INTERNATIONAL STANDARD

ISO/IEC 27050-2

First edition
2018-09

Information technology — Electronic discovery —

Part 2: Guidance for governance and management of electronic discovery

Technologies de l'information — Découverte électronique —

Partie 2: Lignes directrices pour la gouvernance et le management de l'investigation informatique

Reference number
ISO/IEC 27050-2:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **1**
5 Electronic discovery background **2**
6 Governance of electronic discovery **4**
6.1 Context and principles 4
6.2 Mandate and establishment 4
6.3 Evaluate 4
6.4 Direct 4
6.5 Monitor 5
7 Management of electronic discovery **5**
7.1 Context and controls 5
7.2 Archival policies 5
7.3 Discovery policies 5
7.4 Disclosure policies 5
7.5 Capability policies 5
7.6 Risk compliance policies 6
7.7 Monitoring and reporting policies 6
8 Risks and environmental factors **6**
8.1 Overview 6
8.2 Privacy 6
8.3 Detection of other serious issues 7
8.4 Adverse effects on organizational activities 7
8.5 Damage to staff morale 7
8.6 Damage to organizational reputation 7
9 Compliance and review **7**
9.1 Overview 7
9.2 Structural requirements for process delivery 7
9.3 Process control and monitoring 8
9.4 Communication mechanisms and disclosure 8
9.5 Consistency to policy and duty to perform 8
9.6 Effectiveness review 8
9.7 Vendor management 8
Bibliography **9**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 27050 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Engagement in electronic discovery and processes can expose organizations and the stakeholders within and outside those organizations to collective and individual risks, including legal, financial and ethical. This document aims to provide guidance for decision makers and those holding responsible roles to ensure that causes of failure are properly managed and, where possible, minimized while still complying with policy and conformance requirements to enable effective and appropriate electronic discovery and processes.

This document is to be read in relation to ISO/IEC 27050-1 and ISO/IEC 27050-3. Common responsibilities of a governing body is to provide strategic direction in all matters of relevance to electronic discovery and to take ownership of the risks related to electronic discovery. The responsibility of management is to develop and implement the policies, plans and strategies for electronic discovery set by the governing body. The inherent causes of failure and environmental issues associated with electronic discovery governance and management impact the viability of a coherent system that delivers optimal business value. Consequently, the structures, processes and communication requirements of electronic discovery needs to be compliant and open to review.

The measure of success for the investment in the use of electronic discovery services is the benefit that it brings to the organization making the investment. Proper foresight, oversight and direction allow the full scope of the effort required to derive the expected benefits and an appropriate framework for governance, risk and value to be determined. This document addresses the concerns of electronic discovery governance by identifying the risk and the risk owners of potential points of failure in electronic discovery processes.

This document is to provide guidance for the governance and management of electronic discovery.

Information technology — Electronic discovery —

Part 2: Guidance for governance and management of electronic discovery

1 Scope

This document provides 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 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27050-1, *Information technology — Security techniques — Electronic discovery — Part 1: Overview and concepts*

ISO/IEC 38500, *Information technology — Governance of IT for the organization*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27050-1, ISO/IEC 38500 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Symbols and abbreviated terms

ICT	Information and Communication Technology
OCR	Optical Character Recognition
ESI	Electronically Stored Information

5 Electronic discovery background

Electronic discovery is an element of traditional discovery and it is a process that typically involves identifying, preserving, collecting, processing, reviewing, analysing, producing, establishing provenience, and maintaining the chain of custody, of ESI that can be potentially relevant to a particular matter. The guidance provided in this document are in accordance with the electronic discovery concepts described in ISO/IEC 27050-1:2016 Clause 3, 6.4 and 6.5.

ISO/IEC 27050-1 differentiates between generic actions such as "identifying" from the specific electronic discovery process elements by preceding the names with "ESI" (e.g., ESI identification). Likewise, this document follows this approach. Figure 1, repeated from ISO/IEC 27050-1, shows all of the electronic discovery process elements and the interrelationships between them (see ISO/IEC 27050-1:2016, 8.1 for a full description).

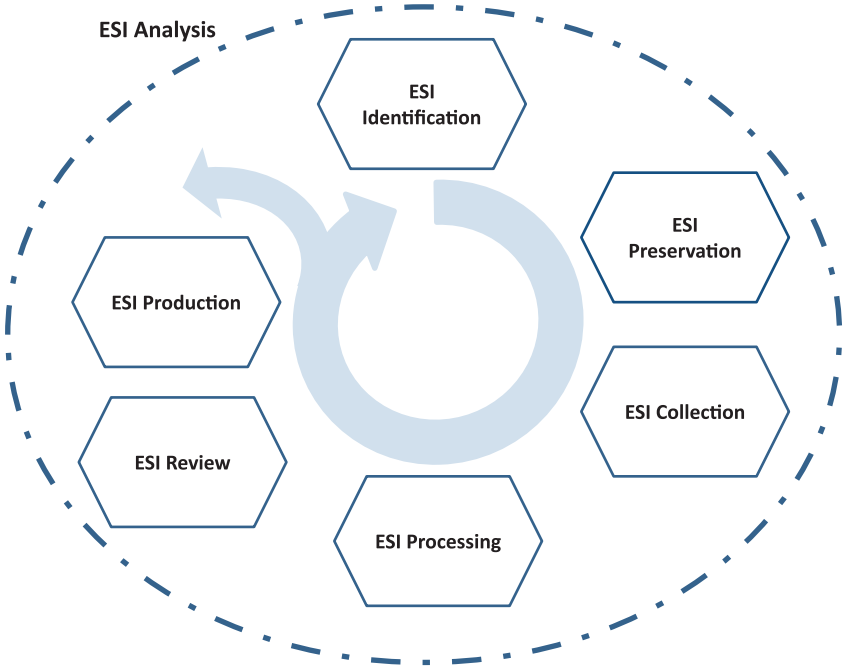

Figure 1 — Electronic discovery process elements

Risks associated with electronic discovery processes require attention from those responsible for governance and management to minimize systemic failures, unpredictable failures, and to maximize the process effects. The goal of electronic discovery is the same as with hardcopy document discovery that is to find and to produce information potentially relevant in a matter. The nature of electronic information adds differing layers of complexity and opportunity, since ESI carries with it such elements as metadata and requisite data processing and management functions that do not exist with paper. In addition, the collection and processing of ESI for discovery presents challenges that can have import either:

— to the viability or accuracy of the ESI produced to the opposing side (e.g., data corruption, password protection, encryption, indexing issues, inadequate keyword search, poor OCR); or

— to the ability to maintain chain of custody.

The escalating volumes of ESI typically created, maintained and collected present challenges for consistency and accuracy in review. The role of those responsible for governance and management is to assure electronic processes are controlled according to the risk criteria and conform to the distributed appetite for risk. Figure 2 describes the responsibilities in relation to electronic discovery roles and the harmonisation of related risks for optimal benefit delivery.

This document addresses the challenges of control by:

— promoting common understanding of various concepts and terminology for governance and management;

— articulating objectives and structures for electronic discovery governance;

— encouraging practical and cost-effective establishment of electronic discovery processes;

— providing guidance and best practices to those responsible for governance and management of electronic discovery strategies and policy;

— identifying tasks and strategy contexts for those responsible for electronic discovery governance and management, that they may set policy and design controls;

— promoting the proactive use of metrics and risk evaluation practices for minimizing failure in electronic discovery processes;

— suggesting ways to avoid adverse effects on reputational factors, organizational activities and staff morale;

— providing guidance for compliance, conformance and effectiveness review.

The overriding goal 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. While this document has been written with larger electronic discovery projects in mind, and therefore covers aspects encountered in the majority of matters, it is not necessarily the case that all steps will be required or proportionate to every matter. For example, in small matters, it can well be that a single person manages and completes every aspect of the project, whereas larger matters can warrant the use of separate individuals, third parties or even teams for each element of the electronic discovery project.

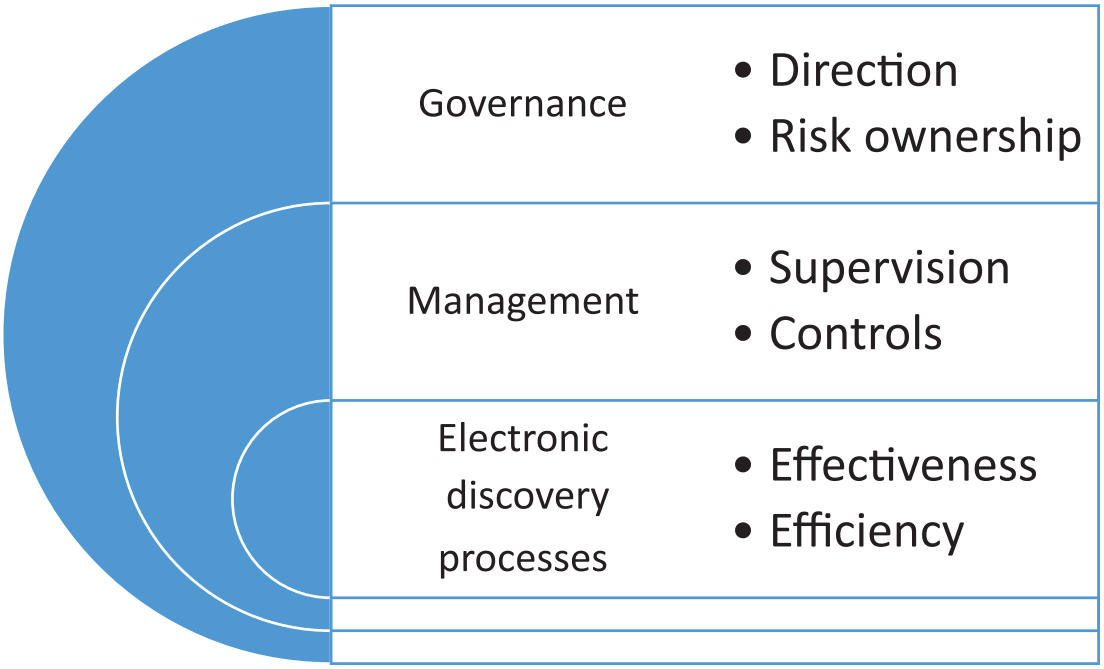

Figure 2 — Electronic discovery governance system harmonization

6 Governance of electronic discovery

6.1 Context and principles

Without sufficient governance as described in this document, electronic discovery is reactive to events and can appear ad hoc. 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. Governance of electronic discovery should be considered in the context of information technology governance. All parties involved in the production of policy, planning and implementation should be aware of the causes of failure associated with the electronic discovery processes, and their responsibilities and potential mitigation actions.

At a minimum, those responsible for governance (normally the governing body or senior management of an organization) should seek to create a culture in the organization which considers ESI as a valuable corporate asset. Consideration should be given to making electronic discovery risk a recurring governing body topic. A member of the governing body should have final responsibility for the discovery process adopted by the organization and be responsible for ensuring that legal, ethical and other requirements are complied with. ISO/IEC 38500 principles underpin the governance context, and ISO/IEC 30121 provides the framework for risk governance. ISO/IEC 31000 underpins management risk. These documents structure the context for electronic discovery governance and policy management.

ISO/IEC 38500 six principles of good governance require the policies for electronic discovery to articulate the following: responsibility for risk, the development of strategy, for asset acquisition, retention and retirement, conformance, performance, and, for the associated human factors. Management should have responsibility for the development and evaluation of the related policies and demonstrate leadership and commitment to adequate risk management that mitigates unacceptable causes of failure. The proper balance of the demand and supply of electronic discovery services is a requirement of effective governance and management, which should be driven and communicated from the top of the organization.

6.2 Mandate and establishment

The governing body should authorize management to develop policies and strategies (see Clause 7) that assure co-operation and interoperability between the enterprise functions, divisions and ICT and Information Systems services including, if appropriate any third party for the seamless delivery of electronic discovery services. Management support is essential for the successful establishment, implementation, maintenance and continual improvement of the electronic discovery processes.

6.3 Evaluate

The governing body should examine and determine the requirements for effective and efficient electronic discovery capabilities, policies and the risk appetite for the organization. This includes strategies, proposals, plans and supply arrangements (whether internal, external or both). Regular reports to the governing body are required so that performance and compliance of the electronic discovery processes can be evaluated in accordance with the goals for current and future use, and the current and future use circumstances.

6.4 Direct

The governing body should distribute decision-making rights, assign responsibility for, and direct preparation and implementation of strategies, plans and policies. The governing body is to evaluate the performance. It should also encourage a culture of good governance of electronic discovery in the organization by requiring senior managers to implement approved policies, comply with strategic directions and conform to the risk criteria.

6.5 Monitor

The governing body should monitor, through appropriate measurement systems, the accuracy, performance and conformance of electronic discovery activities and processes. It should reassure itself that performance is in accordance with strategic plans and its levels of risk are within the organization's risk criteria. Responsibility for the effective, efficient and acceptable use of electronic discovery capabilities by an organization is owned by the governing body and is retained when delegated.

7 Management of electronic discovery

7.1 Context and controls

Senior management is responsible for defining electronic discovery strategies to implement control processes to be efficient and effective. The design and the measurement of control systems for optimal operational efficiency and the development of process capabilities for electronic discovery are managerial accountabilities. ISO/IEC 30121 provides the context for the following processes and strategies. Subclauses 7.2 to 7.7 describe how personnel can identify and take ownership of strategic risks related to electronic discovery and set policy to inform process control.

7.2 Archival policies

Senior management should develop a comprehensive archive and retention policy of information properties and processes. This should include business continuity management plans and legal holds. The policy is to specify admission rules, structure, scope, completeness criteria, efficient storage practices, security provisions, chain of custody and mechanisms to maintain the integrity of the data. Consideration should be given to storage scalability including cloud capabilities, retirement policies and the location of storage, access and readiness for access. The purpose of information retention is to service availability of data for business, legal and other consumption requirements; in a timely and trusted fashion.

7.3 Discovery policies

Senior management should develop efficient and effective electronic discovery capabilities, discovery policies and supporting business processes. The implementation requires acquisition of relevant software and professional skills to execute electronic discovery processes. Standardization of discovery mechanisms for the consistent, timely and relevant retrieval of ESI requires planning, training and resource retention. Accurate and timely access to information is critical for decision-making and the presentation of ESI.

7.4 Disclosure policies

Senior management should develop criteria for the securing and the disclosing of information. Risk criteria are to be determined and the level of risk assessed to judge if the level is acceptable or whether additional mitigation actions are required. Policies should be produced that control any information that is disclosed. Disclosed information should be logged, processes recorded and preserved for audit and future access as required.

7.5 Capability policies

Senior management should develop policies, plans and retain resources to assure the electronic discovery capability is sufficient to deliver the required services, and of the required quantity and quality. Controls for the alignment of the business processes and the electronic discovery processes require adoption into local and professional codes of conduct for optimal capability. Policies should be produced to assure capable delivery of the electronic process elements, the metrics and the audit trails.

7.6 Risk compliance policies

Management should make decisions on whether to own, transfer or treat strategic risk based on the application of its risk criteria for electronic discovery. Policies should be produced that assure the level of failure remains within the organization's risk criteria and that each of the electronic discovery process elements has been evaluated for potential failure within the organization and local environment contexts. Preventive or detective and corrective controls should be designed to assure conformance with all compliance requirements.

7.7 Monitoring and reporting policies

The risk owners of an organization should measure the critical attributes of electronic discovery in order to evaluate plans, to monitor performance and conformance, and to direct strategies and policies. Metrics are to inform the implementation and design of the control framework for electronic discovery. Senior managers should develop metrics that indicate the attributes of lead measures, lag measures, and real-time measures. These metrics apply to each of the electronic discovery process elements, management controls and governance risk ownership attributes.

8 Risks and environmental factors

8.1 Overview

In the processes for governance of electronic discovery, it is important to be aware of, and mitigate, certain causes of failure that can arise which can have potential detrimental effects on an electronic discovery project. The retention and management policies of an organization (which can include business continuity management and legal holds) should mitigate for failure. 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;

— 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.

Determination of the risks and opportunities for the electronic discovery activities and processes requires an evaluation of the internal and external context (that includes business, legal and jurisdictional issues as well as ICT infrastructure). When planning the electronic discovery processes (ESI identification; ESI preservation; ESI collection; ESI processing; ESI review; ESI analysis; and, ESI production), the risk assessment is to assure the achievement of the intended outcomes, prevent or reduce undesirable effects and deliver continuous improvement.

8.2 Privacy

Inappropriate disclosure of information can result in breaches of privacy (see ISO/IEC 27050-1). Prior to, and during, the electronic discovery process, these causes of failure should be identified and

information thought to be discoverable should be reviewed, including by an independent reviewer, where appropriate, to ensure that unwarranted privacy breaches do not occur and that privacy protection failure is continuously reduced. At a governance level, clear policies on appropriate ways to deal with privacy breaches and conflicts arising from the need to disclose versus the need to maintain privacy, should be maintained and reviewed regularly.

8.3 Detection of other serious issues

During the exercise of an electronic discovery process, issues that were not at the heart of the original matter can come to light. For example, the matter can represent an intellectual property dispute, but in the course of the electronic discovery process and incident of unrelated fraud is uncovered. Policies and guidance should be developed that the ownership of these risks is clearly articulated and that the appropriate actions to take upon the discovery of other serious issues is maintained. These should include consideration of how to deal with disclosures which can arise from the need to continue compliance with external drivers (e.g. obligations to continue the discovery process) versus the need to deal with the serious issues detected (e.g. need to involve law enforcement or need to carry out major remediation in response to a security incident).

8.4 Adverse effects on organizational activities

Adverse effects can be mitigated by correct preparation (see ISO/IEC 27050-3) to ensure that inappropriate or excessive ESI collection, storage, retention, and disposition methods do not occur. The implementation of electronic discovery processes also impacts existing business processes and controls, and the adverse effects require mitigation in planning, training and change management strategy.

8.5 Damage to staff morale

Policies should be developed to protect staff integrity and the processes adopted for managing information quality. As part of the planning process, an appropriate communications strategy should be drawn up to ensure that rumours and negative stories are appropriately handled internally. Staff should be given sufficient information so they can understand the process being undertaken, their roles in it and the likely impact and effects for the future.

8.6 Damage to organizational reputation

Appropriate safeguards should be in place to prevent inappropriate disclosure to third parties. Where such disclosure cannot be avoided (e.g. because of disclosure in open court), communications and damage limitation strategies should be in place prior to the disclosure and activated as required.

9 Compliance and review

9.1 Overview

Many organizations are faced with internal and external compliance issues that originate from statutory, regulatory, legal, or other requirements. The 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.

9.2 Structural requirements for process delivery

Within the organization, the structural roles and risk owners should be identified prior to the commencement of a discovery process. These roles and risk owners should be responsible for ensuring

that statuary and policy requirements are complied with. To enable this, the mechanisms for a clear distribution of decision-making rights and responsibilities should be ready for use in response to any situation.

9.3 Process control and monitoring

In addition to the risk-related responsibilities mentioned in 7.1, metrics for monitoring the electronic discovery process and records management should be established (see also 6.2 and 7.2). Consultations with the external parties and the stakeholders that can be adversely affected by typical e-discovery process can be useful for setting the metrics. These metrics should then be used as the basis for monitoring the progress and success, or of the discovery process. Appropriate use of metric-based monitoring can give a good indication of whether or not particular targets (e.g. critical dates or volumes of ESI) are likely to be met. In the event that targets are likely to be missed, the use of metric-based monitoring can allow for re-negotiation of targets in order to avoid or reduce penalties which can be imposed for failure to comply with defined requirements.

9.4 Communication mechanisms and disclosure

In electronic discovery, the lack of communication can equate to a lack of opportunity to review progress, absence of opportunity to evaluate results and absence of opportunity to prevent spoliation, and excessive or inappropriate disclosure.

Prior to commencing the discovery process, exact outputs should be agreed, specifying the format and nature of material which is to be disclosed from the available ESI. Intermediate results should be assessed against this requirement, and the causes of failure identified, before filtering, editing or redacting, as appropriate, for the final disclosure.

9.5 Consistency to policy and duty to perform

The retention of information assets for electronic discovery requires compliance within the local jurisdiction, and compliance with all due processes of ownership or custodianship. To hold, discover and disclose requires the managerial performance and management of the duty of care within acceptable levels for risk and the criteria for risk as required by policy and local conformance of duty. Exemplary professional and ethical conduct should be apparent in all systems and parties associated with the electronic discovery processes.

9.6 Effectiveness review

Governance and management systems review for electronic discovery deliverables should be timely, regular and critical in deciding the effectiveness of the direction and controls chosen for the electronic discovery processes. The review is a quality control exercise designed to reduce variation in outcomes and to gauge the acceptability of the adopted failure levels.

9.7 Vendor management

Monitoring of third parties management of information, includes required security compliance and continuous evaluation of associated risks. These risks include any jurisdictional issues that can arise. For example, how the potential transfer of information can occur where the vendor development team reside, or in an alternative jurisdiction and where the data is hosted by the cloud or offshore. The regular monitoring of any contract or statement of works or other relevant agreement between the parties requires policy compliance articulation.

Bibliography

[1] ISO 15489, *Information and documentation — Records management*

[2] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[3] ISO/IEC 27050-3,*Information Technology — Security techniques — Electronic discovery — Part 3: Code of practice for electronic discovery*

[4] ISO/IEC 30121, *Information technology — Governance of digital forensic risk framework*

[5] ISO/IEC 31000, *Risk Management: Principles and Guidelines*

ICS 35.030

Price based on 9 pages