

Cybersecurity and Digital Forensics for Multimodal Transport Accident Investigation: A Governance, Risk and Compliance Framework

Abidina Tijjani Kalarawi

Shobhit Institute of Engineering and Technology (Deemed to be University)

Sadeeq Muhammad

sadeeqmauwal@gmail.com

Shobhit Institute of Engineering and Technology (Deemed to be University)

Mamta Bansal

Shobhit Institute of Engineering and Technology (Deemed to be University)

Research Article

Keywords: transport security, accident investigation, cybersecurity, digital forensics, governance, risk and compliance, evidence integrity

Posted Date: October 15th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11257589/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Cybersecurity and Digital Forensics for Multimodal Transport Accident Investigation: A Governance, Risk and Compliance Framework

Abidina Tijjani Kalarawi; Sadeeq Muhammad; Mamta Bansal

School of Computational Sciences and Engineering, Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut, Uttar Pradesh 250110, India

Corresponding and submitting author: Sadeeq Muhammad (sadeeqmauwal@gmail.com)

Author emails: abidinakalarawi@yahoo.com; sadeeqmauwal@gmail.com; mamta.bansal@shobhituniversity.ac.in

Sadeeq Muhammad ORCID: <https://orcid.org/0009-0006-4355-4734>

Abstract

Multimodal transport accident investigations increasingly depend on digital control systems, networked communications, and sensor-rich operational data across aviation, rail, maritime, and road domains. This dependence expands the evidentiary surface and creates cyber-enabled failure modes that can alter records, undermine evidence integrity, and complicate attribution. This study develops a Governance, Risk and Compliance (GRC) framework that integrates cybersecurity and digital forensics across the accident-investigation lifecycle. A structured conceptual synthesis of 34 academic, professional, and standards-oriented sources was used to identify recurring governance, threat, evidence-handling, and compliance requirements. The framework was then operationalised in a deterministic prototype using 10,000 synthetic access requests. Under the baseline configuration, 61.13% of requests passed the governance gate; final decisions comprised 52.65% permits, 38.87% governance denials, 4.33% multi-factor authentication challenges, 3.08% algorithmic-risk denials, and 1.07% compliance denials. The prototype is illustrative rather than a measure of field performance. Its contribution is a traceable decision architecture that links authority, contextual cyber risk, evidentiary integrity, and lawful handling. The framework supports earlier preservation of volatile evidence, clearer decision rights, and more defensible cyber-aware investigations across transport modes.

Keywords: transport security; accident investigation; cybersecurity; digital forensics; governance, risk and compliance; evidence integrity

1. Introduction

1.1 Context and motivation

Transport systems have undergone sustained digitalisation over the past two decades, driven by software-defined control, pervasive sensing, and networked communications. Digital transformation across sectors has been widely documented, including its organisational and operational implications for safety-critical services (Vial 2019; Alanazi and Alenezi 2024; Lazarenko and Nagorny 2022; Gorishnyaya and Chmut 2021). In transportation, this evolution is reflected in the increasing coupling of software, communications networks, and physical processes typical of cyber-physical systems (Lee 2008; Humayed et al. 2017). Road-safety and transport outlooks also show the scale and policy diversity of the operational environment in which digital evidence is produced (OECD 2020; International Transport Forum 2021). Consequently, modern accident investigations routinely require access to, and interpretation of, operational datasets such as logs, telemetry, and recorded sensor and controller outputs (Atlam et al. 2020; Kent et al. 2006).

At the same time, the cyber exposure of transport systems has increased. Transport networks and their supporting infrastructures are subject to a wide range of threats—including unauthorised access, data manipulation, and availability disruptions—that can directly affect safety and can also contaminate the evidence available to

investigators (Amoozadeh et al. 2015; Cherdantseva et al. 2016; Boyes et al. 2018; Institution of Engineering and Technology 2022). Research on border-control infrastructure and secure cyber digital twins illustrates how these risks extend across interconnected critical-infrastructure services and system models (De Benedictis et al. 2022; Chatzis and Stavrou 2022). These challenges are amplified in multimodal environments where data and responsibilities are distributed across organisations and technologies, with differing governance and compliance constraints (Sachowski 2016; Bajramovic et al. 2017; Racz et al. 2010). Figure 1 summarises the transport modes and shared digital interfaces considered in this study.

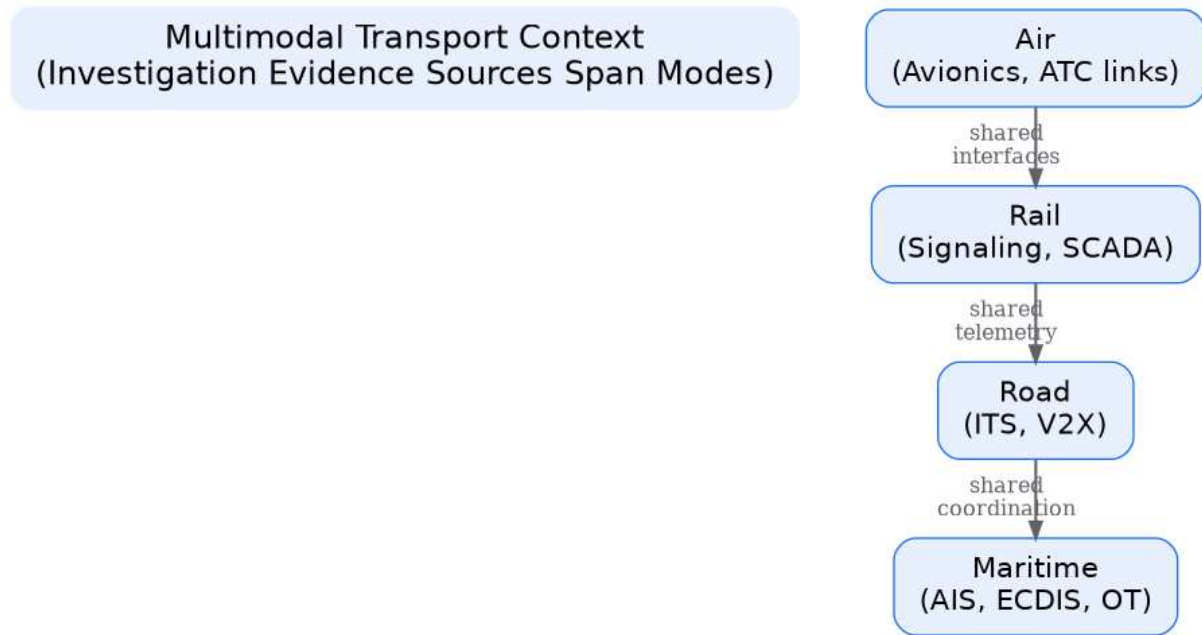


Fig. 1 Transport modes commonly involved in multimodal accident investigations (author-created schematic)

1.2 Problem statement

Conventional accident investigation practice remains strongly grounded in engineering analysis and human factors across aviation, maritime, rail, road, and occupational-safety settings, with digital evidence frequently treated as a technical add-on rather than a first-class investigative artefact (Abeyratne 2012; Andrei 2011; Halstead 2013; Lang 1999; Kim and Yoon 2013; Ayeko 1999; Rudin-Brown and Rosberg 2021; Rajchel 2018; Joseph 2018). Where cybersecurity and digital forensics are not integrated early, investigators may face delayed evidence preservation, unclear authority for access to systems, and reduced confidence in the integrity and provenance of digital records (Atlam et al. 2020; Sachowski 2016; Bajramovic et al. 2017). In multimodal investigations, these problems may be exacerbated by fragmented data ownership, third-party service providers, and cross-jurisdictional constraints that affect disclosure and admissibility (Kent et al. 2006).

1.3 Aim and objectives

The aim of this paper is to propose a GRC framework that integrates cybersecurity and digital forensic practices into multimodal transport accident investigations.

Objectives:

1. Synthesize current literature on transport digitalisation, transport cybersecurity, and digital forensics relevant to accident investigation (Vial 2019; Lamssaggad et al. 2021; Atlam et al. 2020; Cherdantseva et al. 2016).
2. Identify governance, risk-management, and compliance challenges affecting cyber-related evidence handling across modes (Sachowski 2016; Bajramovic et al. 2017; Racz et al. 2010).

3. Propose a mode-agnostic framework with defined roles, decision rights, and evidence-handling controls applicable across investigative lifecycles (Racz et al. 2010).
4. Demonstrate the framework using an illustrative multimodal scenario.
5. Operationalise and stress-test the framework's access-decision logic using a deterministic synthetic prototype.

1.4 Research questions

1. How are cybersecurity and digital forensic practices currently incorporated into multimodal accident investigations?
2. What governance, risk, and compliance factors most strongly influence the integrity and usability of cyber-related evidence?
3. How can a GRC-oriented framework improve consistency and defensibility of digital evidence handling across transport modes?

1.5 Scope and contributions

This is a conceptual, desk-based study focusing on governance structures, investigative workflows, and compliance considerations rather than field deployment of a new security tool. Contributions include:

- A structured GRC model for integrating cybersecurity and digital forensics into accident investigation.
- Practical role definitions and artefacts for evidence governance and chain-of-custody.
- An application walkthrough for multimodal investigations.
- A transparent, reproducible prototype that demonstrates how governance, contextual risk, and evidentiary compliance can be combined in auditable access decisions.

2. Related Work

2.1 Digitalisation and data-centric accident investigations

Digital transformation has shifted many transport functions toward data-centric operations, creating new forms of evidence and new dependencies on software and networks (Vial 2019; Alanazi and Alenezi 2024; Lazarenko and Nagorny 2022; Gorishnyaya and Chmut 2021). Sector-wide road-safety and transport outlooks reinforce the need to interpret these data within diverse modal and regulatory contexts (OECD 2020; International Transport Forum 2021). Within cyber-physical systems, safety outcomes depend not only on physical components but also on software behaviour and networked interactions (Lee 2008; Humayed et al. 2017). As a result, investigations increasingly require reliable access to operational data and assurance that records reflect the underlying events (Atlam et al. 2020).

2.2 Cybersecurity in safety-critical transport systems

Transport cybersecurity research highlights that adversarial actions can affect system behaviour and can also distort monitoring, logging, and situational awareness mechanisms (Amoozadeh et al. 2015; Boyes et al. 2018; Institution of Engineering and Technology 2022). Work on border-control infrastructures and secure cyber digital twins further shows that cyber risk can extend across connected operational platforms, virtual system representations, and organisational boundaries (De Benedictis et al. 2022; Chatzis and Stavrou 2022). These issues are not limited to a single mode: similar threat classes can be expressed differently across aviation, maritime, rail, and road systems depending on architecture and operational constraints (Humayed et al. 2017; Boyes et al. 2018; Institution of Engineering and Technology 2022). A key implication for investigations is that cyber interference may mimic technical failure or human error unless explicitly considered (Amoozadeh et al. 2015; Boyes et al. 2018; Institution of Engineering and Technology 2022).

2.3 Digital forensics and forensic readiness

Digital forensics in transport investigations spans acquisition, preservation, analysis, and reporting of digital artefacts that may be distributed across organisations and systems (Atlam et al. 2020). Research in adjacent critical-infrastructure domains identifies comparable challenges involving heterogeneous devices, distributed evidence sources, and emerging forensic threats (Nelufule et al. 2024). Forensic readiness emphasises preparedness before incidents occur, including policies and procedures that enable lawful and timely evidence preservation (Sachowski 2016; Bajramovic et al. 2017). This is particularly relevant where evidence is volatile or time-bounded (e.g., ring-buffer logs, telemetry retention policies) and where third-party coordination is necessary (Kent et al. 2006).

2.4 Governance and coordination challenges

GRC-oriented perspectives emphasise that governance mechanisms (roles, authority, accountability), risk management (prioritisation and treatment of threats), and compliance (legal and procedural constraints) collectively shape investigation outcomes (Racz et al. 2010). Where cyber and forensic expertise is siloed, investigations risk inconsistent decision-making and reduced defensibility of digital evidence (Bajramovic et al. 2017).

2.5 Synthesis and research gap

Existing work provides strong coverage of digital transformation (Vial 2019), transport cybersecurity (Cherdantseva et al. 2016; Boyes et al. 2018; Institution of Engineering and Technology 2022), and forensic readiness (Sachowski 2016; Bajramovic et al. 2017), but these bodies of knowledge are rarely operationalised together as a coherent accident-investigation framework across modes. This paper addresses this integration gap by proposing a GRC-centric framework grounded in the investigative lifecycle and aligned to evidence handling and compliance constraints. Figure 2 presents the maturity progression used to position that integration, while Table 1 links the principal literature themes to the framework design.

Level	Maturity	What it looks like in investigations
1	Ad hoc	Evidence access decided case by case; inconsistent logging; late forensic involvement
2	Repeatable	Basic role-based access exists; some chain-of-custody forms; partial retention standards
3	Defined	Documented roles and authority; standardised acquisition; consistent audit trails
4	Managed	Risk scoring guides prioritisation; controlled access workflow; regular reviews
5	Optimised	Continuous monitoring; tested exercises; measurable improvements and compliance evidence

Fig. 2 Illustrative policy maturity map for integrating cybersecurity and digital forensics (author-created schematic)

Table 1 Synthesis of related work and implications for a GRC-oriented investigation framework

Theme	Representative sources	Implication for this paper
Digital transformation and data dependence	(Vial 2019; Alanazi and Alenezi 2024; Lazarenko and Nagorny 2022; Gorishnyaya and Chmut 2021)	Digital evidence becomes central to safety and investigation outcomes.
Cyber-physical threat surface	(Lee 2008; Humayed et al. 2017; Cherdantseva et al. 2016; Boyes et al. 2018)	Cyber interference can affect both causation and evidentiary integrity.

Theme	Representative sources	Implication for this paper
Forensic readiness and evidence governance	(Atlam et al. 2020; Sachowski 2016; Bajramovic et al. 2017; Kent et al. 2006)	Readiness requires governance, workflows, and defensible chain-of-custody.
GRC integration	(Racz et al. 2010)	Governance, risk, and compliance must be treated as coupled design concerns.

3. Methodology

3.1 Research design and evidence base

This study uses a qualitative, conceptual framework-development design (Creswell and Creswell 2018; Yin 2018). The evidence base comprises the 34 academic publications, books, standards-oriented documents, and professional reports cited in this article. Sources were purposively retained when they addressed at least one of six domains: transport digitalisation, accident investigation, transport or cyber-physical-system security, digital forensics and forensic readiness, incident-response evidence handling, or integrated GRC. Sources concerned only with general information technology, without a transport, safety, forensic, or governance connection, were excluded from the final synthesis.

The review is a structured conceptual synthesis rather than a systematic review. The original database searches, screening log, and exclusion counts were not preserved; consequently, the study does not claim exhaustive coverage or systematic-review reproducibility. This boundary is stated explicitly to avoid overstating the evidentiary basis of the framework.

3.2 Thematic synthesis and framework construction

The synthesis proceeded in four stages:

1. **Evidence extraction:** each source was examined for statements concerning authority, access, cyber threat, evidence volatility, integrity, chain-of-custody, privacy, disclosure, or admissibility.
2. **Thematic grouping:** extracted concepts were organised under the deductive GRC domains of governance, risk, and compliance, while allowing recurring operational issues such as third-party access, logging maturity, and cross-jurisdictional coordination to emerge within those domains.
3. **Lifecycle mapping:** the themes were mapped to notification and triage, preservation, analysis and reconstruction, and reporting.
4. **Framework specification:** roles, decision rights, control points, and auditable outputs were defined for each lifecycle stage and tested for applicability across aviation, maritime, rail, and road contexts.

No statistical meta-analysis was performed. The purpose of the synthesis was to construct a transparent design argument linking the literature to the proposed framework, not to estimate effect sizes.

3.3 Illustrative scenario and prototype evaluation

The framework was first applied to a hypothetical multimodal incident to test whether its roles and controls could be followed coherently without attributing conduct to a real organisation. This use of a concrete scenario follows established scenario-based design principles for examining how a proposed system supports activities and decisions (Carroll 2000; Yin 2018). The framework was then operationalised as a zero-trust access-decision prototype using a

committed dataset of 10,000 synthetic requests. The reported baseline is computed from that archived dataset, making the evaluation deterministic. A companion generator uses a fixed seed of 42 to create additional synthetic datasets for workflow testing; regenerated datasets are not asserted to be byte-equivalent to the archived baseline and can produce different decision counts. Each request records role, target resource, action, device health, failed logins, location anomaly, VPN status, and access outside business hours.

The prototype applies three decision layers. The governance layer uses a documented role-to-resource allowlist. The contextual risk score is:

$$R = \text{clip}[0,100] (0.4(100-H) + 40L + 15O + 10(1-V) + 5F + 30A),$$

where H is device-health score, L is a location-anomaly indicator, O is an outside-business-hours indicator, V indicates an active VPN, F is the number of failed logins in the previous 24 hours, and A indicates an Isolation Forest outlier. Isolation Forest uses a contamination value of 0.10 and random state 42. Scores below 40 are low risk, scores from 40 to below 75 are medium risk, and scores of 75 or greater are high risk. The compliance layer blocks modification of digital evidence and safety-critical systems.

Final decisions follow an explicit precedence order: governance failure produces a governance denial; a subsequent evidentiary-compliance failure produces a compliance denial; otherwise, high risk produces an algorithmic-risk denial, medium risk produces a multi-factor authentication challenge, and low risk produces a permit. A five-scenario sensitivity sweep varies Isolation Forest contamination and the medium/high thresholds. The resulting counts, stratified summaries, and figures are generated by the accompanying code.

3.4 Reproducibility, ethics, and responsible use

The synthetic dataset, generator, evaluation script, dependency specification, derived CSV files, and performance figure are included in Online Resource 1. Online Resource 1 is a ZIP archive containing the code, synthetic data, generated summaries, notebook, and reproducibility instructions for the prototype evaluation. No human participants, personal data, real operational records, or live transport systems were used. The prototype is therefore an analytical demonstration and must not be treated as a validated production access-control system. Any operational adoption would require local legal review, calibration with representative data, human oversight, security testing, and monitoring for disparate or unsafe outcomes.

Generative artificial intelligence tools were used to support language revision, manuscript organisation, formatting, and consistency checking. No artificial intelligence system is listed as an author. The authors retain responsibility for verifying the content, references, analytical logic, numerical outputs, and final submission.

4. Proposed GRC-Oriented Framework

4.1 Framework overview

The proposed framework is structured around three interacting layers—**Governance**, **Risk**, and **Compliance**—that operate across the full investigation lifecycle (Racz et al. 2010). The framework assumes that cybersecurity and digital forensics are integral investigative disciplines rather than late-stage technical support (Sachowski 2016; Bajramovic et al. 2017). Figure 3 depicts the three-layer framework and its investigative outputs, while Figure 4 maps the layers to the end-to-end investigation lifecycle.



Fig. 3 Proposed GRC-oriented framework

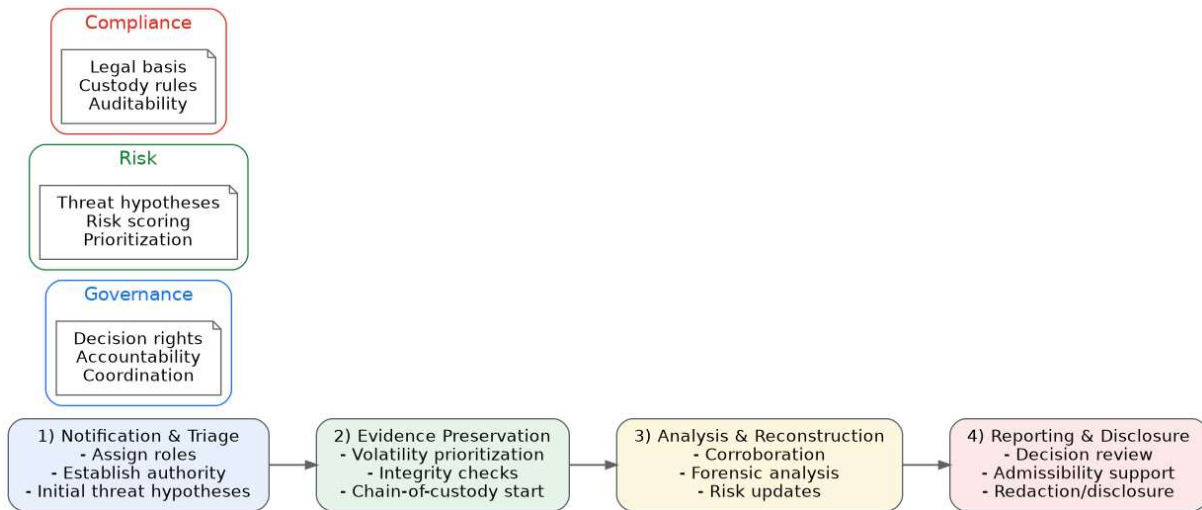


Fig. 4 End-to-end GRC-enabled investigation lifecycle (author-created schematic)

4.2 Governance layer: roles and decision rights

The governance layer defines roles, authority, and coordination mechanisms for digital evidence handling. It clarifies who can authorise system access, who controls evidence preservation actions, and how technical findings are integrated into investigative conclusions (Bajramovic et al. 2017; Racz et al. 2010). Figure 5 shows the coordination relationships among the principal investigation roles, and Table 2 assigns their indicative responsibilities.

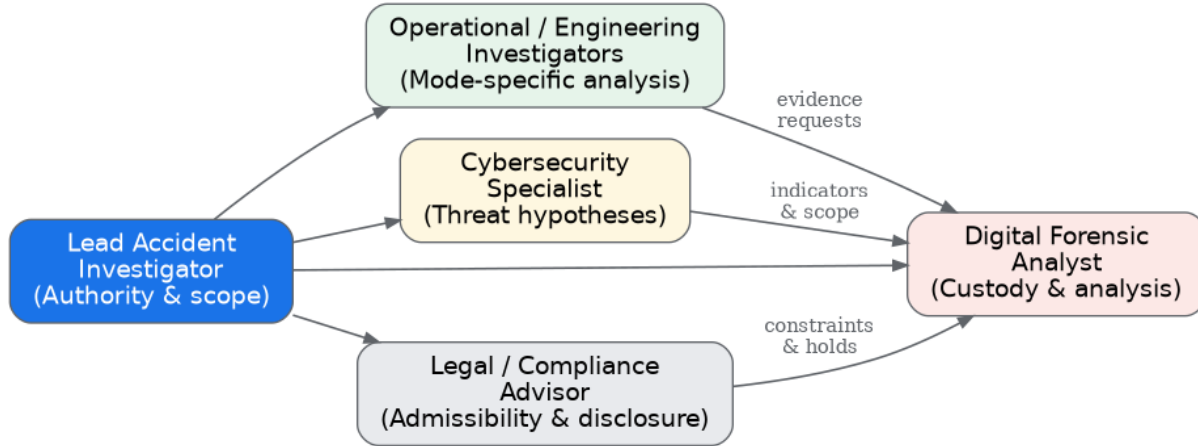


Fig. 5 Governance layer roles and coordination (author-created schematic)

Table 2 Indicative roles and responsibilities under the governance layer

Role	Key responsibilities in a cyber-enabled investigation
Lead accident investigator	Sets investigation scope; approves evidence strategy; integrates findings into causal analysis and recommendations.
Operational/engineering investigators	Analyse mode-specific operational and technical factors; coordinate data requests and technical interpretation.
Cybersecurity specialist	Assesses threat plausibility; identifies attack paths; supports secure access and containment decisions.
Digital forensic analyst	Preserves and analyses digital artefacts; maintains chain-of-custody; produces defensible forensic outputs (Sachowski 2016; Kent et al. 2006).
Legal/compliance advisor	Advises on admissibility, disclosure, privacy, and cross-border constraints affecting evidence handling (Kent et al. 2006).

4.3 Risk layer: cyber-related risk identification and treatment

The risk layer treats cyber threats as safety-relevant risks that may influence both accident causation and evidence integrity (Cherdantseva et al. 2016; Institution of Engineering and Technology 2022). Core activities include threat hypothesis identification (e.g., data tampering, unauthorised access), assessment of evidentiary impact, prioritisation of volatile evidence preservation, and integrity checks and access controls (Sachowski 2016; Kent et al. 2006).

4.4 Compliance layer: admissibility, privacy, and procedural integrity

The compliance layer ensures digital forensic activity aligns with legal and procedural constraints, including admissibility and auditability (Kent et al. 2006). Compliance requirements influence collection, storage, disclosure, and reporting, and should be considered from the outset rather than as a final review step (Sachowski 2016).

4.5 Investigation workflow

Across the lifecycle, the framework emphasises early involvement of cyber and forensic expertise, coordinated evidence preservation, and iterative integration of technical and investigative findings. Table 3 specifies the governance, risk, and compliance outputs at each stage. Figure 6 then presents the corresponding operational workflow.

Table 3 Lifecycle view of GRC outputs in a cyber-enabled accident investigation

Stage	Governance outputs	Risk outputs	Compliance outputs
Notification and triage	Role assignment; access authority	Initial threat hypotheses	Legal basis for access; evidence holds
Evidence preservation	Evidence plan; chain-of-custody start	Volatility prioritisation; integrity checks	Retention, privacy, and disclosure constraints
Analysis and reconstruction	Findings integration routines	Threat evaluation; corroboration plan	Audit trail; admissibility documentation
Reporting	Decision review; sign-off	Residual risk statement	Disclosure and redaction rules

**Fig. 6** Workflow of the proposed GRC-oriented investigation framework (author-created schematic)

5. Application to an Illustrative Multimodal Scenario

5.1 Scenario description

To demonstrate practical use, we consider a hypothetical accident at an intermodal hub (e.g., a port or airport logistics interface) where multiple transport modes share digital coordination services (access control, scheduling, and operational monitoring). The scenario is designed to avoid attributing responsibility to any specific organisation while illustrating realistic digital evidence and coordination challenges (Yin 2018).

The scenario includes: (i) safety-critical operations supported by networked systems (Humayed et al. 2017), (ii) multiple digital evidence sources (logs, CCTV, telemetry) (Atlam et al. 2020; Ramadhan et al. 2019), and (iii) plausible cyber influence affecting record integrity (Amoozadeh et al. 2015; Boyes et al. 2018; Institution of Engineering and Technology 2022).

5.2 Governance-layer execution

On notification, the governance layer activates pre-defined roles and decision rights. Cybersecurity and forensic specialists participate in the initial evidence strategy to ensure timely preservation of volatile data and to avoid actions that could overwrite artefacts (Sachowski 2016; Kent et al. 2006). Evidence access permissions and coordination points with third parties are established early, with legal/compliance oversight to maintain defensibility (Kent et al. 2006).

5.3 Risk-layer execution

Investigators document cyber threat hypotheses alongside conventional safety hypotheses. For each hypothesis, they identify impacted systems and evidentiary artefacts needed to corroborate or refute it (e.g., comparing operational logs with independent sources such as CCTV or external telemetry). Preservation is prioritised by volatility and criticality (Sachowski 2016).

5.4 Compliance-layer execution

Compliance constraints inform evidence handling throughout. The investigation maintains an auditable chain-of-custody; documents acquisition methods; and applies disclosure, privacy, and redaction controls where required (Kent et al. 2006).

5.5 Integrated view

Table 4 consolidates the illustrative governance, risk, and compliance actions across the four investigation stages.

Table 4 Illustrative application of the GRC framework across investigation stages

Stage	Governance	Risk	Compliance
Notification	Assign team; define authority	Identify cyber plausibility	Confirm legal basis; issue evidence holds
Collection	Coordinate access; start custody	Preserve volatile data first	Document methods; privacy controls
Analysis	Integrate technical findings	Corroborate; assess interference	Maintain audit trail; admissibility support
Reporting	Review and approve conclusions	Residual risk statement	Disclosure/redaction rules

5.6 Prototype simulation and evaluation

To provide an operational illustration of the framework’s decision logic, we simulated a zero-trust access-control and logging pipeline using a synthetic dataset of 10,000 access requests. Each request records the investigator role, target resource, requested action, and contextual factors (e.g., device health, recent failed logins, location anomaly, VPN status, and outside-business-hours access). This simulation is not a claim of field validation; it demonstrates how governance, risk, and compliance constraints can be applied consistently to digital evidence access.

Governance gate (RBAC). A role-to-resource allowlist is applied to determine whether the request is authorised at the governance layer. In the simulation, 6,113 requests (61.13%) pass the governance checks; the remainder are denied due to governance restrictions.

Risk gate (contextual scoring and anomaly penalty). Contextual risk is computed from device health and environmental signals, with an Isolation Forest model used to penalise behavioural outliers (10% contamination). Risk is categorised using thresholds at 40 (medium) and 75 (high). The mean risk score is 18.46/100.

Compliance gate (chain-of-custody override). A strict evidentiary constraint blocks modification requests to immutable resources (e.g., digital evidence and safety-critical systems). In the synthetic dataset, 176 requests violate this constraint.

Traceability and auditability. Each request yields an auditable record of governance outcome, risk score and risk level, compliance status, and the final decision (permit/challenge/deny). This supports post-incident review by enabling investigators to reconstruct *why* access was granted or denied and to demonstrate procedural consistency.

Table 5 reports the final access decisions after sequential governance, compliance, and risk checks. Figure 7 shows the ordered access-decision pipeline, and Figure 8 presents the resulting distributions and sensitivity views.

Table 5 Decision distribution for the simulated zero-trust GRC access pipeline (n = 10,000)

Final decision	Count	Share (%)
Permit	5265	52.65
Deny (Governance)	3887	38.87
Challenge (MFA Required)	433	4.33
Deny (Algorithmic Risk)	308	3.08
Deny (Compliance-Forensics)	107	1.07

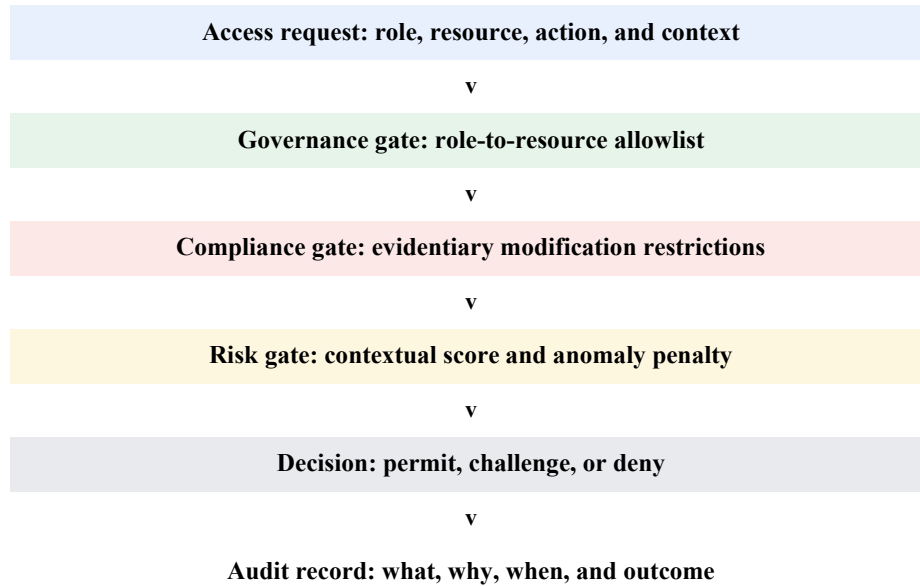


Fig. 7 Author-created schematic of a zero-trust GRC access pipeline

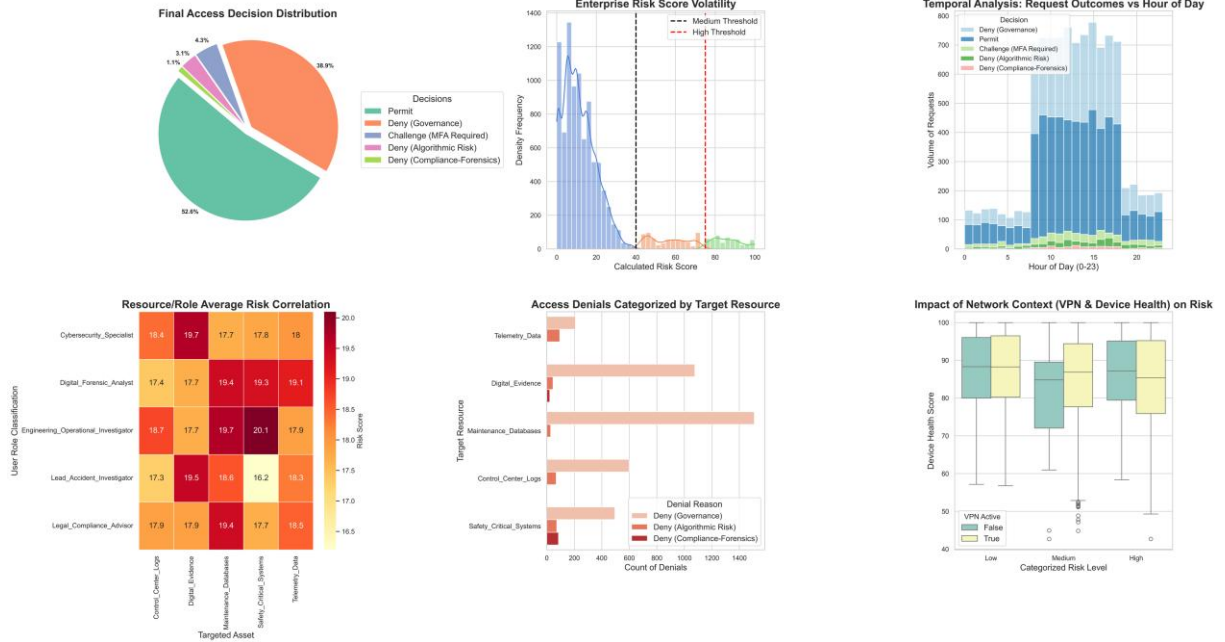


Fig. 8 Performance analysis of the simulated zero-trust GRC access pipeline

6. Discussion

The framework addresses an operational gap: the need to treat cybersecurity, digital forensics, and compliance as integral to investigation governance rather than post-hoc technical activities (Sachowski 2016; Bajramovic et al. 2017; Racz et al. 2010). Practically, it supports earlier and more consistent preservation of digital evidence, improved clarity in decision rights for system access, and better defensibility of findings when cyber interference is plausible (Amoozadeh et al. 2015; Boyes et al. 2018; Kent et al. 2006; Institution of Engineering and Technology 2022).

6.1 Transportation security implications

The framework extends beyond conventional accident reconstruction by treating malicious and adversarial causes as testable investigation hypotheses alongside technical failure and human error. Its outputs support five transportation-security goals. **Deterrence** is strengthened through explicit accountability and complete access logging. **Detection** is supported by early cyber triage, corroboration across independent evidence sources, and contextual anomaly indicators. **Attribution** is improved by preserving provenance, documenting decision paths, and distinguishing an altered record from an originating operational event. **Resilience** is supported by prioritising volatile evidence and maintaining investigative continuity across organisational boundaries. **Lawful evidence handling** is reinforced through access authority, chain-of-custody, privacy controls, disclosure rules, and documented review.

These mechanisms are particularly relevant at multimodal hubs, where shared digital services can create correlated vulnerabilities across operators and transport modes. The framework does not presume that a cyberattack caused an accident; instead, it makes cyber influence examinable without displacing established engineering and human-factors analysis.

6.2 Limitations

This paper proposes a conceptual framework and demonstrates it through a hypothetical scenario and synthetic access-control prototype rather than empirical validation on real incidents. The source corpus was purposively assembled, and the absence of a preserved systematic search and screening log limits claims about literature

coverage. The prototype's distributions, governance matrix, risk weights, and decision thresholds are design choices rather than empirically estimated parameters. Implementation will require tailoring to mode-specific mandates and regulatory environments. Some organisations may also lack the logging, retention, access-control, and cross-organisational agreements needed to realise the framework's benefits (Institution of Engineering and Technology 2022; International Transport Forum 2021).

6.3 Threats to validity

The prototype simulation is intended to illustrate governance/risk/compliance decision logic rather than to estimate operational performance. Key threats to validity include:

- Synthetic data realism:** the dataset is synthetic and may not capture the full distribution of behaviours, adversary tactics, or organisational constraints in real investigations.
- Policy subjectivity:** governance outcomes depend on the chosen role-to-resource allowlist (RBAC-style mapping); different organisational mandates can change the deny/permit profile.
- Model and threshold sensitivity:** risk outcomes depend on the anomaly model and thresholds; this is partially mitigated via deterministic regeneration (fixed seed) and the sensitivity sweep reported in Appendix B.
- Construct validity:** permit and denial distributions demonstrate internal decision consistency, not investigative effectiveness, causal accuracy, admissibility, or safety improvement.
- External validity:** the results cannot be generalised to a transport mode, jurisdiction, organisation, or threat environment without empirical calibration.
- Automation risk:** algorithmic risk scoring can amplify unsuitable assumptions; operational use therefore requires human review, appeal mechanisms, monitoring, and periodic validation.

6.4 Future work

Future research should evaluate the framework through comparative case studies across modes, interviews with investigators, and controlled tabletop exercises that compare baseline and framework-assisted evidence handling. Evaluation should measure preservation timeliness, chain-of-custody completeness, decision consistency, false denial and challenge rates, analyst workload, and the defensibility of final findings. Further work may also test how data analytics and artificial intelligence can support evidence triage while maintaining procedural integrity, human accountability, and mode-specific legal requirements.

7. Conclusion

Digitalisation and cyber exposure have reshaped the evidentiary and causality landscape of transport accidents. Multimodal investigations in particular require governance mechanisms that coordinate access to distributed digital evidence while preserving integrity and meeting compliance constraints. This paper presented a GRC-oriented framework that integrates cybersecurity and digital forensics across the investigation lifecycle, defines roles and outputs, and demonstrates application through an illustrative scenario. The resulting approach supports more consistent, defensible, and cyber-aware investigations across transport modes.

Appendix A: Reproducibility and evaluation artefacts

The simulation and evaluation artefacts used to generate the quantitative results and the detailed performance figure are provided in Online Resource 1:

- `synthetic_data.py`: seeded generator for additional synthetic datasets; it does not recreate the archived baseline byte-for-byte
- `run_evaluation.py`: executes governance/risk/compliance gates, prints decision counts, generates the performance figure, and writes a sensitivity summary

•fig_5_2_zero_trust_grc_performance.png: generated performance figure used in Figure 8

Dataset schema

Table 6 defines the fields in the synthetic access-log dataset.

Table 6 Schema of the synthetic access-log dataset used for the prototype evaluation

Field	Type	Description
Request_ID	string	Unique request identifier (e.g., REQ-000001).
Timestamp	string	Request timestamp (YYYY-MM-DD HH:MM:SS).
Hour_of_Day	integer	Hour extracted from timestamp (0–23).
User_Role	categorical	Investigator role (e.g., lead investigator, forensic analyst).
Target_Resource	categorical	Targeted asset class (e.g., telemetry, evidence, safety-critical systems).
Action	categorical	Requested action (View/Analyze/Extract/Modify).
Device_Health_Score	float	Endpoint health score (0–100; higher is healthier).
Failed_Logins_24h	integer	Count of failed logins for the user/device in the last 24h.
Location_Anomaly	binary	1 if out-of-pattern geographic access is detected.
VPN_Active	boolean	True if request is performed via VPN.
Outside_Business_Hours	binary	1 if request occurs outside typical operating hours.

Governance outcomes by role

Table 7 reports governance-gate outcomes by role in the prototype evaluation (n = 10,000).

Table 7 Governance-gate outcomes by role in the prototype evaluation (n = 10,000)

Role	Requests	Gov. pass	Pass rate (%)
Engineering/Operational investigator	2965	1794	60.51

Role	Requests	Gov. pass	Pass rate (%)
Cybersecurity specialist	2537	1531	60.35
Digital forensic analyst	2009	1188	59.13
Lead accident investigator	1464	1175	80.26
Legal/compliance advisor	1025	425	41.46

Denials by resource (with reasons)

Table 8 reports denials by target resource and primary denial reason in the prototype evaluation (n = 10,000). Values are counts derived from the stratified output `denials_by_resource.csv`.

Table 8 Denials by target resource and primary denial reason (n = 10,000)

Target resource	Deny Gov	Deny Risk	Deny Comp	Total denies
Maintenance databases	1509	28	0	1537
Digital evidence	1077	45	22	1144
Control-center logs	598	68	0	666
Safety-critical systems	495	73	85	653
Telemetry data	208	94	0	302

Appendix B: Sensitivity analysis

Table 9 reports decision-distribution sensitivity to selected risk-model and threshold parameters (n = 10,000).

Table 9 Sensitivity of decision distribution (%) to selected risk-model and threshold parameters (n = 10,000)

Scenario	Permit (%)	Deny Gov (%)	Challenge (%)	Deny Risk (%)	Deny Comp (%)
Baseline (contam.=0.10; 40/75)	52.65	38.87	4.33	3.08	1.07
Lower contamination (0.05; 40/75)	54.00	38.87	4.14	1.92	1.07
Higher contamination (0.15; 40/75)	51.16	38.87	5.08	3.82	1.07
Lower thresholds (0.10; 35/70)	52.45	38.87	3.79	3.82	1.07
Higher thresholds (0.10; 45/80)	53.29	38.87	4.39	2.38	1.07

Abbreviations

- GRC:** Governance, Risk, and Compliance
- CPS:** Cyber-Physical Systems
- ITS:** Intelligent Transportation Systems
- ICT:** Information and Communication Technology

Statements and Declarations

Funding: No funds, grants, or other support were received for conducting this study or preparing the manuscript.

Competing interests: The authors have no relevant financial or non-financial interests to disclose.

Data availability: All data supporting the reported prototype results are synthetic and are included in Online Resource 1. No real-world operational or personal data were collected.

Code availability: The deterministic data generator, evaluation code, dependency specification, derived summaries, and figure-generation workflow are included in Online Resource 1.

Ethics approval: Not applicable. The study did not involve human participants, animals, personal data, or real operational transport records.

Consent to participate: Not applicable.

Consent for publication: Not applicable.

Author contributions: Abidina Tijjani Kalarawi: Conceptualization, Investigation, Methodology, and Writing - original draft. Sadeeq Muhammad: Conceptualization, Methodology, Software, Data curation, Formal analysis, Visualization, Writing - original draft, Writing - review and editing, and Project administration. Mamta Bansal: Supervision, Validation, Methodology, and Writing - review and editing.

References

- Abeyratne R (2012) Aircraft accident and incident investigation. In: Air Navigation Law, pp 105-111. https://doi.org/10.1007/978-3-642-25835-0_5
- Alanazi F, Alenezi M (2024) Driving the future: Leveraging digital transformation for sustainable transportation. *Journal of Infrastructure Policy and Development* 8(3):3085. <https://doi.org/10.24294/jipd.v8i3.3085>
- Amoozadeh M et al (2015) Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine* 53(6):126-132. <https://doi.org/10.1109/MCOM.2015.7120028>
- Andrei F (2011) Safety Management Manual, ICAO Doc 9859 AN/474. *INCAS Bulletin* 3(1):129-130. <https://doi.org/10.13111/2066-8201.2011.3.1.17>
- Atlam HF et al (2020) Internet of Things forensics: A review. *Internet of Things* 11:100220. <https://doi.org/10.1016/j.iot.2020.100220>
- Ayeko M (1999) Integrated Safety Investigation Methodology: A systematic approach to learning from accidents. In: *Learning From Marine Incidents*, pp 97-106. <https://doi.org/10.3940/rina.mi.1999.08>
- Bajramovic E, Waed K, Gao Y, Parekh M (2017) Shared responsibility for forensic readiness-related security controls: Prerequisite for critical infrastructure maintenance and supplier relationships. In: *IEEE EUROCON 2017*, pp 364-369. <https://doi.org/10.1109/EUROCON.2017.8011136>
- Boyes H, Hallaq B, Cunningham J, Watson T (2018) The industrial Internet of Things: An analysis framework. *Computers in Industry* 101:1-12. <https://doi.org/10.1016/j.compind.2018.04.015>
- Carroll JM (2000) Scenario-based design. In: *Making Use: Scenario-Based Design of Human-Computer Interactions*. The MIT Press, Cambridge, pp 45-70. <https://doi.org/10.7551/mitpress/4398.003.0004>
- Chatzis P, Stavrou E (2022) Cyber-threat landscape of border control infrastructures. *International Journal of Critical Infrastructure Protection* 36:100503. <https://doi.org/10.1016/j.ijcip.2021.100503>
- Cherdantseva Y et al (2016) A review of cyber security risk assessment methods for SCADA systems. *Computers & Security* 56:1-27. <https://doi.org/10.1016/j.cose.2015.09.009>
- Creswell JW, Creswell JD (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th edn. Sage Publications, Los Angeles
- De Benedictis A, Esposito C, Somma A (2022) Toward the adoption of secure cyber digital twins to enhance cyber-physical systems security. In: *Quality of Information and Communications Technology*, pp 307-321. https://doi.org/10.1007/978-3-031-14179-9_21
- Gorishnyaya AA, Chmut GA (2021) Digital technologies in transport logistics. *Vestnik Universiteta* 8:34-40. <https://doi.org/10.26425/1816-4277-2021-8-34-40>
- Halstead RW (2013) Railroad accident investigation and reconstruction. In: *Encyclopedia of Forensic Sciences*, 3rd edn, pp 306-312. <https://doi.org/10.1016/B978-0-12-823677-2.00320-2>
- Humayed A, Lin J, Li F, Luo B (2017) Cyber-physical systems security: A survey. *IEEE Internet of Things Journal* 4(6):1802-1831. <https://doi.org/10.1109/JIOT.2017.2703172>
- Institution of Engineering and Technology (2022) *Cybersecurity in Transport Systems*. Institution of Engineering and Technology, London. <https://doi.org/10.1049/pbtr015e>
- International Transport Forum (2021) *ITF Transport Outlook 2021*. OECD Publishing, Paris. <https://doi.org/10.1787/16826a30-en>
- Joseph M (2018) PW 1575 The role of accident investigation in promoting occupational safety in Nigeria. *Injury Prevention* 24:A212.2-A212. <https://doi.org/10.1136/injuryprevention-2018-safety.587>
- Kent K, Chevalier S, Grance T, Dang H (2006) *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86. National Institute of Standards and Technology, Gaithersburg. <https://doi.org/10.6028/NIST.SP.800-86>
- Kim DS, Yoon WC (2013) An accident causation model for the railway industry: Application of the model to 80 rail accident investigation reports from the UK. *Safety Science* 60:57-68. <https://doi.org/10.1016/j.ssci.2013.06.010>

- Lamssaggad A, Benamar N, Senhaji Hafid A, Msahli M (2021) A survey on the current security landscape of intelligent transportation systems. *IEEE Access* 9:9180-9208. <https://doi.org/10.1109/ACCESS.2021.3050038>
- Lang J (1999) Learning from marine accidents: The work of the Marine Accident Investigation Branch. In: *Learning From Marine Incidents*, pp 11-16. <https://doi.org/10.3940/rina.mi.1999.11>
- Lazarenko D, Nagorny V (2022) Digital transformation of the transport complex in Russia. *Transportation Research Procedia* 63:154-159. <https://doi.org/10.1016/j.trpro.2022.05.018>
- Lee EA (2008) Cyber physical systems: Design challenges. In: *11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, pp 363-369. <https://doi.org/10.1109/ISORC.2008.25>
- Nelufule N et al (2024) Digital forensics: A survey of emerging threats, challenges, and opportunities in smart grids. In: *2024 IEEE 12th International Conference on Smart Energy Grid Engineering*, pp 109-114. <https://doi.org/10.1109/SEGE62220.2024.10739495>
- OECD (2020) *Road Safety Annual Report 2020*. OECD Publishing, Paris. <https://doi.org/10.1787/f3e48023-en>
- Racz N, Weippl E, Seufert A (2010) A frame of reference for research of integrated governance, risk and compliance. In: *Communications and Multimedia Security, Lecture Notes in Computer Science*, pp 106-117. https://doi.org/10.1007/978-3-642-13241-4_11
- Rajchel J (2018) The procedures of aviation accidents investigation: The human factor as a greatest aviation safety threat. *Modern Management Review*. <https://doi.org/10.7862/rz.2018.mmr.52>
- Ramadhan RA, Muallfah D, Hariyadi D (2019) Digital forensics: Acquisition and analysis on CCTV digital evidence using static forensic method based on ISO/IEC 27037:2014. In: *Proceedings of the Second International Conference on Science, Engineering and Technology*, pp 85-89. <https://doi.org/10.5220/0009120400850089>
- Rudin-Brown CM, Rosberg A (2021) Applying principles of fatigue science to accident investigation: Transportation Safety Board of Canada fatigue investigation methodology. *Chronobiology International* 38(2):296-300. <https://doi.org/10.1080/07420528.2020.1863976>
- Sachowski J (2016) Accomplishing forensic readiness. In: *Implementing Digital Forensic Readiness*, pp 151-153. <https://doi.org/10.1016/B978-0-12-804454-4.00015-0>
- Vial S (2019) Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems* 28(2):118-144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Yin RK (2018) *Case Study Research and Applications: Design and Methods*. Sage Publications, Los Angeles

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [ESM1GRCPrototype.zip](#)