually amend and adjust audit plans to ensure that the audit objectives can be fulfilled.

6.2 Opening meeting

For standard AN audits the objectives of the opening meeting will be similar to those of a consensual audit. It will be the role of the SA to chair the meeting and the agenda will vary depending on the requirements of the audit and amount of planning that was able to be completed prior to this stage. As a minimum the opening meeting agenda should include:

- introductions,
- overview of the onsite audit process and plans,
- finalise any details that have not been previously agreed or any requested amendments made by the organisation,
- confirm the reporting arrangements and timescales at this stage,
- ensure that the audit team are aware of any housekeeping requirements,
- Publication of the executive summary.

If sufficient time has not been made available to carry out detailed planning prior to the onsite visit then the opening meeting can be used as an opportunity to make or finalise plans to conduct the audit. If this is the case then the SA should allocate appropriate time for this meeting and advise the organisation before hand of the expected duration of this meeting. It is entirely possible that this could take half of day one in the case of short notice and no-notice ANs.

In these circumstances, and in addition to the above, the SA should also seek to include in the opening meeting agenda:

- an overview of the organisations processing related to the requirements of the AN,
- request individuals to speak to and develop an interview schedule,
- develop and confirm a process for requesting additional interviewees during the audit,
- request copies of key documents required at this stage,
- confirm what provisions are available to carry out interviews.

Whilst this may not be 'normal' audit practice, an AN requires an organisation to make relevant staff members available for interview so it would be entirely appropriate for and auditor to request to speak to additional staff members during the

onsite visit, if required. Where it is considered that this may be likely during an audit, the audit team should only contain members who are confident enough to make such requests as it may not always be known during the opening planning meeting.

Consideration should also be given to opening meetings during different site visits and the attendees of that meeting. Agendas and content should be adjusted so that they are relevant and appropriate for the attendees.

Case Study 4

An AN audit begins on two sites simultaneously. It is not possible to arrange for remote access for one opening meeting to take place so two separate opening meetings are held.

Senior representatives of the organisation and the DPO are based on site 1. The SA chairs this opening meeting and includes agenda items covering the scope, plans and reporting process for the audit as outlined above.

At site 2 a designated audit team member chairs the opening meeting which is attended by more operational level staff and POC with responsibility for facilitating the auditors visit. Given the level of the attendees the agenda is limited to cover logistical and housekeeping arrangements for the visit only.

The POC at site 2 asks auditors about the reasons for the audit taking place. In response they are politely informed that it would not be appropriate to disclose this information during this meeting and they should direct these questions within their organisation

6.3 Interviews

The nature of AN audits can result in organisations being more protective and considered about what information is provided during interviews. As a result they may have note takers and /or legal representation present in the individual interviews.

Interview notes can also be used in any subsequent tribunal so should be taken in a clear, coherent and concise manner and where required written up as soon as possible after the interviews, to ensure nothing gets missed. This is also the case for any auditors or colleagues shadowing the interviews whether as part of their training or as a representative of the referring department. Their notes should be considered equally as important for accuracy as the auditors, and can also be used as evidence. All written notes made by everyone attending the audit must be saved in the relevant evidence folder in SharePoint as with a consensual audit.

Where it has not been possible to obtain documents prior to the onsite/remote element of the audit then these should be requested during audit interviews. Auditors should make a note of all documents that have been requested. In addition, where demonstrations of systems have been made any notes or comments about the system should also be recorded within interview notes so that they are available as evidence, if required.

As with the opening meeting, auditors should not discuss the reasons for the audit taking place with interviewees and advise that any questions they have should be directed internally.

6.4 Daily wrap up sessions

It is good practice to notify the auditee of any substantial findings and concerns at end of each days audit activity. Daily wrap up sessions should be planned into the schedule for each day. This is key to fairness and gives the auditee the opportunity to respond meaningfully whilst the ICO team is still onsite. Where audits are carried out simultaneously on separate sites feedback should be collated between the audit team and provided by the SA to the relevant authority within the organisation. Different feedback should not be provided to different representatives of an organisation.

Where serious or substantial concerns are identified and fed back, the feedback should be limited to the facts around what has been identified. Auditors must not express any opinion of the likelihood of resulting action being taken as a result of the concern as this could impact the options available following the audit. It would be best to cover this aspect in the closing meeting as outlined below.

6.5 Closing meeting

At the conclusion of the onsite/remote element of the audit a closing meeting should be held. The purpose of the closing meeting is to:

- thank the organisation for their assistance in facilitating the audit,
- present high level feedback related to the findings of the audit,
- confirm the arrangements and timescales for providing any additional and outstanding documents requested,
- confirm the next steps and timescales for reporting and factual accuracy.

As with the daily wrap up sessions it is important that auditors to not provide an opinion of any likely outcome of the audit in relation to regulatory action. Whilst the potential for enforcement action should be advised where appropriate, it must be done so in a way that cannot be interpreted to be a predetermined outcome. As a public authority any opinion given at this stage could be regarded as a 'legitimate expectation' under public law and may impact the options available to the ICO following the conclusion of the audit. This could lead to a judicial review of any ICO decisions with regard to subsequent regulatory action.

Where audits are carried out on multiple sites, it is not always necessary to conduct a closing meeting. It may not be appropriate to provide POCs at all sites with high level findings or details of the next steps and reporting process. Once interviews have been concluded, the POC should be thanked for their assistance but this does not need to be carried out as part of a formal meeting. The decision on how to close individual site visits should be made with consideration to the requirements of each individual audit and site.

Additionally, it may not always be possible to hold the closing meeting at the end of the site visit where senior representatives or delegated authorities are positioned, particularly when additional site visits have not concluded.

Case Study 5

The site visit where senior representatives of the organisation and the DPO are based concludes however, additional site visits are taking place the following week so the closing meeting cannot take place. The last site visit to conclude is only attended by two of the four audit team members and does not include the SA.

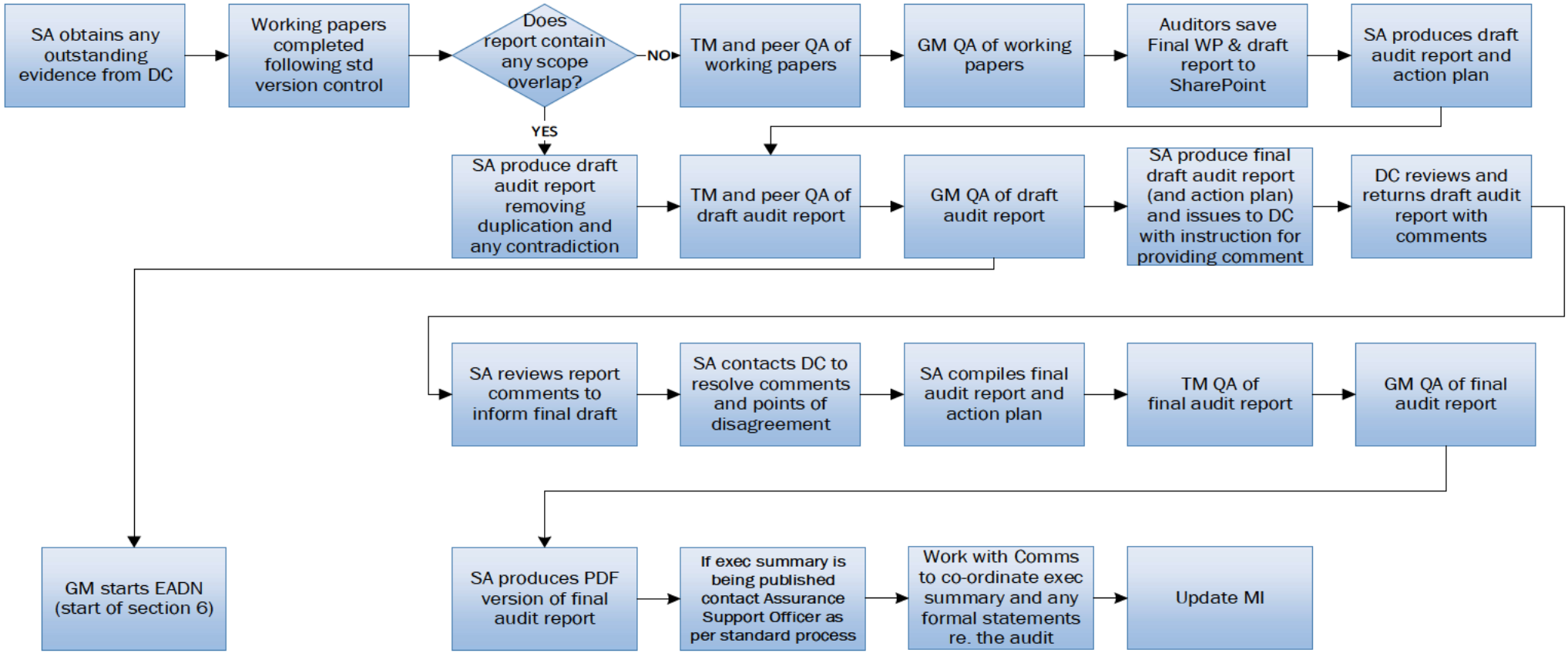
Rather than require that everyone attends the final site at the conclusion of the audit, the SA plans a remote closing meeting for the following day so that all auditors can to attend and allows the audit team to convene and prepare for the meeting.

The organisation requests that the closing meeting is held face to face. As a result, closing meeting plans are amended and, considering the resources required for four auditors to travel to the closing meeting, it is decided that two audit team members will attend the closing meeting and conclude the onsite audit. Amended plans include sufficient time for the attending team members to be briefed on the feedback they are required to provide.

Back to contents

7.0 Reporting, QA, Draft and Final Reports (Stage 5)

7.1 Reporting flowchart



7.2 Report type

The reporting aspect will be dependant on the requirements of each individual audit. This should have been decided as part of the planning stages and will vary depending on the requirements of the audit and stakeholders. As a result the extent to which the report goes to when providing details of the organisations processing activities should be considered. For example, referring departments or other internal stakeholders may be interested and/or benefit from a more detailed overview of the processing activities undertaken. In this case it would be beneficial to include narrative findings within the audit report. Alternatively, where a detailed overview is not required, the exception based reports used in consensual audits would be sufficient.

Again, depending on the requirements of the audit and scope covered, it maybe beneficial to present the findings relative to the principles of the GDPR rather than by scope area, particularly where elements of different scopes all relate to one principle infringement of the legislation. The annex starting on page 38 has sample reports from various previous AN audits to help make a decision on what is the best approach for your engagement.

Regardless of the approach adopted and where conclusions find the organisation in breach of legislation, the key to any reporting approach must be to explicitly detail where the DC has failed to meet the expectations of the GDPR. Findings (or non-conformities in exception based reports) should contain all the evidence used to identify a non-conformity, specifically naming any relevant documents and the section it relates to as well as indicating where something has been disclosed in interviews. When presenting the draft report to the organisation for a factual accuracy review, this will assist them in understanding why the conclusion has been reached and limit the amount of challenges to the report.

If narrative findings are included in the audit report there is greater scope for duplication of similar findings or recommendations, possible contradictions or other issues that could result in significant amendments when combined to form the draft report. In order to reduce the risk of creating additional and unnecessary work the draft audit report should be created prior to the QA process.

7.3 QA

Where narrative findings are used, it would be good practice to include a peer review of the audit report by auditors involved in the audit, prior to TM/GM QA. This will allow auditors, who have gained knowledge and experience of the organisation, to highlight any areas of the report where their understanding, following the audit, may be different and that would not be easily picked up by the TM or GM. It would also allow auditors to make amendments to the report to resolve instances of duplication or contradiction in the findings. The SA should discuss these with the audit team and reach a conclusion of how to combine points of duplication into an area where it has highest impact or relevance as well as resolve points of contradiction based on the evidence available. Once the draft audit report has been completed it should be submitted to the TM for QA.

Where exception based reporting and working papers are used then the TM QA can take place on the working papers and follow the same process as consensual audits whereby a draft audit report is produced and subject to another QA by the TM.

7.4 Enforcement Action Decision Notice (EADN)

Following the TM QA of the draft audit report and once any required amendments have been made, the draft report should be subject to QA by the GM/DA. Having visibility of the findings of the audit the GM should now start work on the EADN. The GM/SA should look to finalise the EADN and submit to the delegated authority (DA) (usually the Assurance Director) or agreed level for sign off within the timescales set out for the issuing of the final audit report. The GM should advise the DA of the timescales required as early as possible in order to mitigate any unnecessary or avoidable delays. Standard audit practice dictates that the audit is complete as the final audit report is issued. Therefore a decision on how the ICO want to manage the findings should be in place prior to the final report being issued so this can be communicated formally to the organisation at the same time. It is not good practice to issue a final report following an AN without notifying the organisation of any potential or pending enforcement action. If the decision is not available then delaying the issue of the final report should be considered so all the messages can be delivered in a single disclosure. The organisation must be notified of any potential delays and where possible an indication of new timescales.

In completing the EADN the GM should consider the findings of the audit and identified infringements against the requirements of the RAP in order to determine the most appropriate course of action. The GM should also consult with the referring department, particularly if the referral formed part of an ongoing investigation or complaint to determine whether there is any impact or cross over with these other work streams or already proposed regulatory action.

7.5 Draft and final reports

This should generally follow the same approach as the consensual audit process. However, the draft report does not have to be accompanied by an action plan as any comments the organisation wish to make can be appended to the draft report. At this stage comments should be restricted to the factual accuracy of the findings or descriptions of processing activities. Where it is decided to issue an action plan then consideration should be given to the removal of the column that allows the organisation to accept or reject a recommendation, particularly where there is potential for enforcement action. It may not be considered beneficial to give the organisation the opportunity to reject the settled opinion/decision of the ICO at this stage.

On receipt of the draft report the organisation may ask for more time to respond, as specified on the ToR, which may be reasonable especially if the findings are numerous or could have substantial business implications. The SA should seek the advice of the legal team and the agreed decision makers depending on the requests the organisation makes at this stage before providing a response. Be prepared for the potential for challenge and escalation depending on the variables and don't rule anything out. Ensure there is access to advice, particularly legal and the appropriate senior level decision makers and that and responses and important decisions are considered, informed and documented, particularly when they result in changes to the audit report.

Requested changes to the draft audit report should only be made where they are supported by sufficient evidence, where they are rejected an explanation should be provided to the organisation.

7.6 Communication with the Organisation

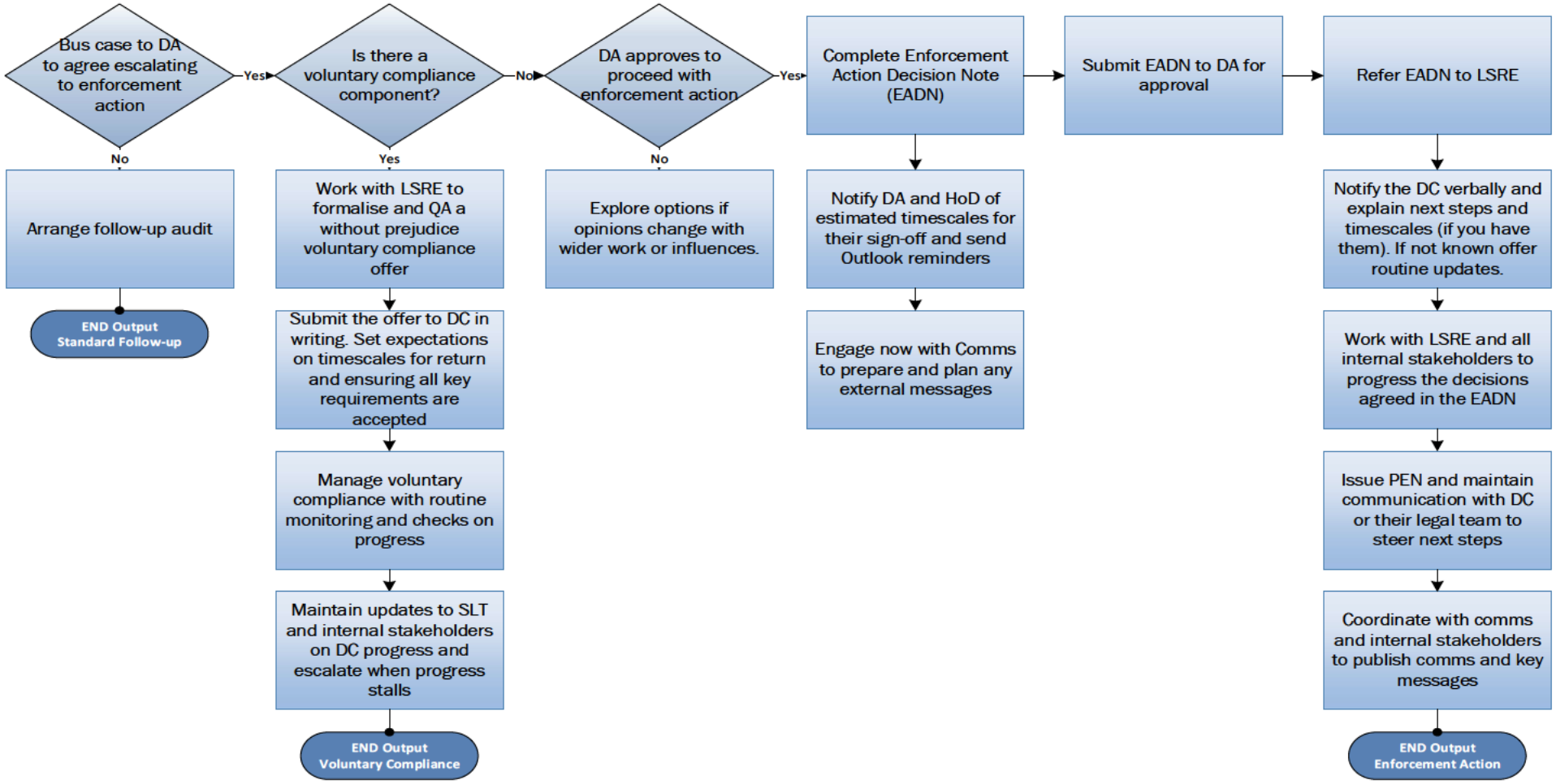
It is important to set realistic expectations and communicate key messages about next steps that aren't covered in the ToR, and particularly where the audit outcome shows there is sufficient evidence to warrant further consideration of enforcement action. The AN template mentions potential enforcement action, but this alone cannot be relied upon to cover expectations once facts and findings have been documented in the draft and final audit reports. It is recommended to have an initial call with the organisation as soon as you know enforcement is a potential conclusion and explain why. Each case will be considered on an individual basis, and at a senior level in accordance with statutory guidance and the RAP, therefore be clear that enforcement action is not pre-determined. Follow up any conversations with an email detailing the points discussed with the organisation. These emails will be included in any submissions to Legal in the EADN.

The response of the organisation, particularly to the findings in the draft audit report will also have an impact on the EADN. The RAP includes the willingness of organisations to accept and remedy any infringements with legislation as a key factor in determining appropriate action where necessary. The SA, through their communications with the organisation, should determine the willingness of the organisation to accept the findings of the audit report and provide this information to the GM/DA to assist in the completion of the EADN.

Back to contents

8.0 Outcomes (Stage 6)

8.1 Decisions and Outcome flowchart



There are three possible outcomes from an AN audit: The above flowchart shows the decision path and high level steps to take for each one.

8.2 Output 1, standard follow up

This is likely when findings and recommendations in the audit report only show minor or few breaches and the conclusion is considered to be best managed using a standard follow up arrangement. This approach must be documented in the EADN and an email to the Delegated Authority (DA) seeking approval of the business case to explain any reasoning and why a standard follow-up is preferred.

NB: Where we find a standard follow up is the most appropriate outcome following an AN and considering the circumstances that resulted in a compulsory approach, we should consider a lessons learned from the risks identified in the original referral and subsequent decisions to complete the engagement on a compulsory basis. This is to help avoiding future use of using audit resources on engagements that may not have been suitable for a compulsory approach.

8.3 Output 2, voluntary compliance

Where audit findings identify serious and fundamental infringements of DP legislation and considering to the number of data subjects affected and the volume of data processed, voluntary compliance may still be an appropriate outcome and preferable to more formal enforcement action, but only under certain circumstances. A voluntary approach can only be entered into where there is full acceptance of the recommendations and the organisation have demonstrated that they are willing to resolve all of the recommendations. Any offer must be made in accordance with regulatory good practice and subsequently agreed at the correct level, via the EADN.

There should be a good indication from the organisation, on return of the accuracy check, whether or not they agree or disagree, in full or in part with the findings and recommendations. The SA should advise the GM of this in order to include in the EADN and with sufficient time for a decision to be made and approved by the DA prior to the issue of the final audit report.

As always, it is best to treat each circumstance on it's own merit, and refer to the RAP and Statutory Guidance where necessary and appropriate. Consult Legal before any decision is made on a voluntary arrangements. Once approved, continue to work closely with Legal to agree voluntary offer conditions and provide a voluntary solution that satisfies the

ICO and expectations as set out in the RAP, provides the best outcome for data subjects and provides enough time for the organisation to make changes. A voluntary offer will always include the right to take enforcement action should progress stall during monitoring.

The voluntary offer should be made in writing, even if it has been advised verbally at the time the final report was issued. The offer letter (see case study) should set out the expectations of the offer and include:

- the reasons behind the decision,
- an overview of the proposed process for monitoring compliance against all recommendations,
- proposed or required timescales,
- consequences of failing to adhere to the offer,
- any other next steps,
- where required, that enforcement action to any ongoing investigations is still a possibility.

Once an agreement has been received, in writing, from the organisation, then a meeting to set out more detailed requirements of the monitoring arrangement should take place. Any conversations with the organisation about next steps should be led by Assurance and these should be documented and followed up in writing for the audit trail.

Monitoring means a plan is put in place for the organisation to submit evidence on an regular, agreed basis that shows the improvements and changes made for each recommendation. Audit will review the evidence and respond with either confirmation that the recommendation action is now complete or an explanation as to why the submitted evidence is not sufficient to complete the recommendation. This is essentially an ongoing follow-up, but starts immediately after the voluntary arrangement is agreed and allows the ICO to keep close to progress.

Where an organisation fails to meet the agreed requirements of voluntary compliance or argues against the requirements of completing a recommendation then it may be necessary to update and resubmit the EADN to propose more formal

action. This would only be appropriate where the recommendation being argued or remaining unresolved demonstrates a direct infringement of DP legislation as opposed to a good practice control measure.

8.4 Output 3, enforcement action

Where an organisation fundamentally disagrees (in full or part) with the findings and recommendations and the ICO, having considered any challenges, remains confident in it's audit opinion then enforcement action can be considered as an appropriate option to achieve compliance.

Arguments to pursue enforcement action can be made in the EADN as the organisation is reviewing the draft report for factual accuracy. It is likely that an opinion on the severity infringements of DP legislation and deficiency of operational practices can be formed through out the audit and as far back as document review. However, opinion of the likelihood of the organisation accepting the recommendations will become apparent during the accuracy check where, if they do not, they will no doubt challenge the findings and recommendations. Accepted and evidenced challenges to the accuracy of the audit report should still be made as with the consensual audit process.

A preliminary enforcement notice (PEN) can take weeks (or months) to prepare, especially if external legal counsel is consulted. So once the EADN recommendation to pursue enforcement action has been approved by the DA, the high level steps would be to:

- advise the organisation verbally and then in writing of the intention to enforce, (running any written comms to organisation via Legal),
- issue the final report to the organisation but do not publish the executive summary or make any comms announcements,
- assist Legal, using the EADN and other experts to prepare the PEN,
- work with comms and key internal stakeholders to plan and position the external messages,

- keep all internal stakeholders updated of progress either via a regular meetings or emails detailing key up to date messages,
- seek approval of PEN at the agreed final level and in accordance with the current situation and assuming no change in regulatory priorities or other influencing factors,
- Issue PEN, coordinating with internal stakeholders to manage expectations.

There is no one size fits all, so guiding principles must be in line with our statutory obligations (as detailed in our Statutory Guidance on our regulatory action), our responsibilities and approach to regulatory action as detailed in the RAP, our internal processes and procedures as detailed in the Investigation Manual and additionally targeted, specific advice from departmental specialists and experts, specifically Legal. Regular consultation with colleagues across the ICO ensures the audit team arrive at an agreed, thoroughly considered decision and plan. Regular project meets to discuss the detail with all agreed stakeholders also benefits the decision making process and may include contributions from other departments such as: Legal, Policy, Enforcement, Comms, HoD and DA.

8.5 Comms

One important consideration at the end of any engagement regardless of the outcome, is Comms. They have an appreciation of both internal and external stakeholder interests. Many of the cases that result in a compulsory audit are from either HPI or Investigations, and as a result may attract interest from the wider general public. As a result and in some cases executive summaries may be published with an accompanying statement or blog so it is critical that Comms are aware of the progress of the audit and intended publication date. This will allow any lines to take, statements and planning to be agreed and put in place without causing unnecessary delay to the intended publication date. Comms will manage all publications, statements and stories from the ICO so it is important that they are able to accommodate any requirement into their calendar so that it is agreed and lined up with when the executive summary is published.

Back to contents

9.0 Annex

Case Studies

- Case study 1 – Data broker

Back to contents

10.0 Appendix

Version History Panel

Version	Changes made	Date	Made By
0.1	Drafting	24/02/2021	[redacted]
0.2	Drafting	27/04/2021	[redacted]
0.3	Drafting	27/07/2021	[redacted]
1.0	Final version created	15/09/2021	[redacted]
1.1	Document layout amended. Contents page added. Detail added about sending AN electronically via audit mailbox. Flowchart references need to contact ASO following the standard process if the Executive Summary is to be published.	15/10/2021	[redacted]
1.2	Link to case studies added to the annex at section nine.	26/10/2021	[redacted]

Back to contents