

Can I Trust It?

Tips for Evaluating Documents

DD-11 Guide, Version 1.1





Version History

Version	Date	Note
1.0	21 January 2025	First version published.
1.1	5 May 2025	Revised to align with Version 1.5 of the Sustainability Framework .



Preferred by Nature has adopted an “Open Source” policy to share what we develop to advance sustainability. This work is published under the [Creative Commons Attribution Share-Alike 3.0 license](#). Permission is hereby granted, free of charge, to any person obtaining a copy of this document, to deal in the document without restriction, including without limitation the rights to use, copy, modify, merge, publish, and/or distribute copies of the document, subject to the following conditions:

- The above copyright notice and this permission notice shall be included in all copies or substantial portions of the document. We would appreciate receiving a copy of any modified version.
- You must credit Preferred by Nature and include a visible link to our website www.preferredbynature.org.

Disclaimer

The information and guidance presented in this tool are provided for informational purposes only and do not constitute legal, financial, or professional advice. Preferred by Nature, makes no representations or warranties, express or implied, regarding the accuracy, completeness, or suitability of the information contained herein. Preferred by Nature is not liable for the use of guidance contained in this or associated tools, developed using the Sustainability Framework, nor for any reliance placed on this document or any financial or other loss caused because of reliance on information contained herein.

Any interpretation of the content of this tool, or resulting action taken, is at the sole discretion of the reader and does not lead to products with any corresponding claim or label to be considered in conformance with the [EU Deforestation Regulation](#) or any other legal statute and thereby gain access to the EU market without the requirement of the appropriate due diligence. The entity subject to legal obligations retains full discretion and accountability for compliance with requirements under the law.

Content

About this Tool	4
Introduction	4
Tip 1: Check for Obvious Mistakes	5
Tip 2: Check for Spelling Mistakes and Inconsistencies	6
Tip 3: Look out for 'different' Formatting or Text	6
Tip 4: Check Documents against an Official Database.....	7
Tip 5: Use Computer Software to help check PDFs	8
Object Analysis	8
Metadata check.....	9
Pixel analysis.....	10
Tip 6: Use of Electronic Signatures	11
Tip 7: Evaluate Documents Continuously	11
Tip 8: Official Document Templates	11
What to Do if You Suspect Your Document is Fake	12
Authenticity Checks as Part of a Wider Due Diligence Processes	12

About this Tool



About this tool

This tool provides guidance on verifying the integrity and authenticity of documents you might receive from suppliers, as part of your due diligence activities.



Other relevant tools

For further guidance on the topic of information verification see also:

- **Scientific Testing Techniques Guide (DD-12)** to support origin and species identification and provide sample guidelines for scientific testing of wood products.

Introduction

Organisations increasingly find themselves under the microscope when it comes to the authenticity and integrity of documents they receive from suppliers. The developing regulatory landscape, on top of voluntary commitments, has led to organisations facing heightened responsibilities. These obligations necessitate not just the collection of documents and other information as evidence of compliance, but also a rigorous verification of their authenticity.

The necessity for such verification is further underscored by the advent of stringent regulations, such as the [EU Deforestation Regulation](#) (EUDR), which places considerable pressure on certain types of organisations to ensure the integrity of their documentation processes.

This guidance seeks to support organisations in verifying the authenticity of the documents they receive as part of their due diligence processes and ensuring compliance with the evolving regulatory landscape. Due diligence systems invariably rely, in part, on collecting documents to provide evidence of legal or sustainable harvesting of wood products or production of agricultural commodities. Documents may include harvest permits, land tenure certificates, management plans, phytosanitary certificates, VAT invoices, etc. The list goes on.

But are the documents your suppliers are sending to you genuine? Over the years, Preferred by Nature has worked with a number of organisations to help them develop and implement due diligence systems. During this time, we've come across quite a few suspicious documents. This document turns our learning into a series of tips for spotting fake or manipulated documents.

Tip 2: Check for Spelling Mistakes and Inconsistencies

Spelling mistakes are surprisingly common in forgeries. A few spelling mistakes in the parts of a form filled in by a company can be excused, of course, but spelling mistakes in the template form itself are a good indication of forgery.

This document (Figure 3) is another CITES permit from Cameroon where the word 'category' is misspelt as '**carategory**'.

Another example we've seen like this is a (pre-sanctions) Russian forest concession agreement between the state and a timber harvesting company. In addition to being full of spelling mistakes, in one part, the document stated that it was valid for 5 years, whereas in another location it stated that it was valid for 17 years. We concluded that the document was a fake.

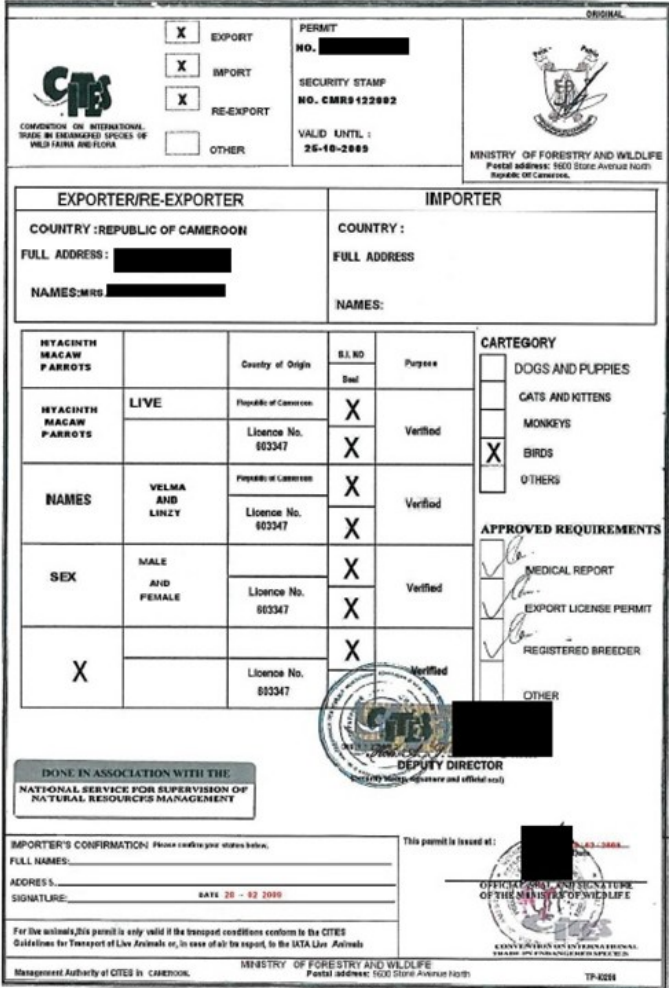
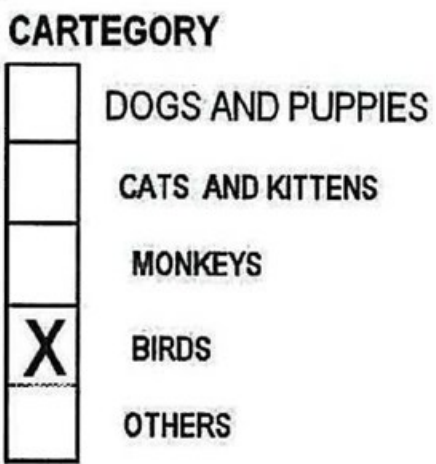



Figure 3: A forged CITES permit from Cameroon, and (right side) an enlargement of the misspelling of category.

Tip 3: Look Out for 'different' Formatting or Text

If a document has been scanned and then doctored, the new text can appear different to the old text: sometimes blurrier, in a different font or with different formatting. Changes like these don't prove that the document is forged. But observations like these should, nonetheless, raise your suspicion.

For example, the document here (Figure 4) is a Certificate of Origin for timber that has allegedly been sent to a company in Vietnam. Yet the company's name and address are in a different font from the rest of the information that has been filled in. Compare 'Vietnam' with 'September 14, 2015' (we have redacted the rest of the name and address to maintain anonymity).

If you come across such documents, we recommend that you:

- Go back to your supplier and ask for clarification, or the correct document to replace the forgery. If the document was previously scanned, then using a different method of copying (such as taking a photograph) may show you whether the image or text that looks odd is present in the original version or not.
- Go directly to the supplier to whom the certificate or officially issued document was issued, the certification body or government authority that issued the document and ask them.



Figure 4: A fake certificate of origin.

Tip 4: Check Documents Against an Official Database

Some documents from some countries can be validated against information contained within an official database. Does the document you've been sent, or the information it contains, appear on the database? Does it have the same details as the one on the database?

Certified organisations and their sustainability certificates can usually be found online. The list below provides some examples:

- [Preferred by Nature Certification](#)
- [FSC](#)
- [PEFC](#)
- [RSPO](#)
- [Sustainable Biomass Program \(SBP\)](#)

Keep in mind that certificate databases mostly just show whether a company is certified or not and sometimes describe which products or materials fall within the scope of the certificate. They do not, for the most part, provide any information on whether the product or material you have purchased was certified.

Overall, centralised official databases are useful and can provide extra assurance that your certificate or officially issued document is genuine. They are limited, however, in what they will tell you. Any document issued by a government authority in a country where the level of governance is low - or there is a known problem of corruption - runs the risk that it could have been issued fraudulently. You could have an authentic document issued, with corrupt practices.

Tip 5: Use Computer Software to Help Check PDFs

If you spot something suspicious in a PDF document, you can try using software(s) to look for evidence of tampering. At this stage, multiple solutions are available, some of them using AI or algorithms capable of a better level of detection of manipulation.

There exists a multitude of different open-source or paid options programmes that can be used to conduct document analysis.

Most solutions can conduct a number of different document verifications, but three key checks should be made: object analysis, metadata checks and pixel analysis. Each of these is discussed below.

Object Analysis

Falsified PDF documents may have one or more layers which overlap. The analysis of those layers is relevant to understanding the level of trust that you could have in a specific document.

A manual check that you could do is in case of scanned documents. A scanned document typically has only one 'object' or 'layer'. In some forged documents, though, you may be able to detect the areas which have been over-written in the form of extra layers or objects.

It is important to note, though, that not all forged documents will have extra layers or objects which are visible. And not all documents with extra objects visible are fakes. Some PDF converters and scanners use text recognition software which can make a PDF look unnatural. This means that if you see extra objects in a PDF, you should not automatically conclude that it is fraudulent. Ask yourself if the extra objects are what a forger would be interested to tamper with. If you ask your supplier to copy the document using a different method and re-send it to you, does it still look odd?

For example, a Vietnamese factory sent a company some documents as evidence that the timber they were buying came from the United States. One of the documents was an invoice that purportedly came from an American company (Figure 5). Preferred by Nature's suspicions were raised about the document because of all the spelling mistakes in it, including in its title (it says 'commercaill invoice' instead of 'commercial invoice'). Additionally, when the PDF was opened, the text in the original layer appeared for a split second, resulting in the company name appearing to change.

We analysed this document (Figure 5) described above and found that almost all of the visible text had been pasted over the text of an older invoice. The only original parts of the document were

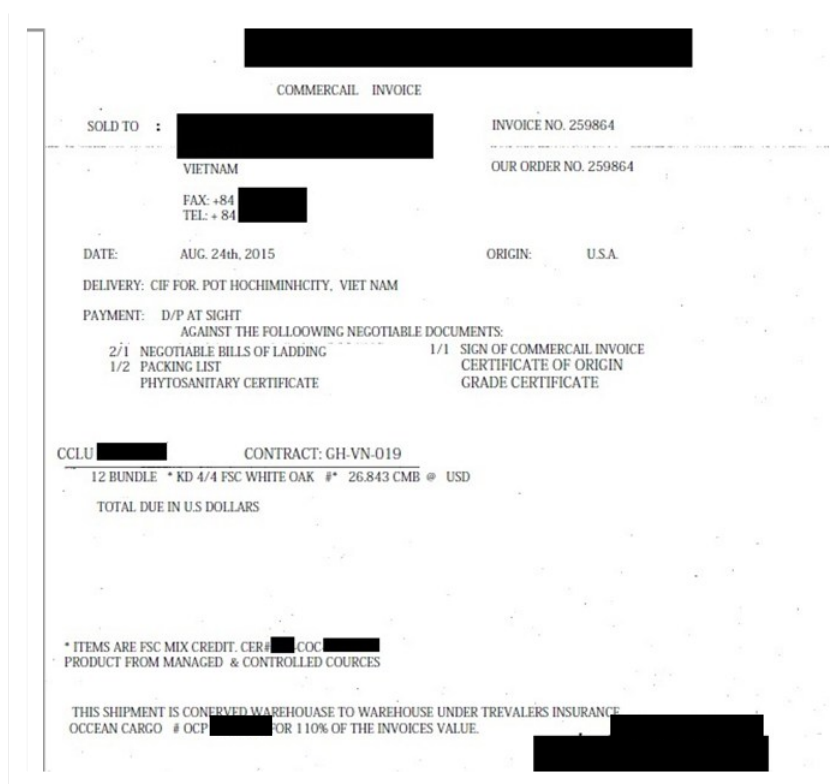


Figure 5: A fake invoice, supposedly from an American company.

the American company's name and logo at the top of the document, and the company president's name and signature at the bottom. The text of the original invoice could be seen: it had been issued from the American company to the Vietnamese company in 2012.

We analysed another document provided by the Vietnamese company using PDF software – a Certificate of Origin (Figure 6; also shown in Figure 4).

As described in Tip 3, we found that the name and address of the company the timber was consigned to was in a different font. Analysis with PDF software also showed that this information was an extra 'object'.

We can't know for sure what happened here, but it seems likely that the Vietnamese company obtained a certificate of origin from another Vietnamese company and forged it to make it appear that it applied to them.

This approach is not entirely foolproof. If a company is adept at altering documents, they could modify the data, print the document, and then scan it anew. This method leaves no trace of the document being tampered with.

Metadata Check

Metadata refers to the underlying data that you won't visibly see within the document itself, but which exists in the background and varies depending on the computer or software that creates it. This hidden layer of information can change when the file is opened or saved in a different computer, and sometimes even by merely copying the files. The relevance of metadata can vary; in some instances, it is crucial, while in others it may not be as significant due to these potential changes. To ensure accuracy and integrity, checks can be performed on the following aspects of metadata:

Creation date



Indicates when the document was originally created.

Verify that the creation date aligns with the expected timeline for the document's issuance. An unexpected creation date can be a red flag for tampering or forgery.

Modification history



Shows when and how often the document has been modified, and by whom.

Frequent or unexplained modifications might suggest unauthorised changes. Consistency in modification dates with the document's lifecycle is crucial.

Author



Identifies the person or entity that created or last modified the document.

Ensure the author's information matches the expected creator. Discrepancies might indicate forgery or unauthorised alterations.

Software used



Details about the software or application used to create or edit the document.

Verify that the software used is appropriate for the document type and consistent with other documents from the same source. Unusual or inconsistent software entries may suggest tampering.

File properties



Includes file size, format, and other technical details.

Compare these properties with other known authentic documents to identify anomalies. Drastic differences might indicate manipulation.

Digital signatures



Contains information about any digital signatures applied to the document.

Check the validity and authenticity of digital signatures to confirm that the document has not been altered after signing.

Pixel Analysis

Pixel analysis is a highly effective method for investigating and interpreting digital images, particularly useful in cases where data integrity is in question. At its core, a pixel is the smallest unit of a digital image, representing a single point of colour. When examined closely, these tiny elements can reveal a wealth of information about the image's authenticity and any alterations it may have undergone.

By conducting a thorough pixel analysis, you can detect subtle changes and anomalies that might indicate tampering. This process involves a meticulous examination of pixel patterns, colours, and distributions. For instance, inconsistencies in the pixel arrangement or unexpected colour shifts can suggest that parts of the image have been edited or manipulated. Such irregularities are often invisible to the naked eye but become apparent under detailed scrutiny.

Pixel analysis can also be used to verify the originality of an image. In digital forensics, this technique is essential for determining whether an image has been altered since its creation. By comparing the pixel structure of a suspected tampered image to that of a known original, forensic analysts can identify discrepancies that signal digital modifications.

CERTIFICATE OF ORIGIN

The undersigned **[REDACTED]** President
ITL, LLC dba **[REDACTED]** (Please print name and title)
for **[REDACTED]** declares
that the following mentioned goods shipped on S/S **[REDACTED]** (Name of Ship)
on the date of **SEPTEMBER 14, 2015** consigned to **[REDACTED]**
[REDACTED] Viet Nam
are the product of the United States of America.

MARKS AND NUMBERS	NO. OF PKGS., BOXES OR CASES	WEIGHT IN KILOS		DESCRIPTION
		GROSS	NET	
TGHU-6226203 17670 GO-VN-005	12 BDLS	24,369		AMERICAN HARDWOOD LUMBER 3/4 WHITE OAK COMSEL KILN DRIED
	12 BDLS	24,369		

CERTIFICATE OF ORIGIN

Sworn to **[REDACTED]** Dated at **[REDACTED]** on the **23RD** day of **SEPTEMBER 2015**
this **[REDACTED]** **CHAMBER OF COMMERCE** **[REDACTED]**
OHIO (Signature of Chamber of Commerce)

The **[REDACTED]**, a recognized Chamber of Commerce under the laws of the State of **[REDACTED]**
We hereby certify to the best of our knowledge and belief, finds that the products named originated in the
United States of North America
contained are true and correct.
Secretary **[REDACTED]**
Bachwood Chamber of Commerce, OH, U.S.A.

Form 10-900 P Printed and Sold by ENZCO, 190 Baldwin Ave., Jersey City, NJ 07308 • (800) 631-3098 • (201) 795-6400

Figure 6: A fake certificate of origin, supposedly from an American company.

Tip 6: Use of Electronic Signatures

It is highly recommended that documents prepared by suppliers should consistently utilise electronic signatures wherever this option is available. Employing an electronic signature adds an additional layer of verification, ensuring the document's authenticity and confirming it was indeed generated by the specified company. This practice not only enhances the reliability of the documentation but also significantly reduces the risk of unauthorised alterations or forgeries.

By adopting electronic signatures, businesses can streamline their verification processes, establishing a more secure and efficient method for confirming the legitimacy of documents received from suppliers. This measure not only strengthens the integrity of the business transactions but also fosters a more trustworthy relationship between parties.

Note that the use of digital signatures cannot protect fully against all types of fraud, but it does add a layer of trust between the parties, like the use of signatures on physical documents.

Tip 7: Evaluate Documents Continuously

Occasionally, it's possible to identify tampered documents by comparing them with other documents received from suppliers earlier. Often, the tampering involves using the same template or background while only altering the data presented in the document. In one instance, we observed that a supplier had consistently reused an official template's background over several years, with only the numerical data being modified.

This repetitive use of a specific background, including creases and shading in the paper, present in documents spanning multiple years, was a key indicator that led to the detection of document tampering. Such observations underscore the importance of meticulous document scrutiny, as subtle consistencies can reveal unauthorised alterations.



Tip 8: Official Document Templates

It is important to ensure that any document received from a supplier adheres to the official template prescribed for that particular region and country. Suppliers might prepare documents that fail to comply with the legally mandated templates. These deviations can range from minor layout changes to significant discrepancies in the format required by regulatory authorities.

Preferred by Nature advises that you familiarise yourself with the specific details and elements that constitute the official template, including logos, font types, and required information fields, to accurately assess the document's authenticity. Moreover, understanding the legal implications of accepting documents that do not meet the standard requirements is important. These due diligence measures not only aid in maintaining regulatory compliance but also safeguard against the potential legal and financial repercussions of accepting improperly formatted documents.

Establishing a routine verification process to compare received documents against official templates can prevent unintentional acceptance of non-compliant documents, thereby ensuring that all transactions and interactions with suppliers remain above board and within the bounds of legal standards.

What to Do if You Suspect Your Document is Fake

If you're suspicious about a document that you've been sent, we recommend that you:



Go back to the supplier who sent you the document and ask for additional information or an additional document that would help you confirm (or otherwise) the authenticity of the suspect document. For example, if you suspect that an invoice is fake, then other official documents that relay financial transactions (e.g., a bank statement, or an official database) may help.



If possible, **ask them to resend the document** in a different format (e.g. photograph) or with a better quality.



Go directly to the supplier to which the official document was issued, the certification body or government authority that issued the document and ask them if they can send you an example of what the document should look like. Or ask them to confirm whether the document you have is genuine or not.



Cross-check the information on the suspicious document with other information or documents. If the same information appears on documents issued by different authorities, you can be sure that your document is genuine.



Understand the implications of fake documents and why the supplier might be incentivised to falsify the document. Ask your supplier if they can explain why the document you have looks weird or conduct a short-notice on-site audit to prevent new forgeries from taking place.



If you're **still not convinced** that the document is genuine, **you should not employ the document** as part of your risk assessment and risk mitigation measures. Additionally, make sure that any future consignments from the same supplier are analysed with additional care.

Authenticity Checks as Part of a Wider Due Diligence Processes

When organisations rely on documents, it is imperative for them to incorporate into their due diligence systems a component related to checking their authenticity. This component could be integrated under different layers of due diligence, from individual assessments of supply chains to periodic checks of representative samples of documents.

Preferred by Nature recommends a structured approach for organisations to verify the authenticity of the documents they receive and ensure compliance with the evolving regulatory landscape.

Introducing a system of *authenticity checks* for documents helps to evaluate and categorise the authenticity of a particular set of documents received from a supplier¹.

The authenticity check could be implemented for sampled document packages sent by suppliers and by implementing a scoring system, such as those categories below:

A. Authentic Document

Document checked using a third-party method and confirmed as valid.

A.1. Certificate checked and valid under the scheme database.

A.2. Document checked and valid under a national, regional or other official database.

E.g. Timber - Phytosanitary certificates from the US; Timber waybills from Romania; Harvest permits from Romania.

E.g. Certificate of origin issued from a chamber part of the International Chamber of Commerce.

A.3. Document with a verified electronic signature document.²

B. Likely to be Authentic

Document which could not be included under A or D and indirectly confirmed through other methods.

B.1. Indirectly validated - In the package of documents, another document is included under category A against which the original document can be validated.

B.2. On-site audit with volume reconciliation

E.g. a package of documents is assessed by an organisation (third/second party) and concluded with negligible risk. Assessment could be conducted for all documents or partially using sampling methods.

B.3. Information confirmed through a scientific method.

E.g. timber test that can confirm species and origin.

C. Unverified

There is no evidence of tampered and/or no way to check the authenticity.

D. Likely to be Tampered

Some information may be subject to alteration, although there is no definitive proof to categorise the document as Category E.

D.1. Copy/picture of scanned documents or pictures of copies.

D.2. Document with multiple formatting and/or text that is visually blurry (Tip 3).

D.3. Indirectly associated with tampering - another document is included under category E in the package of documents.

¹ NOTE: Authenticity checks for documents focus on the authenticity aspect without delving into the specifics of how each document was issued. It's a recognised challenge that in regions with weaker governance structures, documents that appear authentic can be obtained through corrupt practices. To fully ensure the reliability of the supplier's claims, additional verification steps may be necessary.

² This method will verify that the document was created by the entity that signed it. If it is signed by the company, it means that company made that statement. If a company put electronic signature on a harvesting permit, it does not mean that harvesting permit is authentic. Harvest permit is authentic just in case that the state authority will add the electronic signature.

E. Tampered

Document with clear evidence that it has been altered or that fraudulent manipulation has taken place.

- E.1. Document with obvious mistakes (Tip 1).
- E.2. Document with spelling mistakes and inconsistencies (Tip 2).
- E.3. Document with multiple layers where you could see hidden data (Tip 5).
- E.4. Document not under the official template (Tip 8).
- E.5. Other clear evidence that a document is forged (e.g. Tip 7).



Preferred by Nature is an international non-profit organisation working to support better land management and business practices that benefit people, nature and climate. We do this through a unique combination of sustainability certification services, projects supporting awareness raising, and capacity building.

With 30 years of experience, we have worked to develop practical solutions to drive positive impacts in production landscapes and supply chains in 100+ countries. We focus on land use, primarily through forest, agriculture and climate impact commodities, and related sectors such as tourism.

www.preferredbynature.org