



Investigations Management Software: A Buyer's Guide

Investigations can vary greatly in duration, amount of information discovered, manpower, cost, importance and impact. Due to their complexity, information technology is increasingly being applied to improve investigations management.

This guide, based on practical experience in the field, has been developed to help investigators select the best software solutions.

All investigations share a common set of underlying processes which can be broadly divided into three areas:

1. Project management

- goal setting and initial planning
- assigning and managing tasks
- recording the actions taken and results achieved
- further planning based on information and items discovered
- managing resources and people
- reporting progress

2. Recording, managing and exploiting information

- identifying potential offences
- identifying and eliminating suspects
- recording large volumes of items, including structured and unstructured information
- maintaining the continuity or chain of custody of items
- identifying connections from information discovered in current and previous investigations

3. Compiling evidence for use in court

- preparing witness statements
- cross referencing witness statements with items and other witness statements
- providing the prosecution with all information relating to the investigation and brief of evidence

Several investigations management solutions are available, with wide variance in price, suitability and capability. *The one thing they all have in common is the vendors' assurance that the solution in question will solve all your problems!*

To separate the multitude of options, we recommend a four question test which addresses the critical areas of purpose, technical design, ease of configuration and ability to maximise information exploitation.

Question 1: Is the software purpose built for investigations management?

At first glance, apparent similarities between investigations management and generic business activities make it attractive to simply implement a generic business solution such as Customer Relationship Management.

However in reality, fundamental differences exist between maintaining sales leads and running an investigation.

Generic business software exists in a world where data is largely complete and accurate. In comparison, investigation management software must cater for data that is often:

- incomplete – a person's surname is unknown
- vague – a person was born in late 1960
- incorrect – a person gives an address that you know does not exist, but you must record that that address was given
- conflicting – the same person is described as having brown hair and black hair by two different witnesses
- historic – it may be just as important to record where a person lived five years ago as it is to know where that person lives today



While most business software will include security features, these are unlikely to be sufficient for investigations management where lives are at stake. Insist on the following attributes in your solution:

- no back doors exist that allow any user, including administrators, to bypass security to view or change information
- all changes to data are logged for every user, including administrators
- all changes to data are recorded, including the original and changed version
- users can be given different security levels, depending on their role in a case, i.e. an investigator may be Lead Investigator on one case but just a member of an investigating team on another.

- security is so 'fine grained' that a single piece of information in a case can be made secure, not just the whole case

Question 2: Does the investigations management solution operate as a single application?



This is desirable for a number of reasons. Reduced cost is one, as the cost of integration can be more than twice the cost of the applications. A single application will enable easier collation and faster searching as data is not fragmented across multiple applications. If several applications is used, they should be tightly integrated and ideally from the same vendor. Multiple searches to find data in different applications are time consuming and have the potential to miss information altogether.

If data is shared between applications, it should be shared by reference, i.e. both applications point at the same record and therefore always agree. While sharing data by copying seems harmless enough initially, it becomes more complicated over time and prone to errors as it requires both applications to be able to identify the copy in the other application (not easy) and write to its own record as well as the copy every time.

Attempting to integrate records by stripping data from one application and importing it into another to collate information is not a practical solution. The time it takes to strip and import information can be limiting when large data sets are involved and, as soon as the data is stripped, there is no way to check its currency, except to strip the entire data set again. This method also means there is no means to drill back into the original data set.

Question 3: Is the software easily configurable to meet changing operational needs?

Configuration means elements of the application can be changed at runtime by an authorised user, either using the application or an accompanying utility.

Look for software that can be configured without additional programming and at any time, irrespective of whether data has been entered into the application or not.

One of the major benefits of easy configuration is savings in up-front and ongoing costs. An off the shelf commercial investigation management application that can be configured to your needs will be cheaper to purchase than developing one in-house. It will also allow changes to be made by your own team without hiring outside developers. Just as important is achieving the right 'fit' with your organisation's unique operational characteristics, legislation and the criminal environment, and the ability to be used by several different agencies at once. This reduces overall infrastructure costs and increases the potential for data sharing.

Configuration can apply to almost any aspect of the application. Some examples include:

- translation of the interface into multiple languages
- the use of your accepted terminology in the interface (even if the language is not changed)
- creation of entities that can capture information specific to your agency or investigations
- default behaviour of the application
- security behaviour and organisational structure
- the addition of new code tables and code table values
- a thesaurus
- text search stop words

Question 4: Does the software maximise information exploitation (subject to security)?

Information exploitation is the process of using information to further your goals and takes place through two different, but closely related activities. The first is 'collation', a mechanical process of organising information in various ways, so that relationships, patterns and sequences of interest can be seen. The second is 'analysis', a human process that ingests collated information and generates insight, assigns meaning, establishes cause and effect and enables the prediction of future events.

Software can collate, but it can't analyse. It can only show information in various forms such as grids or link diagrams for a person to analyse. Collation relies heavily on structured information. The richer and more structured the information, the more ways it can be organised and the greater chance the human brain has of seeing a connection or pattern. This process is just not possible with unstructured text, irrespective of how well you can find any particular word or phrase. For example, a text search cannot tell you if the number of phone calls between A and B are increasing before a particular event such as robbery.

Configuration allows the application to hold structured information, which is critical because there is no means of predicting all structured information that may be required at any one point in time. Other features important for information exploitation are the ability to import structured information from third parties with a minimum of effort and multiple integrated collation tools that act on all information without data stripping.

Summary of questions to ask a vendor:

Purpose built?

- Who designed this software and for what purpose?
- Who else is using this software and what for?
- How does it cater for incomplete, vague, conflicting and historical information?
- How flexible and granular is your security model?



Single application

- Can/how do I tie the project management, information management and exploitation and evidence presentation activities together using your software?
- How do I record/manage/collate the information in the application?
- How many other pieces of software from you (or anyone else) do I need to cover project management, information management and exploitation and evidence presentation activities?

Configurable

- Tell me if/how I can configure the software to suit my needs?
- Is your software able to include local terminology?
- Is your software available in languages other than English?
- Can I add new entities and attributes?
- Can I add new code tables and code table values?

Maximises information exploitation

- What structured information is your software capable of importing/holding/collating?
- What collation tools does your software have?
- How do these collation tools access information?