

Export Controls Due Diligence

“Houston, we have a problem” – Apollo 13

What is “due diligence”?

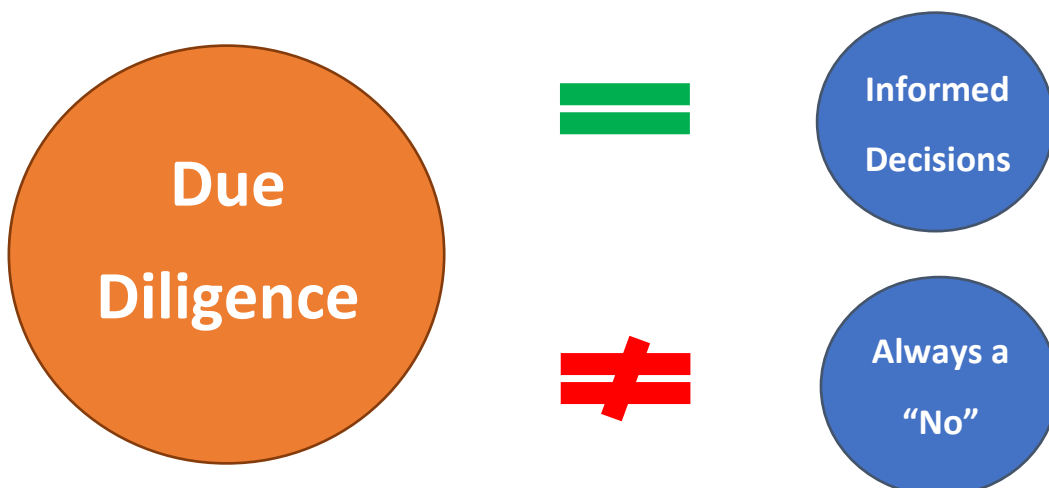
Due diligence is the “reasonable” steps a business undertakes to establish the potential risks and liabilities within a business transaction to establish confidence in its legality and legitimacy.

Though due diligence can seem to be time consuming, over the top and inconvenient for personnel, the hard truth is that it only takes one slip-up or occasion of lapse in attention to make a costly mistake. Ultimately, due diligence assists you to:

- Identify, investigate, evaluate and verify all information and business intelligence,
- Determine which transactions or potential business activities require further information/analysis,
- Better understand your business partners, employees, visitors and transactions,
- Ensure compliance standards,
- Analyse and minimise potential legal exposure risks and costs, and
- Protect yourself from regulatory and reputational risks.

Comprehensive due diligence is not just something nice to highlight within your ethics commitment statement or treat as a rubber-stamping exercise – it means doing your homework and being prepared to back up.

The results of due diligence do not always mean a “no” is coming, it just allows a business to make better-informed decisions as to whether the additional work to complete the analysis is worth the potential benefits and/or to put into place the required protection measures (i.e. “Chinese walls”, contractual arrangements, etc).



Is it a legal requirement?

Though due diligence is not always contained within all countries' export control regulations, practically it is difficult if not impossible to comply with the many regulatory requirements, such as end-use and catch-all controls, without comprehensive due diligence processes in place. Some governments include due diligence requirements within their legislation, such as requirements to inform them if you "know or suspect" certain information or receive a verified Denied/Restricted Party Screening hits – even if you choose not to proceed with the transaction. Other legal requirements are not always defined, such as the term "reasonable".

Another consideration is a government expectation, especially in the context of potential mitigating factors during a legal investigation, versus a written legal regulation. These include the guidance governments issue, such as "Red Flags", as well as advice services. Always be prepared to explain and defend yourself with regards to any decision – this is known as the courtroom test. Additionally, anything you miss or fail to prevent could affect the rest of the supply chain potentially resulting in reputational damage, legal and contractual fines and penalties, loss of contracts and customer dissatisfaction.

What do we need to do?



Like any element of a compliance programme, due diligence awareness and processes should be documented and implemented within your commitment statement, procedures, training programmes, and recordkeeping policies.

Ignorance is not bliss. Choosing to not ask the right questions or ignore potential warning signs does not absolve you of you. Most investigations show that situations of violations are due to the lack of insufficient due diligence having been carried out - the business should have known as the indications of risks were there.

All business partners are required to provide information with regards to your legal due diligence as well as their own. It is best to receive written confirmations to queries rather than oral assurances for your own records.

No customer should be taken aback by due diligence questions as they are responsible for their own due diligence. Always challenge excuses not to answer questions such as IP concerns, revealing ultimate customers which you may target directly, government security classifications, etc. There are always ways to provide assurances to due diligence queries in accordance with concerns.

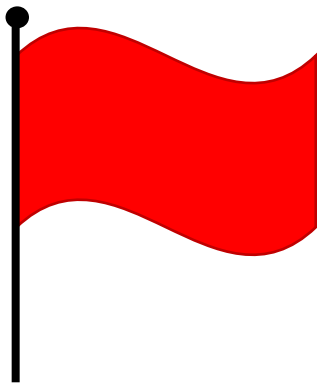
In addition to the procedures and training, **a critical element of due diligence is the empowerment of personnel to raise concerns and be able to say "no".**

Export controls due diligence should be imbedded within the culture of the business like with any other compliance programme – though you might find push-back and complaints that “export controls is taking over” or “costing business”. Some people just don’t like change, but with training and support you can encourage a more seamless integration within business practices.



Once you establish your due diligence processes, keep re-examining, testing and evaluating them. Parties and entities who are trying to circumvent the current controls are constantly changing tactics in the event to make transactions look legitimate or choosing potential sourcing targets based on perceived weakness in their processes. Always remain vigilant – complacency negates compliance efforts and you never want to be the “one”. If in doubt...ask.

No transaction is identical and there is no “one size fits all” guidance document. However, every business has due diligence allies in key departments within the business, such as sales, contracts and purchasing personnel. They are the “front line” defence for your business and will usually be the first to encounter potential risks or concerns due to their business function and their experience as to what is “normal”. Whilst there is a conflict of interest for the sales or purchasing function to be responsible for the overall export control programme within a business, these departments are vital in their ability to spot potential issues so that they can be escalated and resolved in accordance with due diligence procedures.



All personnel will know when something does not feel “right”, even if they cannot pinpoint exactly why. By providing that commitment and support, personnel can feel empowered to identify and raise any “red flags” to the appropriate persons for resolution. Never ignore that sixth sense – your gut is usually correct.

If you are identifying patterns of targeting or attempts through your due diligence process, it might be worth discussing these with the export control authorities for intelligence purposes.

What if something happens?

It is important to distinguish between a “near miss” and a violation, though both can give your heart palpitations. Near misses may need to be reported, though no violation has occurred, so it is best to understand potential reporting requirements. If a violation occurs, an investigation should be conducted to understand the root cause(s) of the violation, determine comprehensive corrective actions, draft and submit your voluntary disclosure, and track corrective actions to completion/implementation.

Both near misses and violations are opportunities to learn from mistakes and show the business what can happen. “Lessons learned” should be communicated to the business, outlining the root causes, the cost to the business, and changes or updates to processes and training.

How it could go wrong – 3 Case Studies

#1 – Email address should have been the first “Red Flag”

An aftermarket site of a major multinational manufacturer receives an initial enquiry email from a potential new customer looking to purchase maintenance technical manuals and spare parts. The email appeared to be a normal request from a potential customer in their industry.

Denied/Restricted Party Screening was conducted on the name of the company provided and there was no “hit”. After confirmation of no “hit”, pricing for the technical manuals and spare parts was provided to the contact. Only once the contact agreed to the pricing and provided the delivery address, for Iran, did the sales person realise that they had potentially contravened sanctions regulations (of that time) – this matter was escalated internally for investigation and resolution.

Internal investigations into the incident found several issues which led to the violation, which was confirmed to occur under the sanctions regulations. Firstly, the sales person did not closely look at the email address of the potential customer – the email address ended with the Iranian country code domain (“.ir”). In addition, if initial checks into the company name were carried out before responding the sales person would have identified that the company was based in Iran. To make matters worse, it had been identified internally that Iranian companies were contacting sites within the multinational in various countries attempting to purchase manuals and spare parts and an internal communication had been sent out to alert the sites of this.

Due to the lack of attention to detail and basic checks the company potentially contravened sanctions against Iran and could have received a penalty for their actions.

#2 – Unnerving social media posts

A growing SME receives a request to buy source material in order to manufacture parts for their customers. Screening, credit and basic KYC checks are performed, and end-use statements are obtained per company export control procedures. The company and all information obtained about the transaction appears legitimate, but an employee still has a feeling that something is not “right”.

After escalating their concerns to senior management, more thorough checks of the company are conducted. To their shock, the new potential customer’s twitter feed contains statements of support for ISIS and even shows a propaganda photo of the ISIS flag.

Due to the employee’s trust in their gut and their empowerment and support to raise concerns for resolution the SME did not conduct a transaction with a potential supporter of terrorist activities.

#3 – “But, what is it going to be used for?”

A metals company receives an order from a well-known OEM who wants a specialist alloy tube cut to specified dimensions. After the initial due diligence checks, the metals company requested end-use information for the tube as the alloy being requested is known to be used in the aerospace and defence industries.

At first, the OEM was reluctant to provide end-use information citing concerns that the metals company would go around them to the final customer. Then the OEM stated that government security classifications made it impossible to provide the requested information. This new rebuttal was challenged by the metals company numerous times, escalating the matter as required. Eventually the OEM provided a written and signed End-Use Certificate stating the final end-user and the end-use, which was a missile.

Whilst the end-use and end-user information was obtained and verified, it led the company to re-evaluate the ECCN classification of the tube they were manufacturing, in accordance with national export control regulations, and obtain an export licence.

How can Customs Connect help?

At Customs Connect, we assist companies to:

Understand their
due diligence
requirements and
expectations

Audit their
processes and
procedures

Draft due
diligence
processes

Draft and deliver
training
programmes

Assist with
investigations and
voluntary
disclosures

If you are interested in learning more about Due Diligence or how we could assist you, please visit our website <https://customsconnect.co.uk/> or give us a call on +44 (0)845 519 0878.