Interdisciplinary Description of Complex Systems 23(3), 217-229, 2025

DIGITAL EVIDENCE MANAGEMENT FOR ORGANIZATIONAL LEGAL COMPLIANCE

Zsolt Illési

Milton Friedman University
Budapest, Hungary

DOI: 10.7906/indecs.23.3.3
Regular article

Received: 20 February 2024.
Accepted: 1 November 2024.

ABSTRACT

With the rise of smart cities integrating advanced technologies into urban infrastructure, effective digital evidence management becomes crucial for organisations to address the complex legal and security challenges accompanying this digital transformation. It is essential for organisations to effectively manage digital evidence, which is crucial for success in legal cases such as criminal, labour, and civil proceedings. They must meet high standards in handling and presenting evidence and dealing with the complexities that computer systems can introduce. Digital forensics, blending law, criminalistics, and information technology, demands better management and governance to keep up with growing data volumes and technological changes. As technology evolves, forensic analysis must adapt from examining inactive systems to actively used business applications and mobile devices which were not initially designed for investigations. This shift requires new, creative approaches to manage and analyse digital evidence amid the challenges of vast complex virtual environments and emerging cyber threats. Effective digital evidence management can bring significant advantages, such as ensuring compliance with strict legal regulations, strengthening legal positions, as well as boosting organisational efficiency and reputation. On the other hand, inadequate evidence management can lead to serious consequences, including legal penalties, weakened defence in legal actions, operational issues, and damage to reputation. Therefore, organisations must focus on strategic evidence management, supported by frameworks like COBIT 2019 and strong leadership, to effectively navigate the complexities of modern digital and regulatory landscapes. This exploration underscores the importance of embedding forensic capabilities directly into ICT systems from the beginning, enabling organisations to proactively and efficiently address legal, regulatory, and security challenges.

KEYWORDS

digital forensics, evidence management, information technology governance

CLASSIFICATION

JEL: L63, L92

*Corresponding author, η: illesi.zsolt@uni-milton.hu; +36 61 454 7600/127;
Milton Friedman University, Kelta utca 2., H – 1039 Budapest, Hungary

INTRODUCTION

As cities worldwide embrace digital transformation to become smarter and more connected, the role of organisations in managing and presenting digital evidence within urban environments has become increasingly critical. Integrating advanced technologies into city infrastructures introduces complex legal and security challenges requiring a proactive approach to digital forensics and evidence management.

Organisations play a pivotal role in preparing and presenting substantial high-quality evidence for a successful outcome in legal cases. Therefore, organisations must prepare digital evidence for different legal proceedings and cases, primarily criminal, labour, and civil ones. From the perspective of digital evidence, the primary issues are related to the different standards of evidence, the burden of proof, and the limitations of the evidence that computer systems can collect.

Computer forensic investigation is an interdisciplinary field where the law outlines the functional requirements, and the framework is derived from criminalistics, but implemented through information technology using proper governance and management. To enhance the effectiveness and efficiency of criminal investigations, organisations must focus on improving the quality and quantity of available digital evidence, ensuring thorough documentation, making investigations repeatable by proper evidence handling, reducing errors through precise analysis, and presenting digital evidence transparently to support their legal position.

The increasing volume of data poses significant challenges to computer forensics. Digital evidence encompasses data from various sources, including computers, applications, transaction logs, system logs, video, and documents. New technologies and forensic methodologies are required to handle large-scale data cases effectively and efficiently.

Technological advancements have introduced new challenges, such as the shift from analysing "dead" systems (static storage devices) to "living" systems (active business applications). Investigators must now extract digital evidence from business applications not designed with forensic investigations in mind. This shift necessitates new research to understand the impact of forensic processes on digital evidence, especially in large businesses where detecting, imaging, and analysing evidence are complex processes.

Furthermore, the growing use of mobile devices and virtual environments adds to the complexity of finding adequate digital evidence in information and communication technology cases. Addressing these challenges requires innovation and the development of new solutions both at the technological and at the organisational level.

THE NEED FOR DIGITAL EVIDENCE MANAGEMENT

ADVANTAGES

Maintaining a sufficient amount and quality of digital evidence offers numerous benefits for organisations, especially in industries governed by strict regulations such as finance and healthcare. This section explores the advantages of robust digital evidence management, which include ensuring compliance with laws, improving legal standing, demonstrating responsible handling of information, increasing operational efficiency, and providing strategic advantages in various organisational dealings.

One of the foremost advantages of effectively managing digital evidence is the fact that it helps organisations comply with laws and regulations. For instance, the European Union’s General Data Protection Regulation (GDPR) and the United States Health Insurance Portability and Accountability Act (HIPAA) require businesses to protect personal data, necessitating solid

evidence management practices [1, 2]. Being able to provide relevant digital evidence quickly shows compliance and reduces the risk of facing legal consequences.

Comprehensive digital evidence also dramatically strengthens an organisation's position in legal matters. In lawsuits or regulatory investigations, having clear and compelling digital evidence can support an organisation's claims or defences and can be decisive in legal outcomes [3]. This evidence is critical for defending the organisation in legal cases and during negotiations.

Effective digital evidence management demonstrates an organisation's commitment to secure data handling and enhances trust among customers, partners, and regulators [4]. Managing digital evidence well shows that an organisation respects privacy laws and ethical standards, thus improving its reputation and building stakeholder confidence.

Organisations that have easy access to quality digital evidence operate more efficiently. They can quickly handle information requests or comply with regulations without diverting too many resources to retrieve such information. Organised digital evidence also supports better workflow and decision-making, which helps address operational issues promptly [5].

Digital evidence provides a strategic edge in negotiations, litigation, and resolving disputes. Organisations with solid evidence can confidently approach negotiations, shape litigation strategies, and manage disputes effectively. This ability helps prevent legal problems and gives organisations an advantage during contract talks and forming partnerships [6].

Lastly, digital evidence is essential for due diligence and implementing preventive, detective, and corrective actions. It allows organisations to assess risks, monitor compliance, and enforce policies to reduce legal and operational risks. Using digital evidence promptly supports proactive management, helping to protect the organisation from potential liabilities and improving governance [7].

RISKS

Organisations must effectively produce, store, manage and protect digital evidence in today's digital landscape. This section explores the significant risks of not having sufficient high-quality digital evidence when needed. These risks include the failure to comply with laws, adverse legal outcomes, damage to the organisation's reputation, disruptions in daily operations, an increased risk of future legal problems, a negative public image, and the poor allocation of resources.

One of the main dangers of not having sufficient digital evidence is violating laws and regulations. For instance, Europe's General Data Protection Regulation (GDPR) requires companies to keep personal data for specific periods [8]. Not being able to provide this data when asked can result in fines and other legal actions, which emphasises the need for effective digital evidence management.

In court cases, lacking strong digital evidence can lead to unfavourable judgments. Courts are increasingly dependent on digital evidence to make decisions. Companies that fail to provide necessary evidence might struggle to defend themselves, leading to adverse outcomes [9].

Failing to manage digital evidence properly can also harm an organisation's reputation. Stakeholders like customers, investors, and partners might see this failure as a sign of broader issues within the organisation, which can decrease their trust and willingness to engage with the business [10].

Effective operation often depends on the availability of critical digital information. Missing crucial digital evidence can cause delays and inefficiencies in the legal process [11]. These issues affect daily operations and can also hinder strategic business plans.

Organisations that do not keep good digital evidence records are more likely to face legal challenges in the future. If policies on evidence retention are lacking, it leaves gaps that can make a company more vulnerable to lawsuits [12].

How the public sees an organisation can significantly influence how it manages its digital evidence. Poor management can lead to public relations problems, especially if the organisation appears careless or secretive [10].

Lastly, not understanding the importance of digital evidence can lead to not giving enough resources to its management. This might result in underfunded IT departments and inadequate technology, further increasing the risks of managing digital evidence [11].

CHALLENGES RELATED TO EVIDENCE STANDARDS

The 'Beyond Reasonable Doubt' standard, the highest level of proof (primarily used in criminal cases), requires the evidence to be so convincing that a reasonable person would not hesitate to act upon it. This stringent standard underscores the gravity of the accusations in criminal cases. For example, in the case of an information and communication technology (ICT) security breach, the defendant can be convicted of the crime if the prosecution can prove beyond reasonable doubt that the defendant intentionally breached the company's cybersecurity protocols [13, 14].

On the other hand, the 'Scintilla of Evidence' standard refers to a minimal amount of evidence that might be considered decisive when going to trial even when only little relevant evidence exists. However, 'Beyond Reasonable Doubt' and 'Scintilla of Evidence' evidence standards are only two ends of the spectrum. There are other ones to consider. For example, in civil cases, the applied standard is the 'Preponderance of the Evidence', which requires the plaintiff to prove that there is a greater than 50% chance that the facts presented are true [13, 14].

Table 1 presents a list of evidentiary standards ranging from the highest (e.g. most challenging to meet) towards the lowest (e.g. least challenging to meet) end of the spectrum.

However, this list of evidentiary standards is only an illustration and, in this form, is mainly applicable to common law legal systems. The overall list of applicable evidentiary standards, definitions, and scope of specific applications may differ depending on the jurisdiction and particular circumstances. Therefore, ICT experts, Internal Audit, and the staff responsible for defining, implementing, and maintaining internal control systems should seek precise guidance and applications from legal professionals.

The other potential issue related to digital evidence is the 'burden of proof' principle, which is fundamental in legal cases, specifying which party should produce evidence and which party has the burden of persuading the court. However, its application is not always straightforward. Some exceptions exist, and the application details can vary depending on the specific legal branch [13, 15, 16]. For instance, in labour or administrative cases, the burden of proof may shift between parties. This variability underscores the need for a nuanced understanding and careful consideration in digital evidence preparation. A clear understanding of the 'burden of proof' concept is essential as it guides the preparation and presentation of digital evidence [17, 18].

Table 1. Contains sample evidentiary legal standards in descending difficulty order (continued on p.222).

Evidence Standard	Description	Example/Comment
Beyond Reasonable Doubt	The standard of proof in criminal cases requires a high degree of quantity and quality of evidence to support a conviction, beginning with the presumption that the defendant is innocent [13-15]	In an IT security breach case, the defendant can only be convicted if the prosecution can prove beyond reasonable doubt that the defendant intentionally breached the company's cybersecurity protocols.
Clear and Convincing Evidence	The standard of clear and convincing evidence is used to measure evidence related to specific issues in a case. It requires more robust and convincing proof than a routine civil trial. This higher standard, often a matter of public policy, plays a significant role in acknowledging that some court actions have more significant consequences, thereby impacting society. It can be understood in terms of probability, implying a high likelihood that a fact is true. It requires stronger evidence, whether in quantity or quality, to meet this burden of proof [14, 15].	In a fraud case, if it can be clearly demonstrated that it is highly and substantially more likely that the defendant did not intentionally mislead the plaintiff, the defendant should not be held liable.
Preponderance of the Evidence	This standard often refers to the 'greater weight' or the '51% probability' that one party should prevail over the other to tip the scales of justice. In other words, the trier of fact (such as a judge or jury) must believe that the existence of a fact is more probable than its nonexistence [13-15].	In digital forensics, this standard plays a crucial role during evidence acquisition. Forensic investigators must ensure that the evidence they collect is relevant, precise, and legally obtained. The outcome of an investigation often hinges on the quality and weight of the evidence acquired.
Substantial Evidence	Substantial evidence is evidence that a reasonable mind would accept as sufficient to support a conclusion beyond scintilla. This standard also means that the evidence is the product of adequately controlled investigations by qualified experts [15].	In cases involving unauthorized access to sensitive data, the "substantial evidence" principle ensures that the court bases its decision on credible digital evidence, such as server logs, email exchanges, and expert testimony, to find the perpetrator guilty.

Table 1. Contains sample evidentiary legal standards in descending difficulty order (continuation from p.221).

Evidence Standard	Description	Example/Comment
Probable Cause	A 'probable cause' characterises a reasonable ground to suspect that a person has committed a crime or a place contains specific items connected with a crime. It is more than a bare suspicion but less than evidence to justify conviction. A 'probable cause' might serve as a basis to support the issuance of an arrest, warrant or search warrant [15].	In the case of an ICT security breach, if the police have enough facts and circumstances to believe that a crime is being committed, they can obtain a search warrant.
Reasonable Belief	A 'reasonable belief' is a belief that the existence or truth of something is likely or fairly certain (e.g., a belief that a crime is being committed or has already been committed) [13, 15].	Where ICT devices, such as phones and computers, were potentially used for planning, reconnaissance, or communication among the perpetrator, the court, applying the 'reasonable belief' principle, must weigh the reliability and credibility of this digital evidence to determine its admissibility and relevance. Also, in an insider trading case, the court might use the 'reasonable belief' principle to determine that encrypted messages and the timing of stock trades provide sufficient grounds to suspect illegal information sharing, establishing intent without absolute proof.
Scintilla of Evidence	The 'scintilla of evidence' rule refers to a very small amount of evidence, which requires that a motion for a directed verdict or summary judgement cannot be granted without the slightest amount of relevant evidence, meaning that the matter will be sent to the jury, even if a small amount of evidence supports a legal claim. This principle contrasts the 'substantial evidence' rule, which requires a party to provide sufficient relevant evidence to support a claim [15].	The 'scintilla of evidence' principle might be decisive when minimal digital evidence, including a single metadata entry linking the defendant's computer to fraudulent transactions, is considered sufficient to establish probable cause for further investigation [16].

CHALLENGES RELATED TO FORENSIC QUESTIONS

In order to be effective and efficient in legal cases, organisations must ensure that their digital evidence addresses the classic forensic questions (5W+1H). This includes identifying the individuals involved (Who), detailing the nature of the events (What), pinpointing the locations (Where), establishing a timeline of events (When), understanding the motivation (Why), and identifying the modus operandi, including methods, tools or exploits used (How). By comprehensively documenting these aspects, digital evidence can provide a robust foundation for legal proceedings, ensuring that all necessary information is systematically collected and analysed. However, all of these questions have their potential issues [18].

The difficulties in attribution (providing evidence about who is involved)

In computer forensics, proving the involvement of individuals in cybercrimes is challenging due to the absence of the perpetrator in a physical form. Computers and user IDs do not directly represent natural persons, necessitating additional non-computer evidence to establish connections between suspects and crimes. This requires specialised investigative skills. Due to varying national legislation, connecting a perpetrator to an organisation or state is particularly difficult in international cases. For instance, the Estonian cyber incident illustrates how state-level involvement can complicate legal proceedings, as differing laws and state secrets can obstruct investigations.

Additionally, distinguishing between perpetrators and victims is problematic, as illustrated by cases where the supposed perpetrator's computer was compromised by a malicious code installed by a third party. The complexity is further exacerbated by the involvement of numerous entities, exemplified by the over 150 countries implicated in the Estonian cyber incident [18].

The difficulties in proving the overall scenario (providing evidence about what happened)

Proving what happened through logging is fraught with challenges. Firstly, many computer systems have minimal or no logging enabled by default, and administrators often do not adjust these settings, leaving insufficient evidence of events. Secondly, different systems log events in varied formats, making correlating data without extensive manual correction difficult. Thirdly, organisational practices regarding log retention vary widely; some are legally required to retain logs, while others do not, and perpetrators may delete logs to evade detection. Lastly, log data may be inconsistent or tampered with, complicating the investigator's task of determining the authenticity and integrity of the logs [18].

The difficulties in proving crime scene locations (providing evidence about where the events happened)

Identifying a crime scene in cyberspace is profoundly challenging compared to physical space. The virtual crime scene can span thousands of sites and computers, lacking clear boundaries like the yellow-black tape used in physical crime scenes. Determining the crime scene involves complex considerations, such as the perpetrator's location, systems used, target, or combined elements. This virtual crime scene can extend across multiple countries and continents, exacerbating the difficulties of investigating transborder crimes due to their international nature. Consequently, proving locations related to cybercrimes presents significant obstacles for law enforcement and investigators [18].

The difficulties in proving the timeline of events (providing evidence about when events happened)

Interpreting dates and times in computer systems poses significant challenges, which complicate the establishment of accurate event timelines. The primary issue is the representation of dates, which has some variations: the USA uses MM/DD/YYYY, the UK DD/MM/YYYY, and Hungary YYYY/MM/DD. Dates can be formatted in short forms, with diverse separators and textual month representations in different languages. Time data also presents difficulties with formats like HH:MM and varying separators used. These date and time fields can be stored differently on physical and logical layers, complicating forensic analysis. Forensic investigators cannot always interpret dates and timestamps accurately, necessitating extensive manual intervention to create a consistent timeline. Precision issues arise due to different system synchronisation practices, reliance on external time servers, or lack of time updates. Investigators must validate date and time integrity across systems. Additionally, counter-forensics tools like DECAF exacerbate these challenges by deliberately confusing dates and timestamps [18].

The difficulties in proving motivation (providing evidence about why events happened)

Defining the motivation behind cyber offences is challenging due to the prevalent use of no-flag and false-flag operations, which obscure the attacks' true origins and intentions. Unlike traditional crimes, where perpetrators are often identifiable, cyber operations often involve deception, making it difficult to discern whether an incident is a diversion or a covert action. Determining the root cause of a cyber-attack may necessitate exposing hidden details about the attack and the involved entities. This complexity complicates attributing responsibility in criminal and civil cases, as it involves unravelling secretive and distorted motivations and activities outside the recorded digital evidence [18].

The difficulties in proving modus operandi (providing evidence about the events that happened)

Defining the tools and methods used in cyber cases is challenging due to complex, distributed control structures. Attackers might leverage multiple command and control machines to orchestrate numerous zombie computers targeting a final victim. They exploit vulnerabilities in ICT systems, organisational processes, products, services, personnel, and facilities. Additionally, encryption obscures communication channels and data storage, complicating the discovery and comprehension of the crime. Consequently, obtaining comprehensive evidence about the actions, tools, and methods is often incomplete, leaving some case elements untraceable [18].

STRATEGIC APPROACH TO MANAGING DIGITAL EVIDENCE

Effective digital evidence management requires a strategic approach supported by top management with a comprehensive understanding of legal frameworks. Top management is crucial in creating a culture that prioritises evidence-based operations. Their deep understanding of legal and regulatory environments and ability to anticipate potential issues are vital for strategic decision-making [19].

Managing digital evidence involves precise, long-term planning and assessing the available resources accurately. The strategies include:

- Corporate-Level Strategy – this broad strategy defines the organisation's scope, including incorporating digital technology and platforms into its primary activities.

- Business-Level Strategy – this strategy outlines how individual organisational units will handle their specific evidentiary responsibilities, adapting processes to meet unique challenges [7, 20].

The COBIT 2019 framework is crucial for managing enterprise IT and governance, particularly in ICT. It provides a structure for transparent governance and management objectives essential for effective evidence management. The framework's flexible architecture allows organisations to modify or add new components as needed without affecting the overall model. It also supports the development of new focus areas tailored to the organisation's specific needs, offering a structured yet adaptable approach to digital evidence management [21].

ENHANCED PROCESS MANAGEMENT TO IMPROVE EVIDENCE QUALITY

The clear definition and documentation of organisational processes are crucial for understanding and interpreting evidence. This detailed documentation is essential because it helps maintain the integrity and clarity of both traditional and digital evidence from ICT systems. This section discusses how proper documentation of organisational processes can improve the interpretation and credibility of digital evidence in forensic investigations.

It is essential to clearly define roles and responsibilities within an organisation to aid forensic attribution. Knowing who is involved in specific activities and identifying conflicting roles helps pinpoint individuals during investigations [17]. This clarity is vital for linking actions directly to individuals, strengthening the investigative process.

A good process model outlines clear timelines and deadlines for each task, including when each task starts and ends or what triggers its start. This structure helps forensic investigators assemble the sequence of events by showing a clear timeline of actions [7]. Knowing the order and timing of events is crucial in digital forensics because it helps investigators identify when specific actions occurred, which is essential for spotting security breaches or malicious activities.

A thorough process model describes each task in detail, explaining all the steps involved. This ensures that everyone knows their specific responsibilities, including what inputs and outputs each task requires [19]. Forensic investigators benefit from such detailed documentation because it allows them to understand exactly what happened, making it easier to spot unusual or suspicious events.

Identifying where events happen, whether in physical space or digital platforms like networks and systems, is crucial in forensic investigations. Process models that identify these locations help investigators track where the actions occurred [20]. Knowing which platforms or software were used is also crucial for entirely digital processes as it helps identify potential areas for illicit activities.

Process models should include detailed documentation of the methods used for each task, including instructions, flowcharts, or diagrams. This level of detail helps forensic investigators by clarifying what procedures were followed and what actions were taken [20]. Understanding these details is essential for pinpointing where security may have been compromised.

Everyone involved in a process must understand why they are doing what they are doing. Knowing the overall goal and how each task helps achieve this goal helps everyone understand the process more deeply [22]. This deep understanding helps identify any process irregularities, enhancing the investigative process [23].

A detailed process model provides forensic investigators with valuable information, improving their understanding and helping them present evidence to stakeholders, law enforcement, or

courts [7]. Better documentation of digital evidence enhances its clarity and relevance to legal arguments, making evidence presentations more effective and increasing trust in the evidence.

ICT FUNCTIONAL DESIGN AND SUPPORT FOR QUALITY AND QUANTITY OF DIGITAL EVIDENCE

ICT systems and applications are often sources of digital evidence and should be designed to support forensic investigations. These systems should be able to answer the core forensic questions: identifying who is involved, detailing what happened, pinpointing where it occurred, establishing when it occurred, understanding why it happened, and determining how it was done using specific methods or tools. Integrating these forensic capabilities into ICT systems from their development is essential for speeding up investigations and ensuring that the evidence collected is valid and usable in court [16].

Designing business systems and applications with built-in forensic capabilities is necessary in today's digital world. The urgency of forensic readiness means preparing systems to efficiently handle legal examinations and minimise the costs of such investigations. Systems designed with these capabilities ensure that their digital evidence is reliable, intact, and acceptable in court. They also allow for quicker, more effective investigations because they organise data easily to analyse.

One essential framework for including forensic features in system design is the Common Criteria (ISO/IEC 15408), a set of international guidelines for evaluating security features in information technology products. This framework helps developers ensure their systems can adequately manage security tasks like data protection and access control. By following these guidelines, developers can make systems that secure data and gather and protect digital evidence correctly.

The Common Criteria organises its guidelines into 'Protection Profiles' and 'Security Targets,' which detail the IT product's security requirements and environment. When creating systems for forensic analysis, these profiles help developers incorporate necessary features for evidence collection, like secure logging of data and enforcing strict access controls.

By incorporating these standards from the start, organisations are not only proactive but also efficient. This approach significantly reduces risks related to digital crimes and aligns with best practices in IT management and risk assessment. It is a reassurance that the organisation is on the right track. Ultimately, organisations can better handle legal or security issues by meeting standards like the Common Criteria, turning sound forensic design into a strategic asset in managing digital risks.

To be able to answer the classic forensic questions, the following ICT functions should be implemented into the affected applications as follows.

1) Access Control: This function is intrinsically linked to the 'who' attribute, determining the individuals authorised to perform specific actions or access resources.
2) User Attribution: This function is solely related to the 'who' attribute, identifying and authenticating the user associated with each action or data set.
3) Timestamping: This function is exclusively related to the 'when' attribute. It provides the precise creation time for each log entry or data record.
4) Data Retention: This function supports all event attributes by determining the duration of data retention.
5) Legal and Regulatory Compliance: This function ensures adherence to relevant laws and regulations when handling all event attributes.
6) Data Integrity: This function guarantees the accuracy, consistency, and reliability of data related to all event attributes.

7) Data Recovery: This function provides mechanisms to restore data related to all event attributes in case of data loss
8) Audit Trails: This function records all actions performed in the system, thus relating to all event attributes.
9) Immutable Logs: This function guarantees the immutability of logged information related to all event attributes.
10) Real-Time Data Capture: This function is related to the 'when' attribute, capturing and processing data as it is generated.
11) Data Provenance: This function is related to the 'how' and 'why' attributes; it records the origin and history of data.
12) Secure Storage: This function protects stored data related to all event attributes from unauthorised access and corruption.
13) Data Redundancy: This function supports all event attributes by storing extra copies of their data to protect against data loss.
14) Incident Response Capabilities: This function supports all event attributes by allowing the ability to respond to security breaches or cyber-attacks.
15) Resilience: This function supports all event attributes by ensuring the system continues functioning and providing an acceptable level of service in the face of faults and challenges.

Table 2. summarises the mapping of the forensic-friendly functional requirements to the core forensic questions. In Table 2, 'P' represents primary, 'S' represents secondary, and '–' represents no relationship between functional requirements and the core forensic questions.

In summary, integrating forensic-friendly features into ICT systems makes them more compliant with the law and strengthens data reliability in forensic investigations. The detailed mapping in this section shows how these features directly answer the main forensic questions, ensuring the systems are ready to handle the complexities of digital forensics while preventing and reducing digital risks. Organizations can create a secure and compliant IT environment by following standards such as the Common Criteria and adding these critical functions. This approach not only protects data integrity and availability but also prepares organizations to effectively handle legal, regulatory, and security issues as they arise.

Table 2. Contains the list of forensic-friendly ICT functions and their mapping to the core forensic questions.

Functional Requirements	Who	When	What	Where	How	Why
Access Control	P	–	–	–	–	–
User Attribution	P	–	–	–	–	–
Timestamping	–	P	–	–	–	–
Data Retention	S	S	S	S	S	S
Legal and Regulatory Compliance	S	S	S	S	S	S
Data Integrity	S	S	S	S	S	S
Data Recovery	S	S	S	S	S	S
Audit Trails	P	P	P	P	P	P
Immutable Logs	S	S	S	S	S	S
Real-Time Data Capture	–	P	–	–	–	–
Data Provenance	–	–	–	–	P	P
Secure Storage	S	S	S	S	S	S
Data Redundancy	S	S	S	S	S	S
Incident Response Capabilities	S	S	S	S	S	S
Resilience	S	S	S	S	S	S

CONCLUSIONS

Handling digital evidence is not only about dealing with technical issues, but it is also vital for legal compliance, maintaining operations, and building trust. Organisations should create solid policies and systems to manage digital evidence effectively. This is crucial for reducing risks and strengthening overall resilience. The benefits of having adequate digital evidence are vast and vital for an organisation's operational, legal, and strategic success. Effective evidence management helps with legal compliance and supports solid legal defences, responsible information management, efficient operations, as well as effective negotiation and dispute resolution.

First, organisations must ensure the strategic management of forensic and evidentiary challenges in order to meet legal and regulatory standards. With top management's commitment to strategic planning and applying frameworks such as COBIT 2019, organisations can significantly improve their ability to manage these challenges. As digital environments change, organisational strategies for handling legal and forensic risks must also evolve.

Second, documenting organisational processes is essential in the digital forensics field. Clear and detailed descriptions of each process step help forensic investigations and improve the clarity and trustworthiness of digital evidence in legal situations.

Third, integrating forensic capabilities into ICT systems and applications is not merely an optional enhancement, but a fundamental requirement in the digital age. As cyber threats evolve and legal and regulatory demands intensify, the need for systems that are forensically ready from the outset becomes critical. The adoption of guidelines such as the Common Criteria (ISO/IEC 15408) in system design not only supports data security and integrity, but also ensures that digital evidence is robust and court-admissible.

REFERENCES

[1] European Commission: *General Data Protection Regulation (GDPR)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed 1st February 2024,

[2] U.S. Department of Health & Human Services*: U.S. Department of Health & Human Services*. https://www.hhs.gov/regulations/index.html, accessed 1st February 2024,

[3] The Sedona Conference: *The Trigger & The Process.* https://thesedonaconference.org/publication/Commentary_on_Legal_Holds, accessed 1st February 2024,

[4] The International Organization for Standardization: *ISO 27001 Information Security Management*. https://www.iso.org/standard/73906.html, accessed 1st February 2024,

[5] Stevenson ,W.J.: *Operational Management*. McGraw-Hill Education, New York, 2021,

[6] Wilson-Kovacs, D.; Helm, R.; Growns, B. and Redfern, L.*: Digital evidence in defence practice: Prevalence, challenges and expertise*. The International Journal of Evidence & Proof **27**(3), 235-253, 2023, http://dx.doi.org/10.1177/13657127231171620,

[7] Magnusson, C. and D. Blume: *Digitalisation and corporate governanc*e. OECD Corporate Governance Working Papers, No. 26. OECD Publishing, Paris, 2022, http://dx.doi.org/10.1787/296d219f-en,

[8] Voigt, P. and Bussche, A.: *The EU General Data Protection Regulation (GDPR). A Practical Guide.* Springer, Cham, 2017, http://dx.doi.org/10.1007/978-3-319-57959-7,

[9] Casey, E.: *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* 3rd edition. Academic Press, New York, 2011,

[10] Tokody, D. and Flammini F.: *Smart Systems for the Protection of Individuals.* Key Engineering Materials **755**, 190-197, 2017, http://dx.doi.org/10.4028/www.scientific.net/KEM.755.190,
[11] Coombs, W.T.: *Ongoing Crisis Communication: Planning, Managing, and Responding*. SAGE Publications, New York, 2014,
[12] Chen, Y.-C.: *Managing Digital Governance: Issues, Challenges, and Solutions*. Routledge, New York, 2017, http://dx.doi.org/10.4324/9781315207667,
[13] Stopp, M.T.: *Evidence Law in the Trial Process*. Delmar Cengage Learning, 1998,
[14] Garner, B.A.: *Black's Law Dictionary*. Thomson Reuters, 2009,
[15] US Law: *United States v. Fazio*. No. 12-3786-cr (2nd Cir. 2014), 2014, https://cases.justia.com/federal/appellate-courts/ca2/12-3786/12-3786-2014-10-22.pdf?ts=1413988218, accessed 1st June 2024,
[16] Tremmel, F.: *Evidence in criminal proceedings*. In Hungarian. Dialóg Campus Kiadó, Budapest, 2006,
[17] Carrier, B.: *File System Forensic Analysis*. Addison-Wesley Professional, Boston, 2005,
[18] Kengyel, M. and Szabó, M.: *The practical manual of civil litigation evidence*. In Hungarian. KJK Kerszöv Jogi és Üzleti Kiadó Kft., Budapest, 2005,
[19] Boros, A.: *Evidence in administrative procedural law I-II.* In Hungarian. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2010,
[20] Illési, Zs.: *Cyberterrorism from IT forensics perspective*. Magyar Rendészet **13**, 55-62, 2013,
[21] Horsman G.: *Digital evidence strategies for digital forensic science examinations*. Science & Justice **63**(1), 116-126, 2023, http://dx.doi.org/10.1016/j.scijus.2022.11.004,
[22] Langer, A.M and Yorks, L., eds.: *Strategic IT: Best Practices for Managers and Executives*. Wiley, New York, 2012, http://dx.doi.org/10.1002/9781119205104,
[23] ISACA: *COBIT 2019 Framework: Introduction and Methodology*. https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf, accessed 1st February 2024.