

MSc Data and Artificial Intelligence

**Module: Research Methods and Professional
Development**

**Title of Proposal: Enhancing Forensic Readiness
in Organisations for Effective Cyber Incident
Investigation.**

Student Name: Ziaur Rahman Ramim

Student Number: 2503796

Table of Content

1. Introduction -----	04
1.1 Context and Background -----	04
1.2 Research Problem -----	04
1.3 Research Aim and Objectives -----	05
1.4 Significance of the Research -----	05
2. Literature Review -----	06
3. Research Design and Methodology -----	08
3.1 Research Design -----	08
3.2 Research Methods and Materials -----	10
4. Expected Outcome -----	12
5. Timeline -----	13
6. References -----	14
7. Appendices -----	15

List of Figures

Figure-1 Research Design of the proposed study----- 10

Figure-2 Project Timing ----- 13

1. Introduction

1.1 Context and Background

Cyber glitches are become a common problem for modern era. Attacks like ransomware, insider abuse, phishing, and unauthorized access can interfere with business operations, reveal private information, and harm a company's finances and reputation. As a result, numerous organizations have made investments in monitoring systems, firewalls, endpoint security, and incident response procedures. However, post-incident inquiry is frequently not prepared to the same extent as prevention and detection.

Organizations frequently don't consider digital evidence until after a cyber event has occurred. Important data might have already been lost by then. Staff may not know how to properly preserve evidence, logs may be inadequate, and timestamps may not match amongst systems. This makes it challenging to comprehend what transpired, how the incident occurred, whose systems were impacted, and whether the information that is currently available can be trusted for internal, legal, or regulatory purposes.

Forensic readiness becomes crucial in this situation. The ability of an organization to get ready for upcoming investigations by making sure the appropriate technical controls, rules, procedures, and awareness are already in place is known as forensic readiness. When a security incident happens, a forensic-ready organization is better equipped to gather, safeguard, and utilize digital evidence. Instead of responding in a hurried and disorganized manner, it can look into the matter more effectively and confidently.

1.2 Research Problem

Considering an acceptance of the need of forensic readiness, many organizations are still unprepared to facilitate successful digital investigations during cyber disasters. There are a number of typical issues in practice. Incident response procedures might not be in line with forensic requirements, logs might not be gathered regularly, evidence retention regulations might be lax, and roles might not be clearly defined.

Another problem is that a large portion of the current topic of discourse about forensic preparation is still theoretical or general. Although there are helpful tips on incident handling, logging, and evidence processing, organizations may still find it difficult to translate these concepts into a workable and controllable preparation strategy. As a result, there is a discrepancy between what organizations ought to achieve in principle and what they can really accomplish in practical situations. The research problem for this study can therefore be stated as follows:

Many organisations are not sufficiently prepared to support timely, reliable, and effective digital forensic investigations during cyber incidents, and there is still a need for a more practical framework to improve forensic readiness in organisational environments.

1.3 Research Aim and Objectives

The aim of this research is to examine the role of forensic readiness in organisations and to propose a practical framework for improving preparedness for digital forensic investigations during cyber incidents.

To achieve this aim, the study will pursue the following objectives:

1. To examine the concept of forensic readiness and its importance in organisational cyber incident response.
2. To identify the technical, organisational, legal, and human factors that influence forensic readiness.
3. To analyse the main challenges organisations face when preparing for digital forensic investigations.
4. To review existing guidance, models, and practices related to forensic readiness.
5. To propose a practical forensic readiness framework that can help organisations improve investigation preparedness.

1.4 Significance of the Research

This research is significant from an academic and practical aspect. From a educational perspective, it adds to the expanding conversation on the connection between incident response, digital forensics, and cybersecurity. Additionally, it covers a topic that is pertinent but yet lacking practical development. Few studies concentrate on how organizations may use forensic preparedness in a straightforward and practical manner, despite the fact that many explain why it is important. Internal investigations, disciplinary measures, regulatory reporting, and legal procedures may all be hampered by insufficient or useless material. Therefore, a useful forensic preparation framework could assist organizations in strengthening their overall cyber resilience, reducing investigative delays, and improving the quality of the evidence.

2. Literature Review

Forensic readiness has become an increasingly important topic in cybersecurity and digital forensics because organisations are no longer judged only by how well they prevent attacks, but also by how effectively they investigate and respond to them. As cyber incidents continue to affect businesses, public services, and other organisations, the ability to identify, preserve, and analyse digital evidence has become a key part of resilience. The literature shows that forensic readiness is closely connected to incident response, logging, monitoring, governance, and evidence management. At the same time, it also shows that many organisations still struggle to translate these ideas into practical day-to-day readiness [1]–[4]. Guidance for your module also asks for recent, relevant literature and a clear gap-led review, so expanding this section with stronger source coverage is exactly the right move.

Forensic readiness has become an increasingly important topic in cybersecurity and digital forensics because organisations are no longer judged only by how well they prevent attacks, but also by how effectively they investigate and respond to them. As cyber incidents continue to affect businesses, public services, and other organisations, the ability to identify, preserve, and analyse digital evidence has become a key part of resilience. The literature shows that forensic readiness is closely connected to incident response, logging, monitoring, governance, and evidence management. At the same time, it also shows that many organisations still struggle to translate these ideas into practical day-to-day readiness [1]–[4]. Guidance for your module also asks for recent, relevant literature and a clear gap-led review, so expanding this section with stronger source coverage is exactly the right move.

Another major theme in the literature is the importance of logging and visibility. NIST SP 800-92 makes it clear that log management is essential for event detection, accountability, troubleshooting, and forensic investigation [3]. NCSC guidance on digital forensics and protective monitoring supports this by stressing the need for forensic visibility before and after a compromise [4]. In simple terms, organisations cannot investigate what they have not recorded. If logs are incomplete, inconsistent, or not retained properly, the ability to reconstruct an incident becomes much weaker [3], [4]. The general concept of forensic readiness is commonly defined as an organisation's ability to maximise the use of digital evidence while minimising investigation cost and disruption, which further supports the importance of proactive evidence collection and management.

Recent UK reports strengthen the practical need for this research. The Cyber Security Breaches Survey 2025 and the Cyber Security Longitudinal Survey both show that cyber incidents remain a continuing problem for organisations, which means investigation preparedness is not a specialist issue but a real operational need [5], [6]. If incidents are frequent, then the ability to investigate them effectively becomes part of normal cyber resilience rather than an optional extra. This supports the argument that forensic readiness should sit alongside prevention, detection, and response as a core organisational capability.

Beyond the standards and government guidance, academic research has also tried to define what readiness looks like in practice. Elyas et al. argue that modern organisations need digital forensic readiness in order to meet legal, contractual, regulatory, security, and operational obligations, but they also point out that the field has lacked clear and coherent guidance on how readiness can actually be achieved [7]. This is an important contribution because it highlights a problem that still appears in the newer literature: organisations often understand the importance of forensic readiness in theory, but implementation remains inconsistent. The same concern appears in later work by Taiwo et al., who note that digital forensic readiness has received limited attention and that many available models have remained too theoretical, with insufficient input from practitioners [8]. Their work proposes an extended digital forensic readiness and maturity model for enterprise settings, showing that readiness needs to be managed in a more structured and measurable way. Both studies point to the same underlying issue: there is still a gap between concept and practice.

Taken together, the literature suggests that forensic readiness rests on several connected dimensions. Technical readiness includes logging, monitoring, evidence preservation, time synchronisation, and secure storage. Organisational readiness includes governance, policy, incident response planning, and role clarity. Legal and procedural readiness includes chain of custody, compliance, admissibility, and documentation. Human readiness includes staff awareness, training, and the ability to recognise when potential evidence must be preserved [1]–[4], [8], [9], [11], [12]. The more recent work consistently supports this multi-factor view, especially the studies on enterprise maturity, Industry 4.0 readiness, and IoT forensic readiness.

However, despite this growing body of work, an important gap remains. The literature is strong in explaining why forensic readiness matters and in identifying the elements that influence it, but it is still less strong in offering a simple and practical framework that organisations can apply in day-to-day operations. Existing guidance often remains high-level, while some academic models are conceptually useful but less accessible for real-world organisational use [7], [8]. This creates the central gap for the present study. Organisations may understand that they need better logs, stronger policies, clearer evidence procedures, and better staff awareness, yet still lack a clear structure that brings these elements together in a manageable way. The current study therefore builds on the literature by aiming to translate those principles into a more practical forensic readiness framework for organisations.

3. Research Design and Methodology

A qualitative approach to research will be used for this research. The research focuses on learning concepts, frameworks, and organizational practices rather than assessing numerical performance through tests, which is why a qualitative method was used. Because it looks into how forensic readiness is defined in the literature, what influences it,

what obstacles organizations encounter, and how these findings may be combined into a useful framework, the study is exploratory in nature.

The study will take an interpretive approach, analyzing and contrasting concepts, models, and recommendations from scholarly and professional sources. In order to ensure that the results are understandable and academically reliable, the study will continue to be organized and methodical. A systematic literature evaluation with thematic analysis will serve as the foundation for the whole approach. This approach is appropriate since it enables the researcher to compile data from several reliable sources, spot recurring themes, contrast viewpoints, and create a logical framework based on earlier study.

3.1 Research Design

Instead of using evaluations or numerical measurements to assess a technical system, this study uses a qualitative research design in order to investigate and comprehend forensic readiness in organizational contexts. The study focuses on how forensic readiness is defined in the literature, what influences it, what obstacles organizations encounter when putting it into practice, and how these insights may be combined into a useful framework. A qualitative design is the best option because the emphasis is on interpretation, comparison, and synthesis of existing knowledge.

Philosophical position:

An analytical philosophical stance serves as the study's compass. Because forensic readiness is more than just a technical subject, this role is appropriate. Organizational decision-making, employee duties, internal regulations, legal and compliance issues, and evidence-handling protocols are all included. These are regions that call for interpretation as opposed to straightforward measurement. Therefore, the study aims to comprehend how various sources define good practice, explain forensic readiness, and point out areas where existing organizational preparation is lacking.

Research Approach:

The research methodology used in the study is inductive. This implies that testing a predetermined hypothesis is not the first step in the investigation. Rather, it starts with gathering and analyzing pertinent literature, after which it finds recurring themes, patterns, and concepts. The study will create a useful framework for forensic preparation based on these findings.

Research Strategy:

A structured literature review followed by thematic analysis is the primary research approach. Because it enables the study to gather data from scholarly papers, official reports, security guidelines, and other standards in an organized and targeted manner, a structured literature review is appropriate. This keeps the review both immediately pertinent to the research issue and academically sound.

Time Horizon:

A time horizon with a cross is used in the investigation. This means that rather than tracing advancements over an extended period of time, the research will investigate the topic based on current knowledge and current literature available within the research period. The goal is to give a clear picture of how forensic readiness is currently understood and the obstacles that organizations must overcome to achieve it.

Sustainability of the Research Design:

This design is appropriate because it matches the nature and purpose of the study. The research is not intended to build a software tool, run a live experiment, or collect field data from an organisation. Instead, it aims to understand the concept of forensic readiness, explore the factors that influence it, identify the key barriers to implementation, and use these insights to develop a practical framework. A qualitative, interpretivist, and inductive design is therefore the most suitable way to achieve the research aim. For better understanding a diagram added below:

Figure 1: Research Design of the Proposed Study

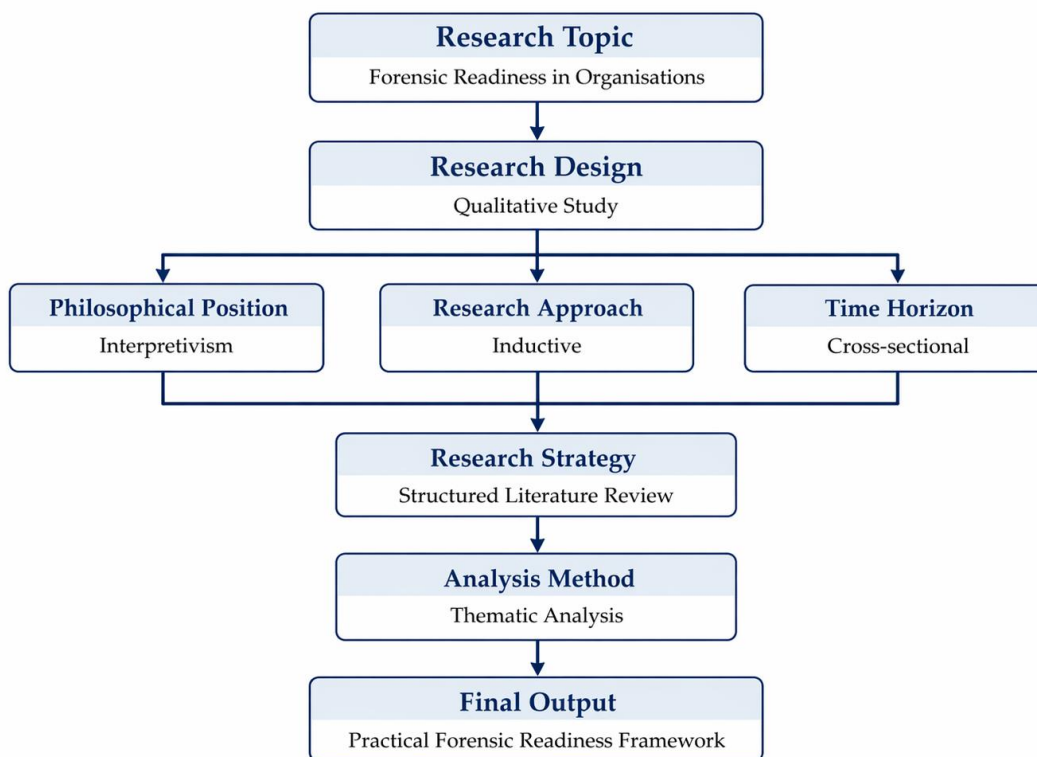


Figure-1: Research Design of the proposed study

3.2 Research Methods and Materials

The study will rely on secondary data rather than primary data. This means the research will use already published material instead of interviews, surveys, or experiments. The main sources will include:

- Peer-reviewed journal articles
- Conference papers
- Government reports
- Professional and technical guidance
- Recognised standards and security frameworks

Forensic preparedness, digital investigations, incident response, evidence preservation, logging, and organizational readiness will be the main topics of the literature search. Academic databases and reliable professional sources, including Google Scholar, IEEE Xplore, SpringerLink, NIST, NCSC, and UK government publications, will be used to choose pertinent materials.

A few older foundational papers will be included where needed, but the analysis will mostly focus on modern era sources, especially those published in the last five years. This strategy will help guarantee that the research acknowledges significant prior work while also reflecting recent advancements.

After collecting the relevant literature, the study will use thematic analysis to identify the main ideas that appear across the sources. Likely themes include:

- logging and monitoring readiness
- evidence preservation and integrity
- incident response coordination
- governance and policy
- legal and compliance considerations
- staff awareness and responsibilities
- continuous improvement and review

These themes will then be compared and synthesised in order to develop a practical forensic readiness framework.

The goal of the suggested framework is to categorize forensic preparedness into distinct areas that are easier for organizations to comprehend and implement. Governance, technical preparedness, procedural safeguards, personnel and training, and review procedures are probably some of these areas. Additionally, the study will assess the suggested framework by contrasting it with the issues and suggestions identified in the literature. This will offer a rational evaluation of whether the framework resolves the persistent flaws found in earlier studies and recommendations, but it won't be a real organizational validation.

Ethical Consideration

As this study depends on publicly available secondary sources rather than human subjects or private organizational data, it is anticipated to pose less ethical risk. Academic integrity will still be crucial, though. IEEE references shall be used to correctly cite all concepts, conclusions, and arguments derived from earlier work. Additionally, the study will seek to correctly and fairly describe prior studies.

Limitations of the Methodology

The lack of direct testing in an actual organizational setting is one disadvantage of this methodology. Consequently, the final framework will not be operationally verified by field testing but instead conceptually grounded. The readiness of the organization might vary based on industry, organization size, regulatory constraints, and technology maturity, which is another drawback. As a result, rather than being universal, the framework will strive to be useful and adaptable.

4. Expected Outcome

This project is expected to produce several useful outcomes.

It will first give a clear explanation of forensic readiness in relation to contemporary organizations and cyber event investigations. Second, it will pinpoint the key elements that affect preparedness, such as organizational, legal, technical, and human concerns. Thirdly, it will draw attention to the typical obstacles that keep organizations from being adequately prepared.

The study's primary product will be an invaluable basis for forensic preparations. It is expected that this approach will support organizations in thinking more clearly about how to get ready for future investigations prior to an occurrence. The framework will attempt to convey preparation in a more organized and practical form rather than merely providing high-level theory.

It is expected that the study will demonstrate the importance of treating forensic preparation as a component of broader cyber resilience. Faster investigations, better evidence preservation, increased accountability, and more efficient event response can all be facilitated by increased preparedness.

The study should always offer helpful advice for organizations, researchers, and practitioners working in cybersecurity, incident response, and digital forensics even though it won't evaluate the framework in a real-world setting.

5. Timeline

The project is expected to be completed over a period of approximately five months.

Month 1:

Finalized the research topic, aim, objectives, and search strategy. Begin collecting academic and professional literature.

Month 2:

Continue literature review and critically read selected sources. Identify major themes and begin organising key findings.

Month 3:

Carry out thematic analysis and compare existing perspectives, models, and recommendations. Start developing the proposed framework.

Month 4:

Write the first full draft of the proposal and framework discussion. Refine arguments and improve structure.

Month 5:

Review, edit, proofread, and finalise the dissertation proposal. Complete formatting, referencing, and appendices.

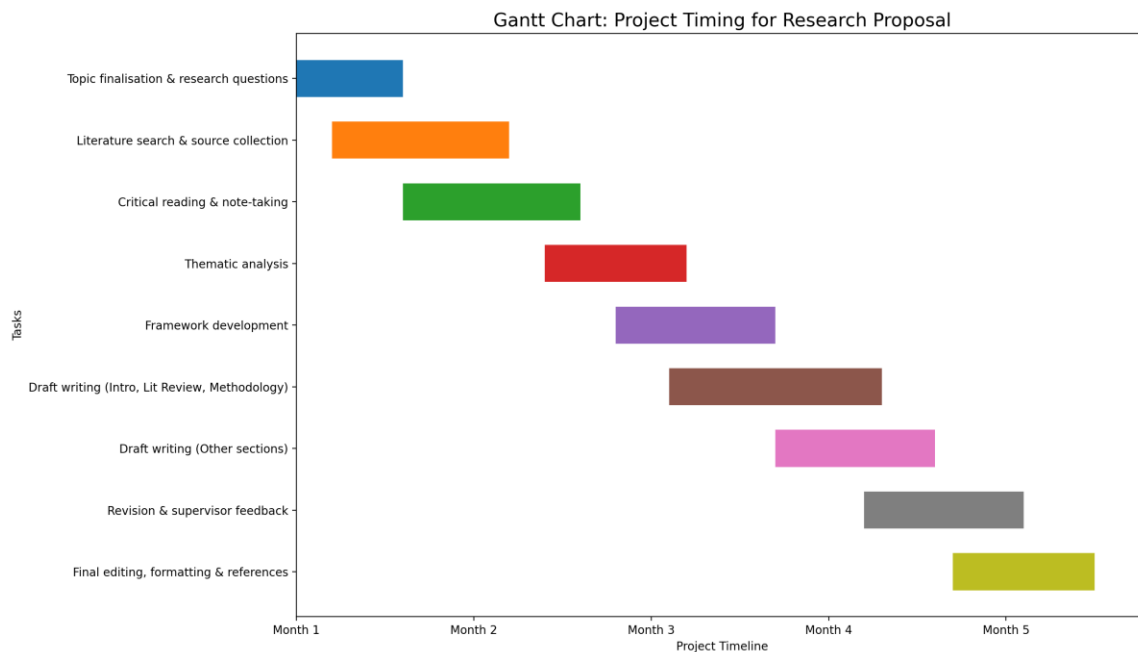


Figure-2: Project Timing

6. References

- [1] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2006.
- [2] A. Nelson, C. Johnson, M. Souppaya, and T. Thomas, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication 800-61 Rev. 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2025.
- [3] K. Kent and M. Souppaya, Guide to Computer Security Log Management, NIST Special Publication 800-92. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2006.
- [4] National Cyber Security Centre, "Guidance on digital forensics and protective monitoring," NCSC, 2025.
- [5] UK Government, *Cyber Security Breaches Survey 2025*. London, U.K., 2025.
- [6] UK Government, *Cyber Security Longitudinal Survey: Wave Five Results*. London, U.K., 2026.
- [7] M. Elyas, M. K. Ahmad, I. Maynard, and A. Lonie, "Digital forensic readiness: Expert perspectives on a theoretical framework," *Computers & Security*, 2015.
- [8] F. Bankole, A. Taiwo, and I. Claims, "An extended digital forensic readiness and maturity model," *Forensic Science International: Digital Investigation*, vol. 40, art. 301348, 2022.
- [9] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," *Computers & Security*, vol. 105, art. 102237, 2021.
- [10] M. Kerrigan, "A capability maturity model for digital investigations," *Digital Investigation*, 2013.
- [11] S. Friedl et al., "IoT Forensics Readiness – influencing factors," *Forensic Science International: Digital Investigation*, 2024.
- [12] O. Kuku, A. Chrysikos, and S. Salekzamankhani, "Preparing IoT-enabled organisations for digital forensics: model for readiness and resilience," *International Journal of Information Security*, 2025.
- [13] V. R. Kebande et al., "Ontology-driven perspective of CFRaaS," 2020.

7. Appendices

Appendix A: Search Keywords

- “forensic readiness in organisations”
- “digital forensic readiness”
- “incident response and digital evidence”
- “logging and monitoring for cyber investigations”
- “forensic readiness framework”

Appendix B: Proposed Thematic Areas

- Governance and policy
- Logging and monitoring
- Evidence preservation
- Incident response integration
- Legal and compliance considerations
- Staff awareness and accountability
- Continuous review and improvement