International Competition Network

ANTI-CARTEL ENFORCEMENT MANUAL

Updated in March 2025

Chapter 1 Raids

Table of Contents

1. INTRODUCTION 6
2. DEFINITIONS 8
2.1. Agency 10
2.2. Agency Staff 10
2.3. Company 10
2.4. Custodian(s) 10
2.5. Evidence 10
2.6. Digital Forensics 10
2.7. Metadata 10
2.8. Offences 10
2.9. Mobile Device 10
2.10. Company Premises 11
2.11. Private Premises 11
2.12. Raid 11
2.13. Raid Authorization 11
3. TYPES OF RAIDS AND AUTHORIZATIONS 12
3.1. Raid Authorization 13
3.2. Responsibility for the Raid 14
4. RAIDS VS. OTHER INVESTIGATIVE TECHNIQUES 15
4.1. Investigation Strategy 15
4.1.1. Deciding Whether to Conduct a Raid 15
4.1.2. Raids in Conjunction with other Investigative Techniques 17
5. ORGANISING THE RAID 19
5.1. Pre-Raid Intelligence Gathering 19
5.1.1. Using Digital Tools 21
5.2. Raid Plan 22
5.2.1. Evidence Gathering Plan 22
5.2.2. Administrative Plan 23
5.3. Raid Team Composition 25
5.4. Role of the Team Leader 27
5.5. The Control Room 29
5.6. Raid Training 29
5.7. Code of Conduct 29
5.8. Pre-Raid Briefings 31
5.9. Safety of Agency Staff During the Raid 33
6. TIMING 35
6.1. Advance Notice 35

6.2. Sequential or Simultaneous Raids 35
6.3. Raid time limits 36
6.4. Duration of the Raid 38
7. COORDINATION WITH OTHER AGENCIES 39
7.1. Domestic Agencies 39
7.2. Foreign Agencies 39
7.2.1. Information Sharing 39
7.2.2. Coordination 41
8. ARRIVAL AT PREMISES 43
8.1. Entry and Identification 43
8.2. Presentation of the Raid Authorization 43
8.3. Requests to Delay the Raid 45
8.4. Obstacles to Entry 46
8.5. Securing the Premises 48
9. CONDUCTING THE RAID 49
9.1. Identifying and Locating the Relevant Evidence 49
9.1.1. Useful Resources 49
9.1.2. Raid Process 50
9.1.3. Scope of the Raid Authorization 51
9.1.4. Additional Considerations for Digital Evidence including Cloud-based Evidence 52
9.2. Documentation 54
9.2.1. Note Taking 54
9.2.2. Photographs and Videos 58
9.3. Special Considerations 58
9.3.1. Private Premises 59
9.3.2. Searching Vehicles 61
9.4. Arrests and Searches of Custodians 62
9.4.1. Requirements and General Considerations 62
9.4.2. Arrests of Custodians 63
9.5. Conducting Interviews to Gather Information or Evidence During the Raid 64
9.6. Evidence of Offences Not Covered by the Raid Authorization 65
9.7. Exiting the Premises 66
10. ALTERNATIVE STRATEGIES FOR RAIDS 67
10.1. When Agency Staff do not Know Where Evidence may be Located 67
10.2. Interviews of Witnesses at an Early Point in the Raid 67
10.3. Microsoft 365 Platform 'Hotspot' Searches 68
10.4. Other Options for Digital Searches 69
10.5. Collecting and Reviewing Material while the Agency's Investigators are On-Site 69
10.6. Remote Searching with the Microsoft 365 Platform 71

10.6.1. The Company Exports Data from the Microsoft 365 Platform to the Agency for Review 71
10.6.2. The Agency Exports Data from the Company for Review 71
11. OBSTRUCTION DURING THE RAID 73
11.1. What is Obstruction? 73
11.2. Necessary Cooperation 74
11.3. How to Minimize the Risk of Obstruction 74
11.4. What to Do in Cases of Obstruction 76
11.5. Consequences of Obstruction 76
12. LEGAL PRIVILEGE 78
12.1. Understanding the Relevant Legal Framework for Handling Legal Privilege Claims 78
12.2. Legal Privilege Considerations When Planning the Raid 79
12.3. Dealing with Legally Privileged Information During the Raid 80
12.3.1. Material Over Which Legal Privilege is Claimed Before the Raid 80
12.3.2. Material Over Which Legal Privilege is Waived 80
12.3.3. Assessing Whether Material is Legally Privileged During the Raid 80
12.3.4. Dealing With Disputed Material 81
12.3.5. Legal Privilege Claims Over Material Contained in a Larger Item 81
12.3.6. Keeping a Record of Potentially Privileged Material 82
12.3.7. Example of Practical Steps Agencies May Consider When Dealing with Legally Privileged Material 82
12.4. Legal Privilege Considerations After the Raid 84
12.5. Additional Legal Privilege Considerations for Digital Information 84
12.6. Illustrations 85
13. SEIZURE 87
13.1. Examination, Selection and Seizure 87
13.1.1. Examination and Selection 87
13.1.2. Seizure 87
13.2. Seize and Sift Powers 89
13.3. Handling Personal Data 89
13.3.1. Mobile Devices 90
13.4. Coding and Other Forms of Evidence Identification 91
13.5. Receipt for Seized Evidence 92
13.6. Continuity of Possession 93
13.7. Security of Evidence During Extended Raids 95
13.8. Providing Copies of Evidence 96
14. DEALING WITH COUNSEL TO PARTIES 98
15. DEALING WITH THE MEDIA 99
16. AFTER THE RAID 101
16.1. Transporting the Evidence Back to the Agency's Offices 101

16.2. Back at the Agency 101

1. INTRODUCTION

Raids are one of the most powerful tools in the fight against cartels. Raids are especially effective in situations where having an element of surprise is important for securing evidence and where other investigative tools could result in evidence being concealed, removed, or destroyed. However, raids are also costly and time consuming, and the decision to enter a private business or residential premises to search through records, seize them and take them away should not be exercised lightly.

Chapter 1- Raids is designed to help both experienced agencies and those with limited raid experience to make the most of raids, offering practical guidance and outlining good practices for planning and conducting the raid. This Chapter also highlights relevant legal issues and reflects the experiences and practices of International Competition Network (ICN) member agencies.

Chapter 1- Raids is intended to be a reference tool:

- To assist agencies in developing their own raid procedures;
- As a resource for agencies to evaluate, update and improve their existing raid policies and procedures; and
- As a training resource and it provides practical tips for this purpose.

The Chapter is intended to provide a useful resource for agencies across different jurisdictions. However, the relevance of some Sections will, to some degree, be determined by the legal and policy environment that governs an agency's enforcement practices. The appropriate choice of approach will depend on each agency's legal framework, resources and the case-specific circumstances.

The original version of this Chapter was based on a survey of ICN members conducted in 2004 and was last updated in 2009. This 2025 revision of Chapter 1- Raids provides new insights, including on digital evidence, and includes the following new sections:

- Coordination With Other Agencies (Section 7)
- Alternative Strategies for Raids (Section 10)
- Obstruction During the Raid (Section 11)

ICN Cartel Working Group (CWG) members and non-governmental advisors (NGAs) were consulted on the changes to this Chapter. The revisions to the Chapter were also informed by material from various international cartel conferences and workshops, including the CWG Back to Basics webinar series.[1]

Chapter 1 – Raids complements existing Chapters on leniency, digital evidence gathering, case initiation, investigative strategy and interviewing techniques and, in particular, should be read in conjunction with Chapter 3 of the Manual, which covers Digital Evidence Gathering in greater detail.

Each section of this chapter also includes suggested 'good practices' and a summary of these is set out in the box below.

[1] During January and February 2023, the CWG organized a series of in-depth webinars on the practicalities of conducting raids.

RAIDS VS. OTHER INVESTIGATIVE TECHNIQUES

It is good practice for agencies:

- ✓ To consider whether to conduct a raid taking into account the investigative tools available and the facts and circumstances of the investigation.

ORGANIZING THE RAID

It is good practice for agencies:

- ✓ To engage in comprehensive planning prior to conducting the raid;
- ✓ To prepare an evidence gathering strategy and update it as necessary;
- ✓ To prepare "search kits" ready-packed with stationery, seals and other necessities for team members;
- ✓ For members of the case team to participate in the raid, and for the team to be augmented with other officers and experts, as appropriate;
- ✓ To appoint a team leader at each premises raided who has overall responsibility for the raid at that premises;
- ✓ To offer training programs to agency staff involved in conducting raids;
- ✓ To be courteous and diplomatic throughout the raid; and
- ✓ To organize briefings for agency staff before conducting the raid.

TIMING

It is good practice for agencies:

- ✓ To conduct aids with the element of surprise; and
- ✓ Where more than one premises will be raided:
  - (i) To raid the premises simultaneously to minimize the risk of tip off and destruction of evidence; and
  - (ii) For each team leader to be in contact with the control room and/or the other team leaders to enable continuous coordination.

COORDINATION WITH OTHER AGENCIES

It is good practice for agencies:

- ✓ To communicate and coordinate with relevant foreign competition agencies, where appropriate. This should be done early in the investigation and on a regular basis. Where the agencies have the same leniency applicant(s), confidentiality waivers may assist in this.

ARRIVAL AT PREMISES

It is good practice for agencies:

- ✓ To preserve the element of surprise during entry by not disclosing your precise purpose (eg to a security guard or receptionist) until the raid authorization has been served;
- ✓ If acceding to a request to delay the raid, to first ensure that the premises have been adequately secured so the delay does not prejudice the outcome of the raid; and
- ✓ To secure the premises and take necessary steps as soon as possible in order to avoid the loss or destruction of evidence.

CONDUCTING THE RAID

It is good practice for agencies:

- ✓ To seize or request certain documents to help locate relevant evidence, such as, organizational charts, floor plans and inventories of company-issued devices;
- ✓ Where possible, to question individuals on-site to assist in locating documents, explaining document entries or acronyms, and providing access to locked safes or electronic devices, including cloud-stored documents;
- ✓ For the team leader to conduct an initial sweep of the premises and for searches to be conducted methodically;
- ✓ To ensure that the agency has sufficient digital forensics resources, such as skilled staff and equipment;
- ✓ Identify and secure any relevant mobile devices as soon as possible, to prevent damage and destruction of the digital evidence;
- ✓ To take notes of events as they happen at the premises;
- ✓ To take photos and video footage during raids to document the condition of the premises to counter claims of damage, to record the location of evidence to ensure due process and maintain chain of custody and capture the placement and condition of seals;
- ✓ To consider the nature of the premises being searched and ensure that the raid team is made up of appropriately trained and/or experienced personnel;
- ✓ To investigate whether key custodians work from home prior to the raid and, if so, obtain a raid authorization for their private premises, if possible, where relevant evidence is likely to be present;
- ✓ When it is likely that vehicles will contain relevant evidence, to gather information on the vehicles registered to a custodian and to ensure the raid authorization includes them, if possible;
- ✓ To search key areas in vehicles, such as, the glove box, dashboard, trunk, and other storage compartments. Navigation logs and toll payment records may also provide evidence of physical meetings between colluders;
- ✓ Where permitted, to ensure the raid authorization covers moveable objects such as briefcases, handbags, laptops and mobile devices;
- ✓ In jurisdictions where arrest of custodians is possible, to obtain authorization or cooperation from police to ensure due process of the arrest;
- ✓ To interview during the raid in individual cases and to assign a separate interviewing team;
- ✓ To make the interviewee aware of all possible legal protections to ensure due process;
- ✓ When evidence outside the scope of the authorization is discovered, to ask the custodian to submit the evidence voluntarily or to request additional authorization(s) immediately; and
- ✓ To dispose of all classified or sensitive information, return any passes or keys provided by the company, check the seized evidence against the evidence list and mark the time of exit when exiting the premises.

ALTERNATIVE STRATEGIES FOR RAIDS

It is good practice for agencies:

- ✓ When agencies are unable to identify in advance where evidence is likely to be found during a raid, to prepare alternative strategies which might enable them to identify where evidence might be found once they have arrived on a company's premises; and
- ✓ To keep these strategies under review as the forms of evidence change and to share successful new strategies with other agencies.

OBSTRUCTION DURING THE RAID

It is good practice for agencies:

- ✓ To ensure that the raid team has been trained to respond to obstruction including unauthorized removal, concealment or destruction of evidence.

LEGAL PRIVILEGE

It is good practice for agencies:

- ✓ To ensure that everyone involved in a raid is aware of the relevant legal framework recognizing legal privilege and the procedures for identifying and handling legally privileged material.

SEIZURE

It is good practice for agencies:

- ✓ To triage the evidence in order to ensure that only evidence relevant to the raid authorization is seized; and
- ✓ To ensure that evidence seized during the raid is coded or labelled to ensure that it can be identified and to preserve the chain of custody.

DEALING WITH COUNSEL TO PARTIES

It is good practice for agencies:

- ✓ To designate one person (for example, the team leader) to communicate with the parties' lawyers during the execution of the raid.

DEALING WITH THE MEDIA

It is good practice for agencies:

- ✓ To designate one spokesperson to respond to media enquiries; and
- ✓ To consider, before the raid is carried out, what the agency's press line should be in the event that the raid becomes public.

AFTER THE RAID

It is good practice for agencies:

- ✓ To deliver all seized documents to the agency's offices as soon as possible upon completion of the raid and to ensure all seized materials are secured in a facility with restricted and monitored access; and
- ✓ Where applicable, to consolidate all notes as soon as possible after the raid to create a complete record of the raid.

2. DEFINITIONS

2.1. Agency

A national competition or antitrust legal body with jurisdiction to enforce anti-cartel legislation. This is also often referred to as an NCA (national competition authority). The definition includes international competition authorities with comparable powers to national competition authorities.

2.2. Agency Staff

Agency personnel, including those responsible for carrying out the raid. This includes staff not directly employed by the agency but working under the supervision of the agency according to the applicable rules.

2.3. Company

The legal person which is the target of the raid. For the purposes of this Chapter, this should be understood as an overarching term which includes any association, business, firm or undertaking and should not be taken to refer to a specific legal or economic form.

2.4. Custodian(s)

Any individual(s) which the raid is targeting. For ease of reference, the term 'custodian' is used in this Chapter instead of 'individual', 'occupant', 'natural person' or 'target'.

2.5. Evidence

The material examined, copied or seized during the course of the raid. For ease of reference, the term 'evidence' is used as an overarching term in this Chapter instead of 'records', 'data', 'materials', or 'documents', except where these terms are specifically relevant.

2.6. Digital Forensics

The use of specialized techniques for the identification, preservation, extraction, authentication, examination, analysis, interpretation and documentation of digital information. Digital forensics also covers issues relating to the reconstruction of computer system usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Digital forensics require specialized expertise that generally goes beyond normal data collection and preservation techniques available to end-users or Information Technology (IT) system support personnel.

2.7. Metadata

Information about a particular data set or digital document, which describes for example how, when, and by whom the data set or digital document was collected, created, accessed, or modified.

2.8. Offences

The alleged breach of the law which is the subject of the raid. For the purposes of this Chapter, this term should be understood to include 'infringement'.

2.9. Mobile Device

This includes any portable electronic equipment, including smartphones and tablets. For ease of reference, the term 'mobile device' is used as an overarching term instead

of ‘smartphone’ or ‘smart device’. For the purpose of this Chapter, mobile device does not include laptops.

2.10. Company Premises

This refers to premises as the target of a raid whose predominant purpose is commercial. For example, offices, production facilities, or similar facilities where a company operates from.

2.11. Private Premises

This refers to premises whose predominant purpose is domestic or residential, but which are nonetheless the target of a raid. For example, as the workplace of a custodian. For ease of reference, the term ‘private premises’ is used in this Chapter instead of ‘domestic premises’ or ‘residential premises’.

2.12. Raid

For the purposes of this Chapter, the term ‘raid’ is used to describe any form of on-site investigation where the agency, police, or other designated enforcement body examines, copies and/or removes relevant paper and/or electronic evidence from a premises. For ease of reference, the term ‘raid’ is used throughout the Chapter instead of ‘search’ or ‘inspection’.

2.13. Raid Authorization

For the purposes of this Chapter, where raids are conducted under some type of advance authorization, the term ‘raid authorization’ is used to describe the order or documentary authority, such as a warrant, that provide this authorization. For ease of reference, the term ‘raid authorization’ is used throughout the Chapter instead of ‘warrant’, ‘inspection order’, or ‘inspection decision’.

3. TYPES OF RAIDS AND AUTHORIZATIONS

While many agencies around the world have the power to conduct raids, the extent of this power and the requirements to exercise it may vary in each jurisdiction. The table below sets out some of the raid powers and restrictions that apply in some jurisdictions and considerations that may be relevant for these different approaches.

<table>
<tr><th>Type of power</th><th>Description</th><th>Considerations</th></tr>
<tr><td>Wide powers to obtain evidence during raids</td><td>In some jurisdictions, the raid authorization confers wide powers on the agency. For example, it may allow them to seize or copy any relevant evidence found at the specified premises or to “seize and sift” (see Section 13.2 for more information).</td><td>Even where agencies are not restricted under their raid authorization or the scope of the investigation is drafted in broad terms, it is still important to plan for the raid appropriately to ensure that only relevant evidence is seized or copied.</td></tr>
<tr><td rowspan="2">Narrow powers to obtain evidence during raids</td><td>In some jurisdictions, there are limitations as to the types of sites that agencies are able to raid. For example, some agencies have the power to raid both company and private premises, while other agencies are only able to raid company premises.
In some jurisdictions, the power to raid premises also extends to raiding vehicles on the premises.</td><td>For considerations in relation to raiding sensitive areas, including private premises and vehicles, see Section 9.3.</td></tr>
<tr><td>In some jurisdictions, the power to obtain evidence during raids is circumscribed. For example, agency staff may be restricted to only seizing or copying specific documents or information mentioned in the raid authorization.</td><td rowspan="2">The planning of the raid and preparation of the raid authorization are particularly important in these situations. By carrying out an extensive and exhaustive pre-investigation, agencies may be able to pinpoint the evidence they need and thus increase the chance that the raid is successful in obtaining all relevant evidence.</td></tr>
<tr><td>Power to request evidence on-site but not search the premises themselves</td><td>In some jurisdictions, agencies have the power to visit the relevant premises and demand that evidence is produced but are not able to search the premises for evidence themselves.</td></tr>
<tr><td>Power to copy documents but not seize the originals</td><td>In some jurisdictions, agencies do not have the power to seize or remove any original evidence from the raid premises and must instead make copies.</td><td>Agencies should ensure that they have an appropriate strategy and equipment for making copies, such as high-speed scanners or tablets.</td></tr>
</table>

Type of power	Description	Considerations
External personnel conduct the raid	In some jurisdictions, agency staff do not have the power to carry out the raid and must instead work with another law enforcement agency or prosecutor's office.	Agencies should ensure that they carefully prepare the team responsible for conducting the raid as they may not be experienced or knowledgeable in relation to competition law.
Power to raid can only be used as a last resort	In some jurisdictions, agencies are only able to conduct a raid after they have exhausted other investigative tools and failed to obtain the relevant information.	Typically, losing the surprise element (which is fundamental to the success of a raid) may endanger the evidence. To prevent this, agencies could consider issuing orders to preserve the relevant evidence from the start of the investigation and using the threat of administrative or criminal sanctions to enforce these orders.
Company to be raided needs to be notified beforehand	In some jurisdictions, agencies must notify the company that they will be executing a raid prior to it commencing.	
No power to conduct raids	In some jurisdictions, agencies do not have the power to conduct raids.	Agencies may be able to use other powers to obtain evidence that is usually found on raids, such as requests for information. Where agencies do not have the power to seize evidence from private premises, guidance should be set out on how evidence would be obtained if not possible from company premises.

3.1. Raid Authorization

The authority enabling agencies to conduct a raid depends on the relevant law. The raid authorization might be issued by:

1. Another authority (for example, a judge or a court)
   - The legal threshold to obtain the authorization may be higher when it has to be issued by a judge or a court.
   - The agency may be required to "present its case" to a judge or a court.

or

2. The agency itself
   - For example, the head of the agency or a decision-making body within the agency, such as the board of directors.

Typically, a fairly high evidentiary standard is required to obtain a raid authorization, with the legal threshold varying by jurisdiction. For example, agencies may be required to demonstrate:

- "Reasonable suspicion" or "probable cause" that an offence has been or is about to be committed; and

- That on any premises to be raided, there is, or is likely to be, evidence or other things that will provide proof of the offence, infraction or contravention of the law.

Some agencies are also required to demonstrate that this evidence cannot be, or likely cannot be, obtained by other investigative means (a type of "needs" test).

In some jurisdictions, the legal threshold is higher when the agency plans to raid private premises (compared to company premises) or a third party that is not involved in the suspected cartel (compared to a party that is suspected to be involved). Meeting the legal thresholds required for a raid authorization may require in-depth pre-raid research and preparation. It is good practice for agencies to consider this in their pre-raid strategy and timing (see Sections 5 and 6).

Depending on the jurisdiction, it is important to consider whether the documents and information which support the raid authorization might have to be disclosed either during or at some point after the raid. Agencies may be able to limit this right of access if it would seriously jeopardize the investigation. In some instances, this can remain confidential if its disclosure would compromise the identity of a leniency applicant or confidential whistleblower. In some jurisdictions, these confidentiality protections will end when the investigation is complete and the case is brought to the stage of making a decision (for example, by a judge, a competition commission or the head of the agency).

3.2. Responsibility for the Raid

Agencies are usually responsible for conducting cartel-related raids. The responsibility for raids generally takes one of the following forms:

- The agency conducts the raid alone or, when the agency deems it necessary, with the assistance of police.

- In some jurisdictions that may conduct administrative and/or criminal raids, the agency can conduct administrative raids alone or, if necessary, with police assistance. Criminal raids are conducted by the federal or state police and the agency requests judicial authorization to participate and use the seized evidence in its administrative proceedings.

- A public prosecutor's office conducts the raid, either alone or with the participation of the agency. In some jurisdictions, the local, federal or national level agency (depending on the geographic scope of the cartel) conducts the raid, in conjunction with a public prosecutor's office (a cooperative arrangement).

- An independent investigative or law enforcement body conducts the raid with the agency being available to respond to questions from an off-site "control room".

- The Judge authorizing the raid exercises control over the raid and can inspect the raided location(s) as well as decide when to suspend or terminate the raid.

4. RAIDS VS. OTHER INVESTIGATIVE TECHNIQUES

Raids are a key tool for proving cartel conduct. Raids can be particularly effective in situations where having an element of surprise is important for securing evidence and where other investigative tools, such as document requests, may result in evidence being concealed, removed, or destroyed.[2] This Section sets out considerations for agencies in deciding their investigation strategy, including whether to conduct a raid or not.

4.1. Investigation Strategy

It is good practice to consider whether to conduct a raid taking into account the investigative tools available and the facts and circumstances of the investigation.

Agencies should consider creating an investigation strategy to determine the investigative and evidence gathering tools to be used during the investigation. This helps to ensure that the investigation is conducted efficiently and effectively. The investigation strategy outlines how the agency will achieve the investigation's goals and sets out the steps that the agency will follow to obtain the relevant evidence (including the investigative tools to be used). The strategy may need to evolve based on developments throughout the investigation.

It is good practice for agencies to consult internally with colleagues outside the case team when developing the investigation strategy to ensure that it is informed by a variety of perspectives, skillsets and experiences within the agency. Depending on the jurisdiction, the strategy may be approved by the department head or responsible officer for the investigation. Agencies may find it useful to utilize digital planning tools to design the strategy and track progress.

The strategy may be useful as a roadmap during the investigation as it sets out the tools to be used, the order for using them, and the resource and time requirements. This helps ensure that the investigation stays on track, even where agency personnel may change. The investigation strategy should also inform the agency's raid planning process, including a risk assessment.[3]

4.1.1. Deciding Whether to Conduct a Raid

The investigation strategy should consider and justify which investigative tool is most appropriate for the agency to use in the circumstances of the case. The following checklist of factors may be relevant to deciding whether to conduct a raid or use an alternative investigative tool.

[2] For more information on other investigative tools and the circumstances in which these may be most effective, see "ICN Recommended Practices for Investigative Process", available at: Introduction (internationalcompetitionnetwork.org), and " Chapter 5: Investigative strategy and interviewing Section I: Investigative strategy" available at: CWG_ACEM_Investigative_Strategy_CH5-2021.pdf (internationalcompetitionnetwork.org).

[3] For more guidance in relation to planning the raid, see Section 5.

Checklist	Comment	Consideration
Destruction, concealment or removal of evidence	Due to the element of surprise, raids may reduce the risk of important evidence being destroyed.	Does the agency consider it likely that evidence would be concealed, removed, tampered with or destroyed if it used other investigatory techniques to obtain the evidence? Conversely, does the agency consider that conducting a raid would likely prevent evidence from being destroyed, concealed, removed or tampered with?
Immediate access to documents	Raids can give agencies immediate access to key documents. Obtaining evidence by document requests may require longer timeframes. Timeliness may also be a consideration if there is an informant who feels under duress or who is expected to leave the company.	Does the agency consider it important to the investigation to have the evidence sooner?
Triaging documents	Document requests may result in the agency receiving huge volumes of evidence. Raids allow agencies to triage documents and ask questions, taking away only those documents which are useful to the investigation.	Does the agency consider it likely that a raid will allow more targeted collection of evidence compared to a document request or an alternative investigative tool?
Likelihood of relevant evidence being found at the premises	It is good practice for agencies to consider the types of evidence that are likely to be relevant and where these are likely to be located, to determine whether a raid or alternative investigative tool is likely to be most effective in obtaining the evidence. Pre-raid intelligence gathering may be useful in this (see Section 5.1 of this Chapter for further information).	Does the agency consider that relevant evidence is likely to be located at the target premises?
Costs	Raids can be resource intensive. Agencies should consider: • The costs of the raid • The costs of reviewing the evidence gathered during the raid • The costs of handling any potential legal privilege claims	Has the agency considered the total cost of the raid and the relative costs, benefits and risks (including the health and safety of agency staff) in carrying out a raid rather than using another investigative tool?

Checklist	Comment	Consideration
	In some cases, raids may save time and/or resources, for example, through providing faster access to critical evidence or through reducing the number of irrelevant documents received.	
Proportionality	Raids can be intrusive, resource intensive and place a burden on both the agency and the company and its employees (or individual(s), in the case of private premises).	What is the most appropriate investigative tool in the circumstances of the case, taking into account the risk of evidence being destroyed?
Digital evidence	Information storage and communications increasingly take place digitally, creating large digital datasets of potentially relevant information, including data stored in the cloud. In order to conduct a successful raid, it is important for agencies to have the legal and technological capability to review and store such information.	Does the agency have the capability and expertise to deal with the anticipated amount and type of digital evidence (including hardware, software and staff)? Does the agency consider that conducting a raid is likely to provide efficient and effective access to the digital data, including data stored in the cloud?
Cooperation	Conducting a raid sends a strong message about the agency's view of the seriousness of the investigation. This may increase companies' cooperation, including through prompting leniency applications.	Does the agency consider that conducting a raid is likely to increase companies' cooperation?
Specific and general deterrence	Conducting successful raids demonstrates that the agency is effective in investigating and prosecuting cartels and sends a message to the markets that may improve compliance and make leniency more attractive.	Has the agency carried out raids that demonstrate its ability to obtain evidence of the cartels it is investigating and delivered successful cases?

4.1.2. Raids in Conjunction with other Investigative Techniques

As part of their investigation strategy, agencies may also consider whether use of other investigative techniques, in conjunction with conducting a raid, may best facilitate the investigation. For example:

- In many jurisdictions, agencies can issue formal requests for information and/or interviews either during the raid or at a later stage of their investigation. Such requests for information or documents might be issued to the parties under investigation where there are no grounds to believe the information would be

destroyed or concealed, or to third party companies that are not suspected of having played a role in the cartel or of being loyal to the target companies or custodians.

- In some jurisdictions, agencies may conduct interviews at the raid premises (either on a voluntary or compulsory basis) and/or conduct simultaneous "drop-in" interviews of custodians in conjunction with the raid.[4]

[4] For more information see Section 9.5.

5. ORGANISING THE RAID

It is good practice to engage in comprehensive planning prior to conducting the raid.

Planning a raid involves many different elements (for example, identifying the premises to be raided, likely custodians, the type of evidence to be seized and the composition and responsibilities of the raid team) and can be time-consuming. It is important to allow sufficient time to complete the necessary planning steps to ensure that the raid runs smoothly and to maximize the opportunity to obtain relevant evidence.

This Section sets out several considerations which may assist agencies in planning and preparing for a raid.

5.1. Pre-Raid Intelligence Gathering

To assist in the planning process, agencies may find it helpful to conduct advance intelligence gathering, where legal and appropriate. If possible, agencies can rely on other law enforcement agencies to carry out this analysis, but they should work closely with them to ensure that no leaks occur. Pre-raid intelligence may be gathered in relation to the following areas:

Area of pre-raid research	Types of information to be gathered/considered
The premises	Premises location(s), including any time zone differences.
	Surroundings (including parking locations, hotels, transportation options and routes to the premises).
	Possible routes of entries.
	Maps or floorplans.
	Whether other companies share the premises with the targeted company, and if they have any relationship.
	Existence and nature of any security systems.
	How to secure the premises.
	History and outcome of any previous raids conducted at the premises.
The company	The IT system used, as well as the platforms and communication channels employees use (see Section 10 for more information).
	The company's working hours (to determine the best time to conduct the raid).
	Market sensitivity considerations.

Area of pre-raid research	Types of information to be gathered/considered
	The inner structure of the company.
	Expected level of cooperation, "style" of in-house and external-lawyers (e.g., shadowing by legal representatives).
Relevant evidence	Types of evidence likely to be seized or copied (including the likely types of digital evidence, such as emails, intranet and (social media) messaging channels, shared drives, local hard drives, mobile devices, portable computers, and cloud storage).
	Amount of evidence likely to be found, including the amount of digital evidence.
	If the premises has been raided before, in what part of the property was the evidence located, modus operandi displayed by the raided custodians.
Personnel, including custodians	Who the likely custodians of the evidence are.
	Whether employees work remotely or are likely to be on the company premises.
	How to prevent tip offs to absent employees, including those working remotely.
	If the premises was searched before, how did people react? Were attempts made to conceal or destroy evidence?
	The profile of the people likely to be on the premises, for example: • The presence of children, spouses, pets and vulnerable persons. • Any history of violence (including domestic violence) or anticipated resistance. • Criminal records checks. • Firearms registry consultations.
	Likelihood of external visitors and how to deal with them.
Risks, including legal considerations	Any risks and how these might be mitigated, including health and safety considerations.
	The level of likely media attention/interest (to inform the agency's media strategy).
	Legal privilege (and how legally privileged material will be dealt with). See also Section 12.
	How to deal with personal data? See also Section 13.3.
	Shadowing by the company's employees or legal representatives/external lawyers.

Agencies may utilize a range of investigative tools to gather this information, including:

- Physical reconnaissance of the premises.
- Use of cooperating parties or individuals, such as leniency applicants or informants, where appropriate.
- Collaboration with other entities, such as police, prosecutors or other agencies (this may be particularly relevant where the agency has limited local knowledge of, for example, the raid location, geography, or community sensitivities).
- Digital tools (see Section 5.1.1).

When conducting pre-raid research, agencies should take care not to tip-off the company or any key custodians to preserve the raid's element of surprise and minimize the risk that relevant evidence is hidden or deleted.

5.1.1. Using Digital Tools

There are several digital tools which agencies may be able to use in their pre-raid planning and intelligence gathering; for example, to assist in drafting the raid authorization and determining the raid targets without tipping off the company or key custodians.

Area of Planning	Source	Comment
Raid authorization (including address, legal name of the company or custodian(s), information about the corporate group)	Government databases	While the amount of available information may vary depending on the market, some government bodies collect information which may be useful. In bid-rigging cases, information regarding procurement processes may be available to consult in some jurisdictions. For example, documents detailing the procurement process may contain participants' addresses and the names of the representatives in charge of bidding.[5] Agencies may also be able to access other useful sources of government information, such as trademark, property, or utilities records. If such information is not publicly available, agencies may consider using legal tools to obtain it from other government bodies, including signing information sharing agreements with the relevant government bodies.
	Open-source intelligence	Depending on the legal powers available to an agency, and the level of tip-off risk, open-source intelligence may provide useful information about the targeted companies and custodians. For example, detailed information on publicly traded companies, directories of

[5] In some jurisdictions, procurement officials may also carry out on-site inspections of company premises. These reports may offer some insights regarding the size and internal distribution of offices.

Area of Planning	Source	Comment
		members, the type of software and technology used by a company or building plans.
Raid premises (location, surroundings, access points)	Online mapping tools	Where agencies are unable to physically survey the premises, agencies may be able to gather some information in relation to the premises' location, layout and surroundings through use of online mapping tools.
Individual custodians	Relationship mapping	Relationship mapping tools may help identify the key custodians. Using intelligence and other information gathered, relationship maps display known relations (for example, personal or professional connections and communications) between individuals involved in the suspected conduct, allowing agencies to better pinpoint key custodians.

When using the above digital tools, agencies should be careful to minimize the tip-off risk by using methods that will not connect the agency to the searches, such as use of anonymized IP addresses or VPN connections.

Agencies should be aware that, in some jurisdictions, certain forms of online reconnaissance can be considered surveillance and thus may require a separate and prior legal authorization.

5.2. Raid Plan

5.2.1. Evidence Gathering Plan

It is good practice to prepare an evidence gathering strategy and update it as necessary.

It is recommended that agencies have a clear and targeted evidence gathering strategy to ensure that all relevant materials are seized and that the agency does not seize a large amount of irrelevant evidence.[6] This could include:

- The aim and scope of the investigation.
- The evidence base (including consideration of any evidence the case team

[6] For more information about developing the evidence gathering strategy, including other tools which may also be used, see Chapter 5 of the Manual: "Investigative Strategy and Interviewing Section I: Investigative Strategy" available at: https://www.internationalcompetitionnetwork.org/portfolio/investigative-strategy/. For specific considerations in relation to digital evidence, see "Chapter 3: Digital Evidence Gathering" available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering/.

already has, what information they still require, what can only be obtained from the raid and what could be obtained through an alternative route).

- What form the evidence might take (including consideration of the type and amount of digital material).
- Who the likely custodians of the evidence are.
- Where the evidence is likely to be found (including whether the custodians are likely to be working remotely and whether the evidence is likely to be accessible to custodians of the raided company, even if stored on an external server).
- Alternative strategies for deciding where to look for the evidence (see Section 10).
- How the raid team will focus the investigation to ensure that the evidence collected is manageable (for example, ensuring that duplicate material is not collected).
- Timing (especially where it is necessary to obtain evidence from a number of sites simultaneously, see Section 6.2 for more information).
- Risks (including tip-off risks).
- Resources (including any specialised digital forensics or legal personnel).
- What to do if agency staff find evidence of criminal offenses unrelated to competition.
- Review strategy (including for legal privilege, see Section 12 for more information).

5.2.2. Administrative Plan

It is good practice to prepare "search kits" ready-packed with stationery, seals and other necessities for team members.

The raid plan should cover the administrative organization of the raid, including the operational and logistical requirements. The following considerations may be relevant:

Administrative need	Planning considerations
Budget and resources	• How many agency staff will be needed. • How many premises will be raided. • Whether raids will be executed simultaneously or sequentially. • The location of the premises. • The size and nature of the premises. • Whether it will be necessary to hire external forensic personnel to assist with the raid.
Health and Safety	• What are the health and safety risks of the raid? • Have they been assessed and what are the proposed mitigations?

Administrative need	Planning considerations
	• Are there any health requirements that team members should prepare for or consider, either due to the nature of the premises, the place where they are located, or the current context? For example, vaccinations, facemasks, gloves, etc.
Travelling to the raid site	How the raid team will travel to the raid site and any issues that this may raise (for example, if the raid team is flying, the raid strategy may need to take into account check-in times and baggage fees).
	How the raid team will travel from their accommodation and meeting point to the raid site. It may be appropriate to have ground transportation and drivers available 24/7, either to transport personnel or store the evidence collected in a safe location. It may not be appropriate to use personal means of transport and be preferable to use official vehicles or rental vehicles.
Accommodation	How long the raid is likely to take and whether accommodation is necessary. When choosing accommodation, agencies should consider distance from the premises and also the proximity of police stations, hospitals and safe zones. Hotel reservations should not be booked under the agency's name, since this might raise a tip-off risk that could endanger the raid.
Legal documents and authorizations	Agencies should ensure that all legal documents and authorizations, such as agency identifications and raid authorizations, are present and correct.
Training and briefings	All raid team members, including those assisting the agency, such as police or external IT experts, should receive appropriate training and briefings. For more information, see Sections 5.6 to 5.9.
Coordination with other public bodies	Agencies should consider the role of other public agencies and departments in their plan and ensure that any non-agency personnel are also aware of the raid protocol and strategy.
Equipment	All raid personnel should be supplied with the necessary equipment for their role and responsibilities.[7] This should be arranged sufficiently in advance of the raid and may include: • A notebook. • Stationery (such as markers, pens, elastic bands, paper clips, binder clips, post-it notes). • Folders, sealable bags or envelopes (for storing selected/seized evidence, depending on agency practice, including any special containers which the agency may use for legally privileged material). • Anti-static bags for electronic media.

[7] Agencies should consider how the equipment listed here will be obtained and allocated for transportation to ensure that the weight and responsibility is appropriately shared between raid team members.

Administrative need	Planning considerations
	• Evidence seals. • Seals for blocking access to doors or other information stores. • Suitable clothing, including gloves. • Trash/garbage bags and cleaning supplies. • Agency identification. • A copy of the raid authorization. • Agency electronic devices (such as laptops, mobile devices, wireless modems, radios, portable scanners, and digital forensics equipment,[8] where relevant), chargers, extension cords, adaptors, as well as regular tools such as screwdrivers and pincers. Devices should be equipped with the relevant, up to date software. • Cameras with photo and video capabilities. It is best not to rely on personal mobile devices. • Key contact details, including phone numbers for any coordinating staff at the agency and other raid team members. • First aid equipment and hand sanitizer. • Sufficient food and drink; and any personal medication. • Money for unexpected expenses, such as extra food or drink, parking, toll charges.

5.3. Raid Team Composition

It is good practice for members of the case team to participate in the raid, and for the team to be augmented with other officers and experts, as appropriate.

The following factors may be considered when deciding the composition of the raid team:

- The size, location and type (whether private or business) of the premises.
- The expected duration of the raid.
- The number of custodians (including how many of these are likely to be at the premises at the time of the raid).
- The number of individuals expected at the premises in total.

[8] For more information regarding forensic tools, see Chapter 3 of the Manual on "Management of Electronically Stored Information (ESI) in searches, raids and inspections", available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering

- The complexity of the case.
- The types of information being searched for and estimates of the volume of evidence likely to be found.
- The type and amount of digital evidence likely to be found and the number of digital devices to be searched, to determine what types of digital forensics expertise and tools are required to deal with this evidence.
- Language proficiency.
- The suspected role in the cartel of the company being raided.
- The anticipated degree of resistance by the premises' custodians.

Depending on these factors and agency practice, for each raided premises, the raid team may include the following:

Role	Responsibilities
Team Leader	The Team Leader has responsibility for conducting the raid at their premises. See Section 5.4 below for more information.
Key Evidence Retrieval staff	Agency staff who are tasked on immediate entry to a premises with locating key custodians and securing their work areas and any laptops or mobile devices that may contain important evidence.
Searcher	Searchers have responsibility for finding and seizing the evidence, including reviewing documents or files for relevant evidence. Members of the agency case team may be involved in the raid as searchers.
Search Coordinator (if needed, for instance, in complex investigations)	Coordinates the key words search for electronic data and the collection and preservation of evidence, keeps detailed records of the areas searched by the raid team, the custodians searched and the size of the data collected.
Note-taker	In some jurisdictions, the agency designates a specific note-taker with responsibility for completing the site log. See Section 9.2.1 for more information and approaches to note-taking.
Site Exhibit Officer	In some jurisdictions, the agency designates a specific site exhibit officer who is responsible for processing and recording the evidence seized, including for chain of custody purposes. For more information on Continuity of Possession see Section 13.6.
Police Officers	In some jurisdictions, police officers may assist during the raid. In particular, this may be the case where resistance is anticipated or arrests are necessary.
Lawyers	Some agencies may bring legal advisers onto the premises to provide advice or resolve legal disputes. In other agencies, legal advisers may be present in the control room. See Section 5.5 below for more information on the control room.
IT Experts, including Digital Forensics Experts	Agencies may find it useful to bring IT experts to the raid premises. For raids where agencies expect to find digital evidence, this may include digital forensics experts who are specially trained in

Role	Responsibilities
	handling and processing digital evidence. For more information in relation to digital forensics staff, see Chapter 3 of the Manual.[9]
Economists	Some agencies may bring economists to the raid premises or the control room to provide specialist advice.
Translators and Interpreters	Where language barriers are anticipated, agencies may find it useful to bring translators or interpreters to the raid premises.

Some agencies also find it helpful to have Floor Leaders or Assistant Team Leaders. This may be appropriate when searching large premises, for example, a multi-story office block, factory or warehouse where it can be difficult for a Team Leader to be in contact with all members of the raid team. The Floor Leaders are typically experienced agency staff.

Floor Leaders can help with:

- Communication between the Team Leader and raid team members. For example, by answering simple questions themselves thus allowing for serious or urgent matters to be prioritized.
- Interactions with company representatives that may be present at different locations in the premises.
- Ensuring procedures are being followed by the raid team.

Raid team sizes vary significantly across agencies and depending on the circumstances of the raid, ranging from a minimum of 2 agency staff to 20 or more officers participating in the raid. Agencies should ensure that the raid team is diverse and sufficiently large to conduct the raid expeditiously, but not so large as to make the process unwieldy. In some jurisdictions, agencies appoint external experts such as police officers or external digital forensics experts as authorized members of the agency for the purpose of the raid.

5.4. Role of the Team Leader

It is good practice to appoint a Team Leader at each premises raided who has overall responsibility for the raid at that premises.

Agencies may find it useful to appoint a Team Leader for each premises being raided. The Team Leader should be an experienced and fully trained individual. It may also be helpful for the Team Leader to be supported by a member of the case team who is familiar with the nature and scope of the investigation.

The Team Leader's responsibilities may include:

[9] ICN Anti-Cartel Enforcement Manual, "Chapter 3: Digital Evidence Gathering" available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering/.

Area	Responsibilities
Presenting the raid authorization and ensuring compliance	Ensuring compliance with all legal requirements and agency procedures, including: • Presenting the raid authorization to the company officials. • Explaining the raid procedures to the company officials and their counsel. • Dealing with any claims that the raid authorization is defective. • Ensuring that all staff carry and display appropriate identification.
Controlling the premises	• Ensuring that the premises are secured. • Monitoring and preventing obstruction.[10] • Monitoring and responding to any identified health and safety risks.
Coordinating the raid team (including external personnel and law enforcement)	• Designating the different raid areas and searchers' responsibilities. • Allocating team members' responsibilities. • Reassigning responsibilities during the raid where appropriate. • Prioritizing and selecting targets in real time and filtering important documents. • Coordinating with external personnel (for example, Digital Forensic Experts) and law enforcement.
Liaising with the company and their counsel	• Dealing with claims of legal privilege. • Answering any questions from the company. • Resolving disputes, for example in relation to the raid authorizations. • Bringing the agency's leniency policy to the company's attention.
Liaising with the agency	• Consulting with the agency in relation to any issues which may require an extension or alteration to the raid authorization (as such decisions require judicial confirmation in some jurisdictions). • Liaising with the agency's communication team in relation to any media inquiries. • In the case of multiple site raids, communicating with Team Leaders of the raid teams at other premises. • Communicating with the agency control room, where relevant. • Drafting or overseeing the raid report (including reporting any circumstances preventing the raid team from fulfilling its duties).

[10] See Section 11 of this Chapter for further information on obstruction.

In some jurisdictions, the Team Leader may participate in the search for relevant evidence. Team Leaders should ensure that, even when participating in the search, they also fulfil their core responsibilities, as set out in the table above.

5.5. The Control Room

Clear and effective communication is important for conducting a successful raid. Depending on agency policy and the specific circumstances of the raid, these communications may be conducted directly, by telephone or online, through the Team Leaders or through a central agency contact.

Where a raid involves multiple raid teams across different premises, agencies may find it helpful to liaise with a central point back in the agency's offices. An off-site "control room" may be established for this purpose. It can be helpful for the control room to be staffed by lead agency staff with a good overview of the case and the premises being raided. The control room's responsibilities may include:

- Gathering progress reports and coordinating between the different premises, including passing relevant information between the raid teams.
- Providing advice and information, where relevant, such as expert legal or economic analysis.
- Assisting with tasks, for example applying for or drafting additional raid authorizations.

5.6. Raid Training

It is good practice to offer training programs to agency staff involved in conducting raids.

Agencies should provide ongoing training sessions for agency staff on the practical issues of conducting raids, for example on how to follow the agency's protocols (such as the agency's notetaking and document coding procedures).

Agencies should also consider profession or role specific training, for example concerning leading raid teams and digital forensics, where that may be helpful.

Delivering or refreshing training prior to a raid can be especially beneficial where agency staff are new or inexperienced or where raids are infrequent.

This Chapter may be an effective training tool for this purpose.

5.7. Code of Conduct

It is good practice to be courteous and diplomatic throughout the raid.

Raids may generate tension between the agency staff executing the raid and the company. If this tension escalates the raid may be derailed. Therefore, it is

recommended that agency staff adhere to a code of conduct to help avoid unnecessary confrontations as well as ensuring that the company or any key custodians are not tipped off. This preserves the raid's element of surprise and minimizes the risk that relevant evidence is hidden or deleted.

Agencies may want to consider the following guidelines when establishing their code of conduct.

Consideration	Comment
Before the raid	Agency staff should refrain from discussing the raid, especially in public or while traveling to the premises, to avoid leaks.
	Agency staff should adhere to the pre-agreed dress code. It may be appropriate for agency staff to wear formal, yet comfortable clothing. However, depending on the nature of the target premises, it may be necessary to change the dress code. For example, due to safety regulations, agency staff may be required by law to wear certain footwear in a factory and may be legally prevented from entering the premises if they do not adhere to these requirements.
	If agency staff are staying in a hotel during the raid, instructions from the raid Team Leader should be followed at all times. This may include whether they are allowed to leave their room before and after the raid, meeting points and food options. Agency staff must follow these rules to preserve the secrecy of the raid and the integrity of the evidence taken during the raid.
During the raid	Agency staff should adhere to their pre-agreed tasks and responsibilities for their respective role. Important decisions and matters should be communicated to the company's representatives and their lawyers only by the Team Leader to avoid conflicts or confusion.
	If agency staff are approached by the company's representatives or their lawyers, they should politely decline to comment and redirect them to the raid Team Leader. Team members should promptly inform their Team Leader what they have been asked or told.
	Agency staff should be assertive but courteous, not rude or aggressive. Disruptions to the company's work should be minimized as much as possible.
	Agency staff should take care when discussing the raid as they may be overheard or recorded. Sensitive or confidential topics should be avoided during the raid.
	Agency staff should avoid expressing excitement or surprise when they come across important evidence or a 'smoking gun'. Agency staff should also avoid reacting when coming across personal material that could be embarrassing for a company representative.
	Agency staff should follow the raid Team Leader's instructions, including in relation to moving within the premises, mealtimes and restroom use. It may not be recommended to accept lunch to avoid raising a potential conflict-of-interest risk.
	Agency staff should remain in contact with the raid Team Leader, updating them on progress made and notifying them if any issues are encountered.
	If appropriate, agency staff should identify themselves when requested. Some agencies prepare an official identification document (ID) for this purpose. Staff should not identify

Consideration	Comment
	themselves with IDs that contain personal and private data, such as birth dates or home addresses.
	If agency staff are threatened by the company's representatives, or face any danger, the raid Team Leader should be notified immediately.
	Raids can take up a significant amount of time. Agency staff should prepare accordingly and ensure that they are eating, rehydrating and resting when necessary.
After the raid	After the raid concludes, and to the extent possible, agency staff should leave the premises in their original state.
Miscellaneous	

5.8. Pre-Raid Briefings

It is good practice to organize briefings for agency staff before conducting the raid.

Agencies are recommended to hold briefing sessions before conducting the raid. Agencies may consider whether it is useful for the written briefing to be made available to agency staff before the oral briefing. The benefits of this approach include:

- Agency staff have the opportunity to familiarize themselves with an overview of the alleged conduct, the companies or custodians involved and the classes of items to be searched for prior to the oral briefing.
- Agency staff can ask questions to clarify any ambiguities at the oral briefing.

However, making the written briefing available prior to the oral briefing may increase the risk of strategic documents or information being accidentally disclosed or leaked, and may divert attendees' attention away from the oral briefing.

It may also be helpful for agencies to hold briefings for individual teams or roles within a team to address particular issues or questions that may arise at each specific site to be raided. Agencies may consider holding the following briefings:

Briefing	**Considerations**
General briefing for the whole team	General briefings may include: • Information in relation to the case and its scope, including the conduct, premises and companies. • Training on digital forensics where agency staff are likely to encounter digital evidence. • Details of coding procedures for agency staff handling the evidence. • Health and safety risk assessment and proposed mitigations
Briefing for site Team Leaders	Briefings for site Team Leaders may include: • Specific strategy to follow and relevant information about the targets. • Contacts and procedures to follow in case of an emergency.

Briefing	Considerations
Briefing for digital forensics/IT experts	Briefings for digital forensics/IT experts may include: • Volume of digital evidence expected. • Likely number of relevant devices. • Likely key custodians. • Intelligence on computer systems/cloud/etc.
Site specific briefings	Site specific briefings may include: • Logistics in relation to the premises, including any premises-specific risk factors. • Details in relation to the premises' occupier. • Details of relevant custodians likely to be onsite.
Dynamic briefings	Dynamic briefings may be held where circumstances change or evolve during the raid, such as: • Dealing with obstruction.[11] • Identification of additional custodians. • Identification of new or unforeseen hazards or risk factors.

The outcome of a raid may depend on the element of surprise. Thus, agencies are advised to carefully consider attendees and timing of the briefing sessions and briefing packages to prevent accidental disclosure.

The content of pre-raid briefings will be specific to the characteristics of the raid in question. Topics to cover during pre-raid briefings may include the following:

Consideration	Comment
Team-related	• The composition of the team(s) and Team Leader. • Lines of authority and communication. • The overall raid strategy and the procedure to follow. • The role/assignments for each team member.
Conduct-related	• An overview of the alleged conduct/case/offence. • Time-frame and geographic location. • The names and descriptions of companies and key custodians allegedly involved in the cartel. • The type(s) of evidence sought. • A list of keywords, phrases and/or dates for electronic and paper document searches.

[11] See Section 11 for further information on obstruction during the raid.

Consideration	Comment
Logistical	• Logistical issues, such as day and time of the raid, rendezvous point, and important mobile phone numbers. • Any occupational health and safety risks. • A description or map of the location of the premises to be searched and the layout of the premises. • Any instructions for dealing with the media.

Agencies should consider the confidentiality of pre-raid briefing documents during the raid. It may be decided to prohibit agency staff from bringing briefing documents to the premises to minimize risk of disclosure to the company. Agencies may also consider using further confidentiality safeguards, such as assigning unique codes to each briefing document and ensuring that they are returned to the Team Leader following the conclusion of the raid.

5.9. Safety of Agency Staff During the Raid

Agency staff may encounter challenges during the raid. Most risks to the safety of agency staff can be mitigated through careful planning and preparation. Agencies should put in place protocols to guarantee the safety of agency staff, covering at least the following.

Consideration	Comment
Emergency contact	Provide a list of emergency telephone numbers to agency staff.
Pre-raid training and preparation	• Train all agency staff conducting the raid on how to respond to an emergency. • Agree on certain signs or signals to indicate a risk and prepare agency staff on what to do if this signal or sign is used. • Pack safety equipment in the raid kit, including masks, gloves and coveralls (see Section 5.2.2 for further information). • Implement an appropriate dress code for agency staff.
Premises	• Gather intelligence on the premises to be raided prior to the raid. Map out entrances and exits and account for any danger points (See Sections 5.1 and 5.1.1 for more information). • Gather intelligence on nearby hospitals, police stations, restaurants and pharmacies.
Travelling to the raid premises	Agencies are advised to consider the following in advance of travelling to the premises: • Plan the route to the premises in advance and agree on an exit strategy in case of an emergency. Plan for additional travel charges, including toll roads and unexpected expenses in case of an emergency.

Consideration	Comment
	• If necessary, coordinate with local police to organize an escort to the premises. This may be appropriate if the safety of agency staff cannot otherwise be guaranteed. Local police may require a written request, which should be prepared in advance.

6. TIMING

It is good practice to conduct raids with the element of surprise.

Timing is a key consideration when planning a raid.

6.1. Advance Notice

In most jurisdictions, agencies have no obligation to, and do not, give advance notice to the companies before conducting the raid. This is because the unexpected nature of the raid is of primary importance to avoid destruction, removal, concealment, or tampering with evidence. When raids will be conducted in multiple jurisdictions, it is good practice for agencies to be aware of whether advance notice is required in the other jurisdictions. This can be accounted for when planning the timing of the raid to preserve the element of surprise.

6.2. Sequential or Simultaneous Raids

Where more than one premises will be raided it is good practice (i) to raid the premises simultaneously to minimize the risk of tip off and destruction of evidence; and (ii) for each Team Leader to be in contact with the control room and/or the other Team Leaders to enable continuous coordination.

When more than one premises will be raided, it is good practice to raid the premises simultaneously to minimize the potential for destruction of evidence (See Section 7 for information on coordinating raids with counterparts in other jurisdictions). Where resources are limited and the premises to be raided are small, simultaneous raids may be achieved by deploying smaller raid teams and/or sharing resources across raid teams. These smaller teams can focus on securing the premises and computer systems and begin searching high priority areas until additional agency staff are able to join them from other premises. Agencies should prioritize sharing resources across premises which are geographically close to one another, allowing staff to be easily redeployed as needed.

If simultaneous raids are not possible due to limited resources, sequential raids may be conducted instead, giving priority to the locations most important to the investigation. For example, key targets, such as the alleged leaders, instigators or coordinators of the cartel should be prioritized.

It can be useful in such cases to seal relevant parts of the premises until they can be searched (see Section 6.3 below). Some agencies can take additional measures to preserve evidence. For example, in some jurisdictions, when a company is aware that the competition agency is investigating, the agency may ask the company to issue

"litigation hold" notices to its employees to ensure that relevant documents are preserved until the agency can conduct the raid.[12]

Agencies may also need to conduct sequential raids when they learn that there is evidence at a new location (e.g., based on their raid at one premises). This may require the agency to obtain an updated or additional raid authorization (see Section 3).

When premises are raided simultaneously, it is good practice to appoint a central coordinator who remains at the agency to perform the tasks described in Section 5.5.

Example 1 – Preserving Evidence

Agencies may be able to obtain a Preservation Order requiring third parties (e.g., cloud providers) to preserve computer data in case agency staff are not able to access the cloud from the raid premises.

6.3. Raid time limits

Raid time limits differ across agencies. Some agencies are limited to raiding during specific hours while other agencies are not. For example, some agencies are restricted to raiding during normal business hours and/or working days, which may depend on the terms of the raid authorization. In some cases, it may be possible to continue the raid beyond these time limits if authorized by the court. Agencies should be aware of the applicable laws and practice regarding raid time limits and plan accordingly.

If agencies have the option to continue a raid beyond regular business hours, it can be useful for them to consider the proportionality and necessity of doing so. For example, whether there is a danger of evidence destruction or obstruction if the agency leaves the premises and returns the next day, as well as the agency's ability to complete the raid within the duration stipulated in the authorization. This may be informed by factors including the size of the premises to be raided and the size of the raid team. The decision on whether to search beyond the regular working hours of the company (if possible) should be revisited as the raid progresses, including consideration of what the team has found on site, the availability of agency staff, the cooperation by the company, and what is left to be searched on the premises.

It is good practice for the agency to advise the company at the beginning of the raid that the raid may extend beyond regular business hours and/or may last for several days (or, in some cases, weeks). Some agencies include such provisions in the raid authorization and highlight them to the company representatives at the beginning of the raid. This helps to manage the expectations of the company's representatives, allows them to rearrange their schedules if necessary and can help to avoid conflicts. Some agencies may be able to continue copying electronic data after the prescribed raid hours and the agency staff have left the premises for the day (for example, overnight).

If an agency decides to pause a raid, such as overnight, it is good practice to seal the relevant areas of the premises until the raid is resumed (in addition to possible

[12] Generally, a litigation hold notice instructs employees to preserve paper and electronic evidence that may be relevant to a legal action involving the company. Certain cloud-based platforms have features to implement litigation holds (e.g., Microsoft Purview in the Microsoft365 platform).

litigation hold notices or preservation orders mentioned in Section 6.2), This could include:

- Sealing any offices, cabinets or other areas that have not yet been searched and that the raid team plans to search.
- Sealing evidence that has already been selected or seized and securing it in a locked container in the raid team's workspace on the premises.[13]
- Sealing the raid team's workspace.
- Taking notes of where they placed seals (which offices, areas, cabinets, etc.) and the date and time that the seals were placed.
- Taking photographs of the places being sealed and creating an inventory.
- Placing signs near the seals warning against breaking any seals and the consequences for doing so.
- Advising the person in charge at the premises of the consequences of breaking any seals and that they should advise their employees accordingly (for more detail, see Section 11). It may be necessary for the company official to advise cleaning staff not to enter the raid premises (or relevant areas of the premises) during the raid to avoid breaking seals.
- Employing security guards to ensure the seals remain intact or recommending that the company does so.

To eliminate any disputes in relation to the agency's return, agencies may also consider seeking oral and written confirmation from the company that the raid is not concluded, prior to exiting.

Upon re-entering the premises, agency staff should verify the condition of the seals they placed upon leaving, unseal as necessary and take notes of this. If photographs were taken, agency staff can use them to verify that everything is in the exact same place as it was when they left the day before.

It should be noted that pausing a raid is not an option for all agencies, as in some jurisdictions the agency can only gain entry to the premises once.

There are additional considerations when raiding private premises. Custodians frequently work from home at least part of the time. This can make it more challenging to determine the ideal start time for simultaneous raids (for example, to ensure that the raid does not start while a key target is in transit between their workplace and home, thus providing an opportunity to destroy evidence). When raiding private premises, some agencies prefer to start the raid early in the morning to ensure that the custodian will be there. However, to comply with the principle of proportionality and to avoid intrusion into a custodian's private and family life, agencies may want to arrange a start time that will minimize the intrusion on other family members living at the home (for example, starting the raid after any children have left for school). In addition, some agencies cannot stay at private premises for as long as they can stay at a company's premises.[14] When planning the raid, it is good practice to determine if custodians work

[13] Some agencies may have the option to temporarily remove evidence from the premises overnight before they are officially seized.
[14] See Section 9.3.1 for further considerations in relation to raiding private premises.

from home and the typical days and hours for this (e.g., through surveillance,[15] cooperating parties, etc.).[16]

6.4. Duration of the Raid

Raid time limitations vary according to the jurisdiction. Some agencies have no limitations on the amount of time they can spend conducting a raid and are therefore able to remain on the premises until the raid is complete and all available evidence has been located. In some jurisdictions, the duration of the raid may be as long as is reasonably necessary and the length of time must be proportional to the goal of the raid. In some jurisdictions, the agency can only gain entry once.

In a number of jurisdictions, the raid authorization specifies the maximum number of days allowed for the raid, which depends on the particular circumstances. Factors that affect the length of time needed to execute the raid include:

- The size of the premises.
- The number of employees and custodians who work at the premises.
- The type/size of computer systems believed to be on the premises.
- Whether the agency plans to review electronic evidence on the premises.
- The anticipated quantity of paper evidence (this is impacted by the duration of the alleged offence, number of bids or products involved, etc.).
- Whether the premises is a business or private residence; and
- The duration authorized for the agency's raids.

These factors should be taken into account in the planning stage (see Section 5.2). It is a good idea for agencies to start the raid on the first day they are permitted to do so under the raid authorization (unless special circumstances necessitate a delay, such as coordinating the raid with the enforcement action of international counterparts). This will allow the agency to have the maximum amount of time to address any unexpected situations, such as discovering a huge volume of evidence or data that is difficult to access. Subject to pre-raid intelligence on the working habits of the company, there are benefits to starting the raid on the second or third day of the work week (Tuesday or Wednesday in most jurisdictions). This allows for one day to finalize any last-minute details, while ensuring sufficient time to finish the raid before the weekend.

[15] Some agencies may require authorization to conduct surveillance of custodians.
[16] See Section 5 for more information in relation to planning the raid and conducting pre-raid intelligence.

7. COORDINATION WITH OTHER AGENCIES

It is good practice, where appropriate, to communicate and coordinate with relevant foreign competition agencies. This should be done early in the investigation and on a regular basis. Where the agencies have the same leniency applicant(s), confidentiality waivers may assist in this.

7.1. Domestic Agencies

As described in Section 5.9, in some jurisdictions, agency staff are accompanied by police officers during raids for security reasons. In addition, some agencies may augment their raid teams with personnel from local police or other domestic government agencies with experience in conducting raids. In such cases, it is important that the assisting agencies are fully briefed in advance and the roles of each are clearly understood (some competition agencies outline this in formal protocols with other domestic agencies). It is good practice to plan in advance how the assisting agencies will provide any deliverables after the raid, such as debriefs, statements or notes so that they are not forgotten. Agencies should also plan how the evidence will be stored at the end of the raid (e.g., if it will be stored at the local police station).

The competition agency may need to be flexible in the event that the assisting agencies become unavailable due to other urgent priorities.[17] Agencies should confirm the assisting agencies' availability the day before the raid to allow sufficient time to develop an alternative plan if necessary.

Other forms of cooperation can include coordinating raids with domestic authorities who are conducting their own raids (for example, domestic tax authorities, consumer authorities, sectoral regulators or anti-corruption agencies). Some competition agencies may even conduct joint raids with another domestic agency, for example when a premises is considered dangerous. This cooperation will require additional planning, such as determining whether the participating agencies are all entitled to the same evidence and how and where the relevant evidence will be available to each agency after the raid.

7.2. Foreign Agencies

7.2.1. Information Sharing

Where appropriate, agencies may share information with foreign agencies investigating the same cross-border cartel. For example, when an international cartel investigation involves a leniency applicant, it is good practice for the agency to identify the other agencies involved by asking the applicant to list the other jurisdictions in which it has applied for leniency, or if it is aware of an investigation in any other jurisdiction. Where

[17] For more guidance in relation to coordinating with other domestic agencies, see Section 6 of the Cartel Working Group's 'Guidance on Enhancing Cross-Border Leniency Cooperation'.

other leniency applications have been made, a full waiver[18] should be sought from the applicant to share information with other relevant competition agencies, as appropriate. Early contact with other jurisdictions where a leniency applicant has also applied for leniency can be fruitful, result in efficiency gains, and enhance coordination at later stages of an investigation. Agencies should consider on a case-by-case basis whether coordination with a specific jurisdiction is likely to be beneficial and whether the timing is right to initiate contact, in light of applicable laws in their jurisdiction and agency priorities.[19]

Discussions between jurisdictions at the beginning of an investigation can help agencies to do the following (among other things):

- Determine the potential scope and timing for cooperation.
- Better align investigative timing and investigative steps.
- Avoid tip-off risk during the covert stage of an investigation.
- Discuss possible investigative opportunities in the covert stage of an investigation.
- Coordinate approaches to communications, including on press notices and whether the parties will be named.

Information sharing may be facilitated between agencies by means of:

- Informal information sharing.
- Regional networks.
- Cooperation agreements, arrangements or memoranda of understanding.
- International treaties.
- Formal legal requests.
- Waivers.

Information sharing may be limited to general information or, in certain circumstances, may include confidential information, for example, in cases where two agencies have the same leniency applicant, and the leniency applicant has provided the agencies with waivers of confidentiality. The exchange of confidential information is subject to applicable policies, laws and cooperation agreements and should only occur if doing so would not jeopardize the investigation.

---

[18] A waiver of confidentiality is consent from a leniency applicant to waive, within the limits set out in the consent, the confidentiality protections afforded to it in the jurisdiction of the investigating competition agency. The waiver mechanism allows leniency applicants to stipulate with which jurisdictions they are willing to allow the agency to share the information and the extent to which the information is shared. Full waivers are more useful as they allow more fulsome information sharing. **Full** waivers allow competition agencies to coordinate on the procedural aspects of an investigation as well as exchange information on the substance of a leniency applicant's submission. **Procedural** waivers only allow competition agencies to coordinate on the procedural aspects of a cartel investigation. For more detail, see: ICN Cartel Working Group, Waivers of Confidentiality in Cartel Investigations.

[19] The laws and policies within various jurisdictions may impact on a competition agency's ability to coordinate, even after the provision of signed confidentiality waivers.

7.2.2. Coordination

As outlined in Guidance on Enhancing Cross-Border Leniency Cooperation, before sharing information or coordinating the timing of the use of formal powers with a foreign agency, agencies may consider the following:

- Whether it is necessary or beneficial to coordinate. For example, whether the alleged conduct has sufficient similarities and/or jurisdictional overlap.
- The agency's ability to share information with a foreign agency is based on several factors, such as the agency's legal framework, applicable policies, cooperation agreement and the receipt of waivers from the leniency applicant.
- The stages of the respective investigations. If agencies do not communicate or coordinate their investigative steps, there is a potential for negative consequences when investigations are at different stages, such as tip-off risk.
- The focus of other jurisdictions, the evidence that has already been obtained and the evidence that is still required. This will enable jurisdictions to better target and coordinate covert investigative steps. It can reduce duplication of effort and result in efficiencies.
- Scope of raids, including:
    - The investigated conduct, the likely period of the potential offence, the companies involved.
    - The geographical scope of the conduct: In what jurisdiction or jurisdictions has the conduct taken place? How to allocate teams to maximize impact?
    - The location of targets where evidence is most likely to be found: considerations concerning the different locations (headquarters/main production sites/main office buildings).
    - Discussions on the names and the likely location of custodians and their offices, considerations of whether to raid private premises.
    - Considerations to focus on specific electronic devices, for example, mobile devices, or other types of evidence.
- Timing of raids (or other investigative measures): different time zones need to be taken into account.
- Regular exchanges are needed and on a strictly need-to-know basis to prevent tipping off.

Where a cartel involves conduct across international borders, it is good practice to communicate and coordinate the timing of raids and other steps that take the investigation into the overt stage, when possible, in order to minimize the risk of destruction of evidence. This may include delaying or expediting a raid in order to coordinate timing with a foreign agency, especially where essential evidence of the cartel is likely to be found in the territory of the requesting agency. In deciding whether to delay a raid, agencies should balance the benefits of cooperation with the risks of delaying the raid (for example, the risk of destruction of evidence and any implications on personnel, costs and logistics).

Where domestic legislation allows (see Sections 3.2.1 and 3.2.4 of Guidance on Enhancing Cross-Border Leniency Cooperation), an agency may also request another jurisdiction to obtain evidence on its behalf. Each jurisdiction has its own rules for how

formal requests for assistance can be initiated. Agencies should work cooperatively to navigate the often-complex official requirements.

Coordination does not need to be limited to simultaneous raids in different jurisdictions but can involve coordinating the use of other formal powers (for example, statutory notices compelling companies to supply documents or information), witness interviews or measures seeking to preserve evidence in other jurisdictions on the same day that raids are conducted in other countries.

It is good practice to continue cooperation with foreign agencies after any raids have been conducted. This could include providing notifications of key case events, discussions of evidence, further investigative steps and the approach to the calculation of fines.

8. ARRIVAL AT PREMISES

8.1. Entry and Identification

It is good practice to preserve the element of surprise during entry by not disclosing your precise purpose (eg to a security guard or receptionist) until the raid authorization has been served

All agency staff involved in raids must be aware of and follow applicable laws and practices regarding entry and identification. Identification requirements vary across jurisdictions. At some agencies, staff are required to carry and display appropriate identification at all times during a raid, which may include wearing jackets with the agency's name written on the back. In some jurisdictions, agency staff are only required to identify themselves upon request of the company. Some agencies try to be discreet and limit knowledge of the raid to only the necessary company employees to avoid alarming other employees or alerting the media or people passing by about the raid.

Some agencies ensure that raid team members have at least two pieces of identification with only a photograph and the employee's name (i.e., no personal information, such as address). This can be used in the event that agency staff are required by law to leave their identification at a central location at the start of the raid (then they have a second piece of identification to show as needed during the raid).

Agencies working with police should decide ahead of time if the police will enter the premises first or at the same time as agency staff, and the steps each team will follow upon entering. As set out in Section 6.2, entry is usually made simultaneously at all raid premises to minimize the risk of co-conspirators informing each other of the raid. It may be more practical for only a portion of the agency staff to enter the premises first (for example, the raid Team Leader, a designated note-taker, a digital forensics expert and a representative of any accompanying police force). The rest of the team can wait for instructions from the raid Team Leader before entering the site. This should be determined in advance.

To avoid revealing the nature of the raid before the raid authorization has been served, in some jurisdictions, the raid Team Leader will identify themself as a government official and ask to speak to someone responsible for the premises, without disclosing their precise purpose for example to a security guard or receptionist (subject to who the raid authorization may be presented to, as described in Section 8.2). However, in some instances, raid Team Leaders may need to provide more details to the receptionist due to company policies governing access to the premises. It is good practice to devise the strategy for this in advance.

8.2. Presentation of the Raid Authorization

The procedure for presenting the raid authorization differs across agencies. Many agencies are required to present the raid authorization to a senior company official (for example, the highest-level manager available, an official authorized to receive official documents on behalf of the company, or an individual in charge of the premises), while in other jurisdictions the authorization must be presented to the company's legal representative. If the required official is not at the raid premises, the raid Team Leader should ensure that they are on their way or request that they be contacted and asked to come to the premises immediately. The raid Team Leader may consider delaying the

start of the raid until that person arrives, if the delay will be minimal and there is no risk that evidence will be destroyed (see Section 8.3).

Some agencies are not required to present the raid authorization to a particular company representative; however, when raiding private premises, they must show the court order to the owner or inhabitant of the house. Agencies should be aware of and follow applicable laws and practice regarding the presentation of the raid authorization.

In some jurisdictions, agencies may carry out a raid in the absence of the occupier or owner of the premises but must leave a notice in a prominent place at the premises stating the date and time the raid authorization was executed, the name of the person who executed the authorization and the fact that evidence was removed from the premises. Agencies should be aware of applicable laws and practices regarding carrying out the raid in the absence of the occupier or owner of the premises.

It is good practice for the Team Leader to serve the raid authorization on the appropriate company representative in a private place, accompanied by a designated note-taker (see Section 9.2.1). The Team Leader should:

- Show the raid authorization to the company representative.

- Explain the authority of the authorization, the duties of the person in control of the premises and the raid process.

- Provide a warning against obstruction as well as explaining the consequences of obstruction (see Section 11).

  Advise the company representative to instruct their employees not to delete, destroy, alter or remove evidence (in some jurisdictions, the agency approves the wording). The Team Leader should also explain that the company could be liable for such actions by their employees.[20]

Agencies may also consider advising the company representative that they may contact legal counsel and explain how the raid team will handle any claims that evidence is protected by legal privilege (see Section 12). Generally, agency staff will not provide additional information beyond the details set out in the raid authorization, but they may explain procedural matters. It is good practice for the raid Team Leader to consult a prepared checklist while serving the authorization to ensure that everything is covered. Some jurisdictions provide general explanatory notes on raids to company representative(s) at the start of every raid. Some provide additional documents outlining the law and the raided parties' rights.

In some jurisdictions, the original raid authorization must remain on the raid premises and should be produced when requested. In others, the company receives a certified copy of the authorization.

The raid Team Leader should determine whether the premises should be secured at the same time as the authorization is being served or if it can be done as soon as the authorization has been served. This will depend on the laws in the jurisdiction (e.g., in

[20] Agencies should be aware that sometimes the interests of employee(s) and the company may be different (e.g., the company may want to cooperate with the raid in order to limit any negative consequences as much as possible while a custodian could be tempted to destroy documents in order to reduce their own risk of sanctions or disciplinary action by the company).

some jurisdictions, the premises cannot be secured until the raid authorization has been served). See Section 8.5 for more detail on securing the premises.

It is good practice for agencies to introduce the other agency staff members to the company representative(s) and make arrangements with the person in charge to have an area, a vacant office or a conference room to use as a work area for agency staff (a private, "sealable" space). The raid Team Leader may also ask for a pass/key to the building/floor/washroom as needed to ensure agency staff can enter and exit as necessary, though the company representative may prefer to accompany agency staff. At this stage, Team Leaders will often ask for a floor plan and/or a tour of the premises and a description of the responsibilities of the different officials of the company. The raid Team Leader will use this information to determine how best to execute the raid.

Meanwhile, the raid team members should identify the locations of garbage bins, shredders and entrances/exits, identify the location of key offices and monitor employees to ensure that evidence is not being destroyed or deleted (see Section 8.5).

The raid Team Leader may also want to consider and advise the company representative should any operations need to be halted during the raid to secure evidence.

The raid Team Leader may also ask the company representative about any off-site storage (a new raid authorization will likely be required) and to introduce the company's IT systems administrator to the agency's lead digital forensics expert.

8.3. Requests to Delay the Raid

It is good practice, if acceding to a request to delay the raid, to first ensure that the premises have been adequately secured so the delay does not prejudice the outcome of the raid.

Agencies may receive requests to delay the raid until the person responsible for the premises has arrived or until the company has consulted with its lawyer. In deciding whether to delay the raid in response to a reasonable request and for how long, the following considerations should be taken into account:

- Is the delay likely to interfere with the effective execution of the raid? (e.g., is there a risk that evidence will be concealed, removed, tampered with or destroyed, does delaying pose a tip-off risk?) This risk may increase if the visit of the agency staff can be observed by a wide range of employees at the company.
- Are the premises adequately secured?
- Is there an in-house lawyer present?
- Is it possible for the company representative(s) to consult with in-house or external lawyers by telephone instead?
- How long is the delay likely to be for?

In some jurisdictions the law provides for a right to have external legal counsel present during a raid. Otherwise, agencies may consider granting a 'reasonable' amount of time for the custodian to obtain legal advice, if it is considered appropriate in the circumstances. In practice, some agencies will grant up to 30 minutes or an hour, after which they will proceed with the raid. Some agencies may start the raid but agree not to remove or copy documents until the external lawyer arrives.

Exercising the right to consult a legal adviser must not unduly delay or impede the raid and any delay must be kept to a strict minimum. While the raid is delayed, it is critical to prevent any attempts to conceal or remove evidence. Accordingly, the raid Team Leader may warn the company representatives about obstruction and attach such conditions as they consider appropriate when agreeing to allow a reasonable delay in order for the party being raided to obtain legal advice. Examples of such conditions include requiring that:

- Cabinets and/or rooms be sealed.
- Business records be kept in the same state and place as when the agency arrived.
- Online and cloud systems be placed under a litigation hold (i.e., the company should take measures to minimize the risk that its employees destroy, delete, conceal or alter any evidence during the raid).
- Digital devices be secured.
- Officers from the agency remain in occupation of selected offices, key documents or electronic storage locations (to prevent any tampering or destruction of evidence).
- The premises be adequately secured.

Practically speaking, the steps the raid team will take to evaluate and gain control of the premises will generally afford a reasonable amount of time for the responsible person to arrive, and/or the raided party to consult counsel, and there may not be a reason to delay longer than that.

In order to expedite the raid once legal counsel has arrived, some agencies may prepare a draft letter in advance to be provided to the company's lawyer following formal service of the authorization so that they can obtain a quick and clear understanding of the circumstances and advise their clients promptly. Some agencies would only prepare a separate document if they are raiding a third party and the usual formal documentation is not available. Many agencies provide legal counsel with a copy of the raid authorization rather than preparing a separate document.

8.4. Obstacles to Entry

To minimize the effects that obstacles, such as a security gate-house or other security systems, can have on a raid, it is good practice for agencies to conduct covert pre-raid reconnaissance of all premises to identify security routines, any obstacles to entry and entry and exit routes (see Section 5). This allows for the risk assessment and deployment of agency staff and/or other measures to address those risks. Agencies should consider making a note of any impediments to gaining entry (such as security measures) and obtain special authorization as necessary (for example, court

authorization) for solutions to address them. Agencies should also build contingencies into the raid plan and pre-raid briefing. For example, agencies may obtain the appropriate tools or hire a locksmith to facilitate entry.

Agencies may also consider seeking police assistance to gain entry, as they may be able to use reasonable force if necessary. If the police station is close to the premises to be raided, some agencies arrange to have police on "stand-by" at the police station in case their help is required to deal with obstacles. This saves police resources for when they are required, rather than having police accompany the raid team at the beginning.

Depending on the risk assessment, it can be good practice to have police accompany agency staff when first entering a raid site as their presence alone may be enough to facilitate entry and deter any obstruction.

In practice, agencies should engage in a multi-step process to gain entry in the face of unexpected barriers:

- **Engagement with the individual in charge:** As a first step, the Team Leader should identify themselves and ask to speak to the individual in charge. When the person in charge is present, the Team Leader will provide that person with a copy of the raid authorization and explain that it allows entry to the premises to conduct a raid. The Team Leader should also explain the potential penalties for refusing entry (in some jurisdictions, impeding entry may be considered obstruction and result in fines or imprisonment). Typically, individuals in charge are less likely to refuse to grant entry when police are present.
- **Assistance of legal representatives:** In situations where the Team Leader cannot reach the individual in charge or they refuse to grant entry, the Team Leader may consider contacting the company's in-house counsel for assistance. The Team Leader could also recommend that the company contact its external counsel for advice (agencies should ensure that they do not try to influence counsel's advice). Counsel may decide to explain to the company that they are legally obliged to provide access to the premises and the consequences of refusing to do so.
- **Discussions with the control room on approach:** When the raid team notices unforeseen obstacles that could prevent them from entering the premises, the Team Leader can alert the control room. The control room can take steps to facilitate the entry (for example, contacting police or a locksmith for assistance) in the event that the options listed above are unsuccessful. The control room may also liaise with the raid teams at other sites and with foreign agencies in case it is necessary to delay entry.
- **Entry with reasonable force:** If the raid team encounters resistance or refusal to provide entry, or if permission to enter is not readily given, entry with reasonable force, with police assistance, may be considered as a last resort so as to eliminate the possibility of evidence being destroyed.

Agencies should consider that a refusal to allow entry changes the risk assessment of the raid and agency staff safety should be considered. The raid team should document any refusals to allow entry to assist with any possible obstruction charges (see Section 11). The possibility that entry could be refused should be considered during the planning stage of the raid (see Section 5 for further information on planning the raid).

8.5. Securing the Premises

It is good practice to secure the premises and take necessary steps as soon as possible to avoid the loss or destruction of evidence.

While company representatives are not usually required to assist with raids, in some jurisdictions interference with the raid could result in their being removed from the premises and/or arrested and charged with obstruction of justice.

Generally, agencies try to interfere as little as possible with the lawful activities of the company. Where agencies have the authority to do so, they may decide to take measures to control offices considered strategic to the raid operation by giving search priority to important areas and offices of key personnel and securing the offices by sealing documents, cabinets or entire rooms. Agencies should assess the need to seal documents, cabinets or entire rooms on a case-by-case basis.

Along with sealing, agencies may take different approaches to control the premises and the integrity of the raid operation upon entry. For more guidance in relation to securing the raid premises and reducing the risk of obstruction, see Section 11.

9. CONDUCTING THE RAID

Once the agency staff have arrived and secured the premises, the process of finding and securing the relevant evidence begins. This Section sets out useful guidance and considerations for agencies in this process.

9.1. Identifying and Locating the Relevant Evidence

As set out in Section 5, it is good practice for agencies to conduct thorough pre-raid research and have a plan which sets out where the relevant evidence is likely to be found.[21] Even with such planning, agencies are likely to encounter new information at the premises which changes their understanding. For example, agency staff may find that target evidence or custodians are in a different location than anticipated, relevant digital evidence may have been migrated from hard drives to a cloud server, or there may be new custodians at the premises whose offices or devices should be searched. This Section sets out a number of considerations which may assist agencies in ensuring that the relevant evidence is identified and located.

9.1.1. Useful Resources

It is good practice to seize or request certain documents to help locate relevant evidence, such as organizational charts, floor plans and inventories of company-issued devices.

Where possible, it is good practice to question individuals on-site to assist in locating documents, explaining document entries or acronyms, and providing access to locked safes or electronic devices, including cloud-stored documents.

During the early stages of the raid, agencies may find it useful to request that a business manager be available during the entire raid and to seize or request the following documents, in order to help locate the relevant evidence:

- Organizational charts or organograms for the relevant divisions and custodians.
- Maps or floor plans of the premises, including where certain divisions or custodians are based and the locations of document stores, electronic devices, or servers.
- A register of the individuals currently onsite and any custodians working from home.

[21] See Section 10 for an explanation of alternative strategies for raids which can be considered when the pre-raid intelligence process has provided little indication as to where evidence may be located.

- An inventory of company-issued mobile devices and computers.

This information may be particularly useful for raids involving companies where employees work remotely or flexibly (as that can make it more difficult for the agency to pinpoint the relevant places to search) and where locating the custodians and areas of business most relevant to the evidence sought upon arrival at the premises is very important.

Typically, agencies may also question individuals at the premises for the purpose of assisting in the conduct of the raid (subject to the jurisdiction's legal framework and avoiding questions which may lead an individual to incriminate themselves). For example, individuals, including the Chief Information Officer or IT manager, may be questioned:

- To understand the company's operating systems, IT set-up and structure.
- To assist with the raid, for example, by providing the combination to a locked safe, or passwords to access computer records, documents stored on the cloud, or electronic devices.

Some agencies may also ask company representatives:

- To assist in identifying and finding relevant documents.
- To provide explanations of documents such as entries in calendars or initials and acronyms found in documents.

9.1.2. Raid Process

It is good practice for the Team Leader to conduct an initial sweep of the premises and for searches to be conducted methodically.

When conducting the raid, agencies may consider the following steps:

- The raid Team Leader, or another member of the search team, conducts an initial sweep of the premises to identify and prioritize search areas. Sometimes, it can be efficient if another team member conducts the initial sweep of the premises while the Team Leader simultaneously serves the authorization documents to company representatives.

- During the initial sweep, team members are assigned to offices or areas (e.g., in an open plan space) to secure them until the actual search starts.

- Once the initial sweep of the premises has been completed, search areas may be allocated. Where practicable and efficient, it is recommended that agency staff search in pairs within visibility of each other to help ensure their safety. Searching in pairs is also helpful for corroboration purposes if cash or other valuables are present.

- It is good practice to adopt a methodical approach when searching; for example, agency staff can start a search in opposite places, search clockwise around a room or by drawer in a logical way such as top to bottom.

- To ensure that all evidence in a search area is captured, agencies may use a reference system assigning an identifier to each building, floor, room, and piece of furniture (including drawers and cupboards containing evidence). A record should be kept of the location of the areas that are being searched and the start and end time of the search.

- Once the search of an area has started, it is recommended that agency staff remain present in that search area until it has been completed. Once completed, it should be recorded in the raid report.

- Agency staff should carefully examine material to determine whether it may be relevant to the investigation or consider if it may be covered by legal privilege before deciding whether it should be seized or copied. See Section 12 for further information on legally privileged material and Section 13 for further information on seizing evidence.

- Material that is seized or copied should be given a unique identifier and be processed by the site exhibit officer, or by another member of the search team during the raid. It is good practice to give the company a list of the seized or copied material. It is recommended that, when the search of an area has been completed, evidence is passed on to the site exhibit officer for processing. A note should be made of the time when the evidence was passed on to the site exhibit officer. See Section 13.4 for further information on coding and other forms of evidence identification and Section 13.6 for further information on continuity of possession of evidence.

9.1.3. Scope of the Raid Authorization

In some jurisdictions, the wording of the raid authorization may strictly limit the scope of the raid area. For example, if the raid authorization refers to a certain area, it would not allow the agency to search other rooms occupied by the company being raided, even if the rooms were adjacent to the area specified in the authorization. To search adjacent areas, agency staff would be required to obtain a new raid authorization. In other jurisdictions, the authorization may be much wider, for example covering the whole building, including any vehicles on the premises.

The scope of the raid authorization may lead to disputes or legal challenges from the company, especially regarding how the authorization's wording should be interpreted (for example, whether certain documents are "related" to the suspected cartel activity, or whether a storage room within an office constitutes "part of the office").

Approaches to resolving such disputes differ across jurisdictions. Some agencies may attempt to resolve the conflict through discussion with the premises' custodians. If this does not lead to a satisfactory resolution, the agency may temporarily seal the area and evidence to avoid possible destruction and apply for an additional authorization for the disputed area or evidence. In other jurisdictions, the raid Team Leader may consult the lead investigator and legal counsel as appropriate to seek their views on whether a new raid authorization is required. If they do not agree that there is an issue with the authorization they may decide to proceed with the raid, rather than discussing this with the custodians. The company may later challenge this decision, should the matter go to court.

The parameters of the raid may not necessarily be fixed from the outset, but rather can evolve and change throughout the duration of the raid. This may result in the scope of

the raid being expanded, requiring more resources than initially anticipated. Agencies should keep the scope of their raid authorization in mind when considering such changes. If the revised parameters, such as the duration or location of the raid, exceed the raid authorization, a new authorization covering this broader scope may be necessary.[22]

Agencies may also need to narrow the scope of the raid, particularly in jurisdictions where the raid authorization is less specific. For example, in some jurisdictions, an authorization may be issued encompassing the entire office space of the raided company. But the practicalities and resource limitations of the raid may require the agency to focus on specific areas.

9.1.4. Additional Considerations for Digital Evidence including Cloud-based Evidence

It is good practice to ensure that the agency has sufficient digital forensics resources, such as skilled staff and equipment.

It is good practice to identify and secure any relevant mobile devices as soon as possible

The type, amount and importance of digital evidence in raids is continuously increasing, including cloud-based evidence and the use of servers, desktops, laptops, mobile devices, GPS/satellite navigation, memory cards, and cameras.[23] While many of the considerations outlined above also apply to digital evidence, there are also a number of specific issues which agencies may find useful to consider when conducting a raid involving digital material. These are set out in the table below.

Consideration	Comments
Resources, training and equipment	Agencies should consider whether they have sufficient digital forensics resources for the amount and types of digital evidence likely to be found, including sufficient skilled staff and equipment. This may affect, for example, the number of devices the agency is able to image.
Limits of the raid authorization	In some jurisdictions, the raid authorization may limit the agency to only searching/seizing/copying relevant evidence.

[22] This is particularly relevant in jurisdictions where the raid authorization mandates a very specific location or locations, such as a certain office or vehicle. See Section 3.1 for more information about to raid authorizations.
[23] For more guidance in relation to digital evidence gathering, see "Chapter 3: Digital Evidence Gathering" available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering/.

Consideration	Comments
	This may mean that where a device or digital dataset contains both relevant and non-relevant information, the agency is unable to seize/copy the whole device or dataset. The agency could consider whether it is possible to filter or select out the relevant information. The following factors may be relevant to this: • Available resources and staff. • Equipment required and skillsets available. • Any relevant agency policies or procedures. • Any limits imposed by the raid authorization. • Impact on the device's custodian (for example, if the device contains personal information). • Presence of potentially privileged evidence on the device
Chain of custody	In some jurisdictions, the agency must demonstrate the integrity of the evidence seized/copied through the chain of custody (i.e., that the evidence relied upon by the agency is the same as that which was seized from the party). See Section 13.6 for more information on continuity of possession. In the case of digital evidence, this may require the use of digital forensic techniques, which can vary depending on the data storage type (e.g. laptop, server, or cloud), the model, and the software used. Agencies should consider whether they have the appropriate tools and trained staff for this purpose.
Accessibility	Developments in technology may make digital evidence more difficult to access, requiring new and adapted tools and techniques. For example, cloud computing systems may bar users without proper authentication from accessing stored data.
Cooperation	In some jurisdictions, companies are mandated by law to cooperate with the investigation. In other jurisdictions, the agency is not able to compel cooperation and this can only be obtained voluntarily. In such cases, it is often in the agency's interests to encourage cooperation as this facilitates the raid running smoothly and efficiently. This is particularly the case in relation to digital material, where cooperation can be particularly important. For example, cooperation may be helpful: • to overcome complex physical or electronic encryption without the company's assistance. • To avoid damaging any devices during the process of decoding or neutralizing the security program. • To help navigate larger and/or more complex digital datasets which are . • To access cloud storage hosted or managed remotely to the premises being raided.
Destruction of evidence	Custodians may attempt to destroy incriminating evidence by "factory-resetting" the mobile device and deleting cloud data. To prevent destruction of evidence, agencies may request activation of a "litigation hold" functionality (or equivalent) on mailboxes or other systems and/or seize the mobile devices upon entry and immediately set them to 'airplane mode' or

Consideration	Comments
	switch them off. Switching the mobile device off may affect the chain of custody in relation to this evidence. Therefore, the agency staff must ensure that the process of securing mobile phone evidence is appropriately recorded.
Cloud, server or back-up in a foreign jurisdiction	Agencies should consider where the evidence is located and determine whether it falls within the authority of the raid authorization. Agencies may consider seeking the consent of the company to obtain the evidence or cooperate with an agency which has jurisdiction over where the evidence is located.

Typically, explaining the agency's digital forensic procedures to the company prior to extracting digital evidence and having the company's IT experts present while the digital evidence is being extracted can be helpful.

Agencies may need to exercise "seize and sift" powers (see Section 13.2) in cases of significant challenge due to the difficulty and time involved in trying to search for only relevant/non-privileged documents in a reasonable timeframe. In jurisdictions where "seize and sift" powers are not available agencies may consider reaching an agreement with the company stating that the relevant drive/drives can be imaged and "seized" but cannot be reviewed by the agency (except those documents in the drive agreed to by the company). Where no agreement can be reached, a process for review by a third party could also be agreed between the agency and the company.

9.2. Documentation

9.2.1. Note Taking

It is good practice to take notes of events as they happen at the premises.

Agencies could consider preparing a raid report or notes of the raid. A raid report can provide important proof that the agency conducted the raid appropriately. In some jurisdictions, such notes may become part of the evidence presented in court. Notes may also be used to refresh the raid team members' memory for testifying at trial or at other legal proceedings.

Agencies take different approaches to note taking. The approach to be taken should be decided prior to the raid. Some of the approaches taken are as follows:

- One member on the raid team is appointed as the designated note taker and is solely responsible for taking notes.
- Several agency staff members are responsible for taking notes, with each responsible for taking notes in relation to the part of the premises they are allocated to search.
- The Team Leader or a different designated agency staff member prepares a written report of the raid with reference to other team members' notes.

Raid reports or notes may capture some, or all, of the following elements:

Part of the raid	Considerations
Before the raid	Details of the briefing relevant to the raid, for example: • What is alleged. • Who are the targets. • What is being searched for.
Upon entry	Details of the premises, including: • The name and address of the premises. • Condition of the premises upon arrival and any damage caused to the premises during the execution of the raid.
	Details of entry, including: • Time of entry. • Identification of the agency staff (including any external personnel, such as police or external counsel). • The fact that all agency staff (and any other personnel assisting) carried and displayed appropriate identification (where statutorily required). • What happened upon entry.
	Details concerning the presentation of the raid authorization, including: • The fact that the authorization was produced upon entry (often to satisfy statutory requirements). • Date and time of presentation of the raid authorization to a company official. • Name and title of the company official(s) the raid authorization was presented to.

During the raid	Explanation of relevant documents to the company representatives and/or their legal representatives. This may include the following:
	• Raid documentation:
	  ○ Powers of the agency under the raid authorization.
	  ○ The company's obligations during the raid.
	  ○ Rights of the party or occupier of the premises.
	• Relevant documents being searched:
	  ○ In some jurisdictions, the explanation of the documents being searched for would be limited to the general descriptions in the raid authorization. This limits disclosure of potentially sensitive information before all of the relevant material has been searched.

	Details in relation to the premises, including: • Description of the premises searched, including sketch diagrams of the areas searched. • Condition of the areas searched and any damage caused to those areas during the execution of the raid. • Steps taken to secure the premises.
	Details of key employees present onsite and any key employees working from home or remotely on the day of the search.
	Any involvement of external experts or other agencies, such as the police.

Part of the raid	Considerations
	Relevant discussions with the company, including discussions of an evidentiary nature or where making notes is prudent from a risk management perspective. For example: • The identity of company employees spoken to. • Discussions relating to the right to consult counsel. • Discussions around consenting to the copying or imaging of evidence. • Discussions around preservation of evidence. • The existence of the agency's leniency policy, where relevant.
	Discussions with the company's legal representatives, including: • Details of the representatives (such as the firm and identity of advisers present). • Discussions relating to relevance and claims of legal privilege. • Discussions relating to the terms of the raid authorization. • Any legal challenges to the raid. • Sealing of premises.
	Details of any interviews conducted during the raid (see Section 9.5 for further information).
	Details of any voluntary admissions or denials made by custodians during the raid.
	Any cautions administered and statements made (word-for-word, if possible).
	Any requests for the production of documents, including: • Details of the request. • The company's response. • Details of any ensuing discussions.
	Steps followed in identifying, gathering, seizing and handling evidence, both physical and digital (including evidence located in the cloud).
	The date, time, location and description of all information, documents and devices (including computers, laptops and mobile devices) produced or seized during the raid and any unique identifying number that was assigned to them (for evidentiary purposes in any subsequent hearing, and to satisfy the requirements of the chain of custody). See Section 13 for more guidance in relation to seizure.
	Details of statements or comments made by any person or events that occurred with a direct relationship to the substance of the investigation (for evidentiary purposes in any subsequent hearing).
	Any instance of obstruction or non-cooperation, including: • Refusal of entry or blocking of access to part of the premises. • Refusal of a request for the production of evidence. • Details of any other events that occurred that may demonstrate that the company or any of its employees failed to provide reasonable assistance during the execution of the raid (for evidentiary purposes in any subsequent hearing).
	The placing of any seals including: • The locations that were sealed. • The time the seals were placed.

Part of the raid	Considerations
	• The identity of the staff placing them. • Any witnesses from the company. • Whether any photographs were taken. • Whether the photographs were shared with the company. • Whether instructions were provided to the company (e.g. any agreement on time of removal of the seal).
	The condition of the seals upon return including: • The time the seals were removed. • The identity of the staff removing them. • Any witnesses from the company (only necessary if there is damage to the seal). • Whether any photographs were taken. • Whether the photographs were shared with the company.
	Any significant deviation from established agency procedures.
	In some jurisdictions, depending on the agency's remit and relevant protocols, details of any conduct which appears to constitute a breach of: • legislation not enforced by the agency or • legislation enforced by the agency which falls outside the scope of the raid authorization or substance of the investigation to which the raid authorization pertains. Any details can then be passed to the relevant enforcement entity or regulator for evidentiary purposes in any subsequent hearing relating to "other" breaches or to the control room to apply for a new raid authorization.[24]
Upon exit	The fact that either a schedule/list of material seized or a notice that evidence was removed was provided to the custodians of the premises (to satisfy statutory requirements in some jurisdictions). Details of any comments made by the custodian concerned during this process.
	The time the raid was completed (for evidentiary purposes in any subsequent hearing).
	The time of exit (and the names of the other agency staff who left at the same time).
	Condition of any seals placed on cabinets, locks, doors, etc.
	Condition of any seized evidence left at the premises.

In some jurisdictions, agencies have their raid report signed by agency staff and the company being raided.

[24] See Subsection 9.1.3 for more guidance in relation to offences outside of the scope of the raid authorization.

9.2.2. Photographs and Videos

It is good practice to take photos and video footage during raids to document the condition of the premises to counter claims of damage, to record the location of evidence, to ensure due process and maintain chain of custody and capture the placement and condition of seals.

In some jurisdictions, agency staff have the power to take photographs and/or video footage at the premises during the raid. Situations where taking photographs and/or video footage might be useful include:

- To document the state of the premises and rebut any subsequent claims that the premises or property was damaged during the raid, especially where the premises are in poor condition upon arrival;
- To document the location of evidence at the raid site for identification and due process (e.g., chain of custody) purposes. Making records of each step of the raid from entry may assist with rebutting any possible procedural challenge; and
- To document the placing of seals and the condition of these seals upon return.

Agencies must comply with all relevant privacy, data protection and human rights legislation if they take photographs and/or video footage at the premises during the raid.

9.3. Special Considerations

It is good practice for agencies to consider the nature of the premises being searched and ensure that the raid team is made up of appropriately trained and/or experienced personnel.

It is good practice for agencies to investigate whether key custodians work from home prior to the raid and, if so, obtain a raid authorization for their private premises if possible, where relevant evidence is likely to be present.

In addition to company premises, some agencies have the power to raid other types of premises, such as private premises or vehicles. This may give rise to special considerations and procedures.

9.3.1. Private Premises

Shifting work patterns have resulted in custodians being more likely to work from home. It is good practice for agencies to investigate whether custodians work from home prior to a raid and if so, obtain a raid authorization in relation to their private premises, where relevant evidence is likely to be present.

However, extra caution should be taken in the case of raids on private premises and particular consideration should be given as to who may be on the premises at the time, including family members, vulnerable individuals (such as children) and (potentially dangerous) pets.

Raids on private premises must be carefully planned to preserve the rights of the custodians and other occupants.

The below table sets out a number of considerations which agencies may find useful when raiding private premises.

Issue	Consideration
Prior to the raid	
Obtaining the search authorization[25]	Raiding private premises may require a separate raid authorization. Requirements vary across jurisdictions. In some jurisdictions, agencies may be required to show that it is likely that the relevant evidence is located at the premises. In other jurisdictions, the agency may have to demonstrate that it is strictly necessary to raid the private premises to obtain the evidence.
Scope of the raid authorization	A court may place certain limitations on the scope of the raid authorization. For example, the starting time and duration of the raid may be more limited compared to company premises.
Timing	Timing a raid at private premises needs careful consideration to balance competing objectives. On the one hand, raiding early in the day can guarantee that the custodian will be present. However, on the other hand, it may be better to raid at a time when the impact on the custodian and others that reside there is minimized. For example, it may be prudent to enter the premises once: • Other adults have left for the day or once children have left for school. • The custodians (or other occupants) are able to easily access legal representation, for example by being able to contact the company (or alternative sources of support) so they can provide legal representation. • The custodian is able to easily access IT support by being able to contact the company. • Given the absence of an in-house lawyer, the agency may be prepared to allow a longer delay to the start of the raid in order to allow an external lawyer to arrive.
During the raid	

[25] Some agencies do not have the power to raid private premises and must rely on the support of law enforcement colleagues, for example the police to do it for them, or the custodian's consent.

Issue	Consideration
Respecting privacy	Agency staff must ensure that the raid is conducted in compliance with the custodian's right to privacy.
	By ensuring that the custodian is present during the raid, agency staff can better consider the right to privacy.
Respecting religious items	Agency staff may encounter religious items within private premises. The items should not be handled or moved by agency staff without due consideration. If religious items must be handled, agency staff must do so with the utmost care and ensure minimal intrusion.
Respecting rights of other residents	Agency staff must ensure that the rights of occupants other than the custodians are respected. Any evidence under the raid authorization that is suspected to be in the possession of other occupants must be obtained with minimal intrusion.
Gathering evidence	Private premises will contain a large amount of material which is not relevant to the raid. Agency staff should ensure that the raid is limited to the evidence within the scope of the raid authorization. In some cases, it may be appropriate to limit the area to be raided within private premises to a defined area.
Safety	In some jurisdictions, searching private premises may have an increased safety risk as such premises may contain firearms or other weapons. Furthermore, searching private premises can lead to heightened tension and aggression from the custodians. Thus, it is important to check for histories of violence or crime as well as access to firearms of the custodians prior to the raid. In addition, searching private premises can expose agents to uncontrolled environments such as the presence of animals or other hazards. Thus, during the raid, agency staff should be paired and keep one another in sight.
Physical space	Planning should take the size of the private premises into account, including the fact that the custodian's lawyer may also need to be present. The agency can consider having a mobile office or using a nearby premises to avoid crowding.

9.3.2. Searching Vehicles

If it is likely that vehicles will contain relevant evidence, it is good practice to gather information on the vehicles registered to a custodian and to ensure the raid authorization includes them.

It is good practice to search key areas in vehicles, such as the glove box, dashboard, trunk, and other storage compartments. Navigation logs and toll payment records may also provide evidence of physical meetings between colluders.

Evidence may be located in vehicles and custodians may attempt to conceal evidence within their vehicle or vehicles of colleagues or visitors. Raiding vehicles can be an effective means of obtaining important evidence. Agencies should be aware of local laws and procedures for searching vehicles. Before deciding whether to search a vehicle, agencies should consider the following:

- Is there likely to be evidence relevant to the investigation in the vehicle?
- Does the raid authorization allow for the searching of the vehicle in question? In most jurisdictions, raids are limited to the locations covered in the raid authorization. It is therefore important for the raid team to check whether the vehicle is within the scope of the raid authorization in advance. This often requires the agency to demonstrate that it is probable that the vehicle contains relevant evidence.

Vehicle and/or owner identification should be confirmed prior to the vehicle being searched. If possible, agencies should also collect additional information when planning a search, such as:

- Number of vehicles registered to the custodian.
- The custodian's use of vehicles under different registrations.

When raiding vehicles, the glove box, dashboard, trunk, and other storage spaces within the vehicle should be searched. In addition, destination logs on navigation systems and automatic toll payment system records may provide evidence of physical meetings between potential colluders.

9.4. Arrests and Searches of Custodians

It is good practice, where permitted, to ensure the raid authorization covers moveable objects such as briefcases, handbags, laptops and mobile devices.

During the raid, agency staff may suspect that custodians on the premises are in possession of relevant evidence. Agencies should be aware of and follow applicable local laws and practice when deciding whether to search custodians.

9.4.1. Requirements and General Considerations

Prior to searching a custodian (i.e. searching a person for evidence or mobile devices they are carrying with them), agencies must ensure that the search is within the scope of the authorization. Depending on the jurisdiction and circumstances, agencies may be required to obtain separate authorization to search custodians, or they may be permitted to do so within the scope of the original raid authorization.

If permitted under the raid authorization, custodians' computers, laptops, and mobile devices must also be carefully examined and, if the devices are not judged to be solely for personal use, may be seized. Moreover, if the conduct of the suspected offence has taken place over an extended period, it is important to secure previously used devices for more effective evidence gathering. Even if the devices are not found to have been used within the suspected period of the offence, securing them may provide important evidence. If it is expected that digital evidence will be encountered during the raid, agencies are advised to refer to Sections 9.1.4 and 13 for procedures on seizing digital evidence.[26]

In some jurisdictions, agency staff or police officers attending the search, are authorized to search custodians present on the premises who are suspected of possessing relevant evidence.

Some agencies require custodians wishing to leave the premises to declare that no specific information or information carriers are being removed and to produce any documents/diaries/agendas before leaving.

Agencies may also be authorized to search briefcases, handbags and similar articles found on the premises. However, this varies by jurisdiction and may be dependent on several conditions:

- There are "reasonable grounds to believe" that evidence specified in the raid authorization would be found.

- The raid authorization specifies that the locations to be searched include briefcases, laptops, other mobile devices, and any other movable document containers located at the premises in the possession of, or readily identifiable as belonging to specific custodians identified in the raid authorization.

[26] For more guidance in relation to digital evidence gathering, see "Chapter 3: Digital Evidence Gathering" available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering/.

- The raid team has reasonable grounds to suspect that a custodian has evidence in their possession and that they are refusing to hand it over for examination. In such circumstances, that custodian may be deemed to be obstructing the investigation (see Section 11 for more detail).

- The custodian has given their consent.

Where it is not possible to search custodians, agencies may ask the custodian to voluntarily submit relevant evidence (having informed them of their legal rights). Where the custodian refuses, it may be useful for the agency staff to record the custodian's identity and attempt to conduct an interview to determine whether evidence is kept on their person, why they are not submitting it, and where the evidence is usually kept. Subsequently, the agency staff may attempt to obtain a new authorization to seize the relevant evidence.

9.4.2. Arrests of Custodians

In jurisdictions where arrest of custodians is possible, it is good practice to obtain authorization or cooperation from police to ensure due process of the arrest.

In some jurisdictions, custodians may be arrested on suspicion of an offence during the raid. A warrant is usually required to make an arrest. However, in some jurisdictions an arrest can be made without a warrant. The raid team must comply with local law and rules when arresting custodians or evidence obtained during the arrest may be inadmissible in court. In some jurisdictions, arrests can only be made by the police.

When arresting a custodian, the arresting officer should immediately search for any weapon in the custodian's possession to quickly seize and minimize any possible threat.

9.5. Conducting Interviews to Gather Information or Evidence During the Raid[27]

It is good practice to interview during the raid in individual cases and to assign a separate interviewing team.

It is good practice to make the interviewee aware of their legal rights to ensure due process.

In some jurisdictions, agencies have the power to conduct voluntary and/or compulsory interviews during the raid. When conducting a compulsory interview, custodians may be entitled to protection from self-incrimination. It is good practice to accommodate any request for legal representation during such interviews.

There are a number of advantages and disadvantages to conducting interviews during the raid.

Advantages of conducting interviews during the raid	Disadvantages of conducting interviews during the raid
Interviews can be a fast way to get information relevant to the investigation, especially where there might be intelligence gaps early on in the raid (see Section 10.2 below).	Interviewing and/or obtaining a signed account or a statement can distract from the raid and/or delay completion of the raid. It may also provide the company with visibility into the key focus areas of the investigation or the raid.
Interviews may provide further information about the suspected conduct and any documents that are deemed relevant.	Agencies may prefer to review the evidence gathered during the investigation, prior to seeking statements from the management or employees of the company.
Agencies may bring their leniency program to the attention of management and employees during the interviews.	Like interviews at other stages of an investigation, if employees are not aware of their rights, any answers provided could later be ruled inadmissible in court due to a perception of unfairness.
	Like interviews at other stages of an investigation, contradictory statements may lead to evidential and disclosure challenges.

[27] See also Section 10.2 and Chapter 6 of the ICN Anti-Cartel Enforcement Manual on Interview Techniques available at: https://internationalcompetitionnetwork.org/portfolio/interviewing-techniques/.

Agencies should consider planning any interviews to be conducted during the search in advance to minimize risks and ensure that relevant legal protections are afforded to the custodians, including identifying relevant custodians and preparing interview plans. It is also recommended for any interviews to be conducted by an interview team which is separate from the raid team.

9.6. Evidence of Offences Not Covered by the Raid Authorization

It is good practice, when evidence outside the scope of the authorization is discovered, to ask the custodian to submit the evidence voluntarily or to request additional authorization(s) immediately.

Evidence found during the raid may relate to offences which are not covered by the raid authorization. In such cases, agencies may consider for example the following options:

- Asking custodians to submit the evidence with voluntary consent.
- Requesting additional authorizations.
- Not seizing the evidence.

However, agencies should be careful when deciding not to seize such evidence, as they may develop a better understanding of the relevant conduct as the investigation progresses which may then affect their initial assessment of the evidence.

In some jurisdictions, there are exceptional cases which allow for the seizure of evidence not covered by the raid authorization, as set out in the table below.

Consideration	Comment
Competition offences:	
How was the evidence found?	In some jurisdictions, agencies have the power to seize evidence relating to other offences if the evidence is found inadvertently or is in "plain view".
Is the material at risk?	In some jurisdictions, agencies are not required to obtain an additional raid authorization if there is a risk of the evidence of the additional offence being removed or destroyed.
What is the nature of the evidence?	In some jurisdictions, agencies are able to seize evidence that goes beyond the scope of the raid authorization (for example in terms of its duration and/or geographic scope, the number of companies involved, or additional products covered by the cartel activity under investigation) and use it to either expand the investigation's scope or launch a new investigation.
Is there 'probable cause'	In some jurisdictions, agencies may request an additional raid authorization on the basis that there is a

Consideration	Comment
that another competition offence has been committed?	"probable cause to believe" that an additional competition offence has been committed and evidence of this offense is likely to be found at the raid premises.
Non-competition offences:	
What are the agencies' legal powers and responsibilities?	Agencies' legal powers and responsibilities vary by jurisdiction. Some agencies do not have the power to use evidence of other offences or share it with other agencies, while in other jurisdictions agencies have a responsibility to seize such evidence or share it with other public bodies such as the police.
Is seizing the evidence in the public interest?	In some jurisdictions, agencies are only able to seize or disclose evidence of other offences if this passes a "public interest" test. This may depend on the nature of the evidence and alleged offence.

9.7. Exiting the Premises

It is good practice to dispose of all classified or sensitive information, return any passes or keys provided by the company, check the seized evidence against the evidence list and mark the time of exit when exiting the premises.

Once the raid is complete and agency staff have possession of the relevant documents, the raid team should prepare to leave the premises. This may include the following steps:

- Ensuring that the workspace provided to the agency is clean and in the same condition as when the raid team arrived. Some agencies take any rubbish away with them and dispose of it at the agency in case it contains classified or sensitive information.
- Returning any passes or keys provided by the company.
- Checking the seized evidence against the evidence list.
- Depending on agency practice, providing a receipt or copy of the list to the company (see Section 13.8 for further guidance).
- Marking the time of exit in the site log (see Section 9.2.1 for more guidance).
- Gathering at a designated meeting spot, along with the seized evidence for transportation back to the agency.

10. ALTERNATIVE STRATEGIES FOR RAIDS

It is good practice, when agencies are unable to identify in advance where evidence is likely to be found during a raid, to prepare alternative strategies for identifying where evidence might be found once they have arrived on a company's premises.

It is good practice to keep these strategies under review as the forms of evidence change and to share successful new strategies with other agencies.

10.1. When Agency Staff do not Know Where Evidence may be Located

The amount of work to be put into pre-raid intelligence and planning (see Section 5.1) should never be underestimated. The more raid teams know about where evidence is likely to be located and stored within the company to be searched, the more likely that the raids will be successful and completed quickly.

However, intelligence gaps may still remain by the time agency staff arrive at the premises to be raided, such that raid teams may arrive at the premises of a large company with no clear indication of where evidence is likely to be located. For example, they may have little indication as to which custodians they should target, which key word search terms to use and/or where digital material is likely to be stored if it has not been possible to gather this intelligence at the pre-raid intelligence/planning stage.

This may be due to short lead-in times, the risk of tip-off or simply the lack of intelligence available pre-raid.

This section aims to describe some of the techniques that agencies may use in this type of scenario. They are additional to the more commonly used approaches set out elsewhere in the Chapter, such as holding discussions to facilitate the raid (see Section 8.2); conducting interviews during the raid, for example with IT staff at the start of the raid to locate where documents are stored and how to access them (see Section 9.5); and the seizure of relevant documents which may themselves indicate where other evidence may be located (see section 13.1). Such techniques include:

- Interviews of witnesses at an early point in the raid; and/or
- Microsoft 365 platform 'Hotspot' searches.

10.2. Interviews of Witnesses at an Early Point in the Raid

Conducting targeted interviews once a raid has begun can help identify the likely custodians of evidence and/or establish where evidence might be found.

Witnesses might include current or former employees of the suspect companies, including leniency applicants' staff, or informants involved in the alleged cartel, where

contactable. These people may have vital information about the key custodians on the premises being raided and may have long-standing relationships with some of them. In many circumstances, it will not be advisable to interview such witnesses before the raid as there may be a high risk of tip-off. Therefore, it might make sense to wait and hold any such interviews after the raids have started (and the tip-off risk ceases to exist).

The types of information to be sought from those early interviews might include:

- Names of key custodians at the companies being raided.
- Working locations and current location of key custodians, including their propensity to work from home (which might lead agency staff to visit their home addresses).
- Contact details of key custodians (including home addresses, email addresses, telephone numbers, etc.).
- Use of social media for business purposes by key custodians (e.g., messaging apps).
- Location of relevant material (which might also reveal other premises to be raided that had not previously been identified) including whether the company being raided uses cloud-based servers and where those servers are located.
- Whether key custodians tend to keep notes in hardcopy notebooks or electronically (e.g., on laptops); whether they have separate mobile devices for business and personal use; and whether they tend to use encrypted messaging apps (including short-lived messages) for business purposes.

The interviews might be kept short and relatively informal (while ensuring to make a good record of the discussion) so that any useful intelligence can be relayed to other premises being raided as quickly as possible. More in-depth evidential interviews can be left to a later stage of the overall investigation. Some agencies conduct this type of interview on a voluntary basis due to concerns that witnesses may be less open in their responses if they have to be compelled to answer.

10.3. Microsoft 365 Platform 'Hotspot' Searches

'**Hotspots**' include the key custodians at the suspect company most likely to have retained digital evidence (for example, in their mailboxes, user profiles, OneDrive and Teams accounts; or on their laptops or mobile devices, etc.); and the shared folders (for example, SharePoint); or paper documents (for example, diaries, notebooks, etc.) used by the suspect company for its cartel activities.

The essence of this technique is to use keyword search reports generated by the Microsoft 365 platform[28] to identify the Hotspots. The searching capability of this platform[29] allows for keyword searches to be carried out across a company's systems in a relatively short period of time.

[28] Microsoft 365 is a cloud-based productivity platform used by Microsoft to provide its productivity apps including Teams, Word, Excel, Outlook, PowerPoint, OneDrive, etc. Similar platforms with similar functionality may be available, and for which the 'Hotspot' searches approach described above may also be used. For example, Google Workspace offers similar functionality.

[29] The version of Microsoft 365 required for this technique is Office 365 E5. This is the only version of Microsoft 365 with the compliance capabilities and Purview (Purview being the tool that allows searching and data export). If a company does not have this level of service,

The technique is likely to be more appropriate for companies with a large number of different business areas where evidence might be located, and where agency staff may not have a clear picture in advance of the raid of who and what the Hotspots are. It also relies on the agency having the legal powers to require the suspect company to run these searches and to produce a search report (or on the company being raided agreeing to do this voluntarily).

This technique can be used alongside:

- Any pre-raid intelligence gathered (see Section 5.1).
- Requirements on the suspect company during the raid to produce:
    - Current and historical staff organizational charts (listing staff in relevant business areas).
    - An overview of the company's IT architecture.
- Interviews of witnesses at an early point in the raid (see Section 10.2).
- Relevant intelligence gathered from other premises being raided.

10.4. Other Options for Digital Searches[30]

In addition to the traditional technique of gathering and imaging digital material on the premises during a raid for review at a later date at the agency's offices, some agencies have successfully used the following techniques:

- Collecting AND reviewing digital material while the agency's investigators are on-site.
- Remote searching using cloud-based platforms, such as Microsoft 365.

10.5. Collecting and Reviewing Material while the Agency's Investigators are On-Site

The following outlines a possible process for collecting AND reviewing digital material on-site:

- Agency staff identify the likely custodians of evidence and which shared folders (e.g., SharePoint sites) are likely to contain relevant evidence (together the 'Relevant Digital Material').
- Agency staff gather digital devices, server locations and cloud locations of the Relevant Digital Material.
- The agency's digital forensic expert extracts possible relevant files (information in certain folders or certain document types) from the Relevant Digital Material by making a forensic image of the content.
- Once a forensic image is made, the digital forensic expert may return the digital device to the raided company.

---

it would be relatively easy for the company to sign up for a free temporary trial for the duration of the raid.

[30] See also "Chapter 3: Digital Evidence Gathering" available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering/.

- The agency's digital forensic expert and/or agency staff upload, index and review the forensic image:
    - An image of all the potentially relevant material is uploaded onto the agency's review platform.
    - All of the uploaded data is then indexed, which means that all of the material is catalogued.
    - Once it is indexed, the data is reviewed by agency staff on review stations who "tag" relevant items. This review is likely to be overseen by the company's legal representatives if they have concerns that legally privileged material might be reviewed.
- The agency's digital forensic expert copies the collection of items tagged relevant onto an encrypted data carrier (e.g., DVD, USB stick or hard disk) together with a list containing the name, the path and a hyperlink to each item. A separate file on the data carrier should show the "hash value" of the container that contains all the data.
- A representative of the company and an agency staff member may agree on and sign off on the items listed.
- Agency staff provide the company with a copy of the data carrier with the data and the list.
- At the end of the raid, the digital forensic expert should "sanitize" all of the agency's equipment that has been used to store the company's digital information before leaving the premises.
- If the review of material cannot be completed during the course of the raid, and where agency staff have the necessary powers to continue their review of the Relevant Digital Material at their offices:
    - It is good practice for agency staff to follow their agency's chain of custody or continuity procedures. For example, placing the forensic image of the Relevant Digital Material in a sealed envelope, anti-static bag or container before removing it for review at the agency's offices.
    - In some jurisdictions, the agency may invite the company's representatives to attend the review.
    - In some jurisdictions, a copy of that forensic image is also provided to the company. Following this continued review, agency staff will tag any relevant documents and provide a copy to the company.
    - On completion of the evidence review, the forensic expert may "sanitize" the storage medium containing the digital forensic image.

In determining where the Relevant Digital Material is likely to be found during the raid, agency staff may wish to consider the other techniques described above in this section. A paper search may still be required in parallel.

10.6. Remote Searching with the Microsoft 365 Platform[31]

This approach involves gaining access to the company's Microsoft 365 platform from the agency's own offices without physically attending the company's premises. It has been shown to lead to benefits both for the company and for the agency. For example, there is likely to be increased efficiency and speed when the company exports the data; and it also minimises the risk of procedural errors by the agency. It can be performed in two ways:

- The agency requires the company to export data from the Microsoft 365 platform to the agency for review (see Section 10.6.1 below), or
- The agency acquires IT permissions to the company's Microsoft 365 platform so that the agency can directly export data from the suspect company for review (see Section 10.6.2 below).

Before considering either approach, the agency should conduct open source intelligence research to ascertain whether the suspect company uses the Microsoft 365 platform. Also, the availability of either approach will depend heavily on the legal regime under which the agency operates (for example, there may be data protection or legal privilege concerns) and the likelihood of voluntary co-operation from the suspect company.

It may be possible to use these methods with other systems that have similar functionality to the Microsoft 365 platform.

10.6.1. The Company Exports Data from the Microsoft 365 Platform to the Agency for Review

The following summarizes a possible approach when an agency requires the company to export data from the Microsoft 365 platform to the agency for review:

- The agency gives the suspect company clear instructions on what data to extract.
- The company is required to appoint a dedicated person to perform the data extraction. That dedicated person is required to share on-line the computer screen showing the extraction.
- The media containing the extracted data is then provided to the agency.
- The company is also required to provide activity log files showing in detail the parameters it used to produce the data and agency staff verify these activity log files before the end of the raid.
    - In verifying the activity log files, the agency can check whether any unexpected filters have been applied to the data exported.
- The agency also acquires the activity logs for each relevant custodian, so that it can check their actions on the day of the raid.
- The data produced is reviewed by the agency at its offices.

10.6.2. The Agency Exports Data from the Company for Review

The following summarizes a possible approach for an agency to export data from the company for review:

[31] Or with another cloud-based platform with similar functionality.

- The company creates a temporary administrator account on its Microsoft 365 platform for the agency. This way, the company does not have to disclose its administrator password to the agency.
- The temporary administrator account gives the agency its own credentials to run its own searches across the company's Microsoft 365 platform and to export data.
- The company is able to obtain activity log files to verify what data has been exported by the agency during the remote search and to verify that only data from relevant custodians has been exported.
- The data produced is reviewed by the agency at its offices.

11. OBSTRUCTION DURING THE RAID

It is good practice to ensure that the raid team has been trained to respond to any obstruction including unauthorized removal, concealment or destruction of evidence.

11.1. What is Obstruction?

Obstruction encompasses any attempt by company representatives to interfere with the raid. This section sets out useful guidance and considerations for agencies in relation to obstruction. Obstruction can take several forms, including:

- **Refusing entry:** Denying or unjustifiably delaying access to the premises or specific rooms.
- **Refusing to provide evidence or information:** Withholding access to evidence (including digital evidence) or other information relevant to the investigation.
- **Obstructing agency staff:** Preventing agency staff from exercising their powers under the raid authorization.
- **Destroying evidence**: Including deleting electronic evidence (including evidence hosted on the cloud or on mobile devices) or destroying computers or mobile devices, destroying physical documents or any steps taken to conceal, remove or alter evidence.
- **'Tipping off'**: Informing other companies or individuals about the investigation. Agencies conducting raids across multiple premises should be particularly aware of the tip-off risk from employees travelling between premises.
- **Providing false or misleading evidence or information.**
- **Threats or intimidation.**
- **Breaching agency seals.**
- **Abuse of short-lived messaging apps** (i.e., communications platforms which automatically delete messages after a certain period of time): in some jurisdictions, and depending on the circumstances of the case, some agencies consider the company's policy in relation to such platforms and any steps taken during the raid to preserve messages sent using these platforms as a factor in assessing their compliance.
- **Other ways to slow down or interfere with the raid:** Obstruction may also manifest itself through slow or difficult co-operation. Deciding when slow co-operation becomes obstruction can be difficult and depends on the circumstances of the case.

11.2. Necessary Cooperation

The agency should inform the company of any legal obligations to cooperate. It can be helpful for companies to inform their employees about the legal consequences of obstruction.

11.3. How to Minimize the Risk of Obstruction

In addition to informing the company of its obligations, the raid team should also be provided with clear instructions on how to minimize any obstruction. There are several mechanisms agencies may implement to minimize the risks of obstruction, including:

Stage of the raid	Process
Before entry	Agencies may wish to consider the likelihood of obstruction occurring in their pre-search planning. And, where they think it is likely, consider whether the presence of police officers at entry (where permitted under the search authorization) may reduce the likelihood of obstruction occurring in the first place.
Upon entry	Identifying and securing key work areas and key custodians' workstations, for example through placing seals.
	Immediately locating and seizing all mobile devices and other easily concealed items that may contain strong evidence from key custodians. Consider switching mobile devices to airplane mode to secure evidence.
	Requesting key custodians to remain on the premises and to collaborate with the raid officers in order to hasten the raid operation.
	Requesting or requiring (where permitted under the search authorization or the agency's powers) key custodians not present at the premises to collaborate with the raid officers in order to hasten the raid operation for example by returning to the premises with any relevant evidence, laptops or mobile devices.
	Considering advising the company representative of any operations that need to be halted during the raid to secure evidence.
	Requesting employees at the premises not to move documents on desks or remove files from drawers until after the raid has been completed.
	Advising the occupants of areas of a premises being raided that they are not permitted to continue to work on their computer or device, and requesting those persons to first seek clearance from agency staff if they require access to any documents located in that area.
	In some jurisdictions, identifying the rooms, computers, and portable devices and documents to be searched, after which the

Stage of the raid	Process
	custodians are forbidden to make any changes to them until the search of the specific room, documents, device or computer is finished.
	In other jurisdictions and circumstances, agencies may avoid identifying areas of interest to the company until resources to examine those areas are available.
	Unplugging, sealing, or otherwise restricting access to paper shredders.
	Where the raid authorization allows, conducting random sampling of desktops, devices or files to check whether they contain any relevant evidence disguised by irrelevant or misleading labelling by the company.
	Instructing employees via an internal communication (in some jurisdictions, the agency approves the wording) not to delete any electronic records and restricting unsupervised physical and remote access to computers and servers (e.g., by preventing email accounts being accessed through alternative devices that may not have been seized). The agency may also find it useful to see evidence of the time at which the message was sent to employees.
	Ensuring that online and cloud data is preserved and retained, such as through a litigation hold (where the company may be able to apply a policy centrally which prevents employees deleting digital material or could advise its employees not to destroy, delete or alter any evidence during the raid) or a court issued preservation order for electronic records held by third parties (e.g., cloud providers).
	Investigating whether short-lived or encrypted messaging apps are enabled or in use by employees, including whether the automatic destruction function can be switched off and whether the messages are preserved or backed up elsewhere by the company.
During the raid process	Accompanying key custodians to ensure they cannot interfere with evidence or ask someone else to do so.
	Keeping an area secure prior to, and during, any search process. For example, by excluding (where a legal power exists) or asking people to leave certain rooms and/or situating agency staff in rooms where relevant evidence is housed to ensure preservation of the evidence.
	Completing the examination of an area before leaving it unattended.
	Checking that anyone leaving the premises is not removing evidence, for example by checking bags or briefcases (where

Stage of the raid	Process
	legally permittable in the agency's jurisdiction).
	Instructing the company to discontinue the removal of evidence to offsite storage or to ask the cleaning staff not to remove garbage from the premises on the first or second day of the raid.
	Prohibiting any person from entering or leaving the site without permission while the raid is being conducted.
When the raid takes more than one day	Hiring a security guard (or recommending this is done by the company) to watch the premises overnight to prevent interference with seals or evidence and to alert the agency should such interference be attempted.
	Sealing areas and storing evidence in a secure place.

11.4. What to Do in Cases of Obstruction

It is important that agencies initiate early communication with the person in charge at the premises regarding the consequences of obstruction. If agency staff are obstructed from conducting the raid, a discussion with the custodian or the company's legal advisor often resolves the situation. Similarly, clarifying to the company what information can be provided to a third party whose cooperation is needed to download/access evidence can often remove blockages.

Where appropriate, the Team Leader may remind the company of the powers granted by the raid authorization and the fines and punishments which exist for obstruction. In some circumstances, agencies may consider calling upon the police for assistance. Some agencies follow a two-step approach to deter obstruction consisting, first, of some form of warning against interfering with the raid, and second, by a possible charge of obstruction if obstructive conduct is discovered.

Detailed notes should be taken of any instances of obstruction. Agency staff may ask a second staff member to also take notes of the obstruction so that they are not the sole witness. If it is permitted, agency staff may also video record any instances of obstruction.

Before coming to any conclusion on obstruction, agencies may wish to investigate whether any delays are beyond the immediate control of the company, e.g., delays in providing digital evidence may be due to the actions of a third party hosting it, which is not in the control of the company.

11.5. Consequences of Obstruction

Depending on the jurisdiction, responses to obstruction include:

- Criminal proceedings and sanctions, for example, prosecutions, fines and/or imprisonment;[32]
- Monetary penalties (fines) imposed by agencies or the courts on companies and individuals for non-compliance; and
- Treating non-cooperation as an aggravating circumstance when considering the level of penalty sought for the cartel offence.

Companies should be incentivized to fully cooperate during the raid and there should be sufficient consequences for companies who do not cooperate to encourage compliance.

[32] Some agencies treat obstruction as an offense in itself, while others require proof of obstructive intent and/or obstructive effect on the investigation.

12. LEGAL PRIVILEGE

It is good practice for agencies to ensure that everyone involved in a raid is aware of the relevant legal framework recognizing legal privilege and the procedures for identifying and handling legally privileged material.

Legal privilege is a right of non-disclosure which attaches to certain communications, typically between a lawyer and their client, that is recognized in many, although not all, jurisdictions.

Treating legally privileged material correctly is important. The consequences of failing to do so can include:

- Agencies collecting material which is protected by legal privilege and which they are therefore unable to rely on during their investigation.
    - Furthermore, if the agency relies on privileged material as evidence (or otherwise) to make a decision, the investigation itself could be compromised and may be vulnerable to appeal.
- In some jurisdictions, agency staff who have been exposed to privileged information may be excluded from the remainder of the investigation.
- Insufficient knowledge of the relevant legal framework, or of the practicalities of handling privilege claims, may lead agencies to accept excessive or unfounded legal privilege claims, and thus miss out on being able to rely on relevant, non-privileged material.

This section covers important considerations for agencies in planning their strategy for managing material that is or may be legally privileged during raids.

Sections 12.1 – 12.4 are relevant both to digital and hard copy evidence. Additional guidance for legal privilege considerations in relation to digital evidence is provided in Section 12.5.

12.1. Understanding the Relevant Legal Framework for Handling Legal Privilege Claims

Recognition of legal privilege and procedures for handling legally privileged material vary significantly between jurisdictions. This includes, for example:

- Whether the concept of legal privilege exists.
- Whether it covers advice provided by external lawyers only or by both external and internal lawyers.
- Whether it covers any legal advice or only covers material related to enforcement proceedings and clients' legal representations in those proceedings.
- If there are certain key requirements for a document to be covered by legal privilege.
- Whether a waiver of legal privilege is a requirement of a leniency application.

- What the scope of legal privilege is, for example:
    - Does it cover legal advice provided by a foreign based legal advisor to a foreign entity controlling the company; or
    - Does it acknowledge foreign legal privilege irrespective of the local position?
- Whether legal privilege also covers documents or communications involving non-lawyers (e.g. competition economists) in certain circumstances where litigation is contemplated.
- Whether legal privilege is lost if privileged legal advice is forwarded either within the company or to external parties.

Agencies should ensure that everyone involved in a raid is aware of the relevant legal framework and any requirements that this imposes in relation to legal privilege.

12.2. Legal Privilege Considerations When Planning the Raid[33]

At the planning stage, legal privilege considerations may include:

- **Briefing and/or training**: Raid team members should be familiar with their agency's, and/or Courts', relevant rules and approach to dealing with potentially legally privileged material so that they are able to handle any such claims and material correctly. It is good practice to cover this during the pre-raid briefing.
- **Equipment**: Depending on an agency's approach to handling potentially privileged material, specific material may be required (such as, special bags, containers or seals). Agencies should ensure that raid teams are sufficiently equipped with such items.
- **Risk assessment**: To ensure that legally privileged material is appropriately handled, it is good practice for agencies to conduct a risk assessment prior to the raid. This risk assessment could include an assessment of the likelihood of legally privileged material being encountered during the raid (with any perceived risks being recorded in a risk register) and the steps put in place to manage or mitigate that risk.
- **Legal Privilege Protocol:** Some agencies provide a pre-prepared document to the company, setting out how the agency proposes to deal with legally privileged material found during the raid. A protocol such as this can be helpful in navigating the issue of legal privilege, helping to reassure the company that the proper process in respect of legally privileged material will be followed.
- **Independent counsel**: For those agencies that rely on independent counsel to make decisions on claims of legal privilege, asking independent counsel to attend raids (or having them on standby to attend if needed) could be considered where an agency considers it likely that legally privileged material may be present. The presence of independent counsel can be helpful in reassuring the company that the proper process, in respect of legally privileged material, will be followed and/or facilitating 'real time' decision making where the legally

[33] See also Section 5: Organizing the Raid.

privileged status of material is in dispute. Independent counsel may also be used to determine whether documents are covered by legal privilege after the raid (see Section 16).

12.3. Dealing with Legally Privileged Information During the Raid

During the raid, officers may come across material which is or may be legally privileged. Agencies' legal frameworks for dealing with legally privileged material vary and the specific considerations and raid practices will therefore differ across jurisdictions. However, it may be useful for agencies to consider some or all of the steps set out below when planning their strategy for handling legally privileged material during a raid.

12.3.1. Material Over Which Legal Privilege is Claimed Before the Raid

Before starting the raid process, it can be helpful for the raid Team Leader to ask the company representative(s) to identify any material which is "seizable" and which may be covered by legal privilege.

- In some jurisdictions, all such materials are treated as "potentially privileged" and the agency's procedure for handling potentially legally privileged material is applied (see Section 12.3.4).
- In other jurisdictions, the raid Team Leader, taking care not to seek details of the content of the material, may ask the company representative to provide an explanation of why they consider this material to be legally privileged. For example, seeking information such as the addressee, addressor, purpose and context.
    - If the Team Leader is satisfied from the explanation that the material is legally privileged, there is no power to seize the material.
    - If the Team Leader is unconvinced, the agency's procedure for handling potentially legally privileged material should be applied (see Section 12.3.4).

Agencies should be aware that, even if they ask the company representative(s) to identify relevant material which may be covered by legal privilege before commencing the raid, there is always the possibility that an agency staff member will still come across material which appears to be covered by legal privilege. The following sections set out guidance for handling such material.

12.3.2. Material Over Which Legal Privilege is Waived

In some jurisdictions, legal privilege may be waived by the company. However, agency staff should exercise caution in such circumstances, particularly where the waiver is given without legal advice. It can be useful for agencies to consult with their legal team and/or independent counsel in such situations and, notwithstanding the waiver, it may be safest for the agency to seal and consider the material as potentially privileged before reviewing it.

The facts and circumstances of the waiver should be documented in the raid notes.

12.3.3. Assessing Whether Material is Legally Privileged During the Raid

When assessing whether material may be legally privileged it is good practice to take a very cautious approach and to make sure that any disputes around such claims are handled appropriately and with due care.

In some jurisdictions, a member of the raid team can take a cursory look at material in order to assess or verify whether the material is privileged.

- If the material is not clearly privileged, the raid team can ask the company representative to explain why the material should be categorized as legally privileged.

- The raid team may browse parts of the material, such as, a letterhead, to determine if the material came from the company's external legal advisers.

- The raid team should be aware that material being sent to a legal advisor does not necessarily mean that this material is covered by legal privilege, even if the presumption may be such. Likewise, it is possible that material which is marked as 'legally privileged' may not be covered by legal privilege.

- Any disagreement as to the status of material may, depending on the provisions of national law, be resolved by independent counsel or the courts (see Section 12.3.4). If the raid team determines that the material is legally privileged, it should not be seized. The raid team may also consider seeking representations from the company.

Agency staff should exercise caution to ensure that this onsite assessment does not result in the raid team being exposed to privileged content and thus possibly compromising the investigation.

12.3.4. Dealing With Disputed Material

In certain cases, it may not be possible to determine whether material is covered by legal privilege during the raid. In such cases, and depending on the provisions of national law, agencies may decide to place such material, which would be seizable under the terms of the raid authorization, in a sealed container, pending review and determination at a later date by independent external counsel or a court.

Agencies should make arrangements to ensure that the content of the sealed container cannot be examined without breaking the seal, providing assurance that the raid team has not examined material which is potentially covered by legal privilege, except under tightly controlled and transparent procedures (if allowed under the legal framework in the jurisdiction).

Agencies should give consideration to the arrangements for safekeeping of the material placed in a sealed container until it can be reviewed at a later date. In some jurisdictions, the raid team takes the sealed material back to the agency. However, agencies may also decide to leave the sealed material on the premises or with independent counsel for safekeeping.

12.3.5. Legal Privilege Claims Over Material Contained in a Larger Item

Legal privilege may also be claimed over material which is part of, or contained within, a larger item. For example, IT images, specific entries in a diary or specific pages in a file may be subject to legal privilege, while the remainder of the material is not. Different jurisdictions handle this situation in different ways.

- In some jurisdictions, agencies may extract the legally privileged material from the larger item (where physically possible) and remove it during the raid.

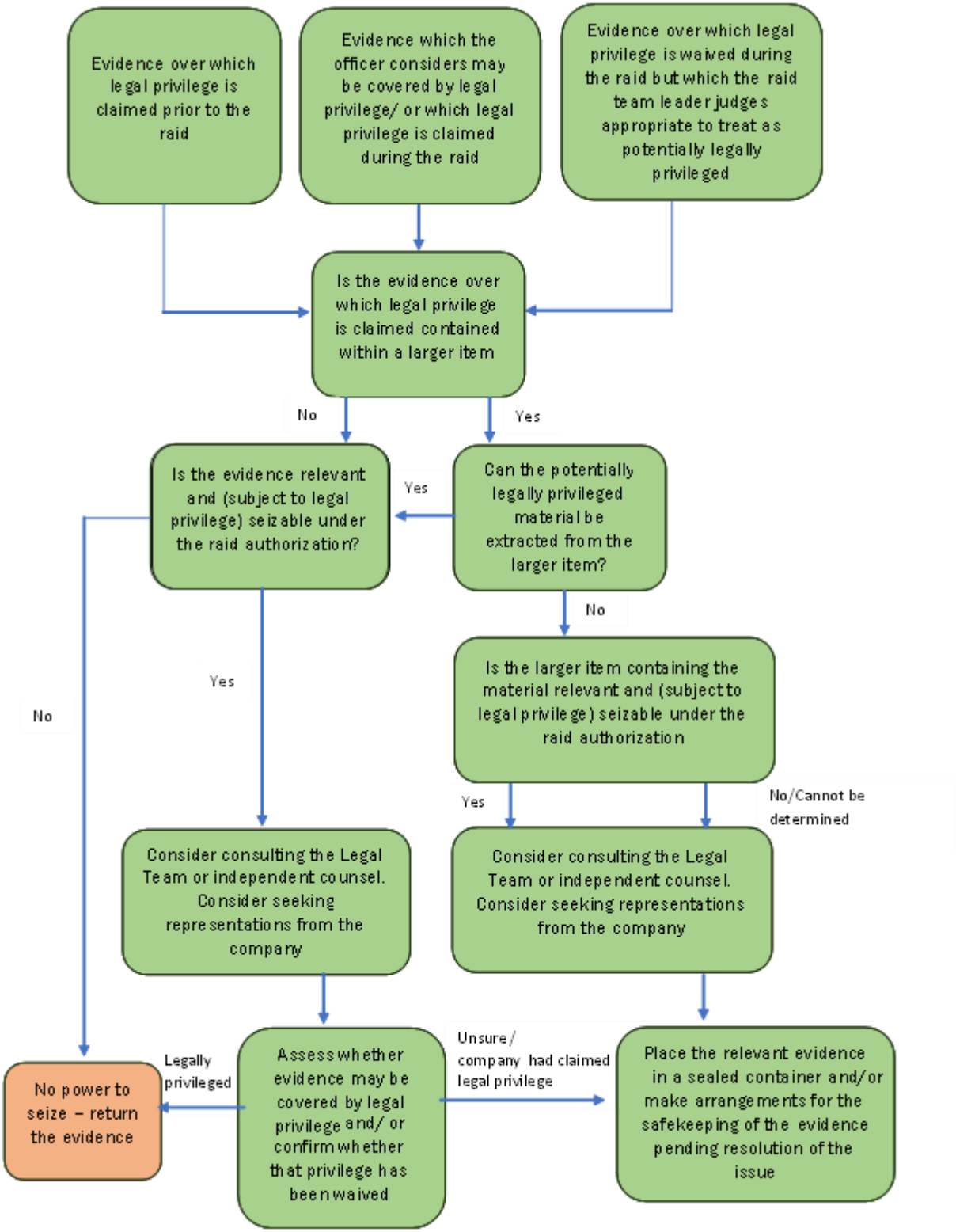
- In other jurisdictions, the whole item is placed in a sealed container pending review after the raid, either by the agency, independent counsel or a court (see Section 12.3.4).

12.3.6. Keeping a Record of Potentially Privileged Material

It is good practice for raid teams to keep a record of the potentially legally privileged material that has been placed in sealed containers. This record should be sufficiently detailed to identify the material, but not so comprehensive that it reveals any information which may itself be legally privileged.

12.3.7. Example of Practical Steps Agencies May Consider When Dealing with Legally Privileged Material

Taking into account the steps set out in Sections 12.3.1 to 12.3.6 above, the following flowchart provides an illustrative example of an approach to dealing with potentially legally privileged material during a raid:


Evidence over which legal privilege is claimed prior to the raid
Evidence which the officer considers may be covered by legal privilege/ or which legal privilege is claimed during the raid
Evidence over which legal privilege is waived during the raid but which the raid team leader judges appropriate to treat as potentially legally privileged
Is the evidence over which legal privilege is claimed contained within a larger item
No
Yes
Is the evidence relevant and (subject to legal privilege) seizable under the raid authorization?
Yes
Can the potentially legally privileged material be extracted from the larger item?
No
Yes
Is the larger item containing the material relevant and (subject to legal privilege) seizable under the raid authorization
Yes
No/Cannot be determined
No
Consider consulting the Legal Team or independent counsel. Consider seeking representations from the company
Consider consulting the Legal Team or independent counsel. Consider seeking representations from the company
Legally privileged
Assess whether evidence may be covered by legal privilege and/ or confirm whether that privilege has been waived
Unsure / company had claimed legal privilege
No power to seize – return the evidence
Place the relevant evidence in a sealed container and/or make arrangements for the safekeeping of the evidence pending resolution of the issue

12.4. Legal Privilege Considerations After the Raid

As described in Section 12.3, approaches to reviewing material flagged as potentially legally privileged vary across jurisdictions. Any material identified as legally privileged following this review should not be accessible to the case team and should be returned to the company. For this reason, it is good practice for material to be returned by agency staff who are not part of the case team.

12.5. Additional Legal Privilege Considerations for Digital Information

The principles set out in the above guidance underpin the handling of legal privilege claims in relation to both hard copy and digital material, including cloud-based material. However, the nature and quantity of digital material often means that it cannot be sifted or reviewed during the raids and/or at the premises being raided. This means that the handling processes for potentially legally privileged digital material will sometimes differ from the handling of potentially legally privileged hard copy material. Agencies should ensure that their legal privilege strategy includes consideration of digital material and takes these differences into account. Depending on the agency's relevant legal framework and search practices, considerations may include:

- **Imaging the digital material for review off-site**: As the amount of digital material is often too large to review at the raid premises, agencies often image and further examine the material when back at their office. Agencies that are not allowed to seize or copy legally privileged material should consider whether it is possible to extract or filter out the privileged material from the wider data carrier, prior to imaging it.
- **Triage**: Prior to the agency reviewing the imaged material to identify relevant evidential material, the imaged material should be triaged for legal privilege. As with hard copy material, practices here vary across jurisdictions. Approaches may include:
    - key word review (where the agency and the company agree on a list of key words likely to cover privileged material, such as names and contact details of lawyers, which are then run over the imaged material), and
    - consultation (where the agency invites the party's lawyers to identify material which they deem to be privileged).

  Generally, the filtering of digital material for legal privilege is not conducted by the case team who will take forward the investigation. For example, in some agencies, this is done by individuals from the agency who will not otherwise have any involvement in the investigation, such as members of the agency's digital forensics team (if available) or other agency staff.
- **Separation**: Any material identified as potentially legally privileged, for example, through the key word or consultation processes, should be isolated from the non-legally privileged material in order to ensure that the case team is not exposed to their contents. Depending on the legal requirements of the jurisdiction concerned this material can then be reviewed by a third party to make a decision on whether it is legally privileged (e.g., independent counsel or a court).
- **Return**: Some agencies do not return digital material. For others, the process for returning legally privileged digital material may differ to that for hard copy material, particularly where the material is contained within a larger data set. In some jurisdictions, the agency may separate out privileged material from that for

the evidence review but retain the original forensic copy (including the legally privileged material) securely and separately for evidential integrity reasons.

Further guidance regarding handling potentially legally privileged digital material can be found in Section 8.3 of Chapter 3 of the Anti-Cartel Enforcement Manual.[34]

12.6. Illustrations

Illustration 1:

An agency could take an image of electronic data for examination at the agency's offices since it is usually not feasible for its digital forensics experts to perform a thorough search of the electronic data on-site due to large volumes of data. The agency and raided company negotiate a protocol in advance outlining how potentially legal privilege material will be identified (based on a standard protocol).

The following are the typical main steps in such protocols. They are performed on true copies of the data in order to maintain the reliability and integrity of the evidence seized.

- Settle a list of search terms to identify potentially legally privileged material (e.g., key words, list of file or folder locations) to the agency's digital forensics expert.
- The digital forensics expert searches the seized electronic evidence using those terms and isolates the evidence that is responsive to the search terms ("potentially privileged evidence") (the case team will not have access to this evidence).
- A copy of the potentially privileged evidence is provided to counsel for the raided company for review.
- Counsel for the raided company will identify the evidence over which the company is claiming legal privilege (they may also provide a revised list of search terms to be applied to the potentially privileged evidence).
- The digital forensics expert will isolate any evidence over which a claim of legal privilege has been made (the case team will not have access to those evidence).
- Evidence not responsive to the search terms and evidence reviewed by counsel for the raided company but not subject to a claim of legal privilege are provided to the case team for review.

[34] ICN Anti-Cartel Enforcement Manual, "Chapter 3: Digital Evidence Gathering" available at: https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering/.

- The case team uses electronic discovery practices and procedures to search for and identify relevant evidence as outlined in the raid authorization (they also follow steps similar to those outlined above if they identify additional evidence they believe may be subject to legal privilege).
- The digital forensics expert provides a list and copy of the relevant evidence to counsel for the raided company to review and identify any additional evidence over which the company is claiming legal privilege.
- Counsel for the raided company and the agency and/or prosecutor agree a procedure to determine whether the claims of legal privilege are valid (if they cannot come to an agreement, it will be determined by the court).

Illustration 2:

In jurisdictions where agencies are not allowed to seize evidence and can only make copies of it, when companies claim legal privilege over some of the documents that the agency intends to reproduce:

- If the copies are physical, the reproductions of the disputed documents can be placed in sealed containers while their privileged nature is reviewed and determined.
- If the copies are digital, some agencies will place the specific files that contain the disputed evidence in a different medium (i.e. DVD, hard drive, flash drive, etc.), separate from the rest of the evidence that was gathered. In turn, that medium can be placed in a sealed container so that it can be analyzed later on. This way, the agency can still access the other documents while the determination on the disputed documents is made.

13. SEIZURE

This section sets out considerations for agencies in examining, selecting and seizing the relevant evidence during the raid. The guidance provided in this Section is intended to apply to both digital and hard copy evidence. However, the nature and amount of digital evidence means that the seizure process may sometimes differ from the process used for hard copy evidence. Where this is the case, the specific considerations for digital evidence are outlined in the text.

13.1. Examination, Selection and Seizure

It is good practice to triage the evidence to ensure that only evidence relevant to the raid authorization is seized.

13.1.1. Examination and Selection

Agencies should ensure that only relevant evidence is seized. In many jurisdictions, this is done through a two-step triage procedure:

- Firstly, an initial selection is made on the basis of the wording or content of the raid authorization. In some jurisdictions, the authorization stipulates the specific types of evidence which may be seized. For example, the raid authorization may refer to:
  - Correspondence between XYZ (Country A) Ltd. and XYZ (Country B) Ltd. relating to contract arrangements with third parties; or
  - Agendas, minutes or other documents that indicate an agreement may exist between competitors as to the price at which goods or services will be bought or sold.
- Secondly, selection of the evidence is completed on the basis of relevancy. Relevant evidence is that which is directly or indirectly related to proving the offence as set out in the raid authorization.

Agencies' approaches to carrying out an initial examination and selection vary. In some jurisdictions, agencies perform both activities during the raid and whilst at the premises. In other jurisdictions the initial examination happens on site with the final selection occurring back at the agency's offices. Where the agency identifies materials which exceed the scope of the raid authorization but may be relevant to the investigation, the agency may apply for an additional or extended authorization or may consider whether the evidence can be obtained through a voluntary submission.

If objections or controversies regarding relevance are raised on-site, it may be appropriate for agency staff to explain why relevance is deemed to exist and to document the explanation given.

13.1.2. Seizure

Hard copy evidence

For hard copy evidence, many agencies seize a copy of the evidence, rather than the original documents. Depending on agency practice and/or the nature of the evidence, this copying may be carried out on the premises or back at the agency. In the latter case, the original documents are returned to the company as soon as the copies are

made. Some agencies may seize original documents on occasions where taking copies is not possible and/or where evidence continuity rules, such as in criminal cases, require it.

Digital evidence

When seizing digital evidence, most agencies use specialist forensic tools. These tools allow the agency to make forensic copies of the dataset (including the metadata), without altering the underlying data.[35] For more guidance in relation to the forensic seizure process for digital evidence, see Chapter 3 of the Anti-Cartel Enforcement Manual on Digital Evidence Gathering.

Illustration 1: Examining, Selecting and Seizing Hard Copy Evidence

In one jurisdiction, the description of evidence listed in the raid authorization serves as a guideline for the preliminary selection of evidence to be seized. Given that at the initial selection stage it is often difficult to determine relevancy, the agency will first select evidence that seems relevant but will, during a secondary selection, reject some of this evidence as unnecessary. A "Location Identifying Note" (LIN) is affixed to the evidence as it is selected by the agency staff member and the evidence is then placed in an expandable folder. The LIN includes information about the precise location where each piece of evidence was found (e.g., third drawer of desk in file labeled "Sales Report" in office of Ms. X, Sales Manager), as well as the agency staff member's name and the date the evidence was selected. Each expandable folder is identified in terms of the area searched (e.g., Office of Mr. X, President or Ms. Y, Accountant, etc). Each time a new office or area is searched, a new expandable folder is used as a temporary repository for the preliminary record selections from that area. Once the search of that area or office has been completed, the folder is sealed and placed in a pre-determined secure area and the agency staff member will proceed to search the next assigned area.

Further examination and culling of records is done during the secondary examination at the raid team's work area at the premises being raided. Records that are deemed not to be necessary during the secondary selection, or culling phase, are returned to the office from which they were initially selected. The secondary, or final selection of documents to be seized, is usually done by the search Team Leader who will have the advantage of looking at all the records. The Team Leader may also consult with the lead investigator when deciding which documents are relevant. The Team Leader also ensures that all selected records fall within the scope of the raid authorization and can therefore be seized.

[35] Beyond that minimally necessary to recover the evidence in the first place.

13.2. Seize and Sift Powers

Agencies in some jurisdictions have "seize and sift" powers which may be used in certain circumstances. Using seize and sift powers, the agency may remove items of evidence which are not covered by the raid authorization from the raid premises where they contain items that are permitted to be seized under the raid authorization or where the relevance cannot be determined onsite. For example, the agency may seize an entire diary or notebook where only one page is relevant, seize an entire file where only certain documents are relevant, or copy an entire hard drive where only certain documents are relevant. Seize and sift powers may be particularly relevant in relation to digital evidence, where the size and nature of the dataset may make relevance sifting on the premises impracticable.

The circumstances in which seize and sift powers may be used are generally restricted, such as:

- Where it is impractical to determine whether something is relevant while at the premises.
- Where the relevance determination or separation would take an unreasonable amount of time.
- When it is suggested by the company if they consider that the time required to determine whether something is relevant may affect the functioning of the business.
- Where it is a private premises, as the time spent on the premises is especially sensitive.
- Where the determination or separation would damage of affect the item.
- Where it would be necessary to use specialist equipment which is not available at the premises, e.g. digital forensic extraction tools.

Following seizure of evidence under seize and sift powers, the agency reviews the evidence when back at the agency's offices. This review should include consideration of relevance, management of personal data, and appropriate handling of any legally privileged material.[36] In some jurisdictions, any subsequent review at the agency's premises of evidence under seize and sift powers should be carried out in the presence of representatives from the raided company (including external counsel).

13.3. Handling Personal Data

As part of their seizure strategy, agencies should consider how they will handle personal data. In some jurisdictions, agencies ask the company for representations as to which evidence is likely to contain personal data, to inform their evidence selection. In other jurisdictions, agency staff make the determination themselves.

Agencies should ensure that they comply with any legal requirements in relation to the processing of personal data. For example, in some jurisdictions, agencies may only

[36] For more guidance in relation to legal privilege, including in relation to evidence where the legally privileged material is contained in a larger document, see Section 12.

process personal data where the processing is necessary for compliance with the agency's legal obligations, for the performance of a task carried out by the agency in the public interest or in the exercise of official authority vested in the agency.

Where the personal data is contained within a larger item containing relevant evidence, agencies may also consider whether it is possible to separate the personal data from the underlying piece of evidence. For example, where the personal data is contained within a diary containing records of meetings which are relevant under the raid authorization, the agency may decide to copy only the pages including the relevant meetings. When separating evidence, agencies should consider any potential impact this may have on the integrity of the evidence. This is particularly the case in relation to digital data, where removing part of a dataset may affect the forensic integrity of the remainder of the data.

13.3.1. Mobile Devices

It is increasingly common for relevant evidence to be stored on mobile devices. The below table sets out a number of considerations for agencies when handling mobile devices which may contain both personal and business material.

Consideration	Comment
Legal powers and restrictions	Some agencies must obtain prior authorization (for example from a judge) to search any mobile devices found on the premises. To obtain such authorization, the agency may be required to demonstrate that they have reasonable grounds to believe that any mobile devices will contain relevant evidence. Some authorizations allow the agency to search for mobile devices on a custodian's person, while in others, the authorization specifies that custodians must hand them over.
Is the device a business device or a personal mobile device?	Some agencies may be more restricted in their powers to seize or search personal mobile devices. Sometimes pre-raid research allows the agency to know in advance if the custodians use their personal mobile devices for business purposes. Otherwise, to help determine whether a device is a business or personal device, agencies may consider: • Whether the device is strictly used for business purposes. • Whether the device belongs to the custodian or to the company. • Whether the custodian or the company pays any bills connected to the device (e.g., for Internet or telecommunications services). • Whether the device is personal but has also been used for business purposes, e.g. conversations with competitors or discussions with other employees on business topics. Some agencies may also conduct a preliminary review of the device to determine whether it contains solely personal information; for example, by checking messaging apps for any contact with competitors. When conducting such a review, the agency should ensure that the tools and processes used do not alter the data contained on the device or its forensic integrity[37].

[37] Beyond what is minimally necessary to recover the evidence in the first place.

Consideration	Comment
Is it possible to separate out the personal data from the device?	Where possible, some agencies may separate the personal and business information contained on the device and only seize the relevant business information. Agencies should ensure that their separation process does not alter the device or the dataset, in order to preserve the forensic integrity of the evidence. [38] Other agencies seize and copy the whole device and deal with issues in relation to personal data when back at the agency's premises.[39]
Consent	Where an authorization does not permit an agency to search a custodian or demand they hand over mobile devices, some agencies may need the custodian's consent to seize their mobile devices, especially where the device is a personal device. Other agencies may involve the custodian and/or company in the review process (for example, by allowing the custodian to shadow the agency staff in their review of potentially personal communications).

13.4. Coding and Other Forms of Evidence Identification

It is good practice to ensure that evidence seized during the raid is coded or labelled to ensure that it can be identified and to preserve the chain of custody.

It is good practice for agencies to code all seized evidence with a unique identifier. This includes copied digital evidence. Coding evidence is usually done at the premises during the raid.

In jurisdictions where agencies are able to seize evidence for relevance review offsite under seize and sift powers, the agency may give the file an initial reference for seizure purposes and then give the individual documents individual references following the sift process.

Approaches to evidence labelling vary across jurisdictions, for example:

- Alpha-numeric identifier: Some agencies use an exhibit label or stamp to create an alpha-numeric identifier for each document, for example a combination of the initials of the agency staff member conducting the search and the name of the company raided, or a unique alpha code with a serial number. Other agencies place the evidence in sealed bags and then affix the label to the bag. In practice, some sealable bags may come with their own pre-printed unique reference or bar code.

[38] Beyond what is minimally necessary to recover the evidence in the first place.
[39] This may fall under seize and sift powers. See Section 13.2 for more guidance.

- "Location Identifying Note" (LIN): In addition to the alpha-numeric code, some agencies attach a LIN to the document which contains information concerning each record or group of records found at any given location.
- Number and list: Some agencies use a numbering and listing approach, whereby a numbered sticker is affixed to the evidence and a separate list is compiled which provides details about the evidence and where it was found.

Whichever identification approach agencies choose to take, it is important to ensure that the evidence coding contains sufficient information to identify the evidence. This might include some or all of the following information:

- The name of the company raided.
- The location where the document was found.
    - For hard copy documents that would typically be the name of the office or general area and the exact location within that area e.g., filing cabinet, desk, box or file name. For digital documents that would typically be a description of the digital data itself e.g. a cloud profile, a server, custodian, laptop or a mobile device.
- A brief description of what the document is.
    - For hard copy evidence this could be for example: "letter dated XX from XX to XX", "Diary of Mrs X" or "File containing project prices".
    - For digital documents this could be a description of the documents copied and the container upon which the copies have been stored. For example: "Hard drive containing forensic copy of Mr Y's laptop", "Hard drive containing forensic copy of cloud profiles of custodians A, B and C" or "Hard drive containing forensic copy of Ms G's mobile telephone".
- The date and time the evidence was found.
- The name of the agency staff member who found the evidence.
- The name of the agency staff member who coded the evidence.

13.5. Receipt for Seized Evidence

In some jurisdictions, agencies provide a list of the seized evidence (or a note confirming that no evidence was seized) to a representative of the company. Some agencies allow the company representative to compare the evidence listed with the actual evidence seized.

The evidence list may include some or all of the following information:

- Information in relation to the agency staff members conducting the raid, such as the initials or signature of the agency staff members conducting the raid or of the Team Leader.
- An overview of the evidence, including:
    - The size of the evidence set seized (such as the number of documents seized or devices imaged).
    - Where the evidence was located (including the number of documents found in certain locations, e.g., in a particular office).
- Identifying information in relation to the seized evidence, including:

  - The alpha-numeric code range identifying the evidence seized, including any missing or unused codes.
  - The types of evidence seized and, where applicable, the document titles.
  - The document's author or, in the case of a device or a cloud data set, the custodian.
  - A brief description of the document.
- Information in relation to the seizure, including:
  - The date and time of the seizure.
  - The agency staff member responsible for the seizure.

In some jurisdictions, agencies also provide the company with a copy of their raid report in addition to the evidence list.[40]

13.6. Continuity of Possession

Approaches to preserving the evidential chain of custody and continuity of possession vary across jurisdictions and depend on the powers used to conduct the raid. Preserving and demonstrating the chain of custody is particularly important for agencies conducting raids under criminal powers. However, even in jurisdictions with administrative regimes, agencies may adopt a chain of custody process similar to that used in criminal regimes or may implement alternative procedures to safeguard the authenticity of the evidence.

Continuity of possession requires agencies to demonstrate that evidence is collected, transported, stored and handled in a way which maintains its nature and the integrity of its content, ensuring that it is not accidentally or deliberately altered, substituted, contaminated or deleted.

This ensures that the agency can later demonstrate that the content of any original evidence relied on is identical to that which was seized during the raid and is unaltered and that any copies are a true copy of the original.

Maintaining continuity of possession by avoiding altering evidence is an important principle. However, strict adherence to that principle is challenging in the context of digital evidence, where altering evidence may be unavoidable to recover it in the first place. For example, switching a mobile device on will alter many aspects of the data without affecting the content of a message. In the circumstances, any alteration should be limited to that minimally necessary to recover the evidence in the first place. Agency staff responsible for collection are encouraged to keep good records documenting any changes which will enable them to acknowledge and articulate the impact of them.

Continuity of possession is achieved through recording the chain of possession from the point that the evidence is located. This may be achieved through one of the following ways:

- Each member of the raid team is responsible for the evidence which they have seized throughout the course of the raid and must keep that evidence in their possession.
- The agency designates a specific site exhibit officer with responsibility for all the evidence seized at the premises. Raid team members hand over the documents which they have found to the site exhibit officer who maintains possession until

[40] For more guidance in relation to the raid report, see Section 9.2.1.

they are brought to the agency. Alternatively, in some jurisdictions, the documents may be transferred to the site Team Leader or lead investigator on the case, who then takes responsibility for ensuring continuity of possession until the documents are taken back to the agency. It is good practice to document the transfer process, for example in the evidence log. The site exhibit officer may also be responsible for maintaining a log of the seized evidence.

- The agency places the evidence in a sealed container. The seals remain intact until the evidence is brought back to the agency. In many jurisdictions, the site exhibit officer is responsible for maintaining possession of the sealed containers and ensuring that the seals are not breached.
- Agency staff request a company representative to be present during the raid, who is responsible for the selected evidence. At the end of the raid, the representative delivers the evidence to the agency with an identifiable seal or with serial numbers to allow for the evidence to be identified.

Illustration 1:

In some jurisdictions, the agency safeguards the authenticity of the evidence through taking two copies of the seized documents. The agency retains one of the copies and leaves the other copy (as well as the original evidence) with the company. If subsequent claims concerning the authenticity of the documents are raised, the agency can compare the copies taken from the premises with the duplicate copies given to the company.

Illustration 2:

Some agencies attach a complete exhibit label to all evidence seized. This information is subsequently noted in the raid team member's notebook. Any movement of exhibits is recorded in the agency's evidence list, including the unique identifier, the name and signature of the agency staff member releasing the exhibit, the name and signature of the person receiving the exhibit, and the reason for the change of custody. The exhibits are stored in dedicated secure exhibits rooms, with entry controlled and restricted by the agency's exhibits officer.

Illustration 3:

Some agencies address issues and potential disputes around the integrity and continuity of evidence by recording (e.g., by videoing or photographing) key stages of the search and seizure process.

13.7. Security of Evidence During Extended Raids

In some circumstances, raids cannot be completed within one day. In jurisdictions where agencies are able to leave the raid premises and return, agencies should implement measures to ensure that evidence is not tampered with if it is necessary to leave the premises overnight and return the next day. Approaches to ensuring that evidence remain secure for extended raids lasting multiple days vary across jurisdictions:

Approach	Description
Leaving the evidence to be seized under seal on the premises	Some agencies seal the evidence, premises or digital devices to be seized if the raid cannot be completed in one day. If agencies decide to leave the evidence to be seized on the premises, the following steps may be considered: *Exiting the premises* • Evidence that has been selected may be placed in a sealed and/or locked container within the agency staff's workspace on the premises. The room may then be sealed with signs warning not to break the seal. • Agency staff may seal rooms which still need to be searched and place signs warning not to break the seal. • The company should make all relevant company staff aware that the agency is sealing the area. • Agency staff should record the location of the evidence and the seals, as well as the end time of the search. In some jurisdictions, agencies may consider hiring a security guard to ensure that evidence is not tampered with. In other jurisdictions, agencies may recommend that the company do so. *Returning to the premises* • Upon returning to the premises, agency staff should check any seals which were placed and record whether there has been any tampering. Penalties for tampering with seals vary across jurisdictions, Agencies should make companies aware of the consequences of breaking a seal.

Approach	Description
Daily removal of the selected documents	Some agencies remove selected evidence on a daily basis if the raid is not completed in a single day. If agencies decide to remove evidence from the premises, it should be considered whether: • The documents need to be sealed for removal; • A receipt needs to be issued for the documents on the day they are removed; and, • The selected documents are to be brought back to the premises each day, or whether they are to be stored somewhere pending the conclusion of the raid.
Combining the removal of the selected evidence and sealing the premises	Some agencies perform a risk assessment to determine whether the evidence should be sealed or removed from the premises on a daily basis. If the Team Leader is of the view that there is little or no risk that the seized evidence will be destroyed, removed or altered then it can be left under seal. Where there is a likely risk, the evidence should be removed from the premises following the agency's usual sealing and receipting protocols.
Remaining on the premises until the raid is completed	Some agencies stay at the premises until the raid is completed. This may be the result of the limitations of raid authorizations, which may only allow for single entry. All seized evidence is removed from the premises when the raid has concluded and agency staff leave the premises.

13.8. Providing Copies of Evidence

In some jurisdictions, agencies may only seize copies of evidence, unless it is necessary to take possession of the original evidence, or it is impractical to copy the evidence on the premises. In other jurisdictions, agencies may seize original evidence. If original documents are seized, companies may be entitled to obtain a copy, either during or after the raid. It is recommended that agencies consider the following factors when assessing requests for copies of evidence:

Factor	Considerations
Whether the agency removed the original documents or copies	If the agency removes copies of the documents and the company continues to hold the originals, they can copy the relevant documents themselves. Conversely, if the agency seizes the original documents, the company will no longer possess the seized material and it may be reasonable to provide copies.
Whether the request concerns physical or digital evidence	Agencies may not be required to provide a copy of digital evidence which has been imaged, as the electronic originals remain with the company. The company continues to have access to the digital material and can copy it themselves.

Factor	Considerations
The availability of photocopy facilities	If sufficient photocopy facilities are not available during the raid, it may not be practicable for the agency to provide copies of documents during the raid.
The volume of evidence to be copied and the time required to make the copies	If providing copies of evidence to the company would disrupt the raid, either because of the volume of the evidence to be copied or the time required to make the copies, it may not be reasonable for the company to request copies of the evidence during the raid. Whether copying can be limited to documents that the company considers are most essential for the running of the business.

If an agency has agreed to provide copies of evidence to the company, there are several practical considerations:

- Agencies may decide to make copies of the evidence on the raid premises to provide to the company;
- Agencies may decide to allow company representatives to make copies of the evidence under close supervision; or
- If it is not feasible to make copies of the evidence on the premises, agencies may decide to return to their office to make the copies. All original evidence should be returned to the company at the earliest opportunity.

14. DEALING WITH COUNSEL TO PARTIES

During the execution of the raid, it is good practice to designate one person (for example, the Team Leader) to communicate with the parties' lawyers.

It is likely that raid team members will be required to deal with lawyers (internal or external) for companies being raided. In some instances, lawyers may provide assistance to enable the raid team to conduct the raid more efficiently (e.g., by providing organizational charts or obtaining the participation of company staff who are not present at the raid premises). Other times, they may make the raid more difficult. It is good practice for agencies to put in place a clear strategy for dealing with lawyers prior to the raid. Examples of strategies for dealing with lawyers include:

- Designating one person (e.g., the raid Team Leader) to communicate with the company's lawyers.
- Developing a clear and simple explanation of the powers being exercised and procedures that will be followed for the designated agency staff member to refer to when speaking with the company's lawyers.
- Developing a culture that empowers and supports the raid team to continue the raid irrespective of possible attempts by lawyers to obstruct or hinder it.
- Referring any legal issues, such as discussions on the validity or scope of the raid authorization, to the lawyer assigned to the agency's inquiry or the "control room" back at the office.
- Communicating clearly that the relevant evidence assessment is a matter of the raid team alone, not of the company's lawyer.
- Communicating clearly that, while the company's lawyer may wish to make representations if the issues are not resolved, the raid will continue, and the company can discuss them with the agency or in court later.
- Creating a chat group before the search that includes the agency's lawyers to facilitate quick consultation if necessary.
- Having a procedure ready to deal with challenges to the seizure or production of evidence which does not affect the rest of the raid. For example, setting the item aside so that it can be considered separately.
- Preparing a process to handle any allegations of illegality or abuse of power, such as recording the situation for the purpose of forwarding it later to the relevant authorities.

15. DEALING WITH THE MEDIA

It is good practice to designate one spokesperson to respond to media enquiries.

It is good practice to consider, before the raid is carried out, what the agency's press line should be in the event that the raid becomes public.

If an agency receives media enquires before a raid, they should use the utmost care when deciding what information, if any, to share to avoid tipping off the target companies.

Agencies may consider the following recommendations for media communications during a raid:

- **Establish a comprehensive media strategy:** Establish a comprehensive media strategy prior to the raid, taking into account the media position of the parties and how to handle potentially market sensitive information. This could include media lines and anticipatory questions and answers. If an agency has a centralized press team, it is advisable to involve this team at an early stage of the raid planning.

- **Develop a Data Disclosure Protocol:** Agencies should develop a protocol to identify the data they can publicly disclose. Before disclosing sensitive data, including the names of custodians allegedly involved, agencies should carefully evaluate the potential impact on ongoing investigations and prioritize the success of the investigation. Agencies should also avoid disclosing competitively sensitive data.

- **Prepare justifications for non-disclosure:** Agencies choosing to withhold information should be prepared to address potential inferences drawn by the media and consider offering a clear rationale for the decision.

- **Designate an official spokesperson:** Appoint a single spokesperson to handle all media inquiries. Agencies with established media departments should direct inquiries to them.

- **Consider a proactive briefing:** Some agencies publish press notices or briefings once a raid has started to manage the narrative surrounding the raids, raise public awareness or encourage whistleblowers or informants to come forward. This briefing could provide details about the operation's scope and purpose. Some agencies publish the names of the companies being raided while others do

not. Agencies typically vary their approach depending on factors such as the necessity to publish, industry in question and whether the company intends to publish a press release itself. Agencies may wish to inform the company being raided in advance of such proactive briefings, so that the companies themselves may also consider their approach. Some downsides to proactive briefings are:

- They can put other companies involved in the cartel on notice. This could result in the loss of evidence before any subsequent raids, for example, if the agency seeks additional raid authorizations based on new information obtained during the initial raids.

- They can attract media to the site, potentially exposing the raid teams and generally being an unwelcome distraction from the raid team's primary objective of the diligent execution of the raid.

- They may raise legal risk where, for example, they prompt assumptions about a company's culpability ahead of any final decision.

- **Consult the raided company:** The raid Team Leaders could ask the companies being raided whether they intend to provide a press briefing. If the companies intend to do so, the raid Team Leader can ask them to share the proposed briefing with the agency and/or to liaise with the agency's press team particularly regarding the timing of issue of such a press briefing.

16. AFTER THE RAID

16.1. Transporting the Evidence Back to the Agency's Offices

It is good practice to deliver all seized documents to the agency's offices as soon as possible upon completion of the raid and to ensure all seized materials are secured in a facility with restricted and monitored access.

It is good practice, where applicable, to consolidate all notes as soon as possible after the raid to create a complete record of the raid.

Agencies should ensure that the seized evidence is transferred back to their office in the safest manner possible and be aware that the chain of custody of all material seized during the raid should be maintained throughout the process. In some jurisdictions, agencies may store the seized data in an encrypted file on a protected device, ensuring that only authorized agency personnel are able to access it. This file may include both digital material and digital copies of hard copy documents, copied at the premises.

Depending on the agency's policy and legal framework, in some jurisdictions, agencies securely delete any intermediate information generated during the raid at a company's premises using certified tools, ensuring that only relevant information is taken out of the company's premises.

16.2. Back at the Agency

After executing the raid, it is good practice for agency staff to complete the tasks listed in the chart below.

Action	Description
Consolidate records	After a raid, agencies should consolidate all statements, notes and reports as soon as possible to create a complete record of the raid. Agency staff should follow the agency's procedures to reconcile records of property so that any inconsistencies or errors in the record keeping are identified and corrected. In some jurisdictions, the agencies need to provide a written report of the conducted raid to the company subject to the raid afterwards or very soon after its conclusion.
Document transfers	Agency staff should properly document any transfers of evidence to ensure continuity of possession.
Return equipment	Agency staff should return all supplies and equipment and

Action	Description
	report any changes in their condition.

Hold debriefing session(s)	Agencies should have a debriefing session(s) with the search teams to:
	• Identify/pull together evidence for the case team.
	• Identify the following for learning purposes:
	  ○ What went well.
	  ○ What did not go well.
	  ○ What can be learned or done differently in future raids.
	Some agencies also include in these sessions the agencies that have assisted them during the raids.

Illustration 1:

In one jurisdiction, raid team members forward copies of all statements, notes and reports to a designated member of the case team as soon as possible after the conclusion of the raid. In addition, each raid team member must provide an affidavit documenting all transfers of records to establish continuity of possession. The legislation governing the agency's raid powers also requires that, when records are seized under the authority of a raid authorization, a report of the evidence or things seized must be provided to a judge.