

MSc Data and Artificial Intelligence

Module: Research Methods and Professional Development

Module Code: ACFA7004

Assessment Component 1: Research Proposal

Submission Deadline: 13th August 2025, 14:00 (2PM)

Lecturer: Dr Suresh Shanmugasundaram

Title of Proposal: A Web-Based Digital Forensic Readiness Assessment System for Small and Medium-Sized Enterprises (SMEs)

Student Name: MD. Asaddoz Jaman

Student Number: 2526322

Table of Contents

List of Figures.....	3
List of Tables.....	4
1. Introduction.....	4
1.1 Context and Background.....	4
1.2 Research Problem.....	4
1.3 Research Aim and Objectives.....	5
1.4 Research Questions.....	5
1.5 Significance of the Research.....	6
2. Literature Review.....	6
2.1 Digital Forensic Readiness.....	6
2.2 SME Cybersecurity Challenges.....	7
2.3 Existing DFR Frameworks.....	7
2.4 ISO 27001 and NIST Relevance.....	7
2.5 Gap Analysis.....	8
2.6 Conceptual Framework.....	8
2.7 Critical Discussion.....	9
2.8 Literature Review Summary.....	9
3. Research Design and Methodology.....	10
3.1 Research Philosophy.....	10
3.2 Research Approach.....	10
3.3 Research Strategy.....	10
3.4 Design Science Research (DSR).....	10
3.5 Research Onion.....	11
3.6 Data Gathering.....	11
3.7 System Development.....	12
3.8 Evaluation.....	12
3.9 Ethical Considerations.....	12
3.10 Limitations.....	13
3.11 System Architecture.....	13

3.12 Presentation Layer.....	14
3.13 Logic Layer.....	14
3.14 Form Processing Engine.....	14
3.15 Automated DFR Scoring Logic.....	15
3.16 Weighted Category Score Calculation.....	15
3.17 Recommendation Engine.....	15
3.18 Database Layer.....	15
3.19 Explanation of Flowcharts & Diagrams.....	15
4. Expected Outcome.....	15
4.1 Expected Software.....	15
4.2 Dashboard:.....	16
4.3 Assessment Reports.....	16
4.4 Benefits for SMEs.....	16
4.5 Academic Contribution.....	16
5. Timeline.....	16
6. References.....	18
7. Appendices.....	19

Table of Figures

Figure 01: Three-Tier Web Architecture of the Proposed Digital Forensic Readiness Assessment System.....	14
--	----

Index of Tables

Table 01: Literature Synthesis Matrix.....	11
Table 02: Project Timeline and Deliverables Schedule.....	19

1. Introduction

1.1 Context and Background

The topic of study for this research lies in the field of Digital Forensics and Cyber Security that particularly examines the aspects of Digital Forensic Readiness (DFR) and Cybersecurity Assessment for SMEs. In light of the fact that the cyber attack mechanisms, such as ransomware attacks, dynamic supply chain attacks, and highly technical data breaches, continue to rise in terms of numbers, magnitude, and impacts, present-day organizations must not only depend on defensive security measures that are designed based on perimeters but also should be able to prepare themselves by employing proactive forensic readiness techniques.

In order to understand this field of research, it is essential to mention that the main feature of SMEs is the fact that they form the backbone of the world economy. However, SMEs are extremely vulnerable to cyber-attacks because of budgetary limitations concerning their information security protection, lack of in-house SOC capabilities and absence of efficient incident response processes. In case a security breach occurs, SMEs cannot cope with the process of digital evidence collection and analysis, which results in huge financial losses and downtime. The current tendencies within this area relate to the transition from the reactive and responsive approach to the preventive and responsive DFR one. Moreover, it is crucial to note that the contemporary approach to the security management consists of utilizing online interactive maturity assessment and telemetry scoring tools and implementing international standards like NIST CSF 2.0 and ISO/IEC 27001 into quantifiable indicators.

1.2 Research Problem

Small and Medium Enterprises (SMEs) are lacking easy-to-use, automated and accessible means of measuring and improving their Digital Forensic Readiness (DFR), which makes them unable to collect, preserve and analyze digital evidence upon occurrence of cyber incidents.

There are three critical problems associated with existing industry approaches and academic literature on this topic:

- Complexity and Costliness: DFR framework for enterprises and commercial security maturity model are costly, highly complex, and require special cybersecurity knowledge to be performed properly;
- Generality of Compliance-Oriented Approaches: Frameworks for standards such as NIST CSF and ISO/IEC 27001 focus on risk management and administrative security compliance in general, and not on developing specific metrics of evidence availability and forensic readiness;

- Lack of Interactive Web Tools: There is a lack of automated interactive web tools that help SMEs measure their technical readiness within key domains and provide automated priority-based recommendations.

If left unsolved, SMEs encountering security incidents will continue to be unable to perform forensic investigation, which will result in additional downtime, increased costs, liability, and permanent loss of court-admissible digital evidence.

1.3 Research Aim and Objectives

This research is designed to develop, implement, and empirically test an interactive, online Digital Forensic Readiness Assessment Tool that will allow SMEs to measure and improve their forensic readiness in a quantitative way. In order to accomplish this objective, there are four specific, measurable, actionable, realistic, and timely objectives that are set out:

- Objective 1: To review the current literature on forensic readiness models and cybersecurity standards to create an appropriate model for assessing SMEs' forensic readiness.
- Objective 2: To develop an interactive 3-tier web application that will include user authentication, domain questionnaires, automated scoring, and interactive dashboard.
- Objective 3: To develop an automated scoring algorithm that will be able to evaluate SMEs' forensic readiness and generate the necessary reports.
- Objective 4: To empirically test the usability and efficacy of the developed software artifact.

1.4 Research Questions

In order to accomplish the stated objective and resolve the core research problem, the following research questions will be answered in the proposed study:

- RQ1: What are the technical criteria, logging parameters, and structural domains that should be included in the lightweight assessment approach in order to reliably measure the digital forensic readiness level of SMEs?
- RQ2: What is the web-based software architecture that can automatically analyze the results of security surveys, perform scoring calculations, and provide visual dashboards in real time?
- RQ3: To what degree does the proposed web-based assessment system increase usability and awareness of digital forensic readiness among SME administrators?

1.5 Significance of the Research

The benefits and impact of this study reach out to a wide variety of important stakeholders in the cybersecurity landscape:

- **Small and Medium-Sized Enterprises (SMEs):** Gives non-technical stakeholders and smaller IT departments access to a no-cost, self-service web-based tool for benchmarking forensic preparedness, detecting gaps in their logging and backup capabilities, and implementing priority-based, cost-efficient countermeasures without resorting to costly external cybersecurity experts.
- **Digital Forensic Analysts and Incident Responders:** Improves the effectiveness of investigations after breaches by establishing an enterprise environment whereby clients have central log management, chain-of-custody protection, and incident response frameworks in place.
- **Academic Researchers & System Engineers:** Provides a validated Design Science Research (DSR) software artifact that showcases how compliance models and theoretical DFR standards (like ISO/IEC 27043) can be converted into web-based software tools.

2. Literature Review

2.1 Digital Forensic Readiness

Digital Forensic Readiness (DFR) is a concept that has gained great significance as a strategic posture in modern information security frameworks [1], [2]. It is described as the capability of an organization to optimize the availability, integrity, and evidentiary value of the digital evidence, while reducing the downtime, cost and complexity of post-breach investigations [1], [3]. In the past, organizations performed digital forensics in a reactive manner whereby they would collect data, conduct memory dumps and keep logs after the occurrence of a breach or compromise of the systems [1], [9].

Nevertheless, current cyber threat topology, which includes ransomware, living-off-the-land attacks and highly dynamic cloud computing environments, make purely reactive measures insufficient [2], [10]. Without proper logging mechanisms, synchronized system clocks and chain of custody procedures, the telemetry required will be usually erased before the actual forensic analysis process is carried out [1], [3]. Therefore, it is argued that for DFR to be successful, it should not only focus on technical elements like continuous auditing and automatic log aggregation and isolation of backups, but also organizational procedures such as incident response plans and forensic training [1], [2], [9]. Implementation of a complete DFR process will ensure that in case there is an incident within the enterprise environment, court admissible evidence will be preserved, rapid analysis of the cause of the incident will be performed, and notification requirements fulfilled [3], [5].

2.2 SME Cybersecurity Challenges

More than 90% of businesses across the globe are Small and Medium-Sized Enterprises (SMEs), acting as key engines for economic development while being extremely prone to targeted cyberattacks [5], [6]. Cybercriminals target SMEs more frequently considering them lucrative targets to attack via which to compromise larger networks of supply chains or launch ransomware attacks [5], [10]. At the same time, despite having similar complexity of threat vectors, SMEs face significant structural challenges [5], [6]. It is about limited IT budget, absence of the SOC, outsourcing IT issues to third parties, and inadequate incident response procedures [5], [6]. In addition, managers in SMEs can have a false sense of safety because of believing that there is no reason to expect attackers who would be interested in targeting smaller companies [5], [6]. Once an attack takes place, the lack of preconfigured loggers and forensic readiness leads to difficulties in estimating the extent of the breach, resulting in serious operational problems, recovery period, client distrust, and compliance issues related to GDPR [3], [5].

2.3 Existing DFR Frameworks

To establish proactive forensic readiness in a formalized manner, numerous DFR frameworks have been suggested by both academics and industry practitioners [1], [2], [9]. Initial theoretical foundations in the form of Rowlingson's ten-step process model include systematic stages of scenario definition, identification of evidence sources, requirements for evidence gathering, and the establishment of evidence handling procedures [9]. Further developments in theoretical foundations include frameworks adapted to different technical environment specifics, including distributed enterprises, cloud technologies, and biometrically secured access environment [1], [2]. Stander and Barske created DFR models applicable for regional enterprise ecosystems focusing on the synchronization of technical log controls with organization's governance [1]. Likewise, Ikuesan and Venter developed advanced behavioral-biometric frameworks for improved user attribution in the post-incident analysis process [2]. Despite their solid theoretical foundation, such models face serious limitations in terms of their applicability to resource-limited environments [1], [5]. The majority of current DFR frameworks presuppose the presence of advanced enterprise architecture with specialized forensic teams [1], [2]. They provide advanced, abstract principles or detailed processes but fail to provide easy-to-use and automated mechanisms for small firms to measure and implement forensic readiness without specific external expertise [5], [7], [8].

2.4 ISO 27001 and NIST Relevance

The main criteria used to evaluate the security posture of an organization through international cybersecurity standards and governance frameworks. Some of them include ISO/IEC 27001 Information Security Management System (ISMS) standard, ISO/IEC 27043 (Incident Investigation Principles and Processes), and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0) [3], [4]. Specifically, ISO/IEC 27043 specifies the process standards for pre-incident readiness, evidence discovery, acquisition, and retention to provide formal evidence rules [3]. The

same way, NIST CSF 2.0 includes six core functions – Govern, Identify, Protect, Detect, Respond, and Recover that focus on log management, monitoring, and configurations of protective technologies necessary for forensic readiness [4]. Nevertheless, the aforementioned standards have a compliance approach to evaluation and are generally comprehensive [3], [4], [7]. They assess general security governance and operation risk management and not specialized quantitative criteria for availability of digital evidence and forensic readiness [3], [7]. In addition, understanding and implementation of such vast standards require significant investments in terms of cost and expertise [5], [7].

2.5 Gap Analysis

A comprehensive analysis of the current literature and the industry approaches shows the existence of a definite gap in the implementation of DFR, SME security dynamics, and software evaluation tools [1], [5], [7]. Even though the existing literature clearly emphasizes the importance of DFR and the vulnerable nature of SMEs, there is no solution that bridges the gap between the security standards and actual execution of the software [3], [5], [8]. Currently available products on the market are enterprise risk management systems that are costly and complicated, or static manual assessment spreadsheets that lack the ability to score software in real time [1], [7]. In addition, general security standards such as NIST CSF and ISO 27001 cannot provide SMEs with specific metrics to check for admissibility of evidence, log retention policies, and evidence integrity [3], [4], [7]. There are no lightweight and free web-based software applications that will be able to score SME's DFR level, calculate the relevant metrics, and create a prioritized list of recommendations for action [5], [7], [8].

2.6 Conceptual Framework

In order to fill the existing literature gap, this research introduces a framework for evaluation which converts the abstract forensic standards into a concrete web based evaluation tool [3], [7], [8]. The framework connects the theoretical DFR criteria, which have been derived from ISO/IEC 27043 and Rowlingson's framework, to the automation of the scoring criteria and makes it specific for SMEs [3], [7], [9]. The framework consists of four key evaluation areas related to the technical and organizational forensic readiness of the SMEs:

- Log Management & Centralization: Assessment of log retention policy, automated ingesting, time synchronization and immutability [1], [9].
- Access Control & Telemetry: Assessment of identity management, MFA logging and endpoint visibility [2], [4].
- Backup Integrity & Preservation: Assessment of isolated backup creation, air gapping and evidence preservation readiness [5], [6].
- Incident Response Governance: Assessment of incident response documentation, notification readiness and staff role definition [3], [5].

The 3-tier web architecture makes the evaluation of these domains possible via the implementation of the weighted scoring engine [7], [8].

2.7 Critical Discussion

The central controversy in the forensic literature is about the execution of security assessments [1], [7]. Traditional theorists emphasize that the forensic readiness of an organization can be properly assessed only via manually performed qualitative security audits carried out by certified external forensic investigators [1], [9]. They state that the automated security assessment techniques are incapable of providing contextual knowledge necessary to analyze the workflows and evidence chain [1], [3]. On the other hand, contemporary cyber security theorists claim that the manual auditing process is too costly, static and inefficient for the current threat landscape [5], [7]. The proponents of automated interactive web application approach to the problem of evaluating forensic readiness maintain that it makes security assessment more affordable, dynamic and immediate [7], [8]. This paper sides with the supporters of automated approach to the problem as it states that although the manual auditing process provides more information about the context of the security practices, the automated light weight tool is the most efficient MVP solution [5], [7], [8].

2.8 Literature Review Summary

To sum up, the literature highlights the importance of DFR as one of the key elements for contemporary cyber resilience; however, the current models are still too complicated and costly for SMEs [1], [3], [5]. The international standards provide a general guidance; however, they do not provide any special DFR scoring automation [3], [4], [7]. This research directly deals with this issue by creating an easy-to-use web application which allows to implement the DFR theoretical models into practical assessment tools [5], [7], [8].

Theme	Major Contributions	Limitations & Unresolved issues
1. DFR Foundations [1], [2]	Establishes pre-incident logging, chain of custody, and evidence preservation principles [1].	Focuses on enterprise SOC environments; overly complex for SMEs [1].
2. International Standards [3], [4]	Standardizes incident investigation and process execution (ISO 27043, NIST CSF) [3].	Abstract and compliance-oriented; lacks automated readiness scoring tools [7].
3. SME Security Dynamics [5], [6]	Highlights budget gaps, lack of skills, and target	Proposes conceptual advice rather than functional, low-

	vulnerabilities [5]	cost software artifacts [5].
4. Scoring Models [7]	Quantifies security posture into actionable maturity tiers [7].	Focuses broadly on general risk, ignoring digital evidence admissibility [7].

Table 01: Literature Synthesis Matrix

3. Research Design and Methodology

3.1 Research Philosophy

The current research takes a Pragmatist epistemological approach alongside the Objectivist/Realist ontological approach [1], [8]. Objectivism holds that the structure of systems, log retention policies, access control data collection techniques, and digital evidence streams constitute facts which are measurable [1], [3]. Pragmatism holds that the truthfulness and validity of any knowledge is determined by its applicability, as well as the functional value of the solution created to address the problem at hand [8]. Pragmatism is clearly the suitable epistemological approach for the current study because the objective of the current research is more than just describing the vulnerabilities of SMEs [5], [8].

3.2 Research Approach

In this study, Mixed-Methods research design is being followed where both the quantitative and qualitative approaches are being combined in a systematic manner [8], [11], [12]. The quantitative approach is being used in the software artifact for computing the scores of DFR, domain percentage, and SUS rating [7], [11]. The qualitative approach includes inductive thematic analysis of user feedbacks through open-ended evaluation surveys about utility of the system, interface of the system, and bottleneck of the system functionality [12].

3.3 Research Strategy

The overall research strategy used in this case is software prototype engineering and user evaluation. The specific approach adopted is Design Science Research (DSR) [8]. This approach involves iterative process that entails requirement definition based on security studies, creation of mathematical algorithm score models, development of 3-layer web platform and user testing [1], [7], [8]. Data collection in this strategy is done via well-defined online surveys and evaluation questionnaires to be filled by IT administrators and SME experts [11], [12]. This strategy ensures linking between theoretical forensic requirements and software engineering [5], [7], [8].

3.4 Design Science Research (DSR)

Design Science Research (DSR) acts as the methodology adopted in this research, as defined by Hevner et al. [8]. The Design Science Research (DSR) approach is a well-

established paradigm in the field of Information Systems that aims at producing new artifacts in order to address the problems identified [8]. In the current research, strict compliance to the six stages of the DSR process model [8] will be maintained as follows:

- Problem identification: Demonstrating the lack of availability of DFR tools for SMEs through literature review [1], [5].
- Objective definition: Developing SMART objectives for the development of an automated web-based assessment tool [1], [7].
- Design and Development: Designing the 3-layer architecture of the system, database structure and scoring scheme [7], [8].
- Demonstration: Implementation of the prototype on the cloud for interactive use by users [8].
- Evaluation: Assessment of usability and usefulness using SUS metric and thematic analysis [11], [12].

3.5 Research Onion

Formalizing the approach with the help of Saunders' Research Onion provides for the methodological compatibility [8]:

- Philosophy: Pragmatism (use-based research) [8].
- Approach: Mixed-method that utilizes both quantifying and qualitative aspects [8,11].
- Strategy: Design Science Research (artifact construction) [8].
- Selection: Multi-method approach based on the use of telemetry and survey data [11,12].
- Time Dimension: Cross-sectional analysis carried out in a specially designed testing period [1].
- Methods & Techniques: Schemes of web-based questionnaires, automatic scoring routines, descriptive statistics and inductive coding [7,11,12]

3.6 Data Gathering

Data gathering follows a well-defined structure of two major channels [11], [12]:

- Primary Telemetry Data: Gathered directly using the interactive assessment module of the web application, where users enter the configuration choices made by organizations in the DFR domains [7].

- Survey Data: Gathered after the demonstration through online questionnaires which include the 10-item System Usability Scale (SUS) and open-ended questions [11], [12].

Sampling is focused on SME IT managers, system administrators, and cybersecurity students [1], [5]. All collected data is transmitted via encrypted HTTPS and stored in an anonymous database [1].

3.7 System Development

The software was developed using contemporary and lightweight web frameworks in order to ensure easy deployment and platform-independent implementation [7], [8]. The technology stack includes [1]:

- Front-end: Responsive HTML5, CSS3, JavaScript, and Bootstrap 5 to provide a friendly user interface [1].
- Back-end engine: Python/Flask (or Node.js) for lightweight REST API endpoints, routing, and scoring calculations [1], [7].
- Database: SQLite (in development) and PostgreSQL (on cloud) implemented using Object-Relational Mapping (ORM) [1].
- Visualization and analytics: Chart.js to draw dynamic radar and bar charts, and PDFKit/ReportLab for report creation [1], [7].

Deployment is done using cloud-based platforms (Render/Vercel) to enable access by users during testing [1].

3.8 Evaluation

The process of evaluation proves the functional usefulness, accuracy, and usability of the created artifact [8], [11]. Quantitative evaluation uses descriptive statistical methods (mean, median, standard deviation) to assess the DFR scores and SUS ratings, setting usability benchmarks compared to industry standards (SUS score > 68) [11]. Qualitative evaluation involves Braun and Clarke's six-step model for thematic analysis coding open-ended participant feedback to find usability issues, functional errors, and recommended features [12]. Through the two evaluations, it is ensured that the prototype effectively bridges theoretical and practical SME standards [5], [7], [8].

3.9 Ethical Considerations

The research meets all university ethical requirements and UK GDPR rules [1]. The participation of participants in this study is fully voluntary and follows the completion of digital informed consent forms embedded in the study [1]. No Personally Identifiable Information (PII), company network credentials, or sensitive IP addresses will be collected [1]. All test data will be fully anonymized and will be stored in database

instances password-protected and accessible only by the primary researcher [1]. Ethics approval was received via Moodle prior to data collection [1].

3.10 Limitations

The most important limitations in research can be considered a dependence on self-reports for assessments that could result in response bias [1], [11]. Moreover, small sample sizes during user testing hinder statistical generalization [1], [8]. The functionality of the system is limited to the evaluation of qualitative/technical questionnaires but not to automatic, intrusive network vulnerability assessments [1], [7]. Schedule risks were mitigated using a strict MVP approach [1].

3.11 System Architecture

The system was developed with the help of 3-Tier Web Architecture, thus maintaining clear separation between concerns, modularity, and maintainability [1], [8]. As we can see on Figure no-01, the layers of architecture comprise Presentation Layer (frontend), Logic Layer (backend application engine), and Data Layer (database & knowledge base) [1]. Information flows from the interface inputs to backend modules and further to the database, providing dynamic visualizations and customized PDF reports for the user [1], [7].

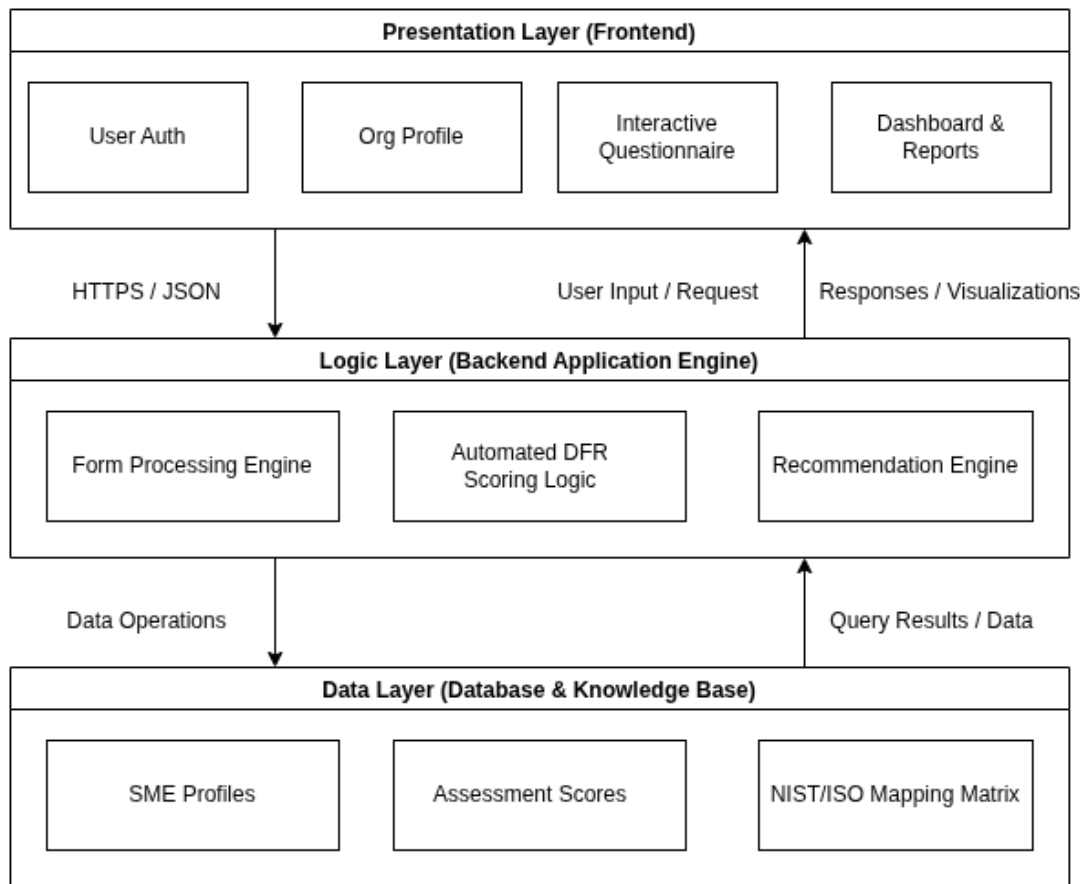


Figure 01: Three-Tier Web Architecture of the Proposed Digital Forensic Readiness Assessment System

3.12 Presentation Layer

Developed using HTML5, Bootstrap 5, and JavaScript technologies, which render authentication forms, survey forms, multi-step dashboards, interactive Chart.js visualization panels, and client-side PDF export [1], [7].

3.13 Logic Layer

Developed using Python/Flask programming language, containing business logic, routing of web services, processing of requests, automatic DFR scoring algorithms, rule mapping, and PDF generation tools [1], [7].

3.14 Form Processing Engine

Processes the incoming JSON objects from questionnaire submissions, validates the presence of all required fields and sanitizes the data to avoid XSS/SQLi attacks, and passes on the validated data to the scoring module [1], [7].

3.15 Automated DFR Scoring Logic

Runs the mathematical scoring engine [7]. The engine matches the categorical answers to the numeric weight vectors following ISO/IEC 27043 and NIST CSF standards [3], [4], [7].

3.16 Weighted Category Score Calculation

The domain score is determined by taking the product of each answer and its associated weight, summing the products, and then comparing them to the maximum possible score obtained after weighting.

Domain Score (%) = (Total Weighted Score / Maximum Possible Weighted Score) * 100

Where:

Total Weighted Score = $\sum (\text{Response} \times \text{Weight})$

Maximum Possible Weighted Score = $\sum (\text{Maximum Score} \times \text{Weight})$

3.17 Recommendation Engine

Compares domain scores with pre-set maturity scores [7]. If the domain score is lower than the acceptable levels (< 70%), the recommendation engine accesses the remediation database to return recommendations [1], [7].

3.18 Database Layer

Uses PostgreSQL/SQLite which is managed through SQLAlchemy ORM to store user accounts, subject matter expert profiles, raw assessment inputs, scores and mapping benchmarks [1], [3], [4].

3.19 Explanation of Flowcharts & Diagrams

Data processing flowcharts and system diagrams showcase the data processing flow [1]. Figure 1 showcases the architectural separation of layers [1].

4. Expected Outcome

4.1 Expected Software

The first output of this study will be a working prototype for an open-source, web-based Digital Forensic Readiness Assessment System prototype. It will have a 3-tier software design and will be composed of secure user registration and login, dynamic multi-domain questionnaire forms, automatic math engine, and database for storing all data. The proposed software system will serve as an interactive solution to link theory on digital forensics readiness to real security technologies [1], [5], [7], [8].

4.2 Dashboard:

This system will have an interactive graphical visualization dashboard, which will use the Chart.js library [1], [7]. After filling the questionnaire, this dashboard will present dynamically created radar charts, bar charts, and maturity score gauge to provide a visual insight into the forensic capabilities and telemetry gaps of the organizations [1], [7].

4.3 Assessment Reports

It is equipped with an automated recommendation engine and PDF exporter feature [1], [7]. It produces prioritized downloadable reports pointing out the most serious security issues, such as a lack of centralization of log retention and backups verification and linking them to corresponding international benchmarks, such as NIST CSF 2.0 and ISO/IEC 27043 [1], [3], [4], [7].

4.4 Benefits for SMEs

It allows SMEs to use the free service for evaluation and improvement of their readiness to forensic examination without spending additional money on external consultancy [1], [5]. Through the detection of the problems with logging and storing data for forensics in advance, SMEs will become more efficient in dealing with post-breach operations, reduce downtime, legal risks, and save digital evidence for the court [1], [3], [5].

4.5 Academic Contribution

This study provides academic contribution in the form of the empirical research and validated Design Science Research (DSR) software artifact to the academic literature [1], [8]. It shows how theoretical standards of forensic readiness (ISO/IEC 27043) and cybersecurity frameworks can be implemented programmatically to produce lightweight algorithms and web tools [1], [3], [7], [8].

5. Timeline

The research process began in June 2026, and during this month, the researcher worked to understand the research requirements, narrow down the research topic and find the literature that was pertinent to this topic. In June, some preliminary literature searching and topic analysis was conducted, which allowed to determine the gaps that existed in the current research regarding digital forensics readiness in SMEs. In July, the literature review was created using systematic search and evaluation of the pertinent academic sources, while the research problem, aim, objectives, and methodology were formulated and refined. Furthermore, the Research Onion was used to determine the research philosophy, approach, methodology, strategy, and methods of data gathering.

During the first ten days of August, all the sections of the proposal were put together, reviewed, and edited to align with the research goals and university requirements.

Project Phase	Target Start Date	Target End Date	Key Deliverable
Phase 1: Course Introduction & Topic Exploration	01 June 2026	07 June 2026	Understanding module requirements, assessment criteria, research expectations, and identifying a suitable cybersecurity/digital forensics research area
Phase 2: Research Topic Refinement	08 June 2026	14 June 2026	Refining the research problem, defining the proposed Digital Forensic Readiness Assessment System for SMEs, and establishing the initial research direction
Phase 3: Preliminary Literature Search	15 June 2026	30 June 2026	Searching Google Scholar, IEEE Xplore, and other academic sources; identifying relevant studies on digital forensics, forensic readiness, SMEs, assessment frameworks, and web-based systems
Phase 4: Literature Review & Research Gap Identification	01 July 2026	15 July 2026	Screening relevant literature, developing the literature matrix, comparing existing approaches, identifying research gaps, and establishing the justification for the proposed research
Phase 5: Research Proposal Development	16 July 2026	31 July 2026	Developing the Introduction, Literature Review, and Research Methodology; defining the research aim, objectives, research questions, and proposed system contribution
Phase 6: Research Methodology &	01 August 2026	05 August 2026	Refining the Research Onion-based methodology, research

Research Design Refinement			philosophy, approach, methodological choice, strategy, time horizon, data collection, and analysis techniques
Phase 7: Proposal Review & Finalisation	06 August 2026	09 August 2026	After going through the entire research proposal, ensuring proper academic format, references, figures and diagrams, consistency, formatting and aligning to the university requirements, and Final Proof Reading and submission of the Research Proposal.

Table 02: Project Timeline and Deliverables Schedule

6. References

- [1] [A. Mouhtaropoulos, M. Grobler and C.-T. Li, "Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives," in 2011 European Intelligence and Security Informatics Conference, Athens, Greece, 2011, pp. 191-196, doi: 10.1109/EISIC.2011.](#)
- [2] [T. Grobler, C. P. Louwrens and S. H. von Solms, "A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations," in 2010 Fifth International Conference on Availability, Reliability and Security, Krakow, Poland, 2010, pp. 677-682,](#)
- [3] [G. I. Pangalos, C. A. Ilioudis and I. Pagkalos, "The Importance of Corporate Forensic Readiness in the Information Security Framework," in 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Laris](#)
- [4] [J. M. Kazadi and H. Jazri, "Using Digital Forensic Readiness Model to Increase the Forensic Readiness of a Computer System," in 2015 International Conference on Emerging Trends in Networks and Computer Communications \(ETNCC\), 2015, doi: 10.1109/ETNCC.2015](#)
- [5] [A. R. Ikuesan and H. S. Venter, "Digital Forensic Readiness Framework Based on Behavioral-Biometrics for User Attribution," in 2017 IEEE Conference on Applications, Information and Network Security \(AINS\), 2017, pp. 54-59, doi: 10.1109/AINS.2017.8270424.](#)

- [6] [M. J. Islam, M. Mahin, A. Khatun, B. C. Debnath and S. Kabir, "Digital Forensic Investigation Framework for Internet of Things \(IoT\): A Comprehensive Approach," in 2019 1st International Conference on Advances in Science, Engineering and Robotics Technolo](#)
- [7] [M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," IEEE Access, vol. 7, pp. 153349-153364, 2019, doi: 10.1109/ACCESS.2019.29](#)
- [8] [S. Zawoad, R. Hasan and A. Skjellum, "OCF: An Open Cloud Forensics Model for Reliable Digital Forensics," in 2015 IEEE 8th International Conference on Cloud Computing, 2015, doi: 10.1109/CLOUD.2015.65.](#)
- [9] [S. Alqahtany, N. Clarke, S. Furnell and C. Reich, "Cloud Forensics: A Review of Challenges, Solutions and Open Problems," in 2015 International Conference on Cloud Computing \(ICCC\), 2015, doi: 10.1109/CLOUDCOMP.2015.7149635.](#)
- [10] [H. Majed, H. N. Noura and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," in 2020 8th International Symposium on Digital Forensics and Security \(ISDFS\), 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116399.](#)
- [11] [S. J. Lee and G. B. Kim, "K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea," IEEE Access, vol. 9, pp. 130094-130110, 2021, doi: 10.1109/ACCESS.2021.3114233.](#)
- [12] [H. A. Nugroho, O. C. Briliyant and S. U. Sunaringtyas, "A Novel Digital Forensic Readiness \(DFR\) Framework for e-Government," in 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity \(ICoCICs\), 2023, pp. 184-189, doi: 10.1109/](#)

7. Appendices