

ISO/IEC JTC 1/SC 27  
IT Security techniques  
Secretariat: DIN (Germany)

**Document type:** Working Draft Text

**Title:** WG4N0233\_1stWD\_27050\_20130708

**Status:** As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

PLEASE submit your comments on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27> by the due date 2013-09-13.

Secretariat's note:

This request for comments is also concurrently being circulated as WG 4 document N0233 for test purposes ONLY as part of the WG 4 Livelink trial via the Working Group Consultation application accessible at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

For the test purposes the National Bodies and liaison organizations of SC 27/WG 4 are kindly invited to send their responses to the hereby attached document via the above-mentioned WG 4 Working Group Consultation application.

Any responses received are greatly appreciated and will be taken into account when assessing the trial results and preparing a report for consideration at the next SC 27 Heads of Delegation meeting in Incheon, Republic of Korea, 24<sup>th</sup> October 2013.

**Date of document:** 2013-07-12

**Source:** Project editors

**Expected action:** COMM

**Action due date:** 2013-09-13

**No. of pages:** 1 + 1 + 23

**Email of secretary:** [krystyna.passia@din.de](mailto:krystyna.passia@din.de)

**Committee URL:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**ISO/IEC JTC 1/SC 27/WG 4**  
**Security controls and services**  
**Secretariat: SABS (South Africa)**

**Document type:** Request for comments

**Title:** Text 1stWD 27050 - Text for ISO/IEC 1st WD 27050, Information technology – Security techniques – Electronic discovery

**Status:** As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

A Working group consultation will be created for submissions to this request. Submissions should be sent directly via the SC 27/WG 4 commenting website at <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4> before the action due date.

A request for review and comment will be issued in parallel by SC 27 as SC 27 N12679.

**Date of document:** 2013-07-08

**Source:** Editor

**Expected action:** COMM

**Action due date:** 2013-09-13

**No. of pages:** 1 + 23

**Email of secretary:**

**Committee URL:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

## **Information technology — Security techniques — Electronic discovery**

### **Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

### Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27  
DIN German Institute for Standardization  
DE-10787 Berlin

Tel. + 49 30 2601 2652  
Fax + 49 30 2601 1723  
E-mail [krystyna.passia@din.de](mailto:krystyna.passia@din.de)  
Web <http://www.jtc1sc27.din.de/en> (public web site)  
<http://isotc.iso.org/isotcportal/index.html> (SC 27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

# Contents

Page

2	<b>Foreword</b>	<b>v</b>
3	<b>0 Introduction</b>	<b>vi</b>
4	0.1 About this standard	vi
5	0.2 Relationship to other standards	vi
6	<b>1 Scope</b>	<b>1</b>
7	<b>2 Normative references</b>	<b>1</b>
8	<b>3 Terms and definitions</b>	<b>1</b>
9	<b>4 Symbols and abbreviated terms</b>	<b>4</b>
10	<b>5 Overview</b>	<b>5</b>
11	5.1 Background	5
12	5.2 Basic concepts	5
13	5.3 Objectives of electronic discovery	6
14	5.4 General principles of electronic discovery	6
15	5.4.1 Competency	6
16	5.4.2 Candour	6
17	5.4.3 Cooperation	6
18	5.4.4 Completeness	7
19	5.4.5 Proportionality	7
20	<b>6 Electronically Stored Information (ESI)</b>	<b>7</b>
21	6.1 General	7
22	6.2 Common types of ESI	8
23	6.2.1 Active data	8
24	6.2.2 Inactive and archived data	8
25	6.2.3 Residual data	8
26	6.2.4 Legacy data	8
27	6.3 Common sources of ESI	9
28	6.3.1 Communications	9
29	6.3.2 Desktop, laptop or home computers	9
30	6.3.3 Databases and applications	9
31	6.3.4 Network storage	9
32	6.3.5 Backups and electronic archives	9
33	6.3.6 Social media	10
34	6.3.7 Potentially excluded sources of ESI	10
35	6.4 ESI Representations	10
36	<b>7 Electronic discovery process</b>	<b>11</b>
37	7.1 General	11
38	7.2 Identification	11
39	7.3 Preservation	11
40	7.4 Collection	12
41	7.5 Processing	12
42	7.6 Review	12
43	7.7 Analysis	12
44	7.8 Production	13
45	<b>8 Additional considerations</b>	<b>13</b>
46	8.1 Electronic discovery readiness	13
47	8.2 Search technologies	14
48	8.3 Technology Assisted Reviews (TAR)	14
49	8.4 Avoiding data breaches	14

1	8.4.1	Disposition of ESI .....	14
2	8.4.2	Maintaining ESI confidentiality.....	14
3		Bibliography .....	15
4			

## 1 Foreword

2 ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies  
3 (ISO member bodies). The work of preparing International Standards is normally carried out through ISO  
4 technical committees. Each member body interested in a subject for which a technical committee has been  
5 established has the right to be represented on that committee. International organizations, governmental and  
6 non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the  
7 International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

8 International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

9 The main task of technical committees is to prepare International Standards. Draft International Standards  
10 adopted by the technical committees are circulated to the member bodies for voting. Publication as an  
11 International Standard requires approval by at least 75 % of the member bodies casting a vote.

12 Attention is drawn to the possibility that some of the elements of this document may be the subject of patent  
13 rights. ISO shall not be held responsible for identifying any or all such patent rights.

14 ISO/IEC 27050 was prepared by Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee  
15 SC 27, *Security techniques*.

## 0 Introduction

### 0.1 About this standard

This International Standard addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI). In addition, it provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. It 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 this guidance is not intended to contradict or supersede local jurisdictional laws and regulations.

Electronic discovery often serves as a driver for investigations (covered in ISO/IEC 27041, ISO/IEC 27042, and ISO/IEC 27043) as well as evidence acquisition and handling activities (covered in ISO/IEC 27037). In addition, the sensitivity and criticality of the data sometime necessitate protections like storage security to guard against data breaches (covered in ISO/IEC 27040).

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

### 0.2 Relationship to other standards

This International Standard is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, Information Security Incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise.

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

This International Standard describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following standards:

- ISO/IEC 27035 Part 1 : Principles of incident management
- ISO/IEC 27035 Part 2 : Guidelines to plan and prepare for incident response
- ISO/IEC 27035 Part 3 : Guidelines for CSIRT operations
- ISO/IEC 27037: Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence.  
This describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.
- ISO/IEC 27038: Specification for digital redaction.  
In some circumstances material which is found during various phases of the investigation must not be disclosed. In these cases, redaction may be required.
- ISO/IEC 27040: Storage security.

ISO/IEC 27040 provides detailed technical guidance on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design,



documentation and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Security mechanisms like encryption and sanitization can affect one's ability to investigate by introducing obfuscation mechanisms. They should be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

— ISO/IEC 27041: Guidance on Assuring the Suitability and Adequacy of Investigative Methods.

It is important that methods and processes deployed during an investigation can be shown to be appropriate. This document provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

— ISO/IEC 27042: Guidelines for the Analysis and Interpretation of Digital Evidence.

This describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence and effective reporting of findings.

— ISO/IEC 27043: Incident Investigation Principles and Processes.

This defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

— ISO/IEC 27044 : Guidelines for Security Information and Event Management (SIEM)

— ISO/IEC 27050 : eDiscovery

ISO/IEC 27050 addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI). In addition, it provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. It 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 this guidance is not intended to contradict or supersede local jurisdictional laws and regulations.

Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities. In addition, the sensitivity and criticality of the data sometime necessitate protections like storage security to guard against data breaches.

— ISO/IEC 30121: Governance of digital forensic risk framework

Figure 1 shows typical activities surrounding an incident and its investigation. The standards listed above are mapped onto this sequence, showing where each is most likely to be directly applicable. It is recommended, however, that all should be consulted prior to, and during, the planning and preparation phases.

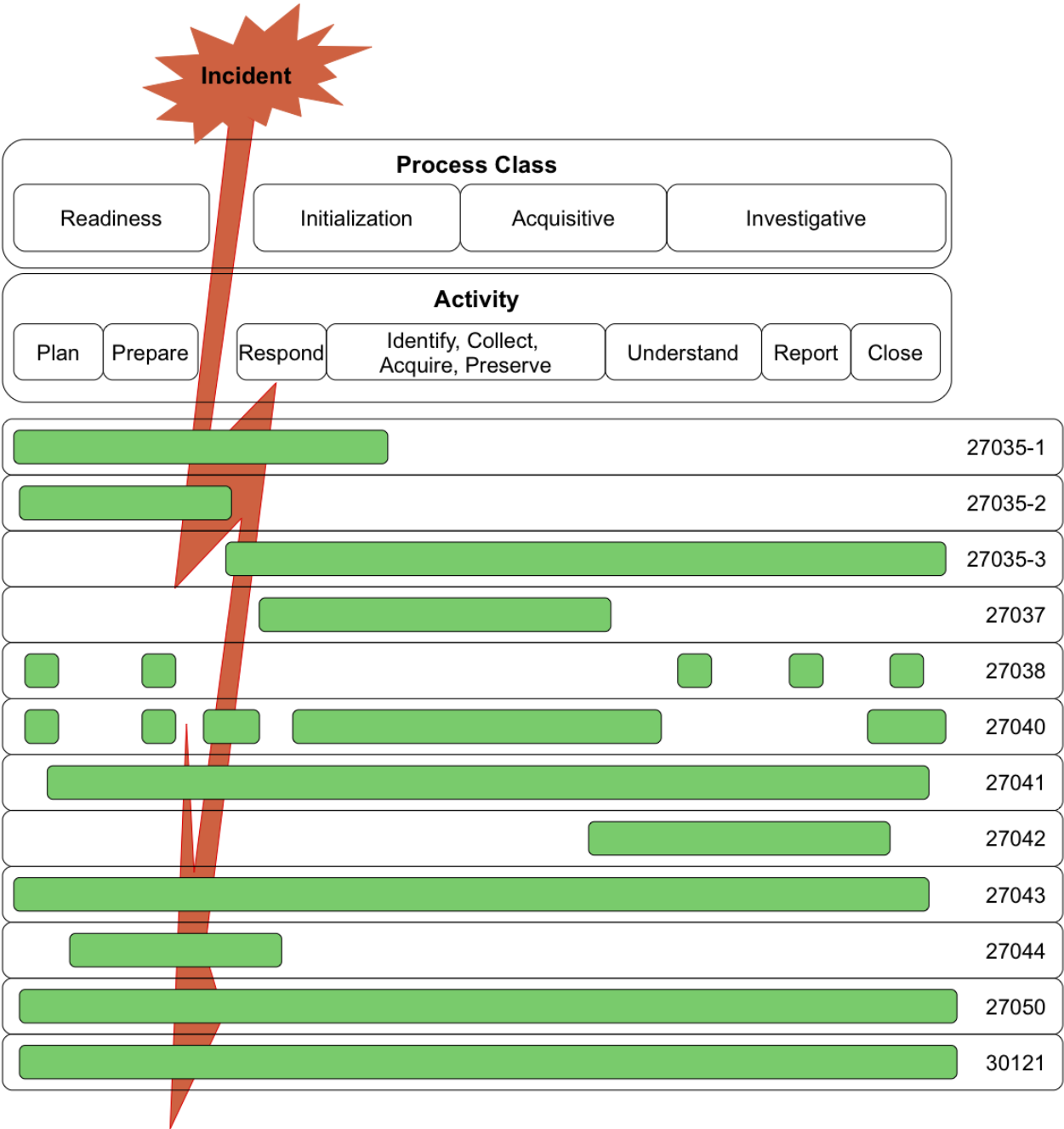


Figure 1 — Applicability of standards to Investigation process classes and activities

# Information technology — Security techniques — Electronic discovery

## 1 Scope

Electronic discovery (also known as eDiscovery and E-Discovery) is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or both parties involved in an investigation and any resulting actions. This International Standard addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of ESI. In addition, this International Standard provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. This International Standard also identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, E-Discovery activities.

This International Standard 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 this guidance is not intended to contradict or supersede local jurisdictional laws and regulations, so care should be exercised to ensure compliance with the prevailing jurisdictional requirements.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27005, and the following apply.

### 3.1 collection

process of gathering the physical items that contain potential digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.3.]

**3.2**  
**data breach**  
compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, *stored* (3.xx) or otherwise processed

[SOURCE: ISO/IEC 27040, 3.7.]

**3.3**  
**data integrity**  
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21.]

**3.4**  
**digital evidence**  
information or data, stored or transmitted in binary form, that may be relied on as evidence

[SOURCE: ISO/IEC 27037:2012, 3.5.]

**3.5**  
**electronic archive**  
long-term repository of *Electronically Stored Information* (3.7)

Note 1 to entry: Electronic archives can be on-line, and therefore accessible, or off-line and not easily accessible.

Note 2 to entry: Backup systems (e.g., tape, virtual tape, etc.) are not considered electronic archives, but rather data protection systems (i.e., recovery mechanisms for disaster recovery and business continuity).

**3.6**  
**electronic discovery**  
**eDiscovery**  
**e-discovery**  
process that includes the *identification* (3.8), *preservation* (3.14), *collection* (3.1), processing, review, analysis, and *production* (3.15) of *Electronically Stored Information* (3.7)

Note 1 to entry: Although electronic discovery is often considered a legal process, its use is not limited to the legal domain.

**3.7**  
**Electronically Stored Information**  
**ESI**  
data or information of any kind and from any source, whose temporal existence is evidenced by being *stored* (3.19) in or on any electronic medium

Note 1 to entry: ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file-associated *metadata* (3.10) such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, storage devices and storage elements.

[SOURCE: ISO/IEC 27040, 3.15.]

**3.8**  
**identification**  
process involving the search for, recognition and documentation of potential digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.7.]

**3.9****legal hold**

issued communication that suspends the normal disposition or processing of records and *Electronically Stored Information* (3.7)

Note 1 to entry: This type of communication may also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice."

**3.10****metadata**

data that defines and describes other data

[SOURCE: ISO/IEC 11179-1:2004, 3.2.16.]

**3.11****native file format**

organization and representation of data and *metadata* (3.10) that an operating system or application uses when data is stored (3.19)

Note 1 to entry: Native file formats are frequently proprietary and typically contain the most complete representation of the data. While it is often possible to convert this data to other formats, there can be a loss of information (e.g., metadata is stripped) or modification of the information.

**3.12****non-volatile storage**

*storage* (3.38) that retains its contents even after power is removed

[SOURCE: ISO/IEC 27040, 3.28.]

**3.13****potential digital evidence**

*digital evidence* (3.4) that has not yet been admitted as such in a court of law or other legal proceeding

[SOURCE: ISO/IEC 27043, 3.12.]

**3.14****preservation**

process to maintain and safeguard the integrity and/or original condition of the potential digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.13.]

**3.15****production**

process of delivering or making available *Electronically Stored Information* (3.7) to another party

**3.16****sanitize**

process to remove information from media such that data recovery is not possible at a given level of effort

[SOURCE: ISO/IEC 27040, 3.33.]

**3.17****spoliation**

act of making or allowing change(s) to the potential digital evidence that diminishes its evidential value

[SOURCE: ISO/IEC 27037:2012, 3.19.]

**3.18**

**storage**

device into which data may be entered, and from which data may be retrieved

[SOURCE: ISO/IEC 27040, 3.38.]

**3.19**

**stored**

process that results in data being recorded on *volatile storage* (3.20) or *non-volatile storage* (3.12)

[SOURCE: ISO/IEC 27040, 3.43.]

**3.20**

**volatile storage**

*storage* (3.18) that fails to retain its contents after power is removed

[SOURCE: ISO/IEC 27040, 3.45.]

**4 Symbols and abbreviated terms**

EDMS	Electronic Document Management System
------	---------------------------------------

ERMS	Electronic Records Management System
------	--------------------------------------

ESI	Electronically Stored Information
-----	-----------------------------------

FTP	File Transfer Protocol
-----	------------------------

IT	Information Technology
----	------------------------

NAS	Network Attached Storage
-----	--------------------------

PII	Personally Identifiable Information
-----	-------------------------------------

RAM	Random Access Memory
-----	----------------------

TAR	Technology Assisted Review
-----	----------------------------

WebDAV	Web Distributed Authoring and Versioning
--------	--

## 5 Overview

### 5.1 Background

Electronic discovery is increasingly important both within organizations and the courts, and this trend is expected to continue as more and more electronic records and information (or ESI) are created, modified, manipulated, used, and ultimately destroyed without ever taking on a physical form (e.g., a printed document). The emergence of ESI as the preferred representation of information is introducing new challenges for the legal community associated with locating the ESI, handling massive quantities of data, preservation and retention of ESI, authenticity, data integrity, data confidentiality, and data/media sanitization, etc. Failure to appropriately handle the electronic discovery processes as well as the ESI can result in costly rework, unnecessary costs, possible sanctions, and legal liabilities.

This International Standard addresses these challenges by:

- promoting a common approach, understanding, and language for eDiscovery
- encouraging practical and cost-effective discovery by those tasked with managing ESI through the process
- providing guidance and best practices for those responsible for delivering eDiscovery projects (e.g. legal practitioners, services providers, independent experts, courts, and any other parties engaged in the process)
- identifying competency areas for those involved in eDiscovery.
- promoting the proactive use of technology, in reducing costs and risks, while increasing efficiencies throughout the discovery process.
- suggesting ways of avoiding inadvertent disclosures of potentially privileged, confidential, or sensitive ESI

The overriding goal is to help organizations comply with their eDiscovery obligation.

### 5.2 Basic concepts

Parties must consider in advance the following eDiscovery issues:<sup>1)</sup>

- preservation of ESI;
- identification of relevant ESI;
- scope of e-discovery;
- form of production;
- anticipated costs and proposed allocation of same;
- disclosure of the programs and manner in which the ESI is stored;
- identification of systems holding relevant ESI; and
- identification of the individuals responsible for ESI preservation.

---

1) The New York Bar Association's *Best Practices in E-Discovery in New York State and Federal Courts* (July 2011)

While attorneys may struggle with the regional and international regulations surrounding E-Discovery, many clients are likely to be less concerned with the practical legal details of a discovery request, and more concerned with the financial cost. The primary factors that contribute to the costs include:

- *Collection*: Finding and retrieving the potentially relevant ESI
- *Volume*: The raw quantity of ESI that must be reviewed by human eyes
- *Number of Custodians*: The number of sources involved in the collection of data can increase exponentially the amount of time and effort involved
- *Human Review*: The need for qualified people who can recognize the actual relevant ESI
- *Case Complexity*: Simple cases may require a limited scope and review process, but more complex cases can involve elaborate document review strategies and processes.

### 5.3 Objectives of electronic discovery

General eDiscovery objectives can be summarized as:

- address the differences in discovery between traditional forms of information and ESI
- identify relevant ESI
- properly preserve and retain relevant ESI
- produce relevant ESI in a form that is usable by the requesting party

### 5.4 General principles of electronic discovery

#### 5.4.1 Competency

Given the complexities associated with eDiscovery, it is important that the parties engaging in the eDiscovery process (see clause 7) have the relevant technical and legal competencies and should be able to demonstrate that they are properly trained and have sufficient technical and legal understanding to handle ESI appropriately and to execute the eDiscovery process.

**Editor's Note:** Should this document include specific competencies in an annex (similar to what was done in ISO/IEC 27037 for DEFR/DES)?

#### 5.4.2 Candour

The parties conducting eDiscovery are expected to be open and completely honest. This means the parties have an obligation to correct and supplement the record (e.g., additional disclosures or to amend prior responses). In addition, purposeful sluggishness in executing the eDiscovery process should be avoided by all parties involved.

#### 5.4.3 Cooperation

Cooperation on issues relating to the preservation, collection, search, review, and production of ESI is often expected in the courts, and further, such cooperation typically does not compromise representation of a client. Cooperation in reasonably limiting ESI discovery requests on the one hand, and in reasonably responding to ESI discovery requests on the other hand, tends to reduce costs and delay. Cooperative exchanges of information at the earliest possible stage of discovery are also particularly important.



#### 5.4.4 Completeness

Within eDiscovery tension exists in processes between completeness, on the one hand, and burden and cost on the other. Responding parties seek to produce all responsive ESI, and at the same time they also seek to identify only the responsive ESI, in order to guard against overproduction or waiver of privilege.

#### 5.4.5 Proportionality

With the explosive growth of ESI, there are increased concerns over how to best address the costs and burdens associated with the discovery process. One approach to address this problem is to ensure that the benefits of discovery be commensurate with the corresponding burdens.

Editor's Note: Should "integrity" be included here as well?

## 6 Electronically Stored Information (ESI)

### 6.1 General

ESI should be considered at the earliest possible stage in a matter. It can be extremely fragile and is easily lost or modified, even through apparently inconsequential processes, such as opening a document. It is not necessary to undertake the full eDiscovery process from the outset; however completing the identification, preservation, and possibly the collection phases in the early days after becoming aware of a matter would be considered good practice and can lead to significant cost savings in the longer term.

Managing ESI increasingly impacts us all in our business and personal lives. The volume, size, complexity, and range of ESI can often be overwhelming. It is often not a priority until the true value and cost of locating ESI becomes apparent as part of a matter. Often organizations:

- Focus their ESI retention efforts on retention for purely business operational purposes rather than considering the wider context.
  - Have minimal consideration of their compliance obligations in respect of electronic records.
  - Have a limited understanding of the evidential value of good business records.
  - Do not have a good understanding of the cost and risk to the organisation of poor information management practices
- There are several major reasons why organisations face significant challenges when it comes to identifying and retrieving ESI in response to a discovery or regulatory request:
- It is often and unnecessarily stored beyond its required lifespan.
  - There is often little knowledge within the organisation as to where potentially relevant ESI can be found.
  - The volume and complexity is overwhelming even for IT professionals.
  - Turnover of staff and organisational changes (e.g., mergers, acquisitions, and divestitures) which result in retention of ESI but the loss of organisational knowledge and context.
  - The IT environment and systems may be poorly documented.

These factors lead to unavoidable, expensive, and disruptive searches through vast quantities of ESI in order to locate that which may be relevant to the matter in hand. This can introduce delays and increase the cost of the discovery process, in addition to increasing the risk of relevant ESI being overlooked.

## 6.2 Common types of ESI

### 6.2.1 Active data

This type of ESI is "actively" in use and resides on employees' computer hard drives or other storage devices and in the organization's servers, drives and databases. Active data generally can be accessed in a file manager or in the application in which it was created. Users can access it immediately without restoration or reconstruction. With the increasing popularity of cloud computing and Internet-based computing services, it may also reside on the storage devices of outside service providers. Most cases and investigations call primarily for the preservation and production of active files.

Active files may be relatively easy to access and collect, at least compared to other types of and legacy data. They can also be easily deleted or altered.

### 6.2.2 Inactive and archived data

This type of ESI is related to closed, completed, or concluded activities, including ESI an organization maintains for long-term storage and record keeping purposes, but which is not immediately accessible to the user of a computer system. It may include many of the same sources of data described above in relation to active data.

Inactive and archived data is often stored in a compressed format and may be maintained on system drives or off-line devices, including backup tapes or disks and optical media. Some systems allow users to retrieve archival data directly while other systems require the assistance of an IT professional. Challenges in preservation and collection include identifying relevant inactive and archived data, locating where and how it is stored, and restoring it from a compressed format. Additionally, as it is common for backup media to be rotated and overwritten, and for archived data to be automatically deleted after a specified time period, determining and suspending the applicable retention periods and rotation of backup media can be important.

### 6.2.3 Residual data

This type of ESI is hidden and cannot be viewed in applications (such as system files) or has been erased, fragmented, or damaged. Collecting this type of ESI usually requires a forensic copy—i.e., an exact, bit-by-bit copy of the entire physical storage media (e.g., hard drive, CD, DVD, tape), including all active and residual data and unallocated or slack space on the media.

Making a forensic copy and then extracting the residual data may require a forensics expert to operate special tools and can be time consuming and expensive. Making a bit-by-bit forensic copy may be unwarranted unless residual data is relevant and necessary in the matter. In some cases, however, companies may choose to image the hard drives of particularly important key custodians to ensure that all their data is preserved, including files that the custodian may have unintentionally, or intentionally, deleted or partially overwritten.

### 6.2.4 Legacy data

This type of ESI is created by software or hardware that is outmoded or has become obsolete (legacy systems). A legacy system may be one that the company still uses but that the hardware or software vendor no longer supports. Or, it may be a system that the company has decommissioned but retains in case its information is needed in the future.

The relevance of legacy data may be difficult to determine without restoration or reconstruction, and it may be costly to do so. In addition to preserving the legacy data itself, the company may need to retain the legacy hardware and software if there is no other way to view or use the data.

## 6.3 Common sources of ESI

### 6.3.1 Communications

Email is often the central source of relevant ESI in litigation and investigations. But other forms of communication are also prevalent and may also warrant consideration for preservation—instant messaging and chat, for example. It may be appropriate to consider whether ESI stored in an electronic fax system, copier, or in a videoconferencing system, is available and should be preserved. And, in some situations, audio recordings may exist that should be considered for preservation.

### 6.3.2 Desktop, laptop or home computers

Relevant ESI may be present on custodians' desktop, laptop or home computers. Even if an organization has network-based document management systems, employees may have also been given the ability to save documents on a local hard drive.

Although some organizations have policies prohibiting employees from using non-work issued computers, it may be advisable in certain situations to confirm whether, for example, key custodians in fact complied with the policy. Custodians may also have copied documents onto removable storage media, such as thumb drives, external hard drives, DVDs or CDs.

### 6.3.3 Databases and applications

ESI related to dynamic databases may be relevant in some cases. For example, an employment matter may involve ESI from a company's human resources system, an antitrust matter may involve customer relationship management, sales or production systems, and a financial fraud case may involve accounting and finance systems. Depending on the issues, a matter may involve a organization's electronic document management systems (EDMS), electronic records management systems (ERMS), or collaborative tools.

Some database applications automatically purge data after a particular time period, so it can be advisable to identify and suspend such processes if necessary. Additionally, legacy systems may exist and their data considered for preservation.

### 6.3.4 Network storage

Documents may be stored in various places on an organization's internal network (e.g., shared drives, network disk drives, and servers). File servers and Network Attached Storage (NAS) important sources of ESI because they are designed to provide centralized storage that can be easily shared and protected. Other forms of network storage include Web-based file services (e.g., WebDAV), cloud storage, and FTP servers.

### 6.3.5 Backups and electronic archives

It is common for organizations to back up the ESI on their information systems onto tape or other media for disaster recovery and business continuity purposes. These backups typically have a relatively short shelf life, so the associated media is often recycled within 30-90 days (sometimes referred to as rotating the backup media). In addition, the recovery process can be complex and cumbersome (e.g., appropriate recovery storage space must be found, the backup may not be on a single piece of media<sup>2)</sup>, etc.).

---

2) Backups can take many forms, but the most common are full backups (all the data is captured on the media), differential backups (captures all changes made since the last full backup), and incremental (captures all changes made since the last backup). A backup solution may apply multiple of these approaches.

An electronic or digital archive is a data repository that is typically part of a records management process that ensures protection, maintenance and accessibility of ESI, beginning from the moment of creating the ESI and ending with its disposition (i.e., destruction according to retention policies) or forever. ESI contained in archives are typically official business records, documents retained for compliance purposes, legacy documents (historical value), etc. The contents of such archives and their management are typically driven by organizational policies that are then implemented the records management system (e.g., destruction may take place automatically based on the expiration of a retention period).

### 6.3.6 Social media

Social media is data that is shared among groups of people, mostly for social purposes but increasingly for both social and business uses. Because social media usually resides outside of the company's control, it can be difficult to collect and hold, assuming the organization is even able to identify that it is relevant to a matter.

### 6.3.7 Potentially excluded sources of ESI

Not all sources of ESI need to be preserved; the following categories of ESI generally are not discoverable in most matters:<sup>3</sup>

- “deleted,” “slack,” “fragmented,” or “unallocated” data on hard drives;
- random access memory (RAM) or other ephemeral data;
- on-line access data such as temporary internet files, history, cache, cookies, etc.;
- data in metadata fields that are frequently updated automatically, such as last-opened dates;
- backup data that is substantially duplicative of data that is more accessible elsewhere; and
- other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business."

It can be beneficial to attempt to reach an agreement with litigation opponents or investigators that such files do not need to be preserved.

## 6.4 ESI Representations

**Editor's Note:** Insert materials describing native format versus alternatives; include guidance.

<sup>3</sup> Source: *Seventh Circuit Electronic Discovery Pilot Program – Final Report on Phase Two*

## 7 Electronic discovery process

### 7.1 General

Actual production of ESI should be conducted in a series of steps, as follows: (1) initial review; (2) search for and collection of ESI; (3) processing of ESI to eliminate duplicates and render it searchable; (4) culling the ESI to reduce volume; (5) review by counsel; and (6) production of reasonably usable or native format ESI.

### 7.2 Identification

Typically identification will involve firstly determining what ESI exists and secondly identifying its location or the means of accessing it.

Gathering information on the existence and location of potentially discoverable ESI is therefore a prerequisite to analysing whether ESI should be preserved, collected, and reviewed, since a party clearly cannot comply with its obligations if it does not know where its own documents are stored. Identification typically takes into consideration the facts of the matter, preservation demands, disclosure requirements, and discovery demands, including categories of ESI requested.

**Editor's Note:** Insert specific guidance here.

### 7.3 Preservation

Preservation is necessary where potentially discoverable ESI may be lost or altered in the normal course of business before a party has the opportunity to collect it. It is prudent to preserve sources of potentially discoverable ESI as early as possible.

**NOTE** Failure to take adequate steps to preserve ESI can result in spoliation, which can negatively impact the organization in the matter.

Once a decision has been made that a duty to preserve has been triggered, the scope of that duty must be evaluated; decisions as to scope may address time frames, custodians, subject matter, and responsive information by source or system, category, or type. Considerations should include: the facts upon which the triggering event is based and the subject matter of the triggering event; whether the ESI is relevant to that event; the expense and burden incurred in preserving the ESI; and whether the loss of the ESI would be.

As part of preservation, issue a legal hold or preservation notice to appropriate parts of the organisation, including data custodians (if known) and IT administrators. If the ESI is held by third party, it may be appropriate to notify them as well.

On the subject of legal holds, the NYBA offers: *"From a technical point of view, implementing legal holds can be easy or difficult (and everything in between) depending on the nature of the sources and systems that must be addressed. Typical technology issues involved in legal hold implementation include, for example:*

- a) the importance of timing because of routine operations of information systems that delete information;
- b) the viability of sending out and following up on hold notices by email or whether in-person contact is required;
- c) tracking the progress of steps to carry out the hold, including notices and systems implementation;
- d) the impact of removing backup tapes from the routine recycling, overwriting, or destruction process;
- e) the automated implementation of holds across various systems, such as emails, databases, file servers, etc.;
- f) whether collection (versus hold-in-place), is the best or most appropriate method of hold implementation under the facts and circumstances presented;

- g) stopping “auto-delete” functions; and
- h) ensuring that all ESI sources are properly identified and addressed, including online, near-line, and offline servers and storage devices and home computers, when applicable."

[There may be a need to archive ESI until litigation runs its course in the courts, which can take many years. The ESI has to be protected to ensure its admissibility as well as protect sensitive information (e.g., encryption)]

Editor's Note: Insert specific guidance here.

## 7.4 Collection

The objective of collection is to take a copy of the agreed ESI sources so that their content can be processed and made available for review. One of the additional objectives of collecting ESI, in many cases, is to secure a forensically sound copy of certain ESI as it was stored on a particular date and time. This may be necessary if the admissibility or validity of the ESI is later questioned.

Editor's Note: Insert descriptive text and specific guidance here.

## 7.5 Processing

In order to efficiently search and review ESI, it is necessary to prepare, or process, the ESI. The extent and nature of processing required in any given project will depend on the nature of the ESI collected, the technology being used, and the expected review process.

Editor's Note: Insert specific guidance here.

## 7.6 Review

As with the traditional discovery process, it is necessary to review a document in order to determine whether any form of privilege applies, to assess relevance, and often to categorise it according to issues in a matter or based on a specific schedule of requests. Electronic documents or ESI, are no different in their requirement for review. The main difference is that there are usually more electronic documents than hardcopy (paper) documents. However, the technology used in the processing phase is used to reduce the number of documents for review, and to focus on those most likely to be relevant.

While much of the work undertaken in order to complete the first five phases will be carried out by IT and/or eDiscovery specialists, in conjunction with legal advisors, review work is typically carried out by subject matter experts, such as trained legal professionals, accountants, or investigators.

< three Cs of document review: context, consistency and cost. An effective e-discovery system should resolve these three critical issues>

Editor's Note: Insert specific guidance here.

## 7.7 Analysis

The objective of analysis is to take a deeper look at a document, for example, to determine its provenance. Structured data, such as accounting systems, can also be analysed to generate insights into specific transactions, or patterns of transactions.

Editor's Note: Insert specific guidance here.

## 7.8 Production

Quite often the final step in the discovery process is providing a copy of the ESI (and hardcopy documents) which have been found to be relevant to the requesting party. It is vital that parties engage early in the process, so that what is produced at the end of the process is not a surprise.

Requests for ESI from litigants and third-parties for ESI are frequently met with objections that the requests are burdensome and overly broad. In addition, in E-Discovery, technical, highly complex issues may render requests inherently ambiguous and render compliance very difficult. To avoid, or contain, potential problems arising as a result of these issues, document requests and subpoenas for the production of ESI, and objections to those requests and subpoenas for ESI, should be written in plain, clear language with as much specificity as possible under the circumstances.

[production of reasonably usable or native format ESI]

The specifications for the exchange of documents and/or data between eDiscovery parties are known as the "form of production." The form of production refers both to file formats (e.g., native vs. imaged format with agreed-upon metadata and extracted text in a load file) and the media on which the documents are produced (paper vs. electronic). It should be noted that not all ESI may be conducive to production in either the native format or imaged format, and some other form of production may be necessary. Databases, for example, present such issues.

Editor's Note: Insert specific guidance here.

## 8 Additional considerations

### 8.1 Electronic discovery readiness

There are several major reasons why organisations face significant challenges when it comes to identifying and retrieving ESI in response to a discovery or regulatory request:

- It is often and unnecessarily stored beyond its required lifespan.
- There is often little knowledge within the organisation as to where potentially relevant ESI can be found.
- The volume and complexity is overwhelming even for Information Technology (IT) professionals.
- Turnover of staff and organisational changes (e.g., mergers, acquisitions, and divestitures) which result in retention of ESI but the loss of organisational knowledge and context.
- The IT environment and systems may be poorly documented.

These factors lead to unavoidable, expensive, and disruptive trawls through vast quantities of ESI in order to locate that which may be relevant to the matter in hand. This can introduce delays and increase the cost of the discovery process, in addition to increasing the risk of relevant ESI being overlooked.

[Include a description of how E-Discovery is related to Information Security]

- Effectively classify and categorize ESI so that eDiscovery is less costly, less resource intensive, and more complete.
- Provide mechanisms to search for relevant ESI and place it on litigation hold, culling it to package all that is required for court cases.

- Provide mechanisms to destroy ESI according to published retention policy, in a manner that will stand up in court.
- Accomplish all of this in the most effective and efficient manner, with the least impact on end users.
- Do this while at the same time addressing IT needs to ensure optimum performance of production systems such as Email, document management and tracking systems, and reducing the storage footprint for electronic and physical records.

## 8.2 Search technologies

## 8.3 Technology Assisted Reviews (TAR)

## 8.4 Avoiding data breaches

### 8.4.1 Disposition of ESI

Editor's Note: Leverage sanitization guidance in ISO/IEC 27040

### 8.4.2 Maintaining ESI confidentiality

- Confidentiality drivers
  - Proprietary materials
  - Privileged materials
  - Sensitive materials (e.g., PII)
- Confidentiality measures
  - Access control
  - Encryption and key management
  - Sanitization
  - Redaction (possibly reference ISO/IEC 27038)



1

## Bibliography

- 2 [01] ISO Guide 73:2009, Risk management – Vocabulary
- 3 [02] ISO/IEC 2nd WD 27040, *Information technology — Security techniques — Storage security*
- 4 [03] ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification,*  
5 *collection, acquisition, and preservation of digital evidence*
- 6 [04] ISO/IEC CD 27041, *Information technology — Security techniques — Guidance on assuring suitability*  
7 *and adequacy of investigation methods*
- 8 [05] ISO/IEC CD 27042, *Information technology — Security techniques — Guidelines for the analysis &*  
9 *interpretation of digital evidence*
- 10 [06] ISO/IEC CD 27043, *Information technology — Security techniques — Investigation principles and*  
11 *processes*
- 12 [07] ISO 15489:2001, *Information and documentation — Records management*

13