ISO PUBLISHES THE ELECTRONIC DISCOVERY STANDARD

Steven W. Teppler and Eric Hibbard

INTRODUCTION

After almost a decade of work, the final part of the international standard on electronic discovery was published in April, 2021.[1] This multi-part standard, known as the ISO/IEC 27050 *Information technology — Electronic discovery* series, is intended to "help organizations plan for and meet their electronic discovery objectives and obligations, if any, commensurate with the needs of each particular matter."[2] These matters can be of a legal, investigatory, records management, etc. nature; and, in such matters, ISO/IEC 27050 is not intended to supersede or override legal, statutory, regulatory, or other obligations.

I. ISO/IEC BACKGROUND

ISO/IEC 27050 is the product of the International Organization for Standardization (ISO),[3] in conjunction with the International Electrotechnical Commission (IEC)[4] and Joint Technical Committee 1 (JTC 1), Information Technology, Subcommittee 27 (SC 27). SC 27 develops and publishes standards in the areas of information security, cybersecurity, and privacy protection,[5] and it is best known for the ISO/IEC 27000 family of standards that provide guidance and requirements on information security management.

---

1. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Notice of Publication ISO/IEC 27050-4*, ISO/IEC JTC 1/SC 27/WG 4 N 4977 (Apr. 20, 2021) [hereinafter *Notice of Publication of ISO/IEC 27050-4:2021*].

2. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *International Standard 27050-1*: *Information Technology— Electronic Discovery — Part 1: Overview and Concepts*, ¶ 6.1, ISO/IEC 27050-1:2019(E) (Nov. 2019) [hereinafter ISO/IEC 27050-1:2019(E)].

3. *About Us*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/about-us.html (last visited Sept.15, 2021).

4. *How & Why the IEC Was Started*, INT'L ELECTROTECHNICAL COMM'N, https://www.iec.ch/history/how-why-iec-was-started (last visited Sep. 15, 2021).

5. *See ISO/IEC JTC 1/SC 27: Information Security, Cybersecurity and Privacy Protection*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/committee/45306.html (last visited Sep. 15, 2021).

ISO is the world's largest developer of voluntary international standards, and it is an independent, non-governmental organization made up of members from the national standards bodies of 167 countries and 3,368 technical bodies. Since its founding in 1947, ISO has published over 24,000 International Standards covering almost all aspects of technology, business, and manufacturing (e.g., from food safety to computers, and agriculture to healthcare).[6]

Founded in 1906, the IEC is a global, not-for-profit membership organization that brings together 173 countries and coordinates the work of 20,000 experts globally in its International Standards (over 10,000 published) and conformity assessment activities. IEC facilitates electricity access, and verifies the safety, performance and interoperability of electric and electronic devices and systems, including, for example, consumer devices such as mobile phones or refrigerators, office and medical equipment, information technology, electricity generation, and much more.[7]

ISO and IEC are two of the three global sister organizations (International Telecommunication Union, or ITU, being the third) that develop International Standards for the world. When appropriate, some or all of these standards development organizations cooperate to ensure that International Standards fit together seamlessly and complement each other.[8] Joint committees (e.g., JTC 1) ensure that International Standards combine all relevant knowledge of experts working in related areas.

"All [ISO/]IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in [ISO/]IEC work."[9] "Every member country, no matter how large or small, has one vote and a say in what goes into an [ISO/]IEC International Standard."[10]

---

6. *About Us*, INT'L ORG. FOR STANDARDIZATION, *supra* note 3.

7. *How & Why the IEC Was Started*, INT'L ELECTROTECHNICAL COMM'N, *supra* note 4.

8. *World Standards Cooperation*, INT'L TELECOMM. UNION, https://www.itu.int/en/ITU-T/extcoop/Pages/wsc.aspx (last visited Nov. 10, 2021).

9. *About the IEC*, INT'L ELECTROTECHNICAL COMM'N, https://www.iec.ch/about [https://web.archive.org/web/20201111084200/https://www.iec.ch/about]; *see also* INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, USING AND REFERENCING ISO AND IEC STANDARDS TO SUPPORT PUBLIC POLICY (2015).

10. *About the IEC*, INT'L ELECTROTECHNICAL COMM'N, *supra* note 9.

II. ISO/IEC 27050 OVERVIEW

A. *Purpose*

SC 27 initiated development on the international electronic discovery standard to harmonize terminology, describe core concepts, offer guidance in several key areas (e.g., electronic discovery governance, processes, readiness), and identify relevant requirements.[11] While ISO/IEC 27050 is not intended to contradict or supersede local jurisdictional laws and regulations, it can have an impact because ISO International Standards play an important role in cross-border issues. If nothing else, it can help address the "reasonableness" of one's actions.

As more electronic records and data (or "ESI") are created, modified, manipulated, used, and ultimately destroyed without ever taking on a physical form (e.g., a printed document), the predominance and importance of electronic discovery has correspondingly increased.[12] The emergence of ESI as the preferred representation of information introduces new challenges associated with locating ESI, handling massive quantities of data, preservation and retention of ESI, authenticity, data integrity, data confidentiality, and data or media sanitization, etc. While electronic discovery needs and responses will vary by matter, failure to appropriately handle the electronic discovery process in view of the context of a particular matter can result in rework, unnecessary costs, possible sanctions, and legal liabilities.

ISO/IEC 27050 purports to addresses these challenges[13] by:

- promoting a common approach, understanding, and language for electronic discovery;

- encouraging practical and cost-effective discovery by those tasked with managing ESI through the process;

- identifying competency areas for those involved in electronic discovery;

---

11. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *New Work Item Proposal for Electronic Discovery*, ISO/IEC JTC 1/SC 27 N11955 (Nov. 5, 2012).

12. *See* Deltona Transformer Corp. v. Noco Co., No: 6:19-cv-308-Orl-41LRH, 2019 WL 5390476, at *14 (M.D. Fla. Sept. 16, 2019), *report and recommendation adopted*, No: 6:19-cv-308-Orl-41LRH, 2019 WL 5558818 (M.D. Fla. Oct. 29, 2019) (recognizing "the predominance of electronic discovery in the modern era" (quoting Weintraub v. Advanced Corr. Healthcare, Inc., 161 F. Supp. 3d 1272, 1283 (N.D. Ga. 2015)).

13. *See* ISO/IEC 27050-1:2019(E), *supra* note 2, ¶ 6.1.

- promoting consideration of the proactive use of technology, in reducing costs and risks, while increasing efficiencies throughout the discovery process; and

- suggesting ways of avoiding inadvertent disclosures of potentially privileged, confidential, or sensitive ESI.

B. *Organization of ISO/IEC 27050*

As of this writing, the ISO/IEC 27050 series standard consists of the following parts:[14]

- ISO/IEC 27050-1:2019 (2nd Edition), *Information technology – Electronic discovery – Part 1: Overview and concepts*, which addresses general electronically stored information (ESI) and electronic discovery terminology and concepts as well as describing the electronic discovery process elements. It is intended to serve a broad audience and to be a foundational source of information on electronic discovery. It does not include any guidance or requirements.[15]

- ISO/IEC 27050-2:2018 (1st Edition), *Information technology – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery*, which focuses on the governance and management aspects of electronic discovery that are relevant to the governing body or senior management of an organization.[16]

- ISO/IEC 27050-3:2019 (2nd Edition), *Information technology – Electronic discovery – Part 3: Code of practice for electronic discovery*, which provides requirements and guidance for "personnel involved in some or all of the electronic discovery activities." Supplemental materials are included to help practitioners understand the objectives of each electronic discovery process element and the associated considerations, which can help

---

14. *See generally ISO Standards Catalogue*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/standards.html (last visited Feb. 28, 2022).

15. ISO/IEC 27050-1:2019(E), *supra* note 2, ¶ 1.

16. Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *International Standard 27050-2*: *Information Technology — Electronic Discovery — Part 2: Guidance for Governance and Management of Electronic Discovery*, ISO/IEC FDIS 27050-2:2018(E) (2018) [hereinafter ISO/IEC 27050-2:2018(E)].

these individuals determine the relevance of each process element and to assist in avoiding failures that can increase risks and expenses.[17]

• ISO/IEC 27050-4:2021 (1st Edition), *Information technology – Electronic discovery – Part 4: Technical readiness*, which provides guidance on the ways an organization can be better prepared to address electronic discovery from the perspective of both technology and processes.[18]

Figure 1 shows the inter-relationship of the various ISO/IEC 27050 parts. It is worth noting that Part 1 lays the foundation for all the other parts and Part 4 addresses issues from the other parts that can help organizations be better prepared to deal with electronic discovery.

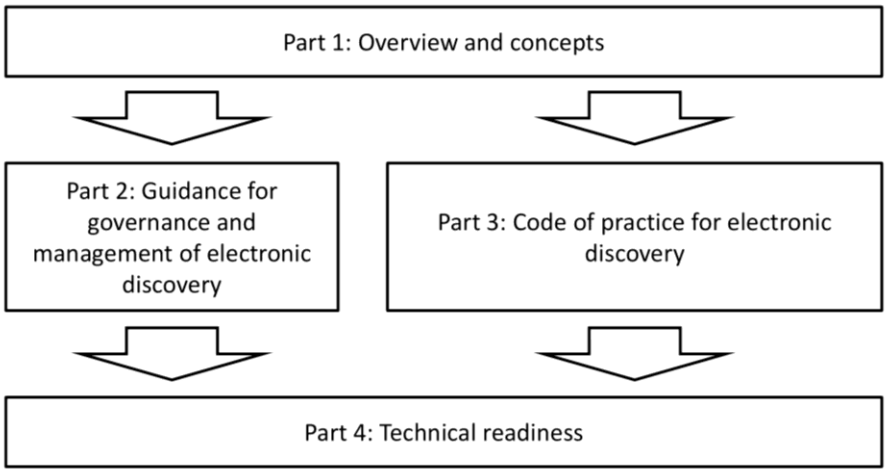

Figure 1. Relationship of ISO/IEC 27050 Parts[19]

An Ave Maria Law Review article published in 2014 chronicled the early work on ISO/IEC 27050 as well as described why and how the project was

17. Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *International Standard 27050-3: Information Technology — Electronic Discovery — Part 3: Code of Practice for Electronic Discovery*, at vi, ISO/IEC 27050-3:2020(E) (2d ed. 2020) [hereinafter ISO/IEC 27050-3:2020(E)].

18. Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *International Standard 27050-4: Information Technology — Electronic Discovery — Part 4: Technical Readiness*, ¶ 1, ISO/IEC 27050-4:2021(E) (Apr. 2021) [hereinafter ISO/IEC 27050-4:2021(E)].

19. Note that a similar figure was removed from Part 1 as revisions were ongoing. As the ISO Project Editor for the 27050 series, the author has provided it here as an update to the figure in the first edition of 27050-1.

undertaken.[20] This Article focuses on the final publications, describing the contents of each part and providing additional insight on how they are and can be leveraged.

III. PART 1—OVERVIEW AND CONCEPTS

ISO/IEC 27050-1 (Part 1) outlines the overall structure of ISO/IEC 27050[21] as well as provides terminology,[22] concepts,[23] and descriptions of other issues[24] that span the various parts. Part 1 does not include guidance/recommendations (often denoted by the verbal form "should") or requirements (denoted by the verbal form "shall"), so it is an informative document that helps with the understanding of materials covered in the other parts.

The first edition of ISO/IEC 27050-1 was published in November 2016,[25] under the title: *Information technology — Security techniques — Electronic discovery — Part 1: Overview and concepts*.[26] Changes were made to the ISO Directives wherein document titles could have no more than three elements.[27] This created a problem because Parts 2 and 4 were not published at the time this change went into effect, so following the new directives resulted in inconsistent naming within the series. SC 27 rectified this situation by undertaking a minor revision of Parts 1[28] and 3[29] with the sole intention of updating the titles to what they are now. Unfortunately, other directives-based

20. Eric Hibbard, *Electronic Discovery Standardization*, 12 AVE MARIA L. REV. 313, 313 (2014).

21. ISO/IEC 27050-1:2019(E), *supra* note 2, ¶ 5.

22. *Id.* ¶ 3.

23. *Id.* ¶ 6.2.

24. *Id.* ¶ 6.

25. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Notice PUB 27050-1 – Notice of Publication of ISO/IEC 270501:2016 (1st ed.) — Information Technology — Security Techniques — Electronic Discovery — Part 1: Overview and Concepts*, ISO/IEC JTC 1/SC 27/WG 4 N 1711 (Nov. 22, 2016) (1st ed.) [hereinafter *Notice of Publication of ISO/IEC 27050-1:2016*].

26. Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *International Standard ISO/IEC 27050-1 Information Technology — Security Techniques — Electronic Discovery — Part 1: Overview and Concepts*, ISO/EIC 27050-1:2016 (2016) (1st ed.).

27. Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *ISO/IEC Directives, Part 2: Principles and Rules for the Structure and Drafting of ISO and IEC Documents*, ¶ 11.4 (2021) (9th ed.).

28. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Published 27050-1 - Notice of Publication of ISO/IEC 27050-1:2019, Information technology – Electronic discovery – Part 1: Overview and concepts*, ISO/IEC JTC 1/SC 27/WG 4 N 1711 (Nov. 29, 2019) (2d ed.).

29. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Published 27050-3 - Notice of Publication of ISO/IEC 27050-3, Information technology – Electronic discovery – Part 3: Code of Practice for electronic discovery*, ISO/IEC JTC 1/SC 27/WG 4 N 3842 (Feb. 8, 2020) (2d ed.) [hereinafter *Notice of Publication of ISO/IEC 27050-3:2020*].

changes were applied to Part 1, resulting in all references to Part 4 being removed, as well as removing a figure that was similar to Figure 1 in this article.

A. *Electronic Discovery Objectives*

Part 1 identifies some or all the following as objectives of electronic discovery:[30]

- comply with confidentiality, data privacy, and other restrictions on data access, use, handling, or transfer imposed by applicable laws, regulations, rules, and expectations;
- identify potentially relevant sources of ESI;
- properly preserve and retain potentially relevant ESI;
- process relevant ESI into a format that facilitates its efficient searching or review;
- minimize the potential of failing to designate as responsive ESI that is responsive;
- minimize the potential of designating as responsive ESI that is not responsive;
- minimize the potential of failing to designate for withholding or special treatment responsive ESI that qualifies for withholding or special treatment;
- minimize the potential of designating for withholding or special treatment responsive ESI that does not qualify for withholding or special treatment;
- produce responsive ESI in a form that is useable by the requesting party;
- consider the proportionality of the response in the context of the matter and the costs;

30. ISO/IEC 27050-1:2019(E), *supra* note 2, ¶ 6.3.

- utilize technology in order to reduce risks and costs throughout the project.

Part 1 acknowledges that these objectives can vary by matter, and they need to be adjusted appropriately.

B. *Electronically Stored Information*

Part 1 dedicates an entire clause on ESI that starts by identifying issues associated with ESI (e.g., fragile and subject to easy loss, volume and complexity, and poor ESI management).[31] Concerns are raised that these issues can lead to delays as well as increased costs to locate and handle data that may be relevant to a particular matter.

The section continues with descriptions of common types of ESI, based on categorizing ESI sources as readily accessible (or "active") or not-readily accessible (or "inactive," "residual," or "legacy"). Such categorization, in conjunction with budget preparation, can assist in determining the proportionality of preserving and collecting such sources. Active data, inactive data, residual data, and legacy data are each described along with comments on the relative difficulty associated with collecting each type.

Common sources of ESI are identified[32] along the lines of custodial data sources[33] (e.g., mobile devices and laptops) and non-custodial data sources[34] (e.g., databases and backups). In addition, potentially excluded sources of ESI are identified (e.g., deleted or unallocated data, random access memory, and test data).[35]

Lastly, ESI representations and their classifications are addressed.[36] Basically, the collection and production formats for ESI files can be classified as native, near-native, image (near-paper), and paper. Issues stemming from conversion between these formats are also explored.

C. *Electronic Discovery Processes*

Part 1 defines the electronic discovery processes that are used throughout ISO/IEC 27050. As noted in the earlier Ave Maria Law Review article, the

31. *Id.* ¶ 7.
32. *Id.* ¶ 7.3.
33. *Id.* ¶ 7.3.2.
34. *Id.* ¶ 7.3.3.
35. *Id.* ¶ 7.3.4.
36. *Id.* ¶ 7.4.

definition of these processes was influenced by the Electronic Discovery Reference Model (EDRM).[37] The following are the ISO/IEC 27050 electronic discovery process elements:[38]

> • ESI identification is the element of the electronic discovery process in which a party, for any number of reasons (e.g., reasonable anticipation of a lawsuit or investigation, receipt of a pre-litigation preservation request, a request to inspect, a demand letter, a cease and desist letter, a cure notice, or even a discussion with an opposing party or its counsel), takes steps to identify information that could be potentially relevant to the matter. . . .
>
> • ESI preservation is the element of the electronic discovery process in which, after a triggering event, efforts are made to keep secure from modification or destruction information that has been identified as relating to the scope of a preservation obligation in a matter. . . .
>
> • ESI collection is the element of the electronic discovery process in which a data set is created from the ESI and hardcopy documents that have been preserved; the collection is then made available for further processing and eventual review. . . .
>
> • ESI processing is the element of the electronic discovery process in which, after data have been preserved and collected, steps are taken to render the data searchable and present them in a reviewable format. . . .
>
> • ESI review is the element of the electronic discovery process which focuses on screening ESI based on specific criteria. In essence, documents that meet the production criteria are separated from those that do not. . . .
>
> • ESI analysis is the element of the electronic discovery process that refers to the task of applying various tools and methods to the ESI in order to gather information that can be utilized in accomplishing the objectives of each of the distinct electronic discovery process elements. . . .
>
> • ESI production is the element of the electronic discovery process in which a party prepares materials for delivery to other parties. . . .

37. *See* Hibbard, *supra* note 20, at 329 (citing *Electronic Discovery Reference Model*, EDRM, https://edrm.net/edrm-model (last visited Dec. 3, 2021)).

38. ISO/IEC 27050-1:2019(E), *supra* note 2, ¶ 8.2–8.7.

Note that ISO/IEC 27050 differentiates "generic actions such as 'identifying' from the specific electronic discovery process elements by preceding the names with 'ESI' (e.g., ESI identification)."[39]

> [Figure 2] shows the interrelationship among the electronic discovery process elements. The positioning of ESI analysis as an outer ring is meant to show that analysis can optionally occur in conjunction with each of the other electronic discovery process elements. For example, a possible scenario is one in which ESI identification can require ESI analysis to be performed, after which the process returns to ESI identification for additional activity. The process flow can move from one process element, other than ESI analysis, to another, and then back to an earlier process element. Lastly, electronic discovery is often an orderly and iterative process undertaken with some or all the process elements, and this is also shown in Figure [2] with the circular arrows.[40]

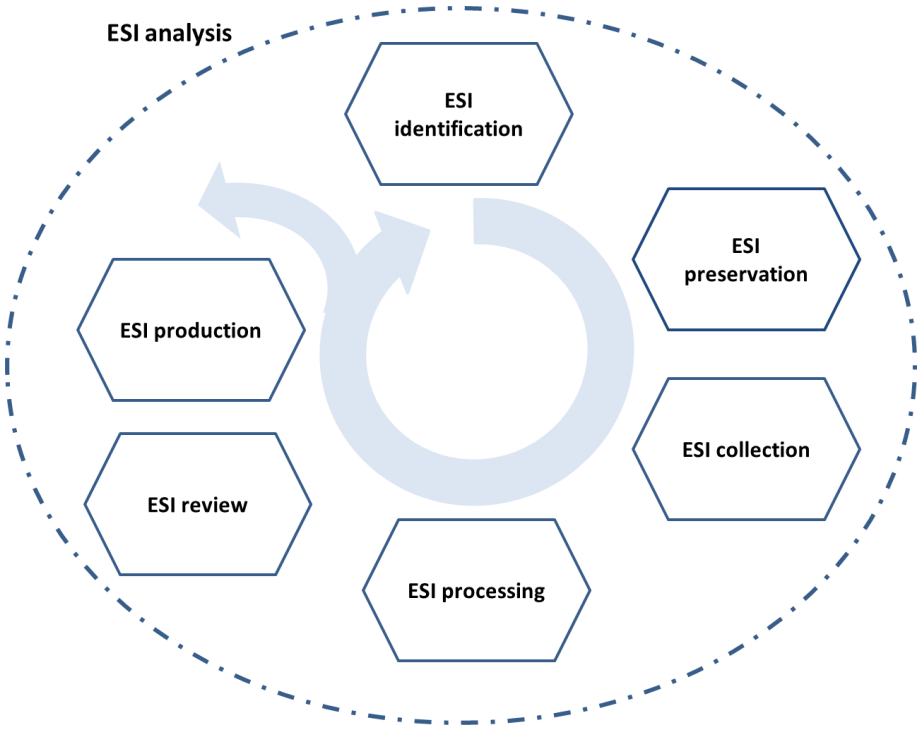

Figure 2. Electronic Discovery Process Elements[41]

39. *Id.* ¶ 8.1.
40. *Id.*
41. *Id.* ¶ 8.1 fig. 1.

It is important to keep in mind that:

> [ISO/IEC 27050] is intended to serve the interests of multiple stakeholders, large versus small entities, legal versus non-legal, etc. While a robust electronic discovery process is described, there is no intention to impose unneeded processes. Large enterprises with complex electronic discovery issues can use most or all the process elements described, but it can be impractical for small organizations or small matters. A matter may use a subset of the process elements.[42]

D. *Additional Considerations*

Part 1 concludes with the following additional considerations:

> • "Presentation of ESI"[43] (discussed in EDRM[44]) is not part of the electronic discovery process, but Part 1 highlights the importance of understanding how ESI can ultimately be used in a matter (e.g., presented in court). Much can be lost when ESI is exhibited in paper form.
>
> • "Chain of Custody and Provenance" can drive the importance of tracking or determining information regarding "the creation, modification history, influences, ownership, or other provenance or lineage information associated with ESI."[45]

IV. PART 2—GOVERNANCE AND MANAGEMENT

ISO/IEC 27050-2 (Part 2) was published in September, 2018[46] with the purpose of providing

> guidance for technical and non-technical personnel at senior management levels within an organization, including those with responsibility for compliance with statuary and regulatory requirements, and industry standards. It describes how such personnel can identify and take ownership

---

42. *Id.* ¶ 8.1.

43. *Id.* ¶ 9.1.

44. *Presentation Guide*, EDRM, https://www.edrm.net/resources/frameworks-and-standards/edrm-model/presentation-guide (last visited Nov. 16, 2021).

45. ISO/IEC 27050-1:2019(E), *supra* note 2, ¶ 9.2.

46. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Publication 27050-2 - Notice of Publication of ISO/IEC 27050-2:2018-09(E) (1st edition) — Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery*, ISO/IEC JTC 1/SC 27/WG 4 N 3332 (May 10, 2019).

> 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.[47]

A. *Governance of Electronic Discovery*

"The overriding goal [of Part 2] is to help organizations establish good governance for their electronic discovery processes by setting targeted policies and measured controls that are responsive to scale and size of an electronic discovery project."[48] "Governance provides the discipline to manage and monitor electronic discovery activities in a proactive manner. A good governance program is likely to put an organization in a better position to deal with electronic discovery issues, and to deliver policy driven processes."[49]

Normally, the governing body or senior management of an organization is responsible for governance, including:

- "Authoriz[ing] management to develop policies and strategies;"[50]
- "Examin[ing] and determin[ing] the requirements for effective and efficient electronic discovery capabilities, policies and the risk appetite for the organization;"[51]
- "Distribut[ing] decision-making rights, assigning responsibility for, and direct[ing] preparation and implementation of strategies, plans and policies;"[52]
- "Monitor[ing], through appropriate measurement systems, the accuracy, performance and conformance of electronic discovery activities and processes."[53]

B. *Management of Electronic Discovery*

"Senior management is responsible for defining electronic discovery strategies to implement control processes to be efficient and effective."[54] In addition, there is a need for personnel to "identify and take ownership of

---

47. ISO/IEC 27050-2:2018(E), *supra* note 16, ¶ 1.
48. *Id.* ¶ 5, at 3.
49. *Id.* ¶ 6.1.
50. *Id.* ¶ 6.2.
51. *Id.* ¶ 6.3.
52. *Id.* ¶ 6.4.
53. *Id.* ¶ 6.5.
54. *Id.* ¶ 7.1.

strategic risks related to electronic discovery and set policy to inform process control."[55]

Part 2 recommends that senior management develop the following policies:[56]

- Archival policies;
- Discovery policies;
- Disclosure policies;
- Capability policies (e.g., resources are adequate for the electronic discovery matter);
- Risk compliance policies;
- Monitoring and reporting policies.

C. *Compliance and Environmental Factors*

Part 2 highlights awareness of and the mitigation of certain causes of failure that can arise as important aspects of the processes for governance of electronic discovery.

> A goal for electronic discovery governance is to avoid negative consequences including those described below:
>
> - breaches of privacy caused by inappropriate methods or excessive or accidental disclosure;
> - legal and financial penalties for non-compliance with law;
> - original damage to ESI caused by inappropriate methods, including the damage to ESI's integrity, authenticity, reliability or usability; and any other potential causes of spoliation;

55. *Id.*
56. *Id.* ¶ ¶ 7.1–7.7.

> • damage to staff morale leading to negative impacts on the organization;
>
> • damage to organizational reputation caused by inappropriate disclosure to any third parties;
>
> • ESI acquisition and collection requirements that take excessive processing power or resource consumption for collections;
>
> • damage to any current or future litigation or other action or the organization caused by inappropriate disclosure of for example, IP, privileged or market sensitive information;
>
> • damage or non-compliant management of the chain of custody, which can render the ESI inadmissible in court.[57]

D. *Compliance and Review*

> Many organizations are faced with internal and external compliance issues that originate from statutory, regulatory, legal, or other requirements. [Part 2 recommends that] management should identify and take ownership of the risks, set policy, and set controls with respect to process review and compliance. It is important to ensure the electronic discovery process is executed within the confines of the relevant compliance and review policy requirements, and the relevant governance structures, processes, and communication mechanisms. Compliance with all due processes, and the regular review of these processes, offers the best assurance protection.[58]

Part 2 identifies the following as important aspects of compliance and review:

- "Structural requirements for process delivery" (e.g., identification of structural roles and risk owners and distribution of decision-making rights and responsibilities);[59]
- "Process control and monitoring" (e.g., metrics for monitoring the electronic discovery process);[60]
- "Communication mechanisms and disclosure;"[61]

---

57. *Id.* ¶ 8.1.
58. *Id.* ¶ 9.1.
59. *Id.* ¶ 9.2.
60. *Id.* ¶ 9.3.
61. *Id.* ¶ 9.4.

- "Consistency to policy and duty to perform" (e.g., "compliance within the local jurisdiction, and compliance with all due processes of ownership or custodianship");[62]
- "Effectiveness review;"[63]
- "Vendor management."[64]

V. PART 3—CODE OF PRACTICE

The first edition of ISO/IEC 27050-3 was published in October, 2017,[65] under the title of: *Information technology — Security techniques — Electronic discovery — Part 3: Code of practice for electronic discovery*.[66] As with Part 1, SC 27 undertook a minor revision of Part 3 to update the title and publish it as the second edition in January, 2020.[67]

ISO/IEC 27050-3 (Part 3) provides requirements and recommendations associated with the electronic discovery process elements described in ISO/IEC 27050-1. Additional materials are provided to help organizations better understand the objectives associated with each electronic discovery process element and considerations to avoid failures, which can mitigate risk and expense if electronic discovery becomes an issue.[68]

A. *Cross-cutting Aspects*

Part 3 identifies behaviors or activities, called "cross-cutting aspects," that span multiple electronic discovery process elements and need to be coordinated across the process elements. These cross-cutting aspects include:

- Planning – from the outset, most process elements need to be planned "with the specific objectives and conditions taken into consideration and with the resources to be deployed readily available."[69]

---

62. *Id.* ¶ 9.5.

63. *Id.* ¶ 9.6.

64. *Id.* ¶ 9.7.

65. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Notice Publication 27050-3 - Notice of the Publication of ISO/IEC 27050-3, Electronic discovery – Part 3: Code of Practice for electronic discovery*, ISO/IEC JTC 1/SC 27/WG 4 N 2208 (Jan. 3, 2018).

66. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *International Standard 27050-3: Information technology — Security techniques — Electronic discovery — Part 3: Code of practice for electronic discovery*, ISO/IEC 27050-3:2017(E) (2017).

67. *See Notice of Publication of ISO/IEC 27050-3:2020*, *supra* note 29.

68. ISO/IEC 27050-3:2020(E), *supra* note 17, ¶ 6.1.1.

69. *Id.* ¶ 6.1.2.

• Transparency – refinements and iterations are often necessary "that have to be readily explained to interested parties."[70]

• Documentation – sufficient documentation on both the scope and activities is necessary to address challenges, "and for the purpose of improving the effectiveness and consistency of future implementations of the process elements."[71]

• Expertise – "certain kinds of specialized expertise and qualifications [will be] necessary for each process element to do the work and to meet any operative standards."[72]

• Informed – "pertinent legal and subject matter experts [are] well informed as to the purposes to be served by the relevant process elements, the relevant requirements . . . , and the landscape of the ESI, as well as . . . understanding the subject matter, scope and timeframe that apply to the situation in question."[73]

• Adaptive – adaptability is often needed for electronic discovery projects because they often "begin in a state of imperfect knowledge when requirements and definitions are not yet fully specified and the ESI landscape is not yet fully mapped."[74]

• Use of technology – application of technology can have a major impact on the effectiveness of an electronic discovery project.[75]

B. *Electronic Discovery Requirements and Guidance*

Each electronic discovery process element is addressed in a separate clause, and each contains the following:[76]

• "[A]n overview of the process element" that goes beyond the basic description contained in Part 1,

• "[O]bjectives for the process element,"

70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*

- "[C]onsiderations to avoid failures" (i.e., issues that need to be managed or addressed),

- Separate "requirements and guidance specific for the process element."

A labeling scheme has been used within the requirements and guidance such that each can be explicitly referenced. This can be useful when a specific element needs to be referenced (e.g., a conformance exception).

Some in the U.S. legal community have expressed concerns that the Part 3 requirements may conflict with federal or state electronic discovery requirements or possibly constitute an overreach from an international entity.[77] To help assess the validity of these concerns, an excerpt of the Part 3 ESI production requirements and guidance is provided below:

> 6.8.5 Requirements for ESI production
>
> The ESI production element of the electronic discovery process carries significant import. In the litigation context, for example, after ESI has been reviewed for relevance, ESI production initiates the process in which parties can determine merits and relevance of ESI that can be material in the matter. An integral part of ESI production relates to the work performed in prior process elements, particularly ESI review. Issues with ESI productions are best remediated via careful planning and documentation. As with other process elements, the best way to avoid possible ESI production issues is with a plan and quality control process that includes documentation relating to content reviewed and produced, as well as tools and procedures employed throughout the ESI production process.
>
> The following are requirements for ESI production.
>
> a) The individuals responsible for ESI production shall, in advance of executing the production, develop a plan to guide the ESI production effort.

77. Kenneth J. Withers, *eDiscovery Counsel, Legal Technologists Express Discomfort with Proposed ISO/IEC eDiscovery Standard*, BLOOMBERG LAW (Nov. 9, 2017, 12:11 PM), https://news.bloomberglaw.com/e-discovery-and-legal-tech/ediscovery-counsel-legal-technologists-express-discomfort-with-proposed-iso-iec-ediscovery-standard.

b) The individuals responsible for ESI production shall be informed with regard to operative requirements that govern ESI production, including:

1) legal requirements;

2) matter-specific requirements;

3) process-specific requirements; and

4) the characteristics of ESI that needs to be produced.

c) ESI production shall be conducted using tools or methods that are appropriate to the ESI to be produced and to the operative requirements that govern the matter and those tools or methods shall be applied in a manner that enables them to have their intended effect.

d) The individuals conducting ESI production shall have the expertise needed to apply the chosen production tools or methods correctly and to conduct quality assurance on the results of the ESI production effort.

e) ESI production shall be conducted in a manner that ensures that sensitive ESI is protected in transit and at rest (e.g. using encryption, access controls, etc.).

f) ESI production shall be sufficiently transparent during its implementation to enable the individuals responsible for ESI production to assess its progress and make adjustments as warranted.

g) ESI production shall be supported by appropriate methods and metrics.

h) ESI production shall be adapted, as needed, to changes in the requirements that govern the ESI production effort and to changes in the hardcopy documents and ESI that is to be produced.

i) The forms of production shall be appropriate, such that the ESI is reasonably usable, and unless unwarranted, searchable.

j) The method by which the production is transferred shall be appropriate to the type and volume of the ESI and the needed speed and security of the transfer.

> 6.8.6 Guidance for ESI production
>
> The following recommendations can be relevant for ESI production.
>
> a) The procedures implemented for ESI production should be documented to accurately reflect:
>
> 1) all procedures followed in the course of production;
>
> 2) all significant decisions made during production; and
>
> 3) any evaluations of the effectiveness of the production effort.
>
> b) The individuals responsible for ESI production should assess the costs and benefits of different forms of production for their particular data set before agreeing to or finally determining a form of production.
>
> c) The final production set should be reviewed before delivery to ensure that any confidential, privileged, or otherwise sensitive documents which remain in the set through error or inadvertence can be removed from the production set before delivery. The use of agreements should be considered (if appropriate) before making production to the requesting party.
>
> d) The individuals responsible for the electronic discovery project should consider whether making production in stages, as opposed to making production of the entire relevant set at once, would be efficient or cost-effective in the particular circumstances and discuss such possibilities with the requesting parties.[78]

The requirements and guidance for the other electronic discovery process elements are similar in nature.

VI. PART 4—TECHNOLOGY READINESS

ISO/IEC 27050-4 (Part 4) was published in April, 2021,[79] with the purpose of "provid[ing] guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both

78. ISO/IEC 27050-3:2020(E), *supra* note 17, ¶¶ 6.8.5–6.8.6, at 25–26.

79. *See Notice of Publication of ISO/IEC 27050-4:2021*, *supra* note 1.

technology and processes."[80] The emphasis is on "proactive measures that can help enable effective and appropriate electronic discovery and processes."[81]

A. *Technology Readiness*

Part 4 describes technology readiness as:

> the knowledge, skills, processes, and technologies needed to address a particular issue or challenge. For an organization, this does not mean that it is all-knowing and able to do everything, but rather it is fit for purpose and ready for the task at hand, including any contingency that can occur. Within the context of electronic discovery, technical readiness means an organization is well positioned to address the tasks associated with the appropriate electronic discovery process elements,[82]

and it should be based on the information architecture, business processes, and data classification and retention policies of the organization.

Part 4 identifies the following as possible electronic discovery readiness objectives:

- comply with confidentiality, data privacy and other restrictions on data access, use, handling, or transfer imposed by applicable laws, regulations, rules and expectations;
- identify potentially relevant sources of ESI;
- properly preserve and retain potentially relevant ESI;
- produce responsive ESI in a form that is useable by the requesting party;
- conduct the electronic discovery process within the time constraints.[83]

B. *Readiness for Electronic Discovery*

Part 4 examines each of the ISO/IEC electronic discovery process elements as they are addressed in the other parts of ISO/IEC 27050. Where

80. ISO/IEC 27050-4:2021(E), *supra* note 18, ¶ 1.
81. *Id.*
82. *Id.* ¶ 6.
83. *Id.*

there are aspects that can benefit from readiness or proactive activities, Part 4 identifies them by process element along with specific, proactive recommendation or measures.

Much of this content is aligned with and expands upon the materials in ISO/IEC 27050-3.

C. *Additional Considerations*

Part 4 identifies the following "dependencies and potential impacts that need to be addressed":[84]

- "Privacy and Data Protection,"[85]
- "Long-term Retention of ESI,"[86]
- "Destruction of ESI" – "[U]se logical or media sanitization to eliminate ESI that is no longer required,"[87]
- "Business Continuity Management" – "The organization's [business continuity management] BCM plan should include mitigation for the potential adverse effects of electronic discovery."[88]

D. *Electronic Discovery Cross-cutting Aspects*

Part 4 "provides additional information and guidance on the planning, documentation, expertise and use of technology cross-cutting aspects,"[89] which are identified in Part 3.

E. *ESI Storage Questionnaire*

Part 4 includes an annex that can be used to gather key details for use in the creation of an ESI data map. See Appendix A,[90] *infra*, for the questionnaire details.

---

84. *Id.* ¶ 8.1.
85. *Id.* ¶ 8.2.
86. *Id.* ¶ 8.3.
87. *Id.* ¶ 8.4.
88. *Id.* ¶ 8.5.
89. *Id.* ¶ 9.1.
90. *Id.* ¶ A.1, at 21.

VII. CROSS

From an American jurisprudential perspective, the ISO Standard 27050 provides a robust set of minimum best practice guidelines, which, for the most part, are already incorporated by implication into the underlying objectives of Rule 1 of the Federal Rules of Civil Procedure.[91] The standard does not purport to either supplant or supersede the existing U.S.-based electronic discovery framework. That framework spans a continuum of litigants' rights and obligations provided by the Federal Rules of Civil Procedure, the various state rules of civil procedure, forum local rules, and even judge-imposed standing orders. Nevertheless, the acquisition and examination of ESI is not unique to the United States.[92] Multi-national organizations that are or may be subject to jurisdiction in the United States and that avail themselves of the standards' requirements and guidelines may provide process defensibility in the United States while maintaining standards compliance in their home jurisdiction.[93]

SUMMARY AND CONCLUSIONS

With the publication of the four parts of the ISO/IEC 27050 standard, SC 27 has concluded its work on electronic discovery. Assuming the typical five-year revision cycle employed by ISO, none of the parts will be subject to a systematic review until late 2023 (i.e., earliest opportunity to consider a revision). The most likely candidate for revision is Part 4 because of its focus on ICT as well as having dependencies on other SC 27 standards like ISO/IEC 27040, which is currently undergoing revision.

ISO/IEC 27050 is expected to help the international community better understand electronic discovery and to set basic expectations as to what is involved. It has been carefully written to avoid conflicts with jurisdictions that

---

91. "These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding." FED. R. CIV. P. 1.

92. Behrens v. Arconic, Inc., 487 F. Supp. 3d 283, 326 (E.D. Pa. 2020) ("No matter where this case proceeds, there will be complicated questions of access to cross-border discovery.").

93. This Article does not address the complex thicket of jurisdictional and privacy issues that inevitably arise where cross-border ESI discovery is sought in American courts. *See generally* EDISCOVERY WORKING GRP., N.Y.C. BAR ASS'N, CROSS-BORDER E-DISCOVERY: NAVIGATING FOREIGN DATA PRIVACY LAWS AND BLOCKING STATUTES IN U.S. LITIGATION (2020), https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/cross-border-e-discovery-navigating-foreign-data-privacy-laws-and-blocking-statutes-in-us-litigation.

have an electronic discover schemes or inadvertently introducing electronic discovery into jurisdictions that have no such process.

U.S. parties interested in acquiring copies of ISO/IEC 27050 can purchase them from the ISO Store[94] or from the ANSI Store[95] with a substantial discount.

94. *Store*, INT'L ORG. FOR STANDARDIZATION (last visited Nov. 19, 2021), https://www.iso.org/store.html (search catalogue for desired parts).

95. *ANSI Webstore*, AM. NAT'L STANDARDS INST. (last visited Feb. 15, 2022), https://webstore.ansi.org (search catalogue for desired parts).

APPENDIX A. ESI STORAGE QUESTIONNAIRE[96]

A. *Key contacts*

Contact details

— Name
— Role
— Telephone
— E-mail address
— Notes

Considerations

— Record the contact details for key individuals not involved with ICT within your organization
— Data owners
— Compliance and legal
— Record the contact details for key individuals involved with ICT within your organization
— Head of ICT
— Information security
— System administrators
— Authentication service administrators
— Directory service administrators
— Establish who within ICT is responsible for backup policies and BCM

B. *Assets*

Considerations

Identify if the organization stores/maintains central/remote logs of assets assigned to staff
— Log any resources that shared within a unit

Questions that should be logged

— Department name responsible for maintenance of a central log of assets
— List devices for new starters

96. ISO/IEC 27050-4:2021(E), *supra* note 18, ¶ A.1, at 21.

— List additional devices used by employees working in a specified team
— List shared assets on which a user can be able to store data

C. *ICT infrastructure (internal/third parties)*

Considerations

— Details of external organizations that host the organization's ICT infrastructure
— Backup management company
— Off-site storage
— Cloud computing-based data

Questions that should be logged

— Log if ICT is managed by an external party
— Log if systems are managed by an external party
— The details of any third-party companies
— Company
— Details of data hosted
— Key contact
— Telephone
— E-mail
— Notes

D. *Authentication services and directory services*

Considerations

— Identifying assets, a user on the domain has used
— Restricting access to individuals on domain if they are not present/working remotely
— Identifying access to shares on file server

Questions that should be logged

— Do you use an authentication server to authenticate users on the network?
— Is your authentication server administered locally? If no, from where and by whom is it administrated?

— Do you log/monitor staff logins and activity? Specifically, do you record which workstations a member of staff has used?
— What are your password policies for users?
— Do all users have home directories on the network?
— What is your naming convention for usernames?

E. *Workstations – laptops/desktops*

Considerations

— What does an employee use to conduct their day to day business on?
— How are their workstations identified on the network?
— What security features do the workstations have (encryption/biometric/card)?
— What can an employee store data on their organization computer?

Questions that should be logged

— Are computers assigned to individual users, or are they shared?
— Do you have an encryption policy for organization computers? (full disk/file system/etc.)?
— Are you able to issue decryption certificates?
— If no, who can? (contact details)
— What is your naming convention for computers?
— What is your policy on users saving files on their local workstation?
— Can an employee install applications on their workstation?
— Can an employee run executables on their workstation?
— Are files stored on a user's profile synchronized/backed up on the file server?
— What can an employee connect to their workstation in order to transfer files on/off?
— Are portable device connections logged centrally?
— What (if anything) is an employee prevented from connecting to their workstation?
— Are mailboxes stored locally on the workstation? (OST/PST/NSF/etc.)
— Is it different on laptops vs. desktops?
— What happens to an employee's computer if they leave/terminated (policy)?
— In the case of repaired/re-issued computers, what happens to the existing data? (migration/backed-up/deleted)

F. *Email servers*

Considerations

— Where is the mail server located and is it administered locally/globally/by third party?
— Are any compliance software/filtering/journaling features activated?
— Identify backup policy/regime
— Identify what happens to terminated employees' e-mails.

Questions that should be logged

— How is email managed:
— in-house?
— cloud computing-based?
— third party?
— What type of email system is currently used?
— What version is installed?
— In the last five years, have you used any other email system?
— Were the emails migrated/archived?
— How many email servers are there globally?
— Are they on separate domains?
— Do you have different domains for email?
— Where are the email servers geographically located?
— Are the retention and archiving policies the same among all domains?
— Are emails stored locally on individual's computers (PSTs, NSFs)?
— Do you retain deleted messages on the email server?
— Is there an auto-delete system?
— If so, can it be turned off for preservation purposes?
— If not, what is the work around?
— Is there a limit imposed on individual mailboxes?
— If so, what is that limit and what happens when it is reached?
— What software is used to back up email servers?
— Are email backups block level or individual mailboxes?
— Do you use an archive? If so, please describe.
— What type of back-up system do you use? Tape or digital? Local or remote?
— If tape, what tapes do you use?
— How are your tapes catalogued and inventoried?
— Are tapes sets clearly identified?

— How often are backups performed?
— What is your retention policy?
— What is your rotation schedule?
— What do you do with an e-mail account when employment is terminated?

G. *File servers*

Considerations

— Understand where employees (individuals, teams) are able to store data
— List folder level permissions/logging
— File servers used for local backups
— Applications that make use of file server to store transactional information (databases)

Questions that should be logged

— What type of files severs are in use?
— How many file servers do you have globally/locally?
— Where are they located geographically?
— Are there any archived/historical file servers?
— What were they used for?
— When were they decommissioned?
— Was the data migrated/archived
— Are they still available?
— What are names of file server?
— What type of files can users store on file servers?
— Any proprietary?
— E-mail? What are the locations?
— Is a user's profile synchronized with the file servers? (client-side caching)
— Is file/folder access on the file servers logged?
— Do you have group directories or public shares?
— Can employees delete permanently from the file servers?
— Prevent that or allow for backup and retrieval if needed?
— What type of back-up system do you use? Tape or digital?
— What software is used to back up file servers?
— If tapes, what type of tapes do you use? By location?
— How are tapes catalogued and inventoried?

— Are tape sets clearly identified?
— How often are backups performed?
— What is your rotation schedule?
— What is your retention policy?
— Is there replication in place?
— Where are the replication servers/storage located?
— How often does replication occur?
— What do you do with a user's home drive when employment is terminated?
— What do you do with a user's files in public locations when employment is terminated?

H. *Print servers/scanners*

Considerations

— Logs of all printing and scanning activity
— Tie in with active directory that shows when a user printed/scanned
— Any leasing company additional logging activation for billing purposes

Questions that should be logged

— Are your printers/scanners organization owned or leased?
— Contact details for lease organization
— What logs are recorded for these devices?
— Are print/scan jobs cached? If yes, how long for?
— Does a user have to authenticate prior to use? If yes, how can a user authenticate?

I. *Backups/off-site media/storage*

Considerations

— Identify if there are any potential issues with preservation and whether or not any relevant data is currently scheduled for destruction.
— Remember to record any third-party arrangements in place for backups and ensure they have been contacted by the firm

Questions that should be logged

— What type of back-up system is used?

— Tape?
— Digital?
— What software do you use?
— Where are backups stored?
— How often are backups performed?
— What is your rotation schedule?
— What is your retention policy?
— How are backups catalogued and inventoried?
— Is there a replication in place?
— What is the name of the off-site storage vendor?
— What is the address and telephone of the facility?
— Who is the contact?
— What type of data do they store?
— Does the vendor have relevant data that is not accessible from your current systems?
— Is there a current inventory of the material in storage?

J. *Applications (local/web-based/cloud computing) – laptops/desktops*

Considerations

— Identify which applications does an employee within the specific team have access to and where the transactional, temporary, cached files stored

Questions that should be logged

— What systems do the individuals/team have access to?
— Do you keep a central register of which applications have been installed on which corporate device?
— Do the applications log user activity?
— Where do the applications store data (file servers/local)?
— Is the system locked down or can employees install/use applications without your knowledge?
— If systems are not maintained by you behind your firewall, where is this information stored?
— Is access to public blog sites allowed (Facebook, Twitter, etc.)
— What type of web-based systems do you use that can have relevant data?
— SharePoint?
— Intranet?

— Extranets?
— Social media?
— Collaboration sites?
— Software as a service?
— Management systems or databases?
— Do you use any cloud computing-based applications?
— Who is the administrator for cloud computing -based applications?
— Are you able to block user access on cloud computing -based applications?
— Is the cloud computing -based applications backed up?

K. *Cell phones\tablets\portable devices*

Considerations

— Identify which communication devices the company use and give to employees
— Identify organization policy and infrastructure on personal devices and what is synchronized with their servers
— Identify what logs, records the organization maintains

Questions that should be logged

— What cell phone models (if any) are issued by the organization
— Are the devices issued by or owned by the organization?
— Are employees able to join their personal devices to the network/enterprise services, e.g. bring your own device?
— Are emails sent by a user on their device synched with the organization's e-mail server?
— Are text messages captured by your server?
— Is voicemail stored on your server?
— What type of data is stored on the device that is not on the server?
— Is the security policy on smart phones the same as internet settings on the computers?
— If not, can users access any kind of site from the smartphone?

L. *Remote access/VPN*

Questions that should be logged:

— Are users able to work remotely?

— How do they join/access the organization's services? (VPN, TeamViewer, etc)?
— Where does a user store their files when connected remotely?
— Are users able to use their own devices to connect to the organization?
— Are remote sessions logged?

M. *Communication applications*

Questions that should be logged

— Do you use or have unified messaging applications within the organization (e-mail, SMS, fax, voicemail, video calling)?
— Do you use instant messaging applications?
— Are conversations/chats logged centrally?
— Do you make use of a PBX (Private Branch Exchange) telephone system?
— What is the retention period for call logs, voicemails?
— Do you log internal-to-internal calls?
— Is voice mail stored on your systems? What is the retention?

N. *Other questions*

Questions that should be logged

— Do you have security-controlled building entry/exit systems?
— Do you have CCTV?
— What is your retention/turnover period?
— When was the last security or vulnerability assessment conducted (i.e. penetration testing)?