INVESTIGATION · METHOD AND THE FUTURE

Investigative Case Management Systems and Knowledge Organization

Investigations produce large volumes of information that must be recorded, linked, prioritised and retrieved. This article explains how case management systems organise investigative knowledge, lessons from major inquiries where information was lost, the core functions such systems need, how entity resolution and indexing work, the risks of poor data, and how to choose and govern a system.

ModQu research article · 2,143 words · 24 references (APA 7th edition)

An investigation is, among other things, an exercise in managing information. Statements, documents, exhibits, tips, interview records, analysis, decisions and actions accumulate quickly, often in the thousands or millions of items. Investigators must be able to record each item, connect it to the people, places, events and objects it concerns, decide what to do next, and later show what was known, when, and what was done about it. Case management systems are the tools for this work. When they function well, they turn scattered information into organised knowledge. When they fail, crucial facts are lost in plain sight. This article explains how case management systems organise investigative knowledge, what they must do, and how to manage them.

Lessons from failure

The importance of information management in investigation was learned the hard way. During the investigation of the "Yorkshire Ripper" murders in northern England between 1975 and 1981, the major incident room relied on paper index cards. By the end, it held so much information that it could not be searched effectively. The offender, Peter Sutcliffe, had been interviewed nine times, but the connections between pieces of information about him were not made. The official review found that the incident room had been overwhelmed and recommended better systems for managing major investigations (Byford, 1981). The result was the development in the United Kingdom of a computerised system for major inquiries, known as HOLMES, and standard procedures for operating major incident rooms (Association of Chief Police Officers [ACPO], 2005).

Later inquiries reinforced the lesson. The Bichard inquiry, following the murders of two schoolgirls in Soham in 2002, found that police forces had held intelligence about previous allegations against the murderer but that it had been deleted, poorly recorded or not shared, so that it was not available when he was vetted for a job in a school (Bichard, 2004). The 9/11 Commission found that United States agencies held relevant information about some of the attackers but that it was not connected or shared (National Commission on Terrorist Attacks Upon the United States, 2004). Sheptycki (2004) described recurring "organisational pathologies" in police intelligence systems, such as information hoarding, duplication of records and the inability to find what had already been collected.

What case management systems do

The information cycle in an investigation

Each item of information passes through the same stages, and results feed back as new information

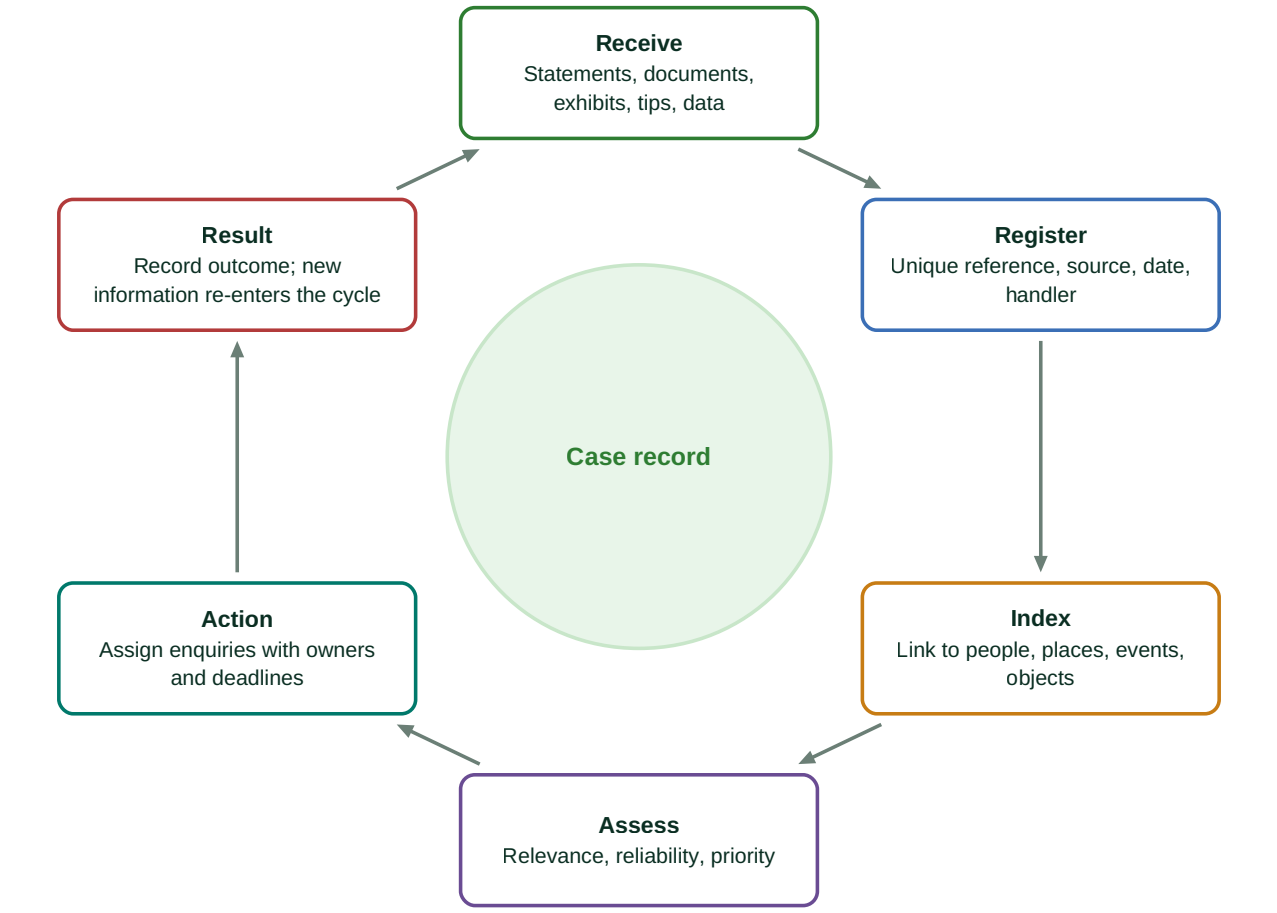


Figure 1. In a well-run investigation, every item of information is registered, indexed, assessed and acted on, and the result is recorded. The case record holds the cumulative knowledge and the audit trail of decisions. Diagram by ModQu.

The structured procedures developed for major incident rooms reflect a cycle that applies to most investigations. Information is received, registered with a unique reference, read and indexed so that every person, location, vehicle, phone number or other entity it mentions is linked to a central index, assessed for relevance and priority, and used to raise actions, which are allocated to investigators with deadlines. When an action is completed, its result is recorded and may itself generate new information, which re-enters the cycle (ACPO, 2005). Innes (2003) described homicide investigation as a process of producing and organising information until an account of the event emerges; the case management system is where that account is built.

Modern systems perform several core functions:

- **Recording.** Capture every item with its source, date and handler, and preserve originals.
- **Indexing and linking.** Connect items to the entities they mention, so that everything known about a person or place can be retrieved at once.
- **Tasking.** Raise, allocate and track actions, so that nothing is forgotten and responsibility is clear.
- **Decision logging.** Record key decisions, the reasons for them and the information available at the time.
- **Exhibit management.** Track physical and digital evidence, its location and its chain of custody.
- **Analysis.** Support searching, timelines, link charts and maps.
- **Disclosure.** Identify material that must be revealed to the defence or other parties.
- **Audit.** Record who accessed or changed what, and when.

Organising knowledge

Knowledge management research distinguishes between information that can be written down and shared, often called explicit knowledge, and the tacit knowledge held in people's experience and judgement (Nonaka & Takeuchi, 1995). Case management systems are good at storing explicit knowledge, but investigations also depend on investigators' tacit understanding of the case: hunches, impressions of witnesses, the sense that something does not fit. Alavi and Leidner (2001) argue that knowledge management systems succeed only when they support the social processes by which people create and share knowledge, not merely the storage of documents. In investigation, this means encouraging investigators to record not only facts but their reasoning, and holding briefings where tacit knowledge can be shared and tested.

Gottschalk (2007) describes stages of knowledge management in law enforcement, from basic tools for individual officers to systems that share information across the organisation, to systems that support analysis and decision-making. Many organisations remain at the earlier stages.

Linking records: entity resolution

The most valuable function of a case management system, and the most technically difficult, is linking records that refer to the same entity. People are recorded under different spellings, nicknames, dates of birth and addresses; phone numbers change; companies use different names. Entity resolution is the process of deciding which records refer to the same real-world entity.

Fellegi and Sunter (1969) provided a formal statistical theory of record linkage, in which pairs of records are compared on several fields and classified as matches, non-matches or possible matches requiring human review. Christen (2012) describes modern techniques for data matching and the trade-off between missing true matches and creating false ones. In law enforcement, systems such as COPLINK were developed to link records across police databases and support investigators in finding connections (Chen et al., 2003), and Chen et al. (2004) described data mining methods for identifying associations and patterns in crime data.

Both kinds of error matter. A missed link can hide a crucial connection, as in the Yorkshire Ripper case. A false link can wrongly associate an innocent person with a crime. Systems should show investigators why records have been linked and allow them to confirm or reject suggested links, with the decision recorded.

Data quality

A case management system is only as good as the information entered into it. Common problems include incomplete records, inconsistent formats, duplicate entries, free-text notes that cannot be searched reliably, and information recorded in the wrong place. The Bichard inquiry found that poor recording and inconsistent data entry, as much as technology, had caused information to be lost (Bichard, 2004). Brayne (2017) found that, as police data systems became more integrated, errors and biases in underlying records could spread more widely and affect people who had little direct contact with the police.

Good data quality depends on clear standards for what must be recorded and how, training for everyone who enters data, validation at the point of entry, regular checks for duplicates and errors, and a culture in which accurate recording is valued rather than treated as administration.

Disclosure and retention

In criminal investigations, case management systems have a legal role. In England and Wales, investigators must record and retain material that may be relevant to the investigation, and prosecutors must disclose to the defence any material that might undermine the prosecution or assist the defence (Criminal Procedure and Investigations Act 1996; Ministry of Justice, 2020). A parliamentary inquiry found that disclosure failures, often caused by the volume of digital material and poor scheduling, had led to cases collapsing and to the risk of miscarriages of justice (House of Commons Justice Committee, 2018). A system that records every item, tracks its review and flags potentially relevant material makes disclosure manageable.

Retention also involves limits. Personal data must not be kept longer than necessary, and data protection law sets requirements for the security and lawful processing of information held in investigation systems (Directive (EU) 2016/680, 2016; Regulation (EU) 2016/679, 2016). Records management standards help organisations decide what to keep, for how long and how to dispose of it securely (International Organization for Standardization [ISO], 2016).

Security and access

Investigation systems hold highly sensitive information about victims, witnesses, suspects and informants. Unauthorised access can endanger people and compromise investigations. Systems should restrict access according to role and need, separate highly sensitive material such as source information, log all access and changes, and be protected according to recognised information security standards (ISO, 2022). Audit logs should be protected from alteration so that they can be relied on if misuse is suspected (Schneier & Kelsey, 1999).

Choosing and governing a system

Large organisations may use specialised commercial or government systems; smaller ones may use general-purpose tools, such as databases or document management systems, configured for investigations. Either way, several questions should guide the choice:

- Does it register every item with a unique reference, source and date?
- Can it link items to people, places and other entities, and show why links were made?
- Does it support tasking, decision logs and exhibit tracking?
- Does it record an audit trail of access and changes that cannot be edited?
- Can it handle the formats and volumes of material the organisation expects, including digital evidence?
- Does it support disclosure, retention schedules and data protection requirements?
- Can data be exported in open formats if the system is replaced?

Core functions of a case management system

What each function protects against

	What it does	Failure it prevents
Registration	Unique reference, source and date for every item	Lost or untraceable information
Indexing and linking	Connects items to people, places and objects	Missed connections, as in the Yorkshire Ripper case
Tasking	Tracks actions, owners and deadlines	Leads never followed up
Decision log	Records decisions and reasons	Unexplained or unreviewable choices
Exhibit tracking	Location and custody of evidence	Broken chain of custody
Audit and access control	Records and limits who sees and changes what	Leaks, tampering and misuse

ModQu analysis based on ACPO (2005), Byford (1981) and Bichard (2004) ModQu.com

Figure 2. The core functions of an investigative case management system, and the failure each is designed to prevent. Diagram by ModQu.

Governance matters as much as technology. Someone must own the system, set recording standards, monitor data quality and review whether it is meeting the organisation's needs. Analysts and investigators should be involved in its design, because a system that does not fit the way they work will be bypassed, and information will migrate to private spreadsheets and notebooks where it cannot be found. Intelligence-led approaches depend on information being recorded where analysts can use it (Ratcliffe, 2016), and structured analytic techniques work best when the underlying evidence is organised and retrievable (Heuer & Pherson, 2015).

Implementing a system

Introducing a new case management system is a project in its own right, and many fail not because of the software but because of how it is introduced. Several steps reduce the risk. First, map how investigations actually work, including the informal spreadsheets, email folders and notebooks people rely on, and design the system to replace them rather than add to them. Second, agree a small set of mandatory fields and recording rules, because a system that demands too much data at entry will be filled with placeholders. Third, decide how existing records will be migrated, and check a sample after migration, because errors introduced at this stage can persist for years. Fourth, train everyone who will use the system, including occasional users such as managers and lawyers, and provide quick reference guides for common tasks. Fifth, run the new system alongside the old one on a small number of live cases before switching over completely. Finally, review the system after six to twelve months, asking investigators and analysts what works, what is bypassed and what information is still being kept elsewhere. Systems need continuing attention: recording standards drift, new types of evidence appear and staff change, so the governance described above must continue after the launch.

A short example

The following hypothetical case shows a system making a difference. A survey company investigates suspected fraud by respondents claiming incentive payments under multiple identities. Using a simple case management database, the investigator registers each suspicious account, links it to the email addresses, payment accounts, device identifiers and postal addresses it uses, and records each enquiry as an action with an owner. After six weeks, the system holds 300 accounts. An entity resolution check, reviewed by the investigator, links 140 of them through shared payment accounts and devices to a group of five people. A search of the index also shows that one of those people had been the subject of a complaint two years earlier, recorded under a slightly different spelling and then closed. The earlier record contains an address that leads to the identification of the organiser. The investigator's decision log shows why each link was accepted or rejected, so that the company can defend its findings when it closes the accounts and recovers the payments.

Conclusion

Case management systems are the memory of an investigation. They record what is known, link it to the people and things it concerns, track what is being done, and preserve the reasons for decisions. Major inquiries have shown that when information is not properly recorded, indexed and shared, offenders can escape detection despite being in the records. Effective systems combine sound procedures, reliable entity resolution, high data quality, strong security, lawful retention and good governance, and they support the human sharing of knowledge as well as its storage. Investigators who treat information management as a core part of their work, rather than an administrative burden, make it far more likely that the knowledge they gather will be found and used.

References

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, *25*(1), 107–136. https://doi.org/10.2307/3250961

Association of Chief Police Officers. (2005). *Guidance on major incident room standardised administrative procedures (MIRSAP)*. National Centre for Policing Excellence.

Bichard, M. (2004). *The Bichard inquiry report* (HC 653). The Stationery Office.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Byford, L. (1981). *The Yorkshire Ripper case: Review of the police investigation of the case*. Home Office.

Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime data mining: A general framework and some examples. *Computer, 37*(4), 50–56. https://doi.org/10.1109/MC.2004.1297301

Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J. (2003). COPLINK: Managing law enforcement data and knowledge. *Communications of the ACM, 46*(1), 28–34. https://doi.org/10.1145/602421.602441

Christen, P. (2012). *Data matching: Concepts and techniques for record linkage, entity resolution, and duplicate detection*. Springer. https://doi.org/10.1007/978-3-642-31164-2

Criminal Procedure and Investigations Act 1996, c. 25 (UK).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. (2016). *Official Journal of the European Union, L 119*, 89–131.

Fellegi, I. P., & Sunter, A. B. (1969). A theory for record linkage. *Journal of the American Statistical Association, 64*(328), 1183–1210. https://doi.org/10.1080/01621459.1969.10501049

Gottschalk, P. (2007). *Knowledge management systems in law enforcement: Technologies and techniques*. Idea Group.

Heuer, R. J., Jr., & Pherson, R. H. (2015). *Structured analytic techniques for intelligence analysis* (2nd ed.). CQ Press.

House of Commons Justice Committee. (2018). *Disclosure of evidence in criminal cases* (Eleventh Report of Session 2017–19, HC 859).

Innes, M. (2003). *Investigating murder: Detective work and the police response to criminal homicide*. Oxford University Press.

International Organization for Standardization. (2016). *Information and documentation — Records management — Part 1: Concepts and principles* (ISO 15489-1:2016).

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022).

Ministry of Justice. (2020). *Criminal Procedure and Investigations Act 1996 (section 23(1)) code of practice*.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report*. W. W. Norton.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

Ratcliffe, J. H. (2016). *Intelligence-led policing* (2nd ed.). Routledge.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union, L 119*, 1–88.

Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security, 2*(2), 159–176. https://doi.org/10.1145/317087.317089

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology, 1*(3), 307–332. https://doi.org/10.1177/1477370804044005