MONTHLY
APRIL 2026

MWEBESA
LAW GROUP

Newsletter

Whats new IN THIS ISSUE

info@mwebesalaw.co.tz

www.mwebesalaw.co.tz

MWEBESA
LAW GROUP

EDITOR'S NOTE -- APRIL EDITION

Dear Clients, Colleagues, and Readers,

By April, the real work begins.
The strategies set at the start of the year are no longer theoretical. They are being tested, in transactions, in financial systems, and in the quiet decisions that rarely feel consequential in the moment but often determine outcomes later. This is the phase where pressure builds, and where the results begin to expose what has been carefully structured, and what has been assumed.

This moth's edition focuses on three areas where issues are arising early, often before businesses realise they are exposed.
We begin with "A conversation on causes and consequences: Why tax disputes escalate before they begin." Tax disputes rarely start with an assessment. They begin earlier, through mismatched electronic sales data, misclassified transactions, and gaps between systems and reported figures. By the time an audit starts, most businesses are already on the defensive. This piece explains how mismatched data, rigid statutory interpretation, and the Revenue Authority's power to re-characterize transactions create exposure that businesses often only recognize once they are already on the defensive. It is a candid look at why reactive compliance fails, and why the real work lies in designing systems that withstand scrutiny from the outset.

We then turn to "Navigating the digital minefield: the admissibility of electronic evidence in Tanzanian courts." In an era where most disputes are built on digital trails, there is a growing and costly misconception that electronic evidence speaks for itself. It does not. Courts are drawing firm lines on authenticity, integrity, and handling. Emails, WhatsApp messages, voice notes, CCTV footage, these can win cases, or be excluded entirely. The difference often comes down to decisions made long before litigation begins. This piece unpacks where cases are being lost, not on substance, but on process. We highlight businesses are going wrong and what must be done early to preserve evidentiary value.

Finally, "Trapped or Compliant? the high stakes of cross-border financing in Tanzania" looks at foreign financing from a compliance standpoint. The movement of funds into and out of the country is no longer routine. Banks act as gatekeepers, regulators assess structure at entry, and reporting requirements are strictly enforced. The piece sets out how to structure and document foreign credit so that funds are properly recognised, usable, and not exposed to delays or restrictions.
Across all three pieces, the message is consistent. The law is no longer waiting for mistakes to surface; it is embedded in how decisions must be made from the beginning. Whether structuring financing, managing records, or running financial systems, precision is no longer a safeguard. It is the baseline.

This edition is written for those who understand that risk is not always loud. Often, it builds quietly, and reveals itself only when it is hardest to fix.
If any of the themes explored raise questions or call for a closer look, we welcome the conversation. Please feel free to connect.

Thank you for reading, for questioning, and for growing with us.

Happy reading!
The Editorial Team
MWEBESA LAW GROUP

CONTENTS

A CONVERSATION ON CAUSES AND CONSEQUENCES: HOW TAX ISSUES ESCALATE LONG BEFORE AN ASSESSMENT IS ISSUED.

In Tanzania, a tax dispute rarely begins with the arrival of a formal assessment; by then, the battle is already half-lost. Disputes emerge quietly, from mismatched EFD/VFD sales data, misclassified transactions, or overlooked ambiguities in the law. What begins as a routine information request or targeted investigation quickly becomes a stress test of internal systems. In this environment, procedural errors and poor documentation are more expensive than the tax itself. Waiting for a formal assessment leaves a company on the defensive; proactive preparation is essential.

The necessity of this proactive approach is supported by current performance data. In the first quarter of 2026, seventy-nine percent of decided appeals were determined in favor of the Revenue Authority. This trend persists because many taxpayers fail to close technical issues at the audit stage or provide adequate reconciliations when the dispute commences. Furthermore, with a revenue gap of 4.305 trillion Tanzanian Shillings remaining for the 2026 fiscal year, administrative pressure to identify and tax system variances will remain intense.

This article will therefore discuss the key causes of disputes, enabling CEOs and CFOs to proactively embed countermeasures within their systems.

1. LEGAL FRAMEWORK

The Tax Administration Act [CAP. 438 R.E. 2023] has effectively engineered a front-loaded dispute environment where the window for strategic maneuver closes almost immediately after an audit commences. To treat tax as a year-end reconciliation is to ignore the structural realities of the law. The necessity of compliance by design is dictated by the interaction of three specific legal levers.

1.1 First, under Section 51, the Commissioner has power to access premises and documents without notice. This means that your audit-ready state must be permanent. If your documentation is not structured for immediate retrieval, the resulting delay or reconstruction of records is often interpreted as non-compliance, triggering punitive assessments that are difficult to unwind.

1.2 Second, the law creates a procedural evidentiary cliff. Under Section 62(5), the requirement to submit all supporting documents at the Notice of Objection stage creates a terminal deadline. If your team fails to produce crucial documentation at this primary stage, the law, and subsequent judicial precedent, effectively locks the door, barring that evidence from future proceedings. In this environment, an unorganized backoffice is a structural liability that effectively concedes the dispute before it ever reaches a courtroom.

1.3 Finally, because the burden of proof remains permanently with the taxpayer, the law assumes the Commissioner's assessment is correct until you prove otherwise. This is catered for under section 19 (2) (b) of the Tax Revenue Appeals Act [CAP. 408 R.E. 2023, which provides that: "In every proceedings before the Board and before the Tribunal, the onus of proving that the assessment or decision in respect of which an appeal is preferred is excessive or erroneous shall be on the appellant". By design, the framework rewards the party with the most robust data trail. If your internal systems do not produce a contemporaneous, record for every transaction, you are operating with an unhedged liability. In Tanzania, you do not win a tax dispute by having the better lawyer; you win by having an operational design that makes the assessment indefensible before it is even issued.

2. THE ANATOMY OF TAX CONFLICT: SOURCES AND PRACTICAL REMEDIES

2.1 Statutory ambiguity and the risk of divergent interpretation

2.1.1 The fundamental source of tax disputes in Tanzania is the ambiguity inherent in the law, which creates a significant gap between the commercial logic of a business and the regulatory objectives of the Tanzania Revenue Authority. This gap often results in divergent interpretations where a business owner identifies an allowable expense or a non-taxable transaction,

while a tax auditor identifies a taxable profit or a failure to comply. These conflicting viewpoints later manifest as significant financial liabilities that often remain hidden until a formal investigation commences. By the time a tax official initiates an audit, the business may have already accumulated years of procedural or substantive errors that the law treats as irreversible debts.

2.1.2 The uncertainty of this landscape is further complicated by the high degree of judicial discretion involved in tax litigation. As noted in the scholarly work of Baraka Melami Saiteu in the third edition of Tax Law and Practice in Tanzania, there is no definitive rule of law that compels a judge to use one specific method of interpretation over another. This leaves the choice of interpretive framework to the individual judge, who must select the most appropriate rule to understand a particular provision. For the executive leadership, this means that even a logical and well-reasoned business position can be undermined if a court finds that an alternative interpretive approach is more credible. A taxpayer who presents a creative or logical basis for their position may still find themselves at the mercy of a judge who opts for a different analytical path.

2.1.3 In most instances, the Tanzanian judiciary adheres to the strict rule of interpretation, as seen in the case of Commissioner General Tanzania Revenue Authority v. Pan African Energy Tanzania Ltd, [2016] TZCA 807. This doctrine dictates that tax statutes must be construed in an exacting manner without adding or reducing words from the specific provision that imposes a tax, charge, or fee. Under this rule, the court assigns words their plain, ordinary, and everyday meaning to honour the explicit wishes of the parliament as expressed in the legislation. This literal approach means that the court is often unwilling to consider the business intent or the perceived fairness of a tax if the language of the statute supports a contrary conclusion.

2.1.4 However, the court does not view these provisions in isolation, as evidenced by the doctrine of harmonious construction. This principle suggests that every statute is formulated with a unified purpose and must be read as a comprehensive whole. Consequently, one section of the law cannot be used to defeat another unless the court is entirely unable to reconcile the two. This judicial philosophy was clearly demonstrated in the recent decision of Mlimani Holdings Limited versus Commissioner General of the Tanzania Revenue Authority, Civil Appeal Number 505 of 2022, decided in April 2025. In this matter, the Court of Appeal prioritized the literal and harmonious reading of domestic statutes over international tax standards. The court's reasoning confirms that the characterization of a transaction is subject to the plain meaning of the law, and businesses cannot rely on foreign guidelines to bypass the strict requirements of Tanzanian tax legislation.

2.1.5 A similar analytical trend was observed in the 2025 decision of the **Court of Appeal in Commissioner General Tanzania Revenue Authority (TRA) vs Vodacom Tanzania Public Limited Company (Civil Appeal No. 485 of 2023) [2025] TZCA 343** where the court harmonized specific withholding tax provisions with general accounting principles. The court determined that the obligation to withhold tax is triggered by the accrual of an expense in the company's books rather than the actual physical payment of cash. This interpretation aligns with the doctrine of harmonious construction by ensuring that different parts of the Income Tax Act work together to prevent tax deferral. For a CEO or CFO, the impact of this reasoning is profound, as it means that an accounting entry alone can create an immediate and mandatory tax debt.

2.1.6 Because the judiciary applies these strict and harmonious rules of interpretation, compliance cannot be a reactive process. The current trend in the Court of Appeal suggests that the law will be applied exactly as written, and the burden remains on the taxpayer to prove that an assessment is incorrect. If the records and the commercial structure of the company do not align with the plain meaning of the statute at the time of the audit, the court is unlikely to offer relief based on equitable arguments or business logic. Therefore, the only viable strategy for protecting corporate capital is to ensure that every transaction is designed to satisfy the literal requirements of the law before a dispute ever arises.

2.2 Methodological mismatches: The conflict between system-driven assessments and financial accounting

2.2.1 Another source of tax controversy in Tanzania arises from the disconnect between the tax authority's reliance on automated system reports and the taxpayer's use of Audited Financial Statements to determine tax liability. While a CEO/CFO views the company's Audited Financial Statements as the definitive record of commercial performance, the Tanzania Revenue Authority increasingly prioritizes data-matching methodologies involving the Electronic Fiscal Device Management System, VAT returns, and customs databases (TANCIS). These two frameworks often fail to align due to legitimate fiscal and accounting reasons.

2.2.2 For starters, under general tax principles, Tanzanian corporations are mandated to account for income tax purposes on an accrual basis. This legal requirement dictates that an expenditure is treated as payable at the moment all events determining the liability have occurred and the amount can be determined with reasonable accuracy, even if the performance of the underlying activity is postponed. This is also the reasoning that was applied by the **Court of Appeal in Commissioner General Tanzania Revenue Authority (TRA) vs Vodacom Tanzania Public Limited Company (Civil Appeal No. 485 of 2023) [2025] TZCA 343.**

2.2.3 When the Tanzania Revenue Authority relies on automated system reports or electronic tracking data to assess financial expenditure rather than the taxpayer's audited financial statements, these two frameworks often fail to align. For instance, digital systems like the Tanzania Customs Integrated System frequently capture only the base import value of raw materials, completely omitting essential landing costs such as port charges, shipping line fees, and inland transportation. Furthermore, corporate accounting adheres to strict accrual principles to manage timing differences like goods in transit, whereas administrative systems may reflect a fragmented, transaction-based view that ignores these standard accounting adjustments. This methodological gap often leads the authority to assume that discrepancies represent under-declared income, forcing the taxpayer to defend legitimate accounting accruals as if they were procedural errors.

2.2.4 Other factors are erroneous data entry, cancelled receipts, and the issuance of credit notes which naturally create a variance between internal accounts and the government's digital ledger. Because the Electronic Fiscal Device Management System (EFDMS) is frequently unable to reflect adjustments like credit notes or reversed transactions automatically, a gap emerges. Historically, many accounting teams have treated these variances as minor administrative reconciliation items that can be clarified during the audit stage. This reliance on the audit as a late-stage opportunity to resolve system-driven errors has, however, become an extremely high-risk strategy in the current Tanzanian legal landscape.

2.2.5 The judicial treatment of these mismatches was recently clarified in the decision of Aggreko Energy Rentals Tanzania Limited versus The Commissioner General of Tanzania Revenue Authority, Civil Appeal Number 216 of 2025 [2026] TZCA 32, decided on 4 February 2026. The appellant argued that its sales data discrepancies were primarily caused by credit notes that the electronic system did not accommodate. However, the court rejected this defense, centering its reasoning on the strict procedural requirements found in Regulation 36(7) of the Tax Administration (General) Regulations. The court reasoned that the law provides a specific, proactive procedure for addressing erroneous data or system limitations. Because the taxpayer failed to print the erroneous records and rectify them with the Commissioner General at the time the transactions occurred, they could not later claim that the system's technical limitations constituted a procedural barrier to justice.

2.2.6 Therefore, relying on the appellate machinery to clarify a reporting failure is a high-risk strategy, as the judiciary treats the objection stage as the terminal point for adducing evidence. If a business identifies that its filed reports do not match its audited financials, the only effective remedy is to amend those filings immediately rather than attempting to justify the discrepancy during an adversarial audit.

2.3 The substance over form mandate

2.3.1 The final pillar of tax risk for the modern enterprise involves the quantification of transactions and the subsequent disagreements over valuation and re-characterization. In the Tanzanian fiscal environment, a Chief Finance Officer must recognize that the legal form of an arrangement is increasingly secondary to its economic substance. Substance not form is the basis of interpretation of transactions. The courts will look at the real substance not the form of the transactions; for example, it does not make any difference whether, a tax-payer labels a payment or consideration for services rendered a salary, gift, commission, pension; gratuity, emolument or benefit.

2.3.2 This doctrine was solidified in the landmark decision of **Mantra Tanzania Limited vs. Commissioner General, Tanzania Revenue Authority (Civil Appeal 380 of 2021) [2023] TZCA 190.** In this matter, the Court of Appeal reinforced the principle that the Revenue Authority is not bound by the nomenclature chosen by the parties to a contract. If a transaction is labelled as one thing but functions as another, the state is empowered to look through the legal veil to tax the underlying commercial reality.

2.3.3 For example, the Revenue Authority is justified in re-characterizing payments if the legal label, such as "management fees" lacks sufficient underlying evidence of actual service delivery. This means that even a perfectly drafted contract can be disregarded if you cannot prove that the commercial substance aligns with the label.

2.3.4 This power is explicitly granted under Section 50 of the Income Tax Act, which allows the Commissioner General to make adjustments which involves re-characterizing arrangements and that are part of a tax avoidance scheme or where the form does not reflect the true substance.

2.3.5 To mitigate this risk, a CFO must ensure that the company's tax governance moves beyond contractual validity toward evidentiary excellence. Because the court prioritizes a harmonious reading of the law that favours the revenue-collecting intent of the parliament, any ambiguity in characterization of a transaction will likely be decided in favour of the state.

3. CONCLUSION

The legal framework, judicial philosophy, and administrative practice all converge to create a front-loaded environment where compliance must be embedded into the daily architecture of corporate systems. Ambiguity in statutes, methodological mismatches between fiscal devices and audited accounts, and the doctrine of substance over form collectively ensure that reactive strategies are inadequate. For CEOs and CFOs, the lesson is governance must be designed to produce contemporaneous, audit-ready records that withstand both administrative scrutiny and judicial literalism. In this landscape, operational discipline is not merely a defensive shield but the decisive factor that determines whether capital is preserved or eroded. The only sustainable strategy is to treat compliance as a continuous design principle, anticipating disputes before they arise and neutralizing them at their source.

A SCHEDULE OF THE MOST IMPORTANT CLOCKS.

Stage of escalation	Typical document/event	Key clock	What to do immediately	What escalates if you delay
Data flag / compliance suspicionagreement).	Internal risk selection (not always disclosed)	No formal clock	Start reconciliation: EFD sales vs VAT returns; withholding registers vs expense ledgers	Audit selection criteria include compliance history/business class; unresolved inconsistencies become audit "themes."
Information notice	Written notice to produce info/documents or attend	14 days from service (extendable on cause)	Log service date; allocate responsibility; respond with complete indexed pack; request extension early if needed	Late documents may be barred as evidence later.
Audit activity	Access to premises/documents; possible copying/-seizure	Often rolling	Require authorization; keep copies/inventory; ensure staff know how to respond; document every request	Disorganized documentation increases arbitrary judgment risk and weakens later objections.
Preliminary findings / meetings	Preliminary/revised findings; exit meeting notes	Usually, short practical windows	Demand the computation basis; rebut in writing; propose agreed facts	These exchanges often shape what becomes the assessment.
Assessment served	Notice of assessment	Objection clock starts	Verify reasons and math; preserve evidence; plan objection	Objection deadline and 1/3rd deposit are strict gating items.
Objection	Notice of objection + documents	30 days; plus, deposit conditions	File within time; attach everything you rely on; pay undisputed/1/3 or seek waiver promptly	Unadmitted objection can finalize the assessment; missing documents can be excluded at appeal.
Appeal chain	TRAB then TRAT then Court of Appeal	Board: 30/45 days; Tribunal: 15/30 days; CAT: law only	Build a clean record; keep grounds consistent; focus on proof and computations	Fresh evidence and new grounds are tightly controlled; Court of Appeal rejects factual appeals.

NAVIGATING THE DIGITAL MINEFIELD: THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN TANZANIAN COURTS

1. INTRODUCTION

The modern corporate world no longer runs strictly on paper trails. Contracts are negotiated on WhatsApp messages, approvals are issued by email, and CCTV footage quietly records events that later become central to disputes. When litigation begins, these digital records later become evidence, yet many organizations discover that crucial records are rejected. The issue is rarely the content itself, but rather the failure to properly present them in court, as any procedural mishap will render them inadmissible.

Tanzania's legal framework has evolved to accommodate the digital evolution through the Electronic Transactions Act, Cap. 442 RE 2023 (ETA), The **Cybercrimes Act CAP. 443 R.E. 2023** and the **Evidence Act Cap. 6 R.E. 2023.** While these reforms provide formal recognition of electronic evidence, they do not grant automatic admissibility. It is therefore crucial for any person relying on digital records to understand the specific legal and procedural requirements involved.

This article examines the legal requirements for admissibility, addresses concerns regarding authenticity, evaluates how courts assess reliability, and offers practical strategies for preserving and presenting digital evidence in Tanzanian courts.

2. THE LEGAL FRAMEWORK FOR ELECTRONIC EVIDENCE

Electronic evidence is now expressly admissible in Tanzania, with the starting point being the **Evidence Act Cap. 6 R.E. 2023**. The Act expands the traditional concept of a "document" under Section 3 to include emails, WhatsApp chats, CCTV footage, computer printouts, and other electronically stored data. This broad definition reflects the realities of modern communication, but it also places a responsibility on litigants to ensure that digital material is properly authenticated before it is relied upon in court. Furthermore, Section 70(1) provides that electronic evidence is admissible in any proceedings, while Section 70 (3) defines such evidence as data stored or retrieved from a computer system. The primary point of evolution is the move from seeing electronic data as an "exception" to the rules of evidence to treating it as a central pillar of modern litigation.

The Electronic Transactions Act, Cap. 442 fundamentally legitimizes digital communications by legally recognizing electronic records as functionally equivalent to traditional physical documents. Furthermore, it strengthens the reliability of digital evidence by establishing strict safeguards such as accessible retention protocols and tamper-evident electronic signatures to guarantee a record's integrity and authenticity before it can be admitted. In practice, this ensures that digital messages are legally binding and fully admissible in court, preventing crucial evidence from being dismissed merely because of its electronic format as long as its origin and reliability can be proven.

The Cybercrimes Act, Cap. 443 completes the framework by regulating how electronic evidence is obtained and preserved. The Act establishes a comprehensive legal framework for the lawful search, seizure, collection, and expedited preservation of fragile digital data, including both traffic and content information. By empowering law enforcement to securely use court-authorized forensic tools and criminalizing the alteration or deletion of data, the Act significantly improves the integrity and reliability

of electronic evidence. In practice, this ensures service providers must cooperate with investigations, allowing authorities to seamlessly authenticate, trace, and utilize digital footprints in legal proceedings while preventing suspects from destroying crucial proof.

Taken together, these three statutes establish a complementary legal framework that governs the admissibility of electronic evidence. The framework addresses the legal requirements for admissibility, highlights concerns relating to authenticity, outlines the manner in which courts assess reliability, and underscores practical considerations for the preservation and presentation of digital evidence before Tanzanian courts.

3. BRIDGING THE FRAMEWORK TO PRACTICAL ANALYSIS

While statutes formally recognize electronic evidence, recognition alone does not guarantee courtroom acceptance. The interplay between statutory law and courtroom practice regarding electronic evidence is indeed a nuanced area of jurisprudence. To put it straightforwardly: the law opens the door, but the court acts as the gatekeeper. Admissibility is dictated by a synergy of both.

Authenticity of Electronic evidence.

The law provides the foundational baseline establishing that electronic records are legally recognizable formats. The Evidence Act, 2023 under section 70(1) explicitly mandates that electronic evidence shall be admissible in any proceedings. To cement the position, Section 19(1) the Electronic Transactions Act Cap 442 RE 2023 establishes that a data message cannot be denied admissibility in legal proceedings solely on the ground that it is a data message. The court plays a highly active, evaluative role before allowing electronic evidence to influence a verdict. The trial magistrate or judge executes this role through several critical functions such as evaluating core dimensions, enforcing preconditions, weighing probative value, scrutinizing the foundation and applying Statutory Guidelines as observed in the case of **Ezekiel Deus @Mvutakamba vs Republic (Criminal Appeal No. 22493 of 2024) [2025] TZHC 2317 (8 May 2025).**

This analysis examines the critical dimensions that determine whether electronic evidence will be admitted and relied upon in court;

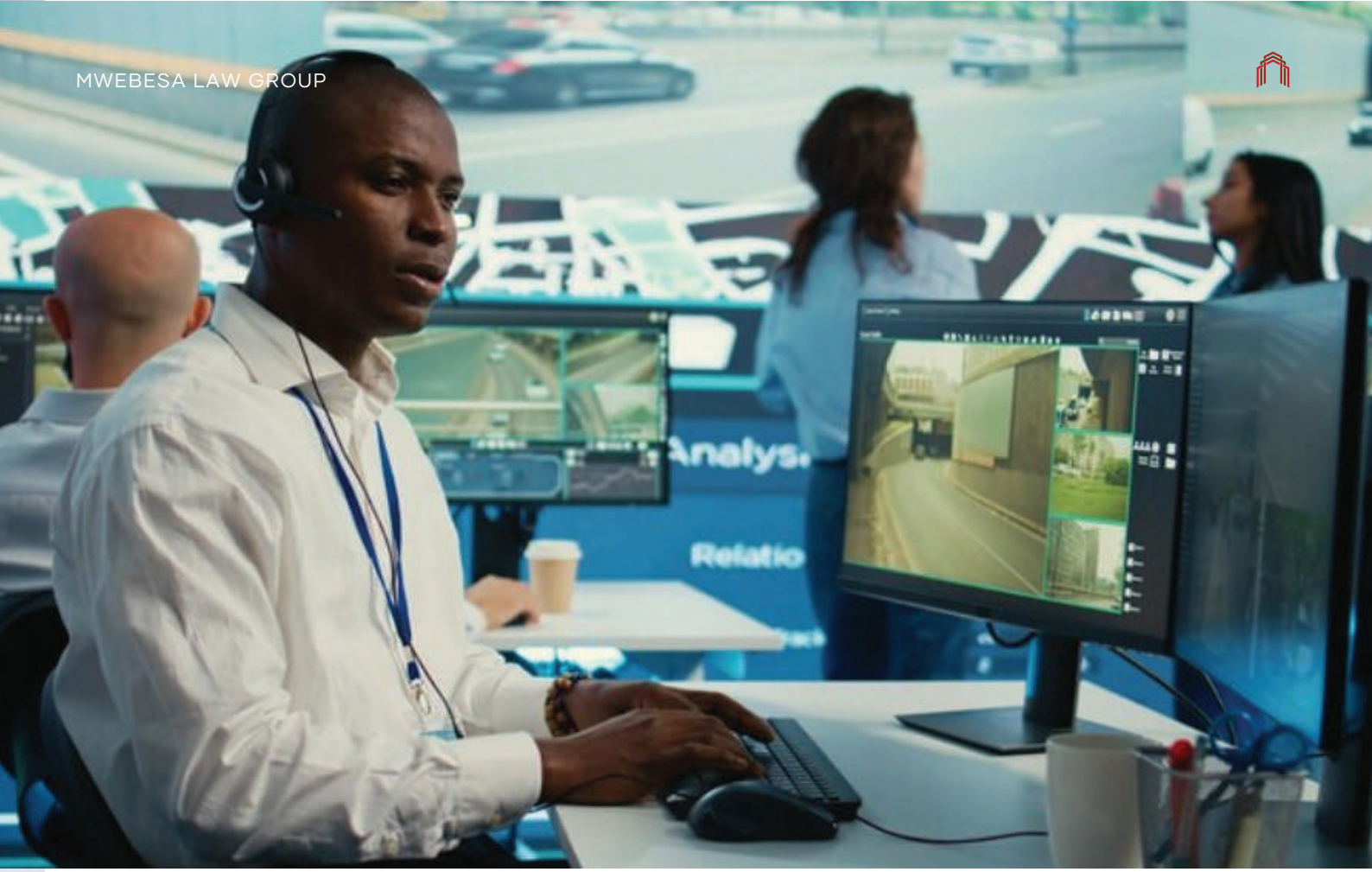
3.1. **Authentication** remains the most significant challenge in admitting electronic evidence. Digital records are inherently fragile as they can be altered, damaged, or deleted with ease. In **Ezekiel Deus @Mvutakamba vs Republic (Criminal Appeal No. 22493 of 2024) [2025] TZHC 2317 (8 May 2025)** it was stated that ""*It is trite law that the authenticity of computer-generated and computer- stored information as part of electronic evidence is potentially open to security vulnerabilities in operating systems and programs that could give rise to the integrity or authenticity of the digital information..... This means that the authenticity of a digital document is a test-checking whether the document, electronic document or data is, in fact, what it claims to be and this test is a pre-condition to the goal of admissibility and determination of evidentiary weight.*"

Further to that, Section 19 of the Electronic Transactions Act (ETA), requires courts to assess the authenticity of electronic evidence through the following steps:

1. **Step 1:** Establishing System Reliability and Proper Operation (ETA Section 19(3)(a).
2. **Step 2:** Proving the Chain of Custody and Data Integrity (ETA Section 19(2)(a)(b).
3. **Step 3:** Verifying the Originator of the Data Message (ETA Section 19(2)(c).
4. **Step 4:** Demonstrating Context, such as creation in the "Ordinary Course of Business" or storage by an adverse party (ETA Section 19(3)(b) and(c).

The decision in **Exim Bank (T) Ltd vs Kilimanjaro Coffee Company Limited (Commercial Case No. 29 of 2011) [2013] TZHC 2683 (28 July 2013)** illustrates the practical application of the above. The court dealt with the admissibility of bank statement, where it required that computer printouts were to be certified true copies, that each print-out must bear a certificate at its foot confirming it is a true copy of an entry contained in the ordinary books of the bank, made in the usual course of business, and that such book remains in the custody or control of the bank and that a certificate must confirm the statements were produced by an electronic process ensuring accuracy, dated and signed by the Principal Accountant or Bank Manager.

The court stated that *"It must be born in mind that electronic evidence must be authenticated because of the potential for unauthorized transaction or of the processing of such evidence. There is also a need to know the history, source and custody of such kind of evidence."* Because these foundational requirements were not satisfied, the electronic evidence



3.2 The Best Evidence Rule and Digital Records

The traditional best evidence rule enshrined under the evidence Act which provides that when proving the contents of a document, the original document must be produced still applies to electronic evidence. This is seen under Sections 69 of the Evidence Act which requires that documents be proved through primary or acceptable secondary evidence. Since electronic records may not have a single "original".

To satisfy the court that an electronic document meets the production requirements, a party must prove that the data's integrity was reliably maintained and that the information is readily accessible for future reference. In practice, it means that organizations must be able to show that an electronic document has been kept safe, unchanged, and can still be accessed when needed. This is usually done through proper IT governance, such as maintaining system logs, using secure electronic signatures, or relying on hash values that help detect any unauthorized changes. The law also recognizes that normal technical processes, like converting a Word document into a PDF, adding server routing details, or automatic "received" timestamps do not affect the authenticity of the document, as long as they do not change its actual content. Just as importantly, the document must remain easy to access and review, which is why evidence should be stored in clear, widely usable formats like PDFs or organized spreadsheets rather than in software that may be difficult for the court or other parties to open.

3.3 Hearsay Considerations

Electronic communications such as emails, WhatsApp messages, and voice notes often raise hearsay issues because they are statements made outside court but relied on to prove the truth of what was said. Example, for a voice note to be admitted, a practical process must be followed. The audio should first be extracted from the phone and saved in an accessible format, then supported by a clear written transcript translated into the court's official language where necessary. The party must also prove who made the recording, for example by recognizing the speaker's voice, confirming the phone number, or showing the context of the conversation. To overcome hearsay objections, the communication must fit within a legal exception, such as being made in the ordinary course of business or where the maker cannot testify because they are deceased, unfit, outside Tanzania, or cannot be found despite reasonable efforts. Where the maker is absent, especially in criminal matters, the transcript should also be served on the other party before the hearing to allow time for objections. By doing this, a simple voice note can be turned into reliable and admissible evidence.

4. Judicial Guidance from Tanzanian Courts

4.1 The High Court in Ezekiel Deus @Mvutakamba vs Republic (Criminal Appeal No. 22493 of 2024) [2025] TZHC 2317 (8 May 2025). The High Court made it clear that electronic evidence cannot simply be produced and accepted at face value. The party relying on it must first show how the data was created, stored, and protected. This usually requires witness testimony explaining the system used, confirming that the document truly came from the claimed source, and proving that it remained authentic and unchanged throughout.

4.2 The Court also emphasized that a conviction cannot stand where the trial court fails to properly evaluate the defence or ignores these strict rules for digital evidence. Simply summarizing evidence without carefully weighing its reliability leads to unfair decisions and a miscarriage of justice. Since electronic records can easily be altered, the prosecution must prove their authenticity and trustworthiness before the court can rely on them. In future cases, parties should establish admissibility from the very beginning by calling a witness with technical knowledge, such as a system administrator or IT officer to explain how the records were generated and retrieved. Just as important, the court must give clear reasons showing that it considered both sides fairly before reaching its decision.

4.3 Similarly, in Lazarus Mirisho Mafie and Another vs Odilo Gasper Kilenga (Commercial Case No. 10 of 2008) [2010] TZHC 725 (1 October 2010), the High Court confirmed that emails are recognized

as documents under the Evidence Act, but they are not automatically admissible in court. The key principle from the case was that authenticity comes first, a party must prove that the email is genuine and truly came from the person claimed before the court can rely on it.

5. PRACTICAL LESSONS

5.1 The admissibility of electronic evidence begins long before litigation. Organizations should preserve native files, maintain metadata, and document the chain of custody to prevent challenges to authenticity. Courts expect parties to demonstrate how evidence was collected and handled, particularly where digital manipulation is possible. When preparing for trial, witnesses familiar with the relevant computer systems should testify about how data was generated, stored, and retrieved. Certified copies confirming system reliability may also be necessary, especially for computer printouts. Relying solely on screenshots is risky because they often omit crucial metadata and are easily challenged.

5.2 Different types of electronic evidence require careful handling. Emails and WhatsApp messages may require proof of authorship, voice notes must be preserved in original form, and CCTV footage requires evidence regarding system accuracy and extraction procedures. Failure to follow these steps can render otherwise compelling evidence unusable.

6. RECOMMENDATIONS

To ensure these legal principles are translated into a seamless corporate workflow, the following refined procedures provide a step-by-step roadmap for maintaining the integrity and admissibility of electronic evidence under Tanzanian law.

6.1 Statutory Data Governance and Retention:

Corporate entities must move beyond passive storage and adopt a Tiered Preservation Matrix to satisfy Sections 5, 6, and 21 of the Electronic Transactions Act. This requires configuring IT environments, such as Office 365 or Google Workspace to "Legal Hold" status, which prevents the permanent deletion of emails and system logs even if a user attempts to purge them. To comply with the Section 21 mandate for integrity, all critical records like CCTV footage and system logs should be centralized in a Write-Once-Read-Many (WORM) environments. Furthermore, IT departments must conduct annual "Restore Tests" to document that archived data remains "accessible and capable of retention" as required by Section 6, ensuring that old files can actually be opened and read when litigation arises.

6.2 Technical Preservation and the Native Format Rule:

Adherence to the "Best Evidence Rule" under Sections 68 to71 of the Evidence Act requires a strict prohibition against relying solely on screenshots, which are often dismissed as unreliable secondary evidence. Instead, organizations must preserve digital files in their native formats (such as .pst for emails or .xlsx for spreadsheets) to protect the underlying metadata, the digital DNA that records IP addresses, edit histories, and timestamps. For high-stakes data, IT personnel should generate a "Cryptographic Hash" (such as SHA-256) immediately upon identifying relevant data. This digital fingerprint allows the legal team to demonstrate, pursuant to Section 19(2) of the Electronic Transactions Act, that the file has remained unchanged from the moment of collection to the moment it is presented in court.

6.3 Formalizing the Chain of Custody:

To satisfy Section 70 of the Evidence Act, which conditions admissibility on the proof of reliability, every piece of electronic evidence must be accompanied by a Digital Evidence Log. This procedural document must record the "who, what, where, and how" of the data collection process, starting from the identification of the source device to its final storage in a secure repository. Access to this repository must be restricted and protected by an automated audit trail that logs every instance the data is viewed or moved. By documenting this unbroken chain, the organization provides the court with the necessary transparency to assess the reliability of the manner in which the data was communicated and stored, as contemplated under Section 19(2) of the Electronic Transactions Act.

6.4 System Integrity and Forensic Standards:

Under Section 19(3) of the Electronic Transactions Act, a court may presume electronic records are authentic if it is shown that the computer system was operating properly. To trigger this presumption, corporate clients must maintain comprehensive System Health Logs that document routine maintenance, security patches, and hardware repairs. When extracting data for litigation, legal teams should bypass general IT workflows in favor of forensic tools that comply with Sections 31 to 35 of the Cybercrimes Act. These tools ensure that "volatile data" information that can be lost if a system is powered down, is captured according to international forensic standards, thereby shielding the evidence from claims of tampering or procedural non-compliance.

6.5 Strategic Litigation Response:

When litigation is anticipated, the transition from routine operations to forensic preservation must be instantaneous. This begins with an immediate internal "Legal Hold" notice to halt all automated data-purging schedules. Legal teams must then collaborate with forensic specialists to perform "Live Acquisitions" under Section 33 of the Cybercrimes Act when dealing with active servers or cloud environments. Finally, any witness called to testify must be prepared to speak not only to the facts contained within the electronic records but also to the security protocols of the systems that generated them. This holistic approach ensures that electronic records satisfy the four pillars of Tanzanian evidentiary law: relevance, authenticity, integrity, and reliability.

7. CONCLUSION

The legal framework now recognizes electronic evidence, but courts require litigants to demonstrate reliability, integrity, and authenticity before such evidence can be relied upon. For corporate clients and other stakeholders, the implication is clear: digital records such as emails, messaging platforms, and system logs must be properly preserved, documented, and authenticated to withstand judicial scrutiny. Proactive data governance, clear retention policies, and proper handling of electronic records can determine whether crucial evidence supports or undermines a case. In the digital minefield of modern litigation, preparation is not a technicality, it is a critical component of effective risk management and successful dispute resolution.

Disclaimer: This article provides general guidance only and does not constitute legal advice. Readers should consult qualified legal practitioners for advice tailored to their specific circumstances.

TRAPPED OR COMPLIANT? THE HIGH STAKES OF CROSS-BORDER FINANCING IN TANZANIA

Cross border financing is the fancy was of saying "getting loan from someone across the map" to help money flow where it is needed most, regardless of where the border lines are drawn. What was historically a relatively open regime for foreign borrowing is now defined by heightened scrutiny over capital inflows, currency usage, and offshore structures. This shift reflects macroeconomic priorities, currency stability, debt monitoring, and domestic monetary sovereignty, but it also introduces structuring complexity for investors and corporates.

LEGAL AND REGULATORY FRAMEWORK

The legal foundations governing cross-border financing in Tanzania are the **Foreign Exchange Act, Cap 271 R.E 2023** and the **Foreign Exchange Regulations, 2022.** The starting point is Regulation 25(1), which is deceptively simple in its wording but far-reaching in its effect. It provides that a resident may access credit accommodation from a non-resident, but only on the condition that the transaction is routed through a bank or financial institution. In practical terms, it means every cross-border financing structure must pass through a regulated intermediary that becomes both a conduit and a checkpoint. The commercial bank is therefore the first line of regulatory enforcement, and if it is not satisfied, the transaction does not move.

This is where Regulation 3 becomes critical, because it expands what counts as "*credit accommodation*" far beyond the narrow idea of a loan. The definition deliberately stretches to capture loans, overdrafts, advances, leasing arrangements, acceptances, performance and bid bonds, letters of credit, guarantees, foreign exchange contracts, and essentially any form of direct or indirect financial obligation. Even unpaid interest is pulled into this net. The implication is that most financial arrangements that create a payment obligation to a non-resident will fall within the regulatory framework, whether parties label them as financing or not.

That breadth closes what might otherwise be seen as structuring loopholes. A company cannot sidestep the regime by recharacterizing a transaction as a guarantee, a supplier credit, or a forex arrangement. If it walks like a financial obligation and creates exposure to a non-resident, it is captured. This is particularly relevant in group structures where intra-company arrangements, treasury support, parent guarantees, or offshore hedging instruments, are often treated casually.

By forcing all such transactions through licensed banks or financial institutions, the system ensures three things at once: visibility of capital flows, enforceability of reporting obligations, and the ability to intervene where necessary. It is through this channel that requirements such as issuance of a Debt Registration Number, and ongoing reporting are operationalized. Without passing through this gateway, a transaction is commercially handicapped, because it cannot be serviced through the formal banking system.

From a structuring perspective, this creates a discipline that businesses must internalize early. Every cross-border financing arrangement must be

designed with the assumption that a Tanzanian bank will interrogate it. Documentation must align with what the bank is required to submit upstream to the regulator. Under Regulation 25(4), the documentation is the substance through which the transaction is assessed. In practice, the required submission typically includes the following:

- **Board Resolutions:**
  Formal resolutions from both the borrower and the lender approving and authorising the financing arrangement on the agreed terms.

- Corporate Profiles:
  Detailed profiles of each party, including ownership structure, governance framework, and nature of business, enabling regulatory assessment of the transaction context

- Executed Financing Agreement:
  The duly signed facility agreement, attested by a licensed lawyer, clearly setting out principal terms, interest, tenure, and conditions.

- Repayment Schedule:
  A structured timetable outlining principal and interest repayments, aligned with the agreed terms and the borrower's projected cash flows. Or where applicable, in the case of a credit line, a tentative drawdown schedule for facilities structured as revolving or tranche-based credit lines.

- Declaration of Source of Funds:
  A formal statement identifying the origin of the funds and confirming their legitimacy and economic basis.

- Security Documents (where applicable):
  Copies of guarantees, debentures, charges, or other instruments creating obligations connected to the facility.

- Late Registration Justification (if applicable):
  A written explanation where submission falls outside the statutory fourteen-day window, addressed to the satisfaction of the Bank of Tanzania.

Yet, even perfect timing and complete documentation do not guarantee success. Regulation 26 introduces a substantive layer of scrutiny that goes to the heart of the transaction. It requires that interest rates and charges reflect prevailing market conditions for the currency of borrowing, effectively imposing an arm's length standard on cross-border financing. It further prohibits loan agreements from including conditions precedent that compel the borrower to open foreign currency accounts outside Tanzania, directly challenging common offshore structuring techniques. Most importantly, it empowers the Bank of Tanzania to refuse registration of any facility that contains unfavourable terms, including those that breach these principles.

The implications become even sharper when one considers how the law treats the character of funds at the time of entry. Regulation 24(2) draws a hard line: funds introduced into Tanzania as equity cannot later be converted into a loan. This provision eliminates what was once a flexible restructuring option and places enormous weight on how transactions are documented at inception. If funds are brought in under share subscription agreements, recorded as equity, and reflected as such in corporate records, that classification is effectively permanent. Any subsequent attempt to recharacterize those funds as debt, through loan agreements or interest-bearing arrangements, runs directly into a regulatory prohibition.

This is where poor structuring at the point of inflow becomes fatal rather than inconvenient. It is not uncommon in practice for parties to move funds quickly as "equity" with an informal intention to later convert them into shareholder loans. Under the current framework, that approach collapses. The banking system and the regulator will look to the original documentation and treatment of the funds. If they entered as equity, they cannot be registered as a loan, cannot obtain a Debt Registration Number, and cannot be serviced as debt through formal channels. The result is commercially trapped capital, funds that cannot be repaid as intended, leaving investors dependent on dividends, themselves subject to profitability and distributable reserves.

Even ambiguity can produce the same outcome. Where documentation at entry is inconsistent or unclear, the system defaults to substance over later assertions. If the initial records point toward equity, the opportunity to restructure is effectively lost. What might have been intended as a flexible funding arrangement becomes rigid, with no clean regulatory pathway to correct it.

CONCLUSION

What emerges, when the provisions are read together, is a system that rewards precision at the point of entry. The practical consequence is that cross-border financing must now be treated as a fully regulated transaction from inception, not as a commercial arrangement to be regularised after the fact. Legal and financial structuring must move in tandem, with documentation prepared not only to reflect the parties' agreement, but to satisfy the regulatory lens through which that agreement will be assessed. In that sense, compliance is no longer a downstream function, it is embedded in the design of the transaction itself.

For practitioners and businesses alike, the shift is subtle but decisive. The question is no longer whether a transaction can be documented to meet the law, but whether it has been conceived in a manner that allows it to pass through the system without friction. Where that discipline is applied early, the framework remains navigable. Where it is deferred, the law offers very limited room for correction.

MWEBESA
LAW GROUP

DAR ES SALAAM (HQ)

House No. 113, Plot No. 948,
Chole Road, Masaki
P. O. Box 23077
Dar es salaam, Tanzania

ZANZIBAR BRANCH

Block 024, Plot No 55
Mbweni Road, Mazizini, Unguja
Zanzibar, Tanzania

For more information:

Phone: +255 767 348 716 / +255 742 812 125
+255 716 955 304

Email: info@mwebesalaw.co.tz

www.mwebesalaw.co.tz

MWEBESA LAW GROUP