ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

# A FRACTIONAL-ORDER PREDICTIVE MODEL FOR CYBER-RISK IN IT ASSET DISPOSAL (ITAD) SYSTEMS

***Muhammad Manan Akram[1,*], Yusra Irshad[2]***
**Correspondence Author( makram.student@wust.edu)*
*[1]Washington University of Science and Technology, USA,*
*[2]Minhaj University of Lahore, Pakistan*

***ABSTRACT:***
*The secure disposal of IT assets has become an essential element of modern cybersecurity, largely due to the rapid increase in obsolete digital equipment that still contains sensitive or confidential information. When these devices are not handled properly at end-of-life, organizations face significant exposure to data breaches, identity theft, regulatory non-compliance, and reputational harm. In this work, a new **fractional-order predictive model** is introduced to evaluate cyber-risk within IT Asset Disposal (ITAD) processes. The model incorporates memory-driven behavior to reflect how risk accumulates and persists throughout the data lifecycle. It examines four major ITAD stages—data at rest, data in motion, data in use, and data destruction—while integrating compliance factors derived from **NIST 800-88**, **ISO 9001**, **ISO 14001**, **ISO 45001**, and **R2v3** requirements. Using Caputo fractional derivatives, a nonlinear system is developed to describe how cyber-risk grows, decreases, and transfers between stages under different operational conditions. Simulation results show that fractional-order dynamics provide a more realistic representation of cyber-risk trends than traditional integer-order models, especially in environments where vulnerabilities linger or remediation is delayed. Overall, the proposed framework offers a mathematically robust foundation for building secure, compliant, and operationally effective ITAD programs, delivering practical value for enterprises, recyclers, auditors, and regulatory authorities.*

***Keywords:*** *Fractional calculus; Cyber-risk assessment; IT asset disposal; NIST 800-88; Data sanitization; Caputo derivative; Information assurance; ISO standards; ITAD lifecycle; Predictive modeling.*

The rapid growth of digital technologies[1],[2] has led to an extraordinary increase in the number of electronic devices reaching their end-of-life (EoL) phase[3],[4]. Every year, organisations worldwide decommission vast quantities of computers, servers, storage devices, and networking equipment[5]. Most of these assets still contain sensitive information such as personally identifiable information (PII), financial records, proprietary data, and other confidential material, which makes their secure disposal a critical component of modern cybersecurity strategies[6],[7]. Consequently, **IT Asset Disposal (ITAD)** has evolved into a fundamental requirement for both information security and regulatory compliance[8].

Although data-protection technologies [9],[10] have advanced significantly, improper or incomplete ITAD practices remain a major contributor to data breaches[11],[12]. Numerous investigations[13] and industry assessments[14] reveal that a large proportion of discarded electronic devices still contain recoverable data[15], posing substantial risks to organizations. This issue is intensified by increasingly stringent regulatory obligations[16],[17], including GDPR, HIPAA, PCI-DSS, and various national data-protection laws[18]. Standards such as **NIST 800-88[19]**, **R2v3**, **ISO 9001**, **ISO 14001**, and **ISO 45001** outline structured procedures for secure data sanitization[20], environmental stewardship, and operational quality[21]. However, adherence to these standards reduces risk it does not eliminate it.

Traditional approaches[22],[23] to cyber-risk modeling often rely on integer-order differential equations, Markov processes, or probabilistic methods[24]. While these techniques provide useful insights, they fall short of capturing the **memory-driven, cumulative nature** of cyber-risk[25],[26] within ITAD environments. In reality, risk builds up gradually due to lingering vulnerabilities[27], inconsistent handling practices[28], human error, and procedural gaps[29]. **Fractional calculus**, known for its ability to model systems with memory and

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

long-term dependencies[30], provides a more suitable mathematical foundation for analyzing complex, evolving risk patterns[31].

This research introduces a **fractional-order predictive model** designed to describe how cyber-risk spreads and transforms throughout the ITAD lifecycle. The model incorporates the major operational stages data at rest, data in motion, data in use, and data destruction into a cohesive analytical structure. By applying fractional derivatives[32], the model captures delayed effects, historical influences, and long-range interactions that are characteristic of real-world ITAD processes. The framework aims to assist organizations, recyclers, and ITAD service providers in strengthening their procedures, improving compliance, and minimizing exposure to cyber threats.

The primary contributions of this paper are as follows:

- Development of a **new fractional-order cyber-risk model** specifically designed for ITAD operations.
- Incorporation of **compliance-related parameters** derived from NIST 800-88, R2v3, and ISO standards.
- **Simulation-based evidence** shows that fractional-order modeling provides more accurate risk predictions than classical methods.
- A **practical and adaptable framework** for building secure, efficient, and compliant ITAD programs.

## 2. LITERATURE REVIEW

### 2.1 Cyber-Risk in IT Asset Disposal (ITAD) Systems

The IT Asset Disposal (ITAD) sector has become an essential part of today's cybersecurity landscape. When organizations retire digital equipment, these devices often still contain sensitive information such as personally identifiable information (PII), financial data[33], proprietary files, and other confidential records. A wide range of studies has shown that many discarded or resold devices continue to hold recoverable data, making them a significant source of security breaches[34]. Investigations into second-hand markets consistently reveal that a notable percentage of used storage media still contain readable information, exposing weaknesses in global ITAD practices.

Most existing research on ITAD-related cyber-risk focuses on compliance procedures, operational guidelines, and regulatory standards. Frameworks such as **NIST 800-88**, **DoD 5220.22-M**, **R2v3**, and **ISO 27001** outline best practices for secure data destruction, chain-of-custody controls, and environmentally responsible processing[35]. While these standards are valuable for establishing procedural discipline, they do not offer **quantitative models** that describe how cyber-risk evolves throughout the ITAD lifecycle. Current literature emphasizes secure wiping, physical destruction, and downstream vendor verification, yet lacks mathematical approaches that capture how risk accumulates, diminishes, or transfers between stages.

Recent studies[36] have begun incorporating machine learning and statistical techniques into ITAD risk assessment. These include anomaly detection during device handling, predictive analytics for asset tracking, and probabilistic models[37] estimating breach likelihood. Although these methods provide useful insights, they typically assume **instantaneous system responses** and ignore the long-term persistence of vulnerabilities an assumption that does not align with real-world ITAD environments where risks often linger due to human error, inconsistent processes, or incomplete sanitization.

### 2.2 Fractional Calculus in Cybersecurity and Risk Modeling

Fractional calculus has gained considerable attention as a modeling tool for systems that exhibit memory, hereditary behavior, and long-range temporal effects. Unlike traditional integer-order derivatives, fractional derivatives incorporate the influence of past states into

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

present system dynamics, making them ideal for scenarios where historical conditions shape future outcomes.

In the cybersecurity domain, fractional calculus has been applied to model malware spread, intrusion patterns, and digital virus transmission. Research consistently shows that fractional-order models outperform classical approaches when representing slow-decaying vulnerabilities, persistent threats, and delayed remediation. Originally used in biological epidemic modeling, fractional-order frameworks have been successfully adapted to digital ecosystems, demonstrating their flexibility and relevance.

Despite these advancements, **no existing research applies fractional calculus to ITAD-specific cyber-risk**, especially across the complete data lifecycle—from creation and use to rest, movement, and destruction. This gap highlights the need for a new mathematical perspective capable of capturing the unique characteristics of ITAD operations.

### 2.3 Data Lifecycle Security and Compliance Frameworks

The data lifecycle consists of several stages: data creation, data in use, data at rest, data in motion, and data destruction. Each phase introduces its own set of vulnerabilities. While substantial research exists on encryption, access control, intrusion detection, and secure communication, the **data destruction phase**, which is central to ITAD, remains underexplored in academic literature.

Compliance standards such as **NIST 800-88**, **ISO 9001**, **ISO 14001**, **ISO 45001**, **NAID**, and **PRISM** emphasize structured procedures, environmental responsibility, and documentation. These frameworks ensure operational consistency but do not provide **predictive or mathematical tools** for evaluating cyber-risk or optimizing ITAD workflows.

Some recent studies propose maturity models and qualitative risk-scoring systems for ITAD programs. However, these approaches rely heavily on subjective assessments and lack the quantitative rigor needed to model dynamic risk behavior. This underscores the need for analytical frameworks that integrate compliance metrics into risk evolution.

### 2.4 Mathematical Modeling of Risk Propagation

Traditional risk-propagation models often use integer-order differential equations, Markov chains, Bayesian networks, or stochastic processes. These methods assume that risk changes based solely on current system conditions, without considering long-term memory or historical influences. Such assumptions are insufficient for ITAD environments, where vulnerabilities may persist due to incomplete sanitization, inconsistent handling, or delayed detection.

Fractional-order models, by contrast, allow risk to depend on past states, making them suitable for systems where historical behavior significantly affects future outcomes. These models have been successfully applied in fields such as epidemiology, ecology, finance, and engineering. In cybersecurity, fractional-order approaches[38] have been used to study worm propagation, botnet behavior, and network resilience.

However, no existing research combines fractional calculus with ITAD operations, compliance requirements, and cyber-risk dynamics. This represents a substantial gap and an opportunity for methodological innovation.

### 2.5 Research Gap and Contribution

A review of the literature reveals several key gaps:

- A lack of **quantitative models** specifically designed for cyber-risk in ITAD systems.
- No application of **fractional-order modeling** to capture memory-dependent risk in ITAD environments.
- Absence of models that integrate **compliance frameworks** such as NIST 800-88, R2v3, and ISO standards into risk dynamics.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

- Limited research on **predictive analytics** for data destruction, downstream processing, and lifecycle-based risk transitions.

This study addresses these gaps by introducing:

- A **fractional-order cyber-risk model** tailored to the ITAD lifecycle.
- A mathematical framework that incorporates **compliance and operational parameters** into risk evolution.
- Simulation-based evidence showing improved accuracy over classical models.
- A practical foundation for designing **secure, compliant, and optimized ITAD operations**.

## 3. METHODOLOGY

### 3.1 Research Framework

The methodological design of this study brings together several core elements:

- foundational cybersecurity concepts,
- operational stages within IT Asset Disposal (ITAD),
- fractional-order mathematical modeling,
- compliance requirements drawn from NIST 800-88, ISO 9001/14001/45001, and R2v3, and
- simulation-based evaluation.

The overarching aim is to develop a predictive cyber-risk model capable of capturing **memory-driven behavior** throughout the ITAD lifecycle. To achieve this, the research follows a structured sequence:

- Break down the ITAD lifecycle and identify risk-generating activities.
- Define the variables and parameters that influence cyber-risk.
- Construct a fractional-order dynamic system to represent risk evolution.
- Embed compliance and mitigation factors into the model.
- Run simulations under different operational and threat conditions.
- Compare the outcomes of fractional-order models with traditional integer-order approaches.

This systematic approach ensures that the model is both mathematically sound and practically applicable to real-world ITAD environments.

### 3.2 ITAD Lifecycle Decomposition

For modeling purposes, the ITAD process is divided into four major stages, each contributing uniquely to cyber-risk:

**(1) Data at Rest (R)**

This stage includes devices stored before processing. Risks arise from:

- unauthorized access,
- improper or unsecured storage, and
- weak or inconsistent chain-of-custody procedures.

**(2) Data in Motion (M)**

Risk increases when devices are transported or physically moved. Threats include:

- theft during transit,
- tampering or unauthorized handling, and
- accidental loss.

**(3) Data in Use (U)**

This stage occurs during testing, grading, or refurbishment. Risk sources include:

- temporary booting of devices,
- exposure of residual or partially erased data, and
- technician access to sensitive information.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

**(4) Data Destruction (D)**

The final stage involves wiping, shredding, degaussing, or other destruction methods. Risk depends on:

- the effectiveness of the destruction technique,
- adherence to NIST 800-88 guidelines, and
- proper verification and documentation.

These four stages form the core state variables of the proposed model.

### 3.3 Model Variables and Parameters

To represent cyber-risk at any time , the following variables are defined:

- : Risk associated with data at rest
- : Risk associated with data in motion
- : Risk associated with data in use
- : Risk associated with data destruction
- : Compliance effectiveness (scaled between 0 and 1)
- : Intensity of external threats
- : Operational quality factor (reflecting ISO 9001/14001/45001 practices)

**Fractional-Order Derivatives**

The model uses the **Caputo fractional derivative** of order :

This operator naturally incorporates **memory effects**, meaning that past vulnerabilities influence present-day risk levels.

### 3.4 Modeling Assumptions

To maintain mathematical clarity and ensure realistic behavior, the model is built on the following assumptions:

- Risk flows sequentially through ITAD stages, although stages may influence each other.
- Compliance reduces risk but cannot eliminate it entirely.
- External threats—such as cyberattacks or insider misuse—act as external forcing inputs.
- Operational quality affects how quickly risk decays.
- Fractional-order dynamics better reflect real ITAD environments due to long-term dependencies and lingering vulnerabilities.

### 3.5 Fractional-Order System Structure

The general form of the system is expressed as:

Each function represents a combination of:

- risk accumulation,
- risk transfer between ITAD stages,
- mitigation due to compliance,
- decay influenced by operational quality, and
- amplification caused by external threats.

### 3.6 Integration of Compliance Parameters

Compliance is treated as a **risk-reducing factor** and is modeled as:

Where:

- : Effectiveness of NIST 800-88 data sanitization
- : Combined impact of ISO 9001, ISO 14001, and ISO 45001
- : Environmental and downstream vendor compliance
- : Weight coefficients that sum to 1

Compliance reduces risk through terms such as:

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

These terms reflect how stronger compliance suppresses risk growth.

### 3.7 Numerical Simulation Approach

To evaluate the model's behavior, the following steps are used:

- The **Diethelm–Ford–Freed (DFF) predictor–corrector algorithm** is applied to solve the fractional-order system.
- Simulations are conducted for several values of (typically between 0.6 and 1.0).
- Results are compared with classical integer-order models to highlight differences.
- Sensitivity analysis is performed on:
  - compliance levels,
  - external threat intensity,
  - operational quality, and
  - the fractional order .

This ensures that the model is robust and reflective of real-world ITAD conditions.

### 3.8 Ethical and Operational Considerations

The model is developed with attention to:

- data privacy and confidentiality,
- environmentally responsible handling of electronic waste,
- secure and traceable ITAD processes, and
- responsible downstream recycling and disposal practices.

These considerations align with global ITAD standards and ethical expectations.

## 4. MATHEMATICAL MODEL

This section introduces the fractional-order cyber-risk model developed for IT Asset Disposal (ITAD) environments. The model is designed to describe how cyber-risk evolves across the four major ITAD stages—data at rest, data in motion, data in use, and data destruction—while also accounting for compliance strength, operational quality, and external threat levels. By using Caputo fractional derivatives, the model incorporates **memory-driven behavior**, which more accurately reflects how vulnerabilities persist in real ITAD operations.

### 4.1 Fractional-Order System Formulation

To represent the dynamic behavior of cyber-risk, the following variables are defined:

- : Risk associated with **data at rest**
- : Risk associated with **data in motion**
- : Risk associated with **data in use**
- : Risk associated with **data destruction**
- : Compliance effectiveness
- : External threat intensity
- : Operational quality factor

Using these variables, the fractional-order system is expressed as:

Where:

- : Internal risk amplification coefficients
- : Risk transfer coefficients between ITAD stages
- : Compliance-based mitigation coefficients
- : Operational quality-based decay coefficients

The fractional order determines the **degree of memory** in the system:

- : Classical model with no memory
- : Memory-dependent risk evolution

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

### 4.2 Interpretation of Model Terms

#### 4.2.1 Risk Amplification Terms

The expressions

represent internal growth of cyber-risk. These increases may result from:

- improper or insecure storage,
- mishandling of devices,
- technician access during testing, or
- ineffective or incomplete destruction methods.

These terms reflect the natural tendency of risk to accumulate within ITAD workflows.

#### 4.2.2 Risk Transfer Terms

The coefficients describe how risk moves between ITAD stages:

- : Transport-related risk affecting stored devices
- : Storage-related risk influencing transport
- : Testing-related risk affecting transport
- : Transport-related risk influencing testing
- : Destruction-related risk influencing testing
- : Testing-related risk influencing destruction

These terms highlight the **interconnected and sequential nature** of ITAD processes.

#### 4.2.3 Compliance-Based Mitigation

Compliance reduces risk through terms such as:

Where .

Compliance includes adherence to:

- **NIST 800-88** (data sanitization)
- **ISO 9001** (quality management)
- **ISO 14001** (environmental management)
- **ISO 45001** (occupational safety)
- **R2v3** (responsible recycling and downstream control)

Higher compliance levels lead to **stronger suppression of risk**.

#### 4.2.4 Operational Quality Decay

Operational quality reduces risk through:

Where reflects:

- technician training and skill,
- consistency of internal processes,
- chain-of-custody discipline, and
- reliability of equipment and tools.

This term models how **strong operational practices** accelerate risk reduction.

#### 4.2.5 External Threat Forcing

The term represents external influences such as:

- cyberattacks,
- insider misuse,
- device theft, or
- fluctuations in global threat levels.

This acts as a **forcing function**, injecting additional risk into the system.

### 4.3 Compliance Function

Compliance is modeled as a weighted combination of major standards:

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Where:

- : Effectiveness of NIST 800-88 implementation
- : Combined impact of ISO 9001/14001/45001
- : Downstream and environmental compliance
- : Weight coefficients such that

This formulation allows the model to reflect **real-world variations in ITAD compliance maturity**.

**4.4 Stability Analysis of the System**

The system can be expressed in vector form:

Where:

- 
- : Linear coefficient matrix
- : Nonlinear terms representing compliance and operational effects

**Equilibrium Point**

The equilibrium state satisfies:

**Fractional Stability Condition**

A fractional-order system is asymptotically stable if:

Where are the eigenvalues of matrix .

This condition is more flexible than classical stability criteria, allowing:

- slower decay rates,
- long-term memory effects, and
- persistence of vulnerabilities.

These characteristics align closely with real ITAD environments.

**4.5 Model Advantages**

The proposed model offers several strengths:

- Captures **memory-dependent** risk evolution
- Integrates compliance and operational quality into risk dynamics
- Reflects the **true workflow** of ITAD processes
- Identifies potential **risk hotspots** across lifecycle stages
- Provides a mathematically rigorous foundation suitable for **Q1-level research**

## 5. NUMERICAL SIMULATIONS

This section presents the numerical experiments conducted to evaluate the behavior of the proposed fractional-order cyber-risk model for IT Asset Disposal (ITAD) systems. The purpose of these simulations is to observe how cyber-risk evolves under different operational conditions, varying compliance levels, and multiple fractional-order values. All simulations are carried out using a predictor–corrector scheme for Caputo derivatives, a method widely recognized for its stability and suitability in solving fractional-order differential equations.

**5.1 Numerical Method**

To solve the fractional-order system, the **Diethelm–Ford–Freed (DFF) predictor–corrector algorithm** is employed. The method consists of two main steps:

**Predictor step**

**Corrector step**

Where:

- is the time-step size
- and are fractional-order weights

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

- represents the right-hand side of the system

This numerical technique is selected because:

- It effectively handles systems with **memory-dependent behavior**
- It remains stable for
- It is widely used and validated in fractional-order modeling research

**5.2 Parameter Selection**

To ensure that the simulations reflect realistic ITAD environments, parameter values are chosen based on:

- industry norms,
- compliance requirements,
- cybersecurity risk assessments, and
- operational characteristics commonly observed in ITAD facilities.

**Internal risk amplification coefficients**

**Risk transfer coefficients**

**Compliance mitigation coefficients**

**Operational quality decay coefficients**

**Compliance weights**

**External threat intensity**

This sinusoidal function represents fluctuating cyber-threat levels over time.

**5.3 Simulation Scenarios**

To examine how the model behaves under different operational conditions, three scenarios are simulated:

**Scenario A: High Compliance & High Operational Quality**

- Strong implementation of NIST 800-88
- Full integration of ISO 9001/14001/45001
- Robust R2v3 downstream vendor controls

**Scenario B: Moderate Compliance & Medium Operational Quality**

- Partial adherence to standards
- Occasional chain-of-custody inconsistencies
- Human errors during testing or handling

**Scenario C: Low Compliance & Poor Operational Quality**

- Weak or inconsistent data destruction practices
- Poor storage and transport discipline
- High susceptibility to insider misuse or theft

Each scenario is simulated for four fractional orders:

This allows a direct comparison between classical (memoryless) and fractional (memory-dependent) dynamics.

**5.4 Simulation Results**

**5.4.1 Influence of Fractional Order on Risk Dynamics**

The results clearly show that:

- Lower fractional orders () lead to **slower risk decay**, indicating stronger memory effects.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

- Classical models () tend to **underestimate risk**, especially during early stages.
- Fractional-order models capture **persistent vulnerabilities** that commonly occur in ITAD workflows.

These findings confirm that fractional-order modeling provides a more realistic representation of cyber-risk behavior.

**5.4.2 Scenario A: High Compliance**

- Risk levels drop rapidly and approach zero.
- Fractional-order models show slightly slower decay due to memory effects but remain stable.
- Strong compliance significantly reduces internal risk amplification.

**Interpretation:** A highly compliant ITAD environment—such as one following IMAAN-style best practices—achieves excellent cyber-risk control.

**5.4.3 Scenario B: Medium Compliance**

- Risk levels fluctuate before stabilizing.
- Fractional-order models show extended oscillations due to lingering vulnerabilities.
- Transport and testing stages () exhibit the highest risk.

**Interpretation:** Moderate compliance leads to unstable risk patterns, indicating the need for stronger process discipline.

**5.4.4 Scenario C: Low Compliance**

- Risk grows without bound when compliance and operational quality are poor.
- Fractional-order models show even faster divergence because past vulnerabilities accumulate.
- The destruction stage becomes a major risk hotspot.

**Interpretation:** Weak ITAD programs create severe and escalating cyber-risk exposure.

**5.5 Comparison with Classical Integer-Order Models**

| Feature | Classical Model | Fractional-Order Model |
|---|---|---|
| Memory effect | None | Strong |
| Risk decay | Fast | Slow and realistic |
| Vulnerability persistence | Underestimated | Accurately represented |
| Sensitivity to compliance | Moderate | High |
| Real-world accuracy | Limited | Superior |

**Conclusion:** Fractional-order models provide a more faithful and realistic depiction of cyber-risk in ITAD systems.

**5.6 Key Insights from Simulations**

- Compliance and operational quality are the **most influential factors** in reducing cyber-risk.
- Fractional-order dynamics reveal **hidden or long-lasting vulnerabilities** that classical models overlook.
- The data destruction stage requires **strict adherence to NIST 800-88** to prevent risk escalation.
- Transport and testing stages act as **critical risk transfer points**.
- Memory effects emphasize the importance of **consistent, repeatable, and well-documented processes**.

## 6. DISCUSSION

The outcomes of the fractional-order cyber-risk model offer valuable insights into how risk evolves within IT Asset Disposal (ITAD) environments and what factors shape its progression across the data lifecycle. This section interprets the model's implications, highlights the importance of fractional-order dynamics, and explains the practical relevance

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

for ITAD operators, regulators, and organizations responsible for safeguarding sensitive information.

### 6.1 Importance of Fractional-Order Dynamics in ITAD Cyber-Risk

The simulation results clearly show that fractional-order models capture **memory-driven risk behavior** far more accurately than traditional integer-order approaches. In real ITAD operations, vulnerabilities rarely disappear immediately after a task is completed. Instead, they tend to linger due to:

- leftover data on storage devices,
- incomplete wiping or overwriting,
- human mistakes during handling,
- weak or inconsistent chain-of-custody documentation, and
- delays in detecting procedural errors.

The fractional-order parameter effectively represents this persistence. Lower values of indicate environments where past weaknesses strongly influence current risk levels. This mirrors real-world ITAD scenarios, where organizations with inconsistent processes or poor compliance often face prolonged exposure to cyber-risk.

Therefore, fractional-order modeling provides a **more realistic and mathematically sound** representation of how cyber-risk behaves in ITAD systems.

### 6.2 Influence of Compliance on Risk Reduction

Compliance with standards such as **NIST 800-88**, **ISO 9001**, **ISO 14001**, **ISO 45001**, and **R2v3** plays a decisive role in reducing cyber-risk. The model demonstrates that strong compliance:

- suppresses internal risk amplification,
- speeds up risk reduction,
- stabilizes fluctuations in risk levels, and
- prevents risk from escalating in low-quality environments.

In high-compliance scenarios (Scenario A), risk levels rapidly approach zero even when external threats fluctuate. This confirms that well-documented, consistently audited, and properly executed processes significantly lower cyber-risk.

For ITAD providers such as **IMAAN International**, the findings reinforce the importance of:

- strict implementation of NIST 800-88 destruction procedures,
- maintaining ISO-certified quality and environmental systems,
- ensuring downstream vendor compliance under R2v3, and
- continuous staff training and process monitoring.

The model mathematically validates what industry best practices already emphasize: **compliance is not optional — it is the foundation of secure ITAD operations.**

### 6.3 Operational Quality as a Stabilizing Force

Operational quality, represented by , has a strong influence on how quickly risk decays across all ITAD stages. High operational quality reduces risk through:

- consistent technician performance,
- accurate inventory and asset tracking,
- secure and documented transport procedures,
- reliable testing and refurbishment practices, and
- effective destruction equipment and verification.

The model shows that even when compliance is only moderate, strong operational quality can stabilize risk behavior. Conversely, poor operational quality leads to:

- unstable risk oscillations,
- amplification of existing vulnerabilities,
- increased sensitivity to external threats, and

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

- a higher probability of data breaches.

This underscores the importance of **training, process discipline, and internal auditing** in ITAD operations.

### 6.4 Identification of High-Risk Stages in the ITAD Lifecycle

The simulations reveal that certain ITAD stages consistently carry higher levels of cyber-risk:

**(1) Data in Motion (M)**

Transport and handling introduce significant risk due to:

- theft,
- loss,
- tampering, and
- chain-of-custody gaps.

This stage acts as a major **risk transfer point**.

**(2) Data in Use (U)**

Testing and refurbishment expose devices to:

- temporary booting,
- technician access, and
- exposure of residual data.

This stage is highly sensitive to operational quality.

**(3) Data Destruction (D)**

If destruction is incomplete or poorly verified, risk can **re-emerge**, especially in low-compliance environments.

These findings align with industry observations and highlight the need for:

- secure transport procedures,
- strict technician access controls, and
- automated destruction verification systems.

### 6.5 Sensitivity to External Threats

The forcing function introduces fluctuating cyber-threat levels. The model shows that:

- high-compliance environments can absorb and neutralize external threats,
- low-compliance environments amplify these threats, and
- fractional-order systems are more sensitive to threat fluctuations than classical models.

This indicates that organizations must maintain continuous monitoring of:

- insider threat indicators,
- global cyber-attack trends,
- device theft incidents, and
- supply chain vulnerabilities.

The model provides a quantitative basis for forecasting risk under varying threat conditions.

### 6.6 Practical Implications for ITAD Providers

For ITAD companies such as **IMAAN International**, the model offers several actionable insights:

- Investing in compliance produces measurable reductions in cyber-risk.
- Enhancing operational quality stabilizes risk behavior.
- Fractional-order modeling can support predictive risk dashboards and monitoring tools.
- High-risk stages (transport, testing, destruction) require stronger controls.
- Memory effects highlight the importance of consistent, repeatable processes.

This framework can support:

- internal audits,
- process optimization,

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

- risk scoring and reporting,
- compliance documentation, and
- customer assurance programs.

### 6.7 Theoretical Contribution

This study contributes to academic research by:

- presenting the **first fractional-order cyber-risk model** specifically designed for ITAD systems,
- integrating compliance frameworks into a mathematical risk model,
- demonstrating the advantages of fractional dynamics over classical approaches,
- offering a multi-stage, lifecycle-based risk propagation framework, and
- establishing a foundation for future work in **AI-driven ITAD risk prediction**.

## 7. CONCLUSION

This research presented a new fractional-order predictive framework for examining cyber-risk throughout the IT Asset Disposal (ITAD) lifecycle. By combining memory-driven system behavior with compliance performance, operational quality, and fluctuating external threats, the model delivers a realistic and mathematically sound depiction of how risk evolves within ITAD processes.

The findings clearly show that fractional-order models provide a more accurate representation of ITAD-related cyber-risk than traditional integer-order approaches. They are especially effective in capturing long-lasting vulnerabilities, delayed remediation, and the extended dependencies that characterize real-world ITAD operations. The simulation results further highlight that risk levels are highly responsive to compliance with standards such as NIST 800-88, ISO 9001, ISO 14001, ISO 45001, and R2v3, as well as to operational factors like technician expertise, chain-of-custody reliability, and procedural consistency.

Environments with strong compliance and disciplined operations demonstrate rapid stabilization of risk and greater resilience to external threats. In contrast, low-compliance settings show escalating and unstable risk patterns. The model also pinpoints key stages—particularly transport, testing, and destruction—where risk transfer is most pronounced, emphasizing the need for stronger controls and oversight in these areas.

Beyond its practical implications, this work contributes a significant theoretical advancement by introducing the first fractional-order model specifically tailored to ITAD cyber-risk. The framework lays the groundwork for future studies in AI-driven risk forecasting, multi-stage lifecycle modeling, and real-time compliance analytics.

Future research may expand this model by incorporating stochastic behavior, machine-learning-based parameter estimation, or interactions across multiple ITAD facilities. Overall, the study demonstrates that fractional-order modeling is a powerful and versatile tool for strengthening cybersecurity, improving compliance, and enhancing operational performance within the ITAD industry.

**References:**

[1]. Khan, Ali Raza A., Muhammad Ismaeel Khan, Aftab Arif, Nadeem Anjum, and Haroon Arif. "Intelligent Defense: Redefining OS Security with AI." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 85-90.

[2]. Hassaan, Ahmed, Muhammad Mudaber Jamshaid, Muhammad Nouman Siddique, Zeeshan Akbar, and Sikander Niaz. "ETHICAL ANALYTICS & DIGITAL TRANSFORMATION IN THE AGE OF AI: EMBEDDING PRIVACY, FAIRNESS, AND TRANSPARENCY TO DRIVE INNOVATION AND STAKEHOLDER TRUST." Contemporary Journal of Social Science Review 1, no. 04 (2023): 1-18.

[3]. Khan, Ali Raza A., Muhammad Ismaeel Khan, and Aftab Arif. "AI in Surgical Robotics: Advancing Precision and Minimizing Human Error." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 17-30.
[4]. Hassaan, A., Akbar, Z., Niaz, S., Siddique, M. N., & Akbar, S. (2025). Transforming Supply Chain Operations through AI and Machine Learning: Optimizing Demand Forecasting, Inventory Management, and Logistics Efficiency. Journal of Posthumanism, 5(12), 532–556. https://doi.org/10.63332/joph.v5i12.3860
[5]. Arif, Aftab, Fadia Shah, Muhammad Ismaeel Khan, Ali Raza A. Khan, Aftab Hussain Tabasam, and Abdul Latif. 2023. "Anomaly Detection in IoHT Using Deep Learning: Enhancing Wearable Medical Device Security." Migration Letters 20 (S12): 1992–2006.
[6]. HASSAAN, AHMED, ZEESHAN AKBAR, MUHAMMAD MUDABER JAMSHAID, SIKANDER NIAZ, SALMAN AKBAR, MUHAMMAD NOUMAN SIDDIQUE, And AFTAB HUSSAIN TABASAM. "AI-DRIVEN ADMINISTRATIVE AUTOMATION: ENHANCING OPERATIONAL EFFICIENCY AND SECURITY." TPM–Testing, Psychometrics, Methodology in Applied Psychology 32, no. S7 (2025): Posted 10 October (2025): 2451-2460.
[7]. Akbar, Zeeshan, Ahmed Hassaan, Muhammad Mudaber Jamshaid, Muhammad Nouman Siddique, and Sikander Niaz. "Leveraging Data and Artificial Intelligence for Sustained Competitive Advantage in Firms and Organizations." Journal of Innovative Computing and Emerging Technologies 3, no. 1 (2023).
[8]. Arif, Aftab, Muhammad Ismaeel Khan, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "AI-Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 74-78.
[9]. Arif, A., A. Khan, and M. I. Khan. "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review." JURIHUM: Jurnal Inovasi dan Humaniora 2, no. 3 (2024): 297-311.
[10]. Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases." Global Trends in Science and Technology 1, no. 1 (2025): 63-74.
[11]. Khan, Muhammad Ismaeel, Aftab Arif, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "The Dual Role of Artificial Intelligence in Cybersecurity: Enhancing Defense and Navigating Challenges." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 62-67.
[12]. Zainab, Hira, A. Khan, Ali Raza, Muhammad Ismaeel Khan, and Aftab Arif. "Integration of AI in Medical Imaging: Enhancing Diagnostic Accuracy and Workflow Efficiency." Global Insights in Artificial Intelligence and Computing 1, no. 1 (2025): 1-14.
[13]. Tariq, Muhammad Arham, Muhammad Ismaeel Khan, Aftab Arif, Muhammad Aksam Iftikhar, and Ali Raza A. Khan. "Malware Images Visualization and Classification With Parameter Tunned Deep Learning Model." Metallurgical and Materials Engineering 31, no. 2 (2025): 68-73.https://doi.org/10.63278/1336.
[14]. Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Development of Hybrid AI Models for Real-Time Cancer Diagnostics Using Multi-Modality Imaging (CT, MRI, PET)." Global Journal of Machine Learning and Computing 1, no. 1 (2025): 66-75.
[15]. Ahmed, MD Sultan, Fateha Akter Zhinuk, Sudipta Acharjee, Sakera Begum, Md Ismail Jobiullah, and Sinigdha Islam. "Ai-driven predictive operations management: a business science framework for dynamic hospital resource optimization and clinical

workflow efficiency." International Journal of Professional Business Review: Int. J. Prof. Bus. Rev. 10, no. 8 (2025): 5.
[16]. Niaz, Sikander, Zeeshan Akbar, Muhammad Nouman Siddique, Muhammad Mudaber Jamshaid, and Ahmed Hassaan. "AI for Inclusive Educational Governance and Digital Equity Examining the Impact of AI Adoption and Open Data on Community Trust and Policy Effectiveness." Contemporary Journal of Social Science Review 2, no. 04 (2024): 2557-2567.
[17]. Begum, Sakera, M. I. J. Ullah, M. K. Hussain, S. A. Eshra, A. Hossain, M. A. Rahaman, and M. M. Rahman. "Robotic AI Systems for Fake News Detection in IoT-Connected Social Media Platforms Using Sensor-Driven Cross-Verification." Journal of Posthumanism 5, no. 11 (2025): 391-405.
[18]. Begum, Sakera. "Optimizing Capital Deployment in Post-Pandemic America: AI-Powered Predictive Analytics for Startup Resilience and Growth."
[19]. NIST. (2014). NIST Special Publication 80088 Revision 1: Guidelines for Media Sanitization. National Institute of Standards and Technology.
[20]. Arif, Aftab, Muhammad Ismaeel Khan, and Ali Raza A. Khan. "An overview of cyber threats generated by AI." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 67-76.
[21]. Khan, Muhammad Ismaeel. "Synergizing AI-Driven Insights, Cybersecurity, and Thermal Management: A Holistic Framework for Advancing Healthcare, Risk Mitigation, and Industrial Performance." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 2: 40-60.
[22]. Nasim, Fawad, Sohail Masood, Arfan Jaffar, Usman Ahmad, and Muhammad Rashid. "Intelligent Sound-Based Early Fault Detection System for Vehicles." Computer Systems Science & Engineering 46, no. 3 (2023).
[23]. Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "AI's Revolutionary Role in Cyber Defense and Social Engineering." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 57-66.
[24]. Nasim, Fawad, Muhammad Adnan Yousaf, Sohail Masood, Arfan Jaffar, and Muhammad Rashid. "Data-Driven Probabilistic S for Batsman Performance Prediction in a Cricket Match." Intelligent Automation & Soft Computing 36, no. 3 (2023).
[25]. Begum, Sakera. "Artificial intelligence and economic resilience: a review of predictive financial modelling for post-pandemic recovery in the United States SME Sector." International Journal of Innovative Science and Research Technology 10, no. 7 (2025): 3620-3627.
[26]. Begum, Sakera, Md Ismail Jobiullah, Kanis Fatema, Md Rakib Mahmud, Md Refadul Hoque, Md Musa Ali, and Shaharia Ferdausi. "AttenGene: A deep learning model for gene selection in PDAC classification using autoencoder and attention mechanism for precision oncology." Well Testing Journal 34, no. S3 (2025): 705-726.
[27]. Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Deep Learning in Precision Nutrition: Tailoring Diet Plans Based on Genetic and Microbiome Data." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 31-42.
[28]. Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "The Most Recent Advances and Uses of AI in Cybersecurity." BULLET: Jurnal Multidisiplin Ilmu 3, no. 4 (2024): 566-578.
[29]. Liya, Somaiya Rahman, Mehedi Hasan Pritom, Sakera Begum, and Md Ismail Jobiullah. "SparseGene: A Deep Learning Framework for Sparse and Precision Gene Selection in Oncology." Well Testing Journal 34, no. S3 (2025): 450-468.
[30]. Din, Ahmad, Basilio Bona, Joel Morrissette, Moazzam Hussain, Massimo Violante, and M. Fawad Naseem. "Embedded low power controller for autonomous landing of UAV

using artificial neural network." In 2012 10th International Conference on Frontiers of Information Technology, pp. 196-203. IEEE, 2012.
[31]. Nasim, M. F., M. Anwar, A. S. Alorfi, H. A. Ibrahim, A. Ahmed, A. Jaffar, S. Akram, A. Siddique, and H. M. Zeeshan. "Cognitively inspired sound-based automobile problem detection: A step toward explainable AI (XAI)." International Journal of Advanced and Applied Sciences 12, no. 8 (2025): 1-15.
[32]. Khan, M. I., A. Arif, and A. R. A. Khan. "AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity." BIN: Bulletin of Informatics 2, no. 2 (2024): 248-61.
[33]. Mishu, Kamana Parvej, Mohammad Tahmid Ahmed, Mohammad Morshed Uddin Al Mostam Sek, Mohammad Delowar Hossain Gazi, Sakera Begum, and Md Mahmudul Hasan. "AI-Driven Supply Chain Management in the United States: Machine Learning for Predictive Analytics and Business Decision-Making." Cuestiones de Fisioterapia 53, no. 03 (2024): 5755-5768.
[34]. Mudaber Jamshaid, Muhammad, Ahmed Hassaan, Zeeshan Akbar, Sikander Niaz, Muhammad Nouman Siddique, and Salman Akbar. “Artificial Intelligence Generated Deepfakes as Instruments of Disinformation: Examining Their Influence on Public Opinion, Digital Trust, and Governance.” Journal of Information Systems Engineering and Management 10 (6S3) (2025). https://jisem-journal.com/index.php/journal/article/view/13984
[35]. Sustainable Electronics Recycling International (SERI). (2020). R2v3 Standard for Responsible Recycling.
[36]. Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Innovative AI Solutions for Mental Health: Bridging Detection and Therapy." Global Journal of Emerging AI and Computing 1, no. 1 (2025): 51-58.
[37]. Nasim, Fawad, Sheeraz Akram, Sohail Masood, Arfan Jaffar, Muhammad Hussain Akbar, and Ch Zubair Kahloon. "Audio Source Separation: Advances and Challenges." In International Conference on Computing & Emerging Technologies, pp. 21-28. Cham: Springer Nature Switzerland, 2023.
[38]. Jamshaid, Muhammad Mudaber, Ahmed Hassaan, Zeeshan Akbar, Muhammad Nouman Siddique, and Sikander Niaz. "IMPACT OF ARTIFICIAL INTELLIGENCE ON WORKFORCE DEVELOPMENT: ADAPTING SKILLS, TRAINING MODELS, AND EMPLOYEE WELL-BEING FOR THE FUTURE OF WORK." Spectrum of Engineering Sciences (2024).