ISO/IEC 27050:2018-2021 — Electronic discovery *(4 parts)*

Introduction

The fundamental purpose of the ISO27k digital forensics standards is to promote good practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organisations and jurisdictions may well retain certain methods, processes and controls in compliance with local laws, regulations and established practices, it is hoped that standardization will (eventually) lead to the adoption of similar if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organisations and potentially across different jurisdictions.

Scope and purpose

This multi-part standard concerns the discovery phase, specifically the discovery of **E**lectronically **S**tored **I**nformation, a legal term-of-art meaning (in essence) forensic evidence in the form of digital data. Electronic discovery (eDiscovery) involves the following main steps:

1. **Identification:** ESI that is potentially relevant to a case is identified, along with its locations, custodians, sizes/volumes *etc.* This can be more complex than it may appear, for instance involving information assets belonging not just to the individual suspects but also their employers, friends and other organisations such as phone companies and the suppliers of services such as email and Internet access (ISPs), even social media. Operational/online data, backups and archives may all contain relevant data. Often, this phase is time-critical since potential evidence (especially ephemeral operational data) may be spoiled or destroyed before it has been captured and preserved;
2. **Preservation:** the identified, potentially relevant ESI is placed under a legal hold, starting the formalized forensic process designed to ensure, beyond doubt, that they are protected through the remaining steps against threats such as loss/theft, accidental damage, deliberate interference/manipulation and replacement/substitution, any of which might spoil, discredit and devalue the data, perhaps resulting in the ESI being ruled inadmissible or simply becoming unusable. The legal hold is essentially a formal obligation on the custodian not to interfere with or delete the ESI. Note: this may have implications on live systems

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

since their continued operation may spoil the ESI;

3. **Collection:** the ESI is collected from the original custodian, typically by physically removing the original digital storage media (hard drives, memory sticks and cards, CDs, DVDs, whatever) and perhaps associated physical evidence (such as devices, media storage cases, envelopes *etc*. that might have fingerprints or DNA evidence linking a suspect to the crime) into safe custody. In the case of Internet, cloud or other dispersed and ephemeral data including RAM on a running system, it may be impracticable or impossible to secure the data by capturing physical media, hence the data rather than the media may need to be captured directly in a forensically sound manner. Note: the original evidence may later be produced in court hence all subsequent forensic analysis must be performed in such a way that there is no credible possibility that it might have been spoiled *e.g.* by analysing bit-copies made with suitable forensic tools and methods rather than the original evidence itself. Note also that physically removing systems and media into the custody of a third party could itself be classed as an information security incident with clear implications on the confidentiality, integrity and availability of the information, particularly since, at this stage, the case is not proven: in other words, liabilities may be accumulating;
4. **Processing:** forensic bit-copies are stored in a form that allows them to be searched or analysed for information that is relevant to the case, using suitable forensic tools and platforms. Sifting out the few vital bits of data from a much larger volume typically collected is the crux of this step;
5. **Review:** forensic bit-copies are searched or analysed for information that is relevant to the case;
6. **Analysis:** the information is further analysed and assessed as to its relevance, suitability, weight, meaning, implications *etc.* Useful information is gleaned from the selected data;
7. **Production:** relevant information from the analysis, plus the original storage media *etc.*, is formally presented to the court as evidence. This inevitably involves demonstrating and explaining the meaning of the evidence in terms that make sense to the court. Hopefully, something along the lines of "I state, under oath, that we complied fully with ISO/IEC 27050" will, in future, side-step a raft of challenges concerning the eDiscovery processes!

ISO/IEC 27050-1:2019 — Information technology — Security techniques — Electronic discovery — **Part 1: Overview and concepts** *(second edition)*

- **Abstract:** *"Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. [ISO/IEC 27050-1] provides an overview of electronic discovery ..." [Source: ISO/IEC 27050-1:2019]*
- Gives an overview of eDiscovery.
- Defines the terms, concepts, processes *etc*. such as **E**lectronically **S**tored **I**nformation.
- Introduces and defines the scope and context of this multi-part standard.
- **Status**: the *first* edition of part 1 was published in **2016**. The *second* edition was published in **2019**.

ISO/IEC 27050-2:2018 — Information technology — Security techniques — Electronic discovery — **Part 2: Guidance for governance and management of electronic discovery** *(first edition)*

- **Abstract:** part 2 "*provides guidance for technical and non-technical personnel at senior management levels within an organisation, including those with responsibility for compliance with statuary and regulatory requirements, and industry standards. [Part 2] describes how such personnel can identify and take ownership of risks related to electronic discovery, set policy and achieve compliance with corresponding external and internal requirements. It also suggests how to produce such policies in a form which can inform process control. Furthermore, it provides guidance on how to implement and control electronic discovery in accordance with the policies." [Source: ISO/IEC 27050-2:2018]*
- Guides management on identifying and treating the information risks related to eDiscovery *e.g.* by setting and implementing eDiscovery-related policies and complying with relevant (mostly legal) obligations and expectations.
- Provides guidance on good governance for forensics work *i.e.* the overarching framework or structure within which digital forensic activities take place and are managed through a controlled, repeatable and trustworthy suite of activities.
- Suggests a few possible metrics.
- **Status:** the *first* edition of part 2 was published in **2018**.

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

ISO/IEC 27050-3:2020 — Information technology — Security techniques — Electronic discovery — **Part 3: Code of practice for electronic discovery** *(second edition)*

- **Abstract:** part 3 "*provides requirements and recommendations on activities in electronic discovery, including, but not limited to, identification, preservation, collection, processing, review, analysis and production of electronically stored information (ESI). In addition, this document specifies relevant measures that span the lifecycle of the ESI from its initial creation through to final disposition. [Part 3] is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that the user is expected to be aware of any applicable jurisdictional requirements." [Source: ISO/IEC 27050-3:2020]*
- Identifies requirements and offers guidance on the seven main steps of eDiscovery noted above (ESI identification, preservation, collection, processing, review, analysis and production).
- Essentially, a basic, generic how-to-do-it guide laying out the key elements that will no doubt form the basis of many digital forensics manuals.
- **Status:** the *first* edition of part 3 was published in **2017**. The *second* edition was published in **2020**.

ISO/IEC 27050-4:2021 — Information technology — Electronic discovery — **Part 4: Technical readiness** *(first edition)*

- **Abstract:** part 4 *"provides guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both technology and processes. [Part 4] provides guidance on proactive measures that can help enable effective and appropriate electronic discovery and processes. [Part 4] is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities." [Source: ISO/IEC 27050-4:2021]*
- Guidance on preparing the technology (*i.e.* the forensic tools and systems supporting the collection, storage, collation, searching, analysis and production of ESI, plus the related processes) and processes that will be required for eDiscovery.
- 35 pages describe the selection, preparation and use of tools supporting each step of the electronic discovery process, including the retention/storage, production and eventual destruction of ESI.
- The standard offers generic advice and does not specify or recommend specific commercial or open source tools.
- **Status:** the *first* edition of part 4 was published in **2021**.

Related standards

ISO/IEC 27037 concerns the initial *capturing* of digital evidence.

ISO/IEC 27041 offers guidance on the *assurance* aspects of digital forensics *e.g.* ensuring that the appropriate methods and tools are used properly.

ISO/IEC 27042 covers what happens *after* digital evidence has been collected *i.e.* its analysis and interpretation.

ISO/IEC 27043 covers the broader *incident investigation* activities, within which forensics usually occur.

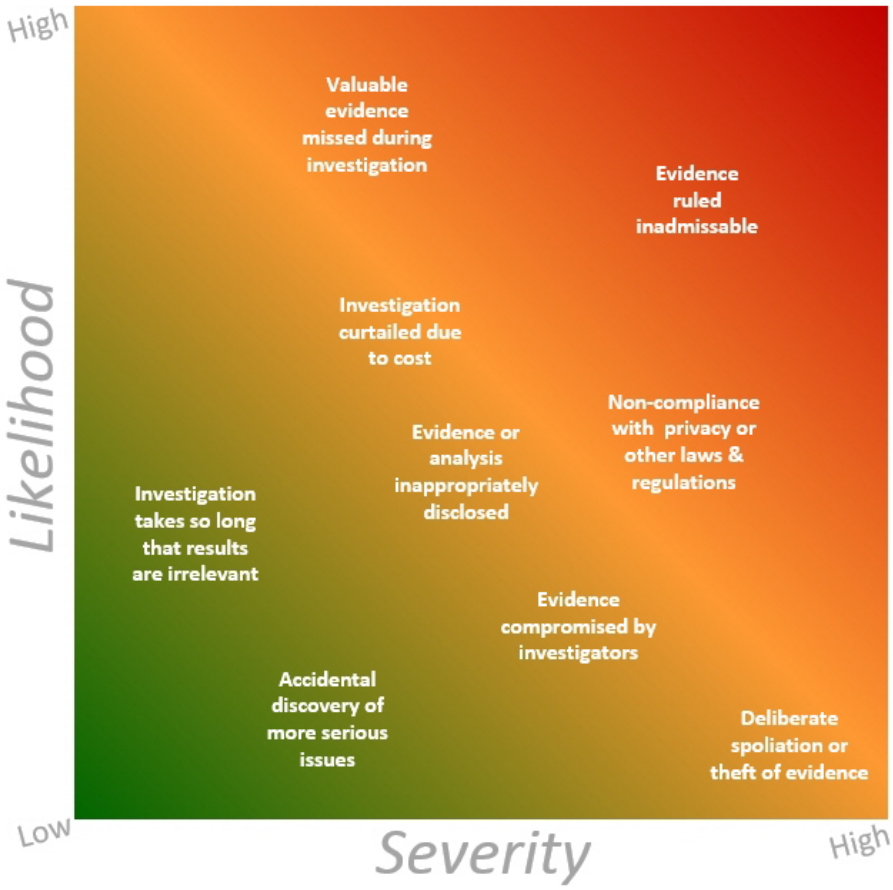
The 4 parts of this standard concern *electronic discovery ...* which is similar to the other standards.

British Standard BS 10008 "Evidential weight and legal admissibility of electronically stored information (ESI), Specification." may also be of interest.

Personal comments

The word "evidence" has been eliminated from the standard, presumably because of troubling differences of interpretation and implication in various jurisdictions. "**E**lectronically **S**tored **I**nformation" is a clumsy replacement but thankfully it is abbreviated to "ESI".

I'm pleased to note that part 2 includes a set of information risks. The list is incomplete, for example it fails to mention that damage, theft, loss or some other incident affecting ESI can compromise its value and admissibility in court, potentially decimating an otherwise valid case. Although also incomplete and subject to discussion, the generic **P**robability **I**mpact **G**raphic below represents how various risks in this context compare to each other using two key risk parameters *i.e.* likelihood (relative probability) and severity (relative organisational/business impact, importance or consequence):



Given that these are all aspects of eDiscovery, it makes sense to cover them as one multi-part coherent standard. This should be a very worthwhile international standard, particularly if it aligns the terminology, processes and controls across various jurisdictions. It would be wonderful if the digital forensics-related laws, regulations and practices were also aligned but that's just a pipe dream!

I wonder if there is demand for *certification* against ISO/IEC 27050 and perhaps the other digital forensics standards, as a way to add credibility to the assertion noted in step 7 above ... ?

< Previous standard ^ Up a level ^ Next standard >