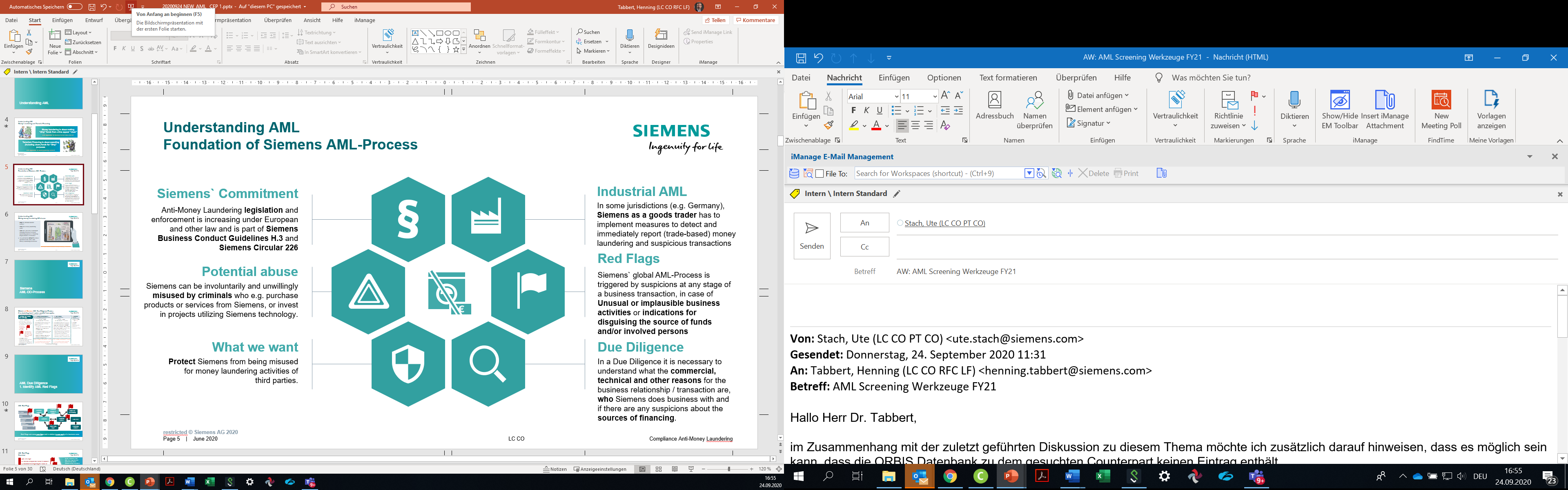
C. Anti-Money Laundering (AML)

Delivery and supply activities entail the risk of being abused for money laundering or terrorist financing. Siemens strives to maintain business relationships only with reputable customers, partners, and companies whose business activities comply with legal requirements and whose financial resources are not of illegitimate origin.

The global Siemens Anti-Money Laundering (AML) System focusses on the Siemens goods trading business and aims at combating money laundering and terrorism financing by creating the necessary transparency in business conducted with **Counterparts**[[1]](#footnote-2). It consists of the following obligations, unless stricter local / sector specific legal requirements must be complied with:

|  |
| --- |
| **Fundamental Principles and Rules of our BCG - H3: This is what we do:**   * We use a risk-based approach to verify the identity and economic background of customers, business partners, and other third parties, and the origin of payments to ensure they come from legitimate sources. * We immediately inform Legal and Compliance or our manager in the event of suspicious activity. When necessary, Siemens reports suspicious activity to law enforcement authorities. |
| **In addition to the fundamental principles and rules of our BCG, the following applies:**   * In case of an indication of money laundering or terrorism financing (“AML Red Flag”, [Chapter C.1.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),1.-AML-Red-Flags)) in relation to a Counterpart, its Business Model, the Transaction / Financing e.g.   + Unusual or implausible business activities or   + Indications for disguising the source of funds and/or involved persons   or even a concrete suspicion of money laundering or terrorism financing, the responsible Compliance Officer must be informed[[2]](#footnote-3) and an AML-specific Due Diligence (AML DD) must be performed ([Chapter C. 2](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),2.-AML-Due-Diligence).) before entering into, or continuing with a business relationship or performing any transaction with a Counterpart.   * Where required by local / sector specific AML regulations, additional or deviating measures might have to be taken ([Chapter C.3.](#_3._Local_/)). * If an AML DD required by law cannot be performed, performing transactions and entering into or continuing a business relationship are generally prohibited. The same applies when the Compliance Organization issues a respective instruction ([Chapter C. 4](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),4.--Prohibited-transactions-or-business-relationships)). * The cash handling rules for incoming and outgoing cash payments according to [Siemens Circular 208 “Treasury Transactions in the Company“](file:///C:/Users/z003a3vj/Downloads/SC_208.pdf) must be adhered to (as a general rule prohibited at or above 10,000 EUR; further details see [Chapter C.5.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),5.-Cash-Handling-Rules)). |



# 1. AML Red Flags

Unless stricter local / sector specific legal requirements must be complied with ([Chapter C.3.](#_3._Local_/)), the existence of an AML Red Flag requires contacting the responsible Compliance Officer so he or she can start a AML Due Diligence with the support of the business ([Chapter C. 2](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering,2.-AML-Due-Diligence)).

AML Red Flags describe circumstances that could be seen asindicationof money laundering or terrorism financing such as

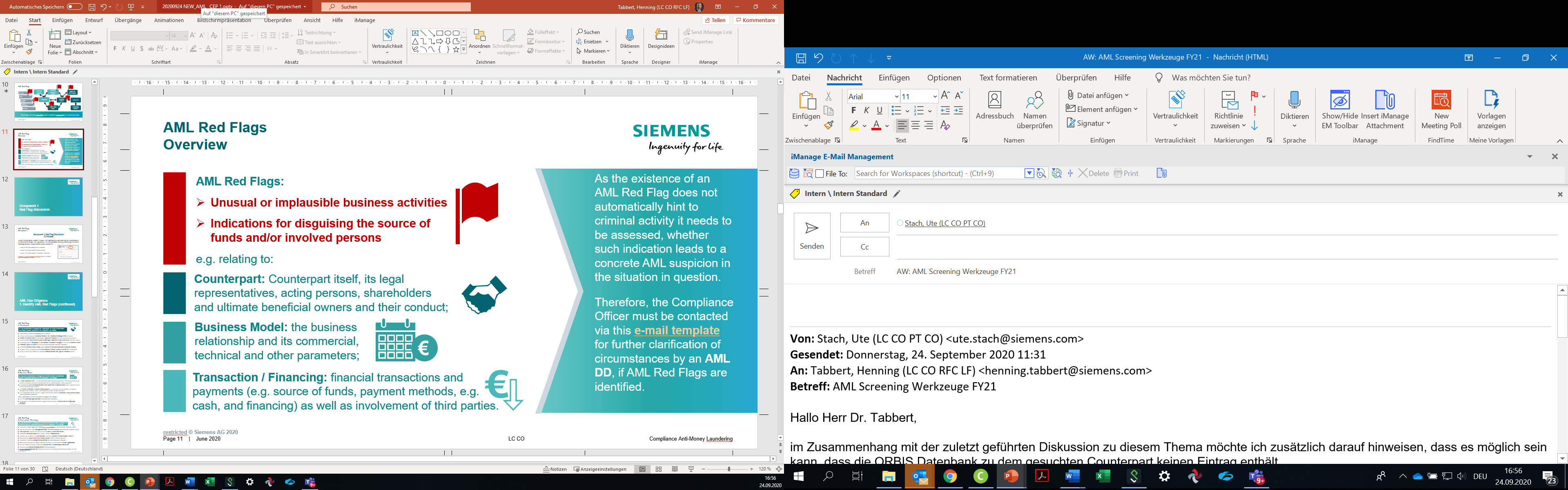
AML Red Flag: Unusual or implausible business activities

AML Red Flag: Indications for disguising the source of funds and/or involved persons

Above AML Red Flags may relate to the

* **Counterpart:** The Counterpart[[3]](#footnote-4) itself, its representatives and ultimate beneficial owners and their conduct.
* **Business Model:** The business relationship and its commercial, technical and other parameters.
* **Transaction / Financing:** Thefinancial transactions and payments (e.g. source of funds, payment methods, e.g. cash, and financing) as well as the involvement of third parties.

As the existence of an AML Red Flags does not automatically hint to criminal activity it needs to be assessed, whether such indication leads to a concrete AML suspicion in the situation in question. Therefore, the Compliance Officer must be contacted for further clarification of circumstances by an AML DD, if AML Red Flags are identified.



## 1.1. AML Red Flag Examples

AML Red Flag: Unusual or implausible business activities, e.g.:

* **Counterpart:**
  + Counterpart **founded only recently, lacks expertise** in his claimed field of business;
  + Location of office or bank account has **no relation to residence or place of business** of Counterpart;
  + Counterpart has **questionable reputation / integrity** or even **known criminal records**;
  + **Politically Exposed Person (PEP)[[4]](#footnote-5)** involved without plausible legitimate explanation;
* **Business Model:**
  + Planned business not consistent with **Counterparts` regular field** **of business**.
  + It “**lacks economic sense**”, e.g. unusually high margin, high upfront payments, other unusual terms to the benefit of Siemens or business is questionable from a technical, logistic or other perspective;
  + Counterpart has low sensitivity and interest to commercial / technical details with no apparent reason (such as an urgent spare delivery).
* **Transaction / Financing**
  + Planned business **not consistent** with Counterparts` financial situation
  + **Cash payments / deposit** onto Siemens’ account **above Siemens thresholds[[5]](#footnote-6);**

AML Red Flag: Indications for disguising the source of funds and/or involved persons, e.g.:

* **Counterpart:**
  + Counterpart is a letter box company**[[6]](#footnote-7)** (shell company) and / or has a complex and in-transparent **company structure,**
  + **role / function of acting persons** is unclear; **legal representatives[[7]](#footnote-8)** seem to avoid personal contacts**;**
  + Usual information **not provided, provided data vague, difficult to verify or not in line** with other sources;
* **Business Model:**
  + Business structure is **unnecessarily complex**, e.g. it involves several companies or suppliers through several countries, where a direct business would be feasible and easier;
  + Counterpart requests a service / supplies from Siemens, which he **could have easily sourced locally,** without a plausible explanation.
* **Transaction / Financing**
* Transaction **unusually complex**, the source of funds is **in-transparent**;
* Transaction via **AML High Risk Country[[8]](#footnote-9)** without plausible legitimate reason;
* Payments[[9]](#footnote-10) proposed / made **through third party** / **letterbox company[[10]](#footnote-11)** without plausible legitimate reason or **split and / or from multiple sources**;
* Transaction or financing **changed unexpectedly** and without plausible explanation;
* Payment **exceeds amounts due / are unrequested**, followed by request for reimbursement, sometimes also to different country / account.
* Payments using **informal banking systems** ([Hawala Banking](https://en.wikipedia.org/wiki/Hawala));

## 1.2. Letterbox company

A letter box company often shows at least some of the following indicators:

* no or no **sufficient personnel, office resources or financial background** for business transaction;
* a business address that is **shared by numerous other companies**, avoids to reveal address;
* **lacks expertise** in his claimed field of business, has **no visible (lawful) business activity or income**;
* legal representatives **exercise similar functions** in many other companies;
* administered by a law firm or other firm **known to be administrating letter box companies**;
* located in an **AML High Risk Country[[11]](#footnote-12)**.

## 1.3. AML High Risk Countries

The involvement of an AML High Risk Country is only considered an AML Red Flag if there is no plausible legitimate explanation.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Afghanistan** | AML HRC (EU) | **Grenada** | OFC (EU) | **Niue** | OFC (EU) |
| **Albania** | AML HRC (FATF) | **Guernsey** | OFC (EU) | **Pakistan** | AML HRC (EU / FATF) |
| **Andorra** | OFC (EU) | **Hong Kong** | OFC (EU) | **Panama** | AML HRC (EU / FATF), OFC (EU) |
| **Anguilla** | OFC (EU) | **Iran** | AML HRC (EU / FATF) | **Philippines** | OFC (EU) |
| **Antigua and Barbuda** | OFC (EU) | **Iraq** | AML HRC (EU) | **Saint Lucia** | OFC (EU) |
| **Aruba** | OFC (EU) | **Isle of Man** | OFC (EU) | **Seychelles** | OFC (EU) |
| **Bahamas** | AML HRC (EU); OFC (EU) | **Jamaica** | AML HRC (EU / FATF) | **Singapore** | OFC (EU) |
| **Bahrain** | OFC (EU) | **Jersey** | OFC (EU) | **Sint Maarten** | OFC (EU) |
| **Barbados** | AML HRC (EU / FATF), OFC (EU) | **Korea, North** | AML HRC (EU / FATF) | **St. Kitts and Nevis** | OFC (EU) |
| **Belize** | OFC (EU) | **Lebanon** | OFC (EU) | **Syria** | AML HRC (EU / FATF) |
| **Bermuda** | OFC (EU) | **Liberia** | OFC (EU) | **Trinidad and Tobago** | AML HRC (EU) |
| **Botswana** | AML HRC (EU / FATF) | **Liechtenstein** | OFC (EU) | **Turks and Caicos Islands** | OFC (EU) |
| **British Virgin Islands** | OFC (EU) | **Marshall Islands** | OFC (EU) | **Uganda** | AML HRC (EU / FATF) |
| **Cambodia** | AML HRC (EU / FATF) | **Mauritius** | AML HRC (EU / FATF), OFC (EU) | **US Virgin Islands** | OFC (EU) |
| **Cayman Islands** | OFC (EU) | **Montserrat** | OFC (EU) | **Vanuatu** | AML HRC (EU), OFC (EU) |
| **Cook Islands** | OFC (EU) | **Myanmar** | AML HRC (EU / FATF) | **Yemen** | AML HRC (EU / FATF) |
| **Curacao** | OFC (EU) | **Nauru** | OFC (EU) | **Zimbabwe** | AML HRC (EU / FATF) |
| **Dominica** | OFC (EU) | **Nicaragua** | AML HRC (EU / FATF) |  |  |
| **Ghana** | AML HRC (EU / FATF) | **Saint Vincent and the Grenadines** | OFC (EU) |  |  |
| **Gibraltar** | OFC (EU) | **Samoa** | OFC (EU) |  |  |

The internal Siemens list of AML High Risk Countries is based on the following three official sources. As Siemens for its core business as an industrial company (“goods trading”) is generally not obliged to strictly apply those lists (in contrast e.g. to the financial sector), the updates of the consolidated Siemens might deviate slightly from official enactments by the referenced institutions.

1. AML HRC = AML High Risk Country
   1. EU: [Commission Delegated Regulation (EU) 2020/855 of 7 May 2020](https://eur-lex.europa.eu/eli/reg_del/2020/855/oj) amending [Delegated Regulation (EU) 2016/1675 of 14 July 2016](http://data.europa.eu/eli/reg_del/2016/1675/2018-10-22)
   2. FATF: [Call for action](http://www.fatf-gafi.org/countries/#high-risk) and [other monitored jurisdictions](http://www.fatf-gafi.org/countries/#other-monitored-jurisdictions)
2. OFC (EU) = Offshore Financial Center according to [EU statistical office Eurostat](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:List_of_offshore_financial_centres)

**Status: 1 April 2021**

Changes relating to last version (1 January 2021) of consolidated list:

* **Deleted:** Mongolia

# 2. AML Due Diligence

Unless stricter local / sector specific legal requirements must be complied with ([Chapter C.3.](#_3._Local_/)), the existence of an AML Red Flag ([Chapter C.1.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering,1.-AML-Red-Flags)) requires contacting the responsible Compliance Officer so he or she can start a AML Due Diligence with the support of the business.

AML Red Flags describe typical situations, that bear a higher AML risk. The goal of the AML DD is to assess, whether an AML Red Flag - meaning a factual constellation that **typically** indicates a high AML risk - also means that the **concrete situation** bears a high AML risk. Therefore, it needs to be checked whether the concrete situation that triggered an AML Red Flag

* **leads to a concrete AML suspicion or**
* **we can be reasonably confident (after mitigation measures) that counterparts` funds are not related to criminal activities**

Following this goal, the completion of an AML DD comprises of the following steps:

Step 1: Clarify Circumstances to

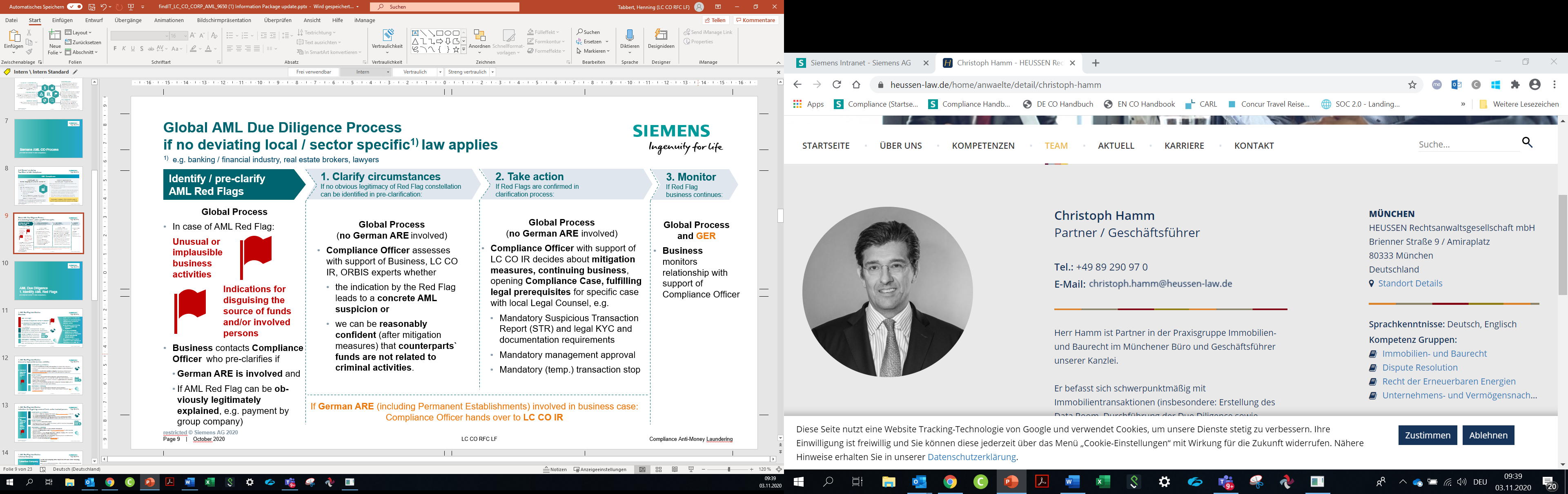
* Know and transparently understand the **commercial, technical and other reasons** for the business relationship / transaction and its form.
* Know and transparently understand **who Siemens does business with** and who represents, owns and ultimately benefits from this business.
* Plausibly understand the sources of **financing of the Counterpart** and their **financial transactions** with Siemens.
* Find out if there are indications for a **criminal origin of the funds**.

Step 2: Take action to

* **Mitigate the risk** of Siemens being abused for money laundering and
* Fulfill possible **legal requirements.**

Step 3: Monitoring to observe if changes require further actions.

The AML Due Diligence (AML DD) must be performed **before** entering into or continuing with a business relationship or performing any transaction with a Counterpart. The AML DD must be started immediately when the AML risk occurs/becomes known.



## 2.1. Clarify circumstances

The clarification of circumstances is comprised of two steps, the

* confirmation of the AML Red Flag by the Compliance Officer as a kind of pre-check on the basis of the information provided by the business ([Chapter C.2.1.1.)](#_2.1.1._Confirmation_by) and
* the actual collection and assessment of further facts ([Chapter 2.1.2.).](#_2.1.2._Collection_and)

### 2.1.1. Confirmation by the Compliance Officer

The Compliance Officer performs a first check, if

* the concrete situation indeed shows all **factual** elements as described in the AML Red Flag or if the AML Red Flag situation is given but may be **obviously plausibly and legitimately** explained, e.g. if from his perspective
* the company structure is also complex / in-transparent or if the setup had been previously reviewed and approved also from a Compliance perspective;
* the business models lacks economic sense or it is an obviously legitimate business model (as opposed to formally legal only);
* it is a third party through which a payment was made or
  + errors in name spellings led someone to believe, that there was a third party paying or
  + it is a third-party payment but it is obviously legitimately made by a group company of the customer.
* A **German ARE** is involved in the business case.

This decision must be taken without delay and on the basis of the information available to the Compliance Officer at the time; there is no need for internal reviews, audits or investigative measures at this point.

There is no need for further clarification or actions where it is – contrary to the first assessment of the business – obvious from the perspective of a Compliance Officer that no AML Red Flag exists.

If the existence of the AML Red Flag can be confirmed by the Compliance Officer, it is necessary to further clarify the circumstances (see next subchapter). In all cases where a **German ARE** is involved, the Compliance Officer reports the confirmed AML Red Flag-situation to LC CO IR. For the reporting of the AML Red Flag-situation the Compliance Officer may use the suggested [e-mail notification](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9110.msg).

### 2.1.2. Collection and assessment of facts

In any case where an AML Red Flag is confirmed by the Compliance Officer, a further clarification is needed. This clarification is needed to assess, whether the AML Red Flag-Situation that typically indicates a high AML risk also means that the **concrete situation** bears a high AML risk.

The responsibility for collection and assessment depends on the fact if a German ARE (e.g. the legal entity Siemens AG itself or any of its German subsidiaries) is involved in the business case or transaction where the AML Red Flag has been identified.

No German ARE involved: Compliance Officer

In all cases where no German ARE is involved, the Compliance Officer will assess whether the AML Red Flag-situation that typically indicates a high AML risk also means that the **concrete situation** bears a high AML risk. Therefore, it is necessary toassess the

* **plausibility of business activity**
* **integrity of involved parties and legitimacy of source of funds**

Depending on the circumstances the clarification may require, in particular, but not limited to some or all of the following:

* Internal information about **the business relationship / case**, e.g. an overview of the involved parties and the contractual and financial setup as well as business judgement about the economic and technical adequacy
* Plausibility check of **legal nature / source of funds** of the Counterpart
* name and registered business address of the **Counterpart**
* the Counterpart`s **ownership and control structure(s) to see** whether an AML Red Flag is indicated in **ORBIS** (see chapter [C.2.1.3.](#_2.1.3._ORBIS_access)), e.g. because one of the individuals raises integrity concerns

to see if there are any **indications for illegitimate sources of the funds of the Counterparts** or any of the persons identified is involved in illegitimate business.

German ARE involved: LC CO IR

In all cases where a German ARE is involved, the Compliance Officer reports the confirmed AML Red Flag-situation to LC CO IR. For the reporting of the AML Red Flag-situation the Compliance Officer may use the suggested [e-mail notification](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9110.msg).

The Business supports this by giving the necessary information. Also, third party information can be accessed e.g. via **ORBIS**.

Generally, the AML risk evaluation refers to the Siemens Counterpart. In circumstances where Third Parties make payments to Siemens (transactions), the AML Due Diligence should be performed for those Third Parties.

On the basis of the collected information, it can be assessed whether a high AML risk exists in the concrete situation. Therefore, it has to be assessed if a situation or conduct of the Counterpart is unusual compared to the standards in the relevant industry and no sufficiently plausible explanation exists based on currently available information.

LC CO IR will support, upon request, with the assessment whether a high AML risk exists. To get support from LC CO IR the Compliance Officer may use the suggested [e-mail notification](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9110.msg).

The relevant business relationship should - wherever possible - be suspended and no further transactions be performed until the clarification is finished and – if needed – further actions according to the next subchapter have been defined.

If the assessment confirms a high AML risk or even leads to positive knowledge of AML infringements in the concrete situation, further actions have to be taken.

### 2.1.3. ORBIS access

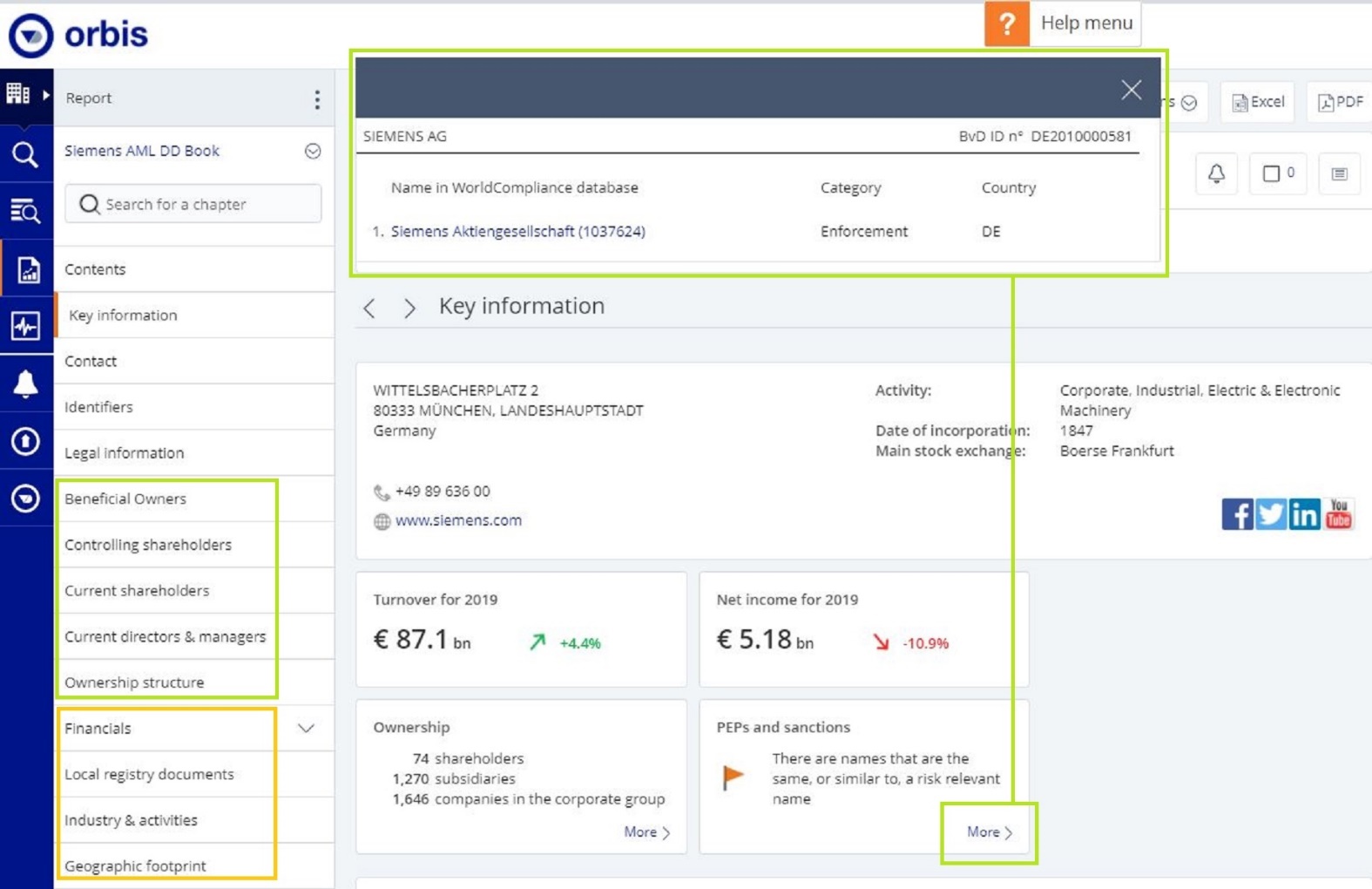
Check plausibility of business activity

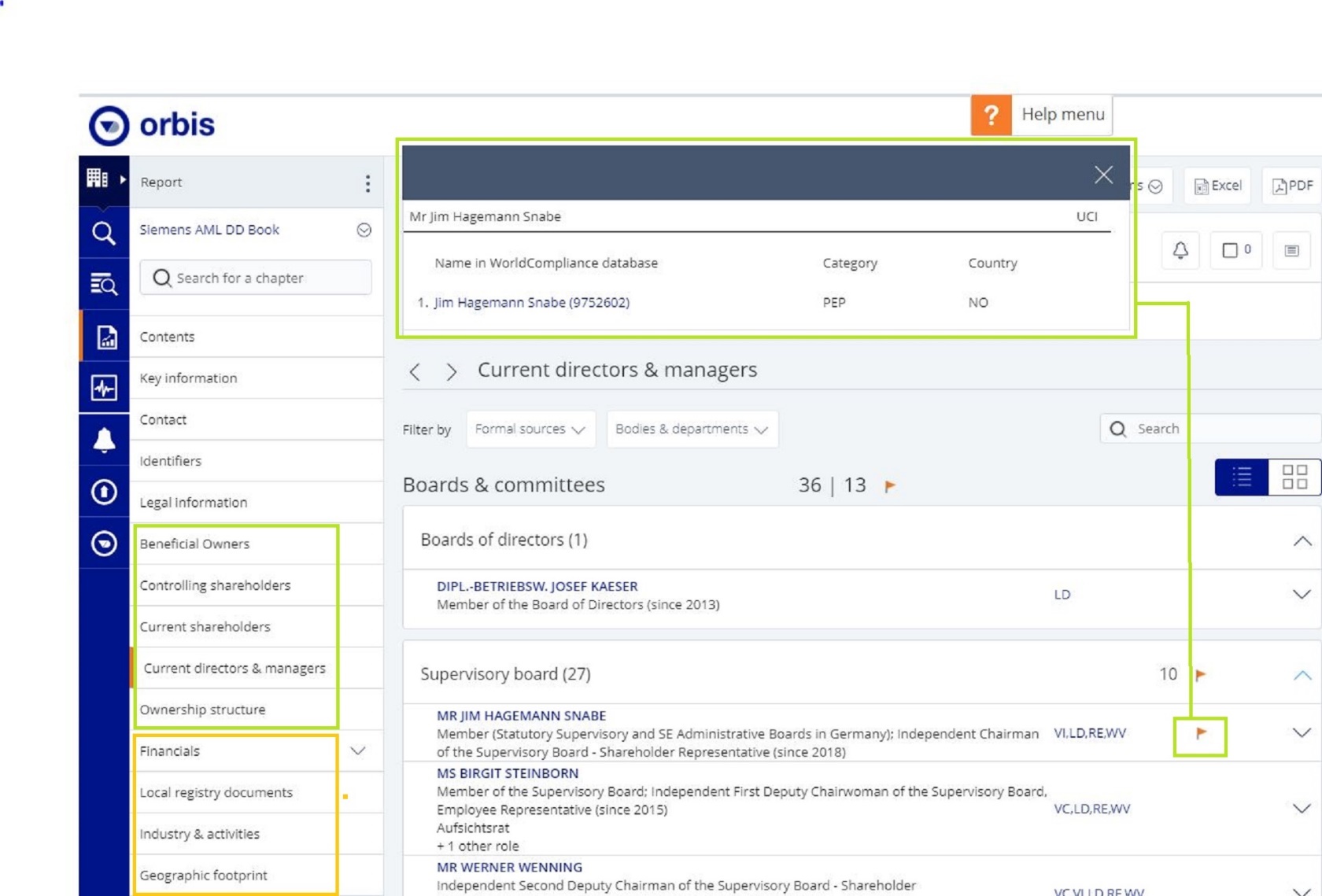
Besides information from the business, ORBIS information especially from the categories “Financials”, local registry documents” Industry & activities” as well as “Geographic footprint” might be helpful (fields marked with an orange frame on the screenshots below)

Check for ORBIS Flags

ORBIS shows orange Flags in the overview category “Key Information” as well as relating to individuals and companies in the categories “Beneficial Owners”, Controlling shareholders”, “Current directors & managers” as well as “Ownership structure” (fields marked with an green frame on the screenshots below).

The orange flags may relate to the [LexisNexis / WorldCompliance-categories](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_7463.pdf) “Enforcement”, “Adverse Media”, “Sanction List”, “PEP”, “Associated Entity”, or “Registrations”. Only “**Enforcement**” and “**Adverse Media**” should be screened for relevant findings hinting at an illegal source of our Counterparts funds.





Hit evaluation

The guidance on hit evaluation of SETIS hits applies accordingly, see [chapter A.4.C.2.4.4.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,A.-Anti-Corruption,4.-Cooperation-with-Business-Partners,C.-Relevance-only-for-Tool-Users-(Tool-description),C.2.-Business-Partner-CDD-Process,C.2.4.-Risk-Assessment,C.2.4.4.-Internet)

Access to ORBIS

As Compliance Officer, please refer to your responsible regional, Business or Service & Governance Head of Compliance / Department Head. Accesses to ORBIS have be allocated to the Compliance office of the following Siemens units:

|  |  |  |
| --- | --- | --- |
| **Assignment of Access to Countries** | | **Assignment of Access to Businesses** |
| **Country** | **Shared with** | DI |
| USA | Netherlands | SI |
| Brazil | Turkey | MO |
| France | Canada | CD |
| Austria | Japan | SFS |
| Switzerland |  |  |
| Portugal | Australia | **Assignment of Access to Service & Governance** |
| Spain | Argentinia | IR |
| Italy |  | PT |
| Indien | Sweden | EX |
| Singapore | UK | RFC |
| South Africa |  |  |
| UAE | Mexico |  |

Access Rights

The Access Right-Holders can also found on this [list](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9601.xlsx).

User Manual

An ORBIS **user manual** is available [here](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9549.pdf).

Important Restrictions:

* Due to export control regulations and the fact that Orbis is owned by Bureau van Dijk (owned by Moody's) Russia and China need to receive the reports from other countries. Recommendation: China to receive reports from Singapore or via Business (DI, SI, MO, CD); Russia to receive reports from Austria or via Business (DI, SI, MO, CD) same applies for Iran - obtain report over UAE or Business and all other embargoed countries.
* Each account can have more than one user by sharing the user name and password. *Please keep* [*Ute Stach*](https://scd.siemens.com/luz/IdentitySearch?cn=ute+stach&suchart=schnell&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A)*, LC CO PT CO informed about any active users within your organization. Rec*ommendation: Within your time zone max. two user per account - otherwise the account is not accessible if another user is already logged in.
* DO NOT set the value to "always logged in”
* Note: the annual amount of ORBIS reports is limited. Please do not request reports without necessity.

Technical Questions

For any technical question in relation to ORBIS, please refer to [Ute Stach](https://scd.siemens.com/luz/IdentitySearch?cn=ute+stach&suchart=schnell&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A), LC CO PT CO

## 2.2. Take action

The responsibility for further actions depends again on the fact if a German ARE is involved in the business case or transaction where the AML Red Flag has been identified.

No German ARE involved

In all case where no German ARE is involved, the Compliance Officer will decide on further measures. LC CO IR will support upon request. A decision has to be taken about

* **continuing business**,
* **mitigation measures** which would reduce the AML risk to a level where the business can be continued, e.g, agreeing on a direct payment by the customer instead of a third party payment
* opening a **Compliance Case** and
* **legal prerequisites** for specific case (see [chapter C.3.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),3.-Local-/-sector-specific-AML-requirements))

LC CO IR will support, upon request, with the assessment of possible actions. To get support from LC CO IR the Compliance Officer may use the suggested [e-mail notification](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9110.msg).

German ARE involved

LC CO IR continues handling the issue.

## 2.3. Monitoring

The AML DD requires appropriate follow up and monitoring procedures concerning the Counterpart, the business model and or any transactions with the Counterpart. Such follow-up and monitoring may vary from case to case; its frequency, scope and depths shall be defined jointly with the mitigation measures.

The overall responsibility for the completion of the follow up and monitoring lies with the Business. The Compliance Officer supports the monitoring of the business relationship.

The same applies, if any Siemens colleague becomes aware of new information or data about a Counterpart that deviates from information or data obtained previously or any new doubts with regards to the potential involvement of the Counterpart in money laundering or terrorism financing occur.

If any AML risk was identified in the course of the AML DD an enhanced monitoring is needed based on the defined mitigation measures.

The integrity information ([chapter C.2.1.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),2.-AML-Due-Diligence,2.1.-Clarify-circumstances)) should be monitored on a regular basis or at any time e.g. in case of

* new information or data about a Counterpart that deviates from information or data obtained previously, or
* any new doubts with regards to the potential involvement of the Counterpart in money laundering or terrorism financing.

# 3. Local / sector specific AML requirements

The global Siemens Anti-Money Laundering (AML) System has been designed with a focus on Siemens` industrial / goods trading business. It is applicable, as far as no deviating local / sector specific law, e.g. for banking / financial industry, real estate brokers or lawyers, applies. The global Siemens Anti-Money Laundering (AML) System is administered by LC CO RFC / LC CO PT CO. SFS issues are handled by LC CO SFS.

The responsible Compliance Officer is obliged to check (e.g. as part of the assessment of the regulatory risk in the CRA) if his or her local or sector specific requirements are fulfilled by the global Siemens Anti-Money Laundering (AML) System or if additional measures need to be taken. In that case, further measures are to be aligned with LC CO RFC / LC CO PT CO respectively LC CO SFS for SFS.

## 3.1. Germany

The German AML Law (Geldwäschegesetz, GwG) contains duties for several types of “obliged parties”:

* **German Siemens entities selling Siemens products, services and projects** are an obliged party as “Goods Trader” (Güterhändler, Sec. 2 para. 1 No. 16 GwG). The global AML DD Process is designed to identify critical situations in accordance with the applicable law. In case of involvement of German AREs, those AML Red Flag situations will be handled by the experts for German AML law at LC CO IR.
* **Financial industry activities** lead to the status of an obliged party (Sec. 2 para. 1 Nos. 1-9 GwG). For AML of the financial industry, please contact [SFS Compliance](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx). For Next47 as “Financial company”, please contact the [Compliance Officer for Next47](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx).
* **Real Estate Brokers** are obliged parties (Sec. 2 para. 1 No. 14 GwG). For real estate matters, please contact the [Compliance Officer for SRE](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx).
* For the **Transparency Register** (Sec. 18 GwG), please contact the [Compliance Officer for CF R](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx).
* **Lawyers and other professionals** are obliged parties (Sec. 2 para. 1 Nos. 10-12 GwG). For lawyers and other professionals, please contact the [Compliance Officer for LC](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx) or [Jürgen Krais](https://scd.siemens.com/luz/IdentitySearch?cn=j%C3%BCrgen+krais&maxanz=50&suchart=schnell&tab=tabs-1), LC CO IR and see [Chapter C.3](https://webbooks.siemens.com/public/LC/chde/index.htm?n=Teil-1-Compliance-Aktivit%C3%A4tsfelder,C.-Geldw%C3%A4schebek%C3%A4mpfung-(AML),3.-Lokale-/-sektorspezifische-AML-Anforderungen). of the German version of this Handbook.

# 4. Prohibited transactions or business relationships

Where an AML Due Diligence (AML DD) that is obligatory by law cannot be performed, for example because the Counterpart does not provide the information relevant for such AML DD, it is prohibited to do business with the Counterpart. An existing business relationship must be terminated. In particular, no transaction or payment must be performed or received from the Counterpart.

The same applies where LC CO RFC LF or LC CO IR issue a corresponding instruction in the course of an AML DD with view to the risk of money laundering or terrorism financing.

Following a suspicious activity report (`SAR`) or a suspicious transaction report (`STR`) the relevant business relationship, transaction or payment must remain suspended for at least three full working days or longer, where the local law requires.

# 5. Cash Handling Rules

For incoming and outgoing cash payments in any currency the conditions of the [Siemens Circular 208 (Treasury Transactions in the Company)](https://regulations.siemens.com/content/sc/208/en) apply (Sec. 4.10.1 and 5.4):

*“Payments with Cash are specifically regulated in many jurisdictions according to money laundering or other laws. The governance for Anti-Money Laundering lies with Legal & Compliance (LC CO RFC / LC CO SFS) and supports the BizCos by appropriate processes.*

* *If there are no stricter requirements under local law, Cash transactions (whether incoming or outgoing) at or above*
  + *€ 2,000 or equivalent for transaction of precious metals (e.g. gold, silver, platinum and others for use in Siemens products or for sale as scrap metals) are prohibited.*
  + *€ 10,000 or equivalent for any other transaction are prohibited.*
* *Splitting of Cash payments into smaller amounts which in total exceed the above thresholds to circumvent those thresholds is prohibited.*
* *It is also prohibited to circumvent the thresholds by making or receiving Cash transactions via third parties.*
* *For transactions exceeding the above thresholds, Non-Cash payment methods (e.g. electronic funds transfer, check, etc.) are to be used.*

*Exemptions from these rules are not permitted for payments by or in the name of or for any German ARE (e.g. by a local Siemens ARE afterwards internally invoicing the German ARE).*

*For all Non-German AREs, the ARE-CFO jointly with the responsible ARE Compliance Officer, may grant exemptions for payments exceeding the above thresholds, provided that*

* *the payment method used is in accordance with local legal requirements*[[12]](#footnote-13)*,*
* *no German is directly or indirectly involved in the transaction and*
* *it does not constitute a Cash payment for the purpose of the German Anti-Money Laundering Act (GwG).*

*The responsible ARE Compliance Officer needs to inform LC CO RFC LF of all exemptions granted.”*

Approvals of deviations for non-Germen ARE

The Compliance Officer at ARE level may grant such deviation if the above prerequisites are met and

* no cashless solution is available and
* the Counterpart (originator of a payment to Siemens or recipient of a cash payment from Siemens) has undergone a complete AML Due Diligence (including Know Your Counterpart (KYC) and AML Assessment) in line with Siemens’ internal AML requirements ([see Chapter C. 2](#_2._AML_Due).).
* Additionally, in case of incoming payments (to Siemens), Siemens must ensure the Counterpart can reasonably demonstrate that the cash money is from a legal source/ has been obtained through legal activities.

The competent ARE Compliance Officer must inform LC CO RFC LF of any such exception granted.

Examples for Cash Payments

Typical situations where cash payments may occur and that are impacted by the regulations above include, but are not limited to:

* Paying of **stamp duties**,
* Selling of **scrap material**,
* Purchasing of **material on a construction site**,
* Paying of **contractually agreed Daily Allowances**,
* Payments **into or out of cash boxes approved** under [Siemens Circular 208 `Treasury Transactions in the Company`](https://regulations.siemens.com/content/sc/208/en).

The following scenarios are not affected by the regulations above.:

* The creation and existence of a **cash box in accordance with** [Siemens Circular 208 `Treasury Transactions in the Company`](https://regulations.siemens.com/content/sc/208/en), even if the cash amount contained in such cash box exceeds the 10.000 EUR threshold; however payments by third parties into, or to third parties out of such cash boxes are fully subject to the regulation in [Chapter C.1.1](#_1.1._AML_Cash).;
* The **(physical) transport of cash by Siemens employees** as long as there is no payment involved (for example, a cash withdrawal of 10.000 EUR from the bank).

# 6. Training and supporting material

Basic AML information for Business and Compliance

* [AML Homepage](https://intranet.for.siemens.com/cms/059/en/processes/publications/Pages/compliance_aml.aspx)

* [AML Information Package](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9650.pptx)
* [AML Scribble Video](https://findit.compliance.siemens.com/content/10000101/Compliance/CL_CO/CL_CO_AT/findIT_CL_CO_AT_4551.wmv)

Further AML awareness and training for Compliance

* [AML Awareness Package FY 2021 - House of Risks](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9651.pptx)
* [Integrity Moment FY 2020](https://findit.compliance.siemens.com/content/10000101/Compliance/CL_CO/L_GF/findIT_L_GF_8581.pptx)

* [AML Game: “Too good to be true” (2018)](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_6173.pptx" \o "AML Game: \“Too good to be true\”" \t "_blank)

AML awareness and training for specific local / sector requirements

* Please see [Chapter C. 3.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),3.-Local-/-sector-specific-AML-requirements)

# 7. History of changes

|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Major changes of binding content** |
| 01.10.2017 | Y. Hamm-Dueppe/U. Stach | Initial Version of KYC Guidance (V.1.0) and AML Assessment Guidance (V.1.0) |
| 24.11.2017 | A. Schieffer | Modifications to Cash-Handling and Accounting Controls: Prohibition of cash payments of >= 10.000 Euros; only for Non-German AREs exceptions are permissible, if unavoidable;  Corresponding [Siemens Circular 208 (Treasury Transactions in the Company)](https://regulations.siemens.com/content/sc/208/en) came into effect on Dec. 15, 2017 |
| 08.01.2018 | Y. Hamm-Dueppe | Former KYC Guidance (V.1.1):   * Exceptions for end-user/end-customer * Description of necessity of deemed UBO * Guidance for evaluation of PEP Hits |
| 09.04.2018 | Y. Hamm-Dueppe/U. Stach | Former KYC Guidance (V.1.2):   * New EX trigger: end-customer in Russia * Disapproved Counterparts to be transferred into Business Partner Tool (today: NextGen) * Definition of relevant shareholder   Former AML Assessment Guidance (V.2.0):   * Exceptions in case of EX trigger: no need for AML Assessment * Particularities in case of real estate agency business * LoA – Limits of Authority particularities * Additional requirements:   + Management approval   + for cash payments |
| 01.07.2018 | Y. Hamm-Dueppe/ U. Stach | Former KYC Guidance (V.1.3):   * Deletion of risk trigger: “whitelisted EPCs” * Data collection of five legal representatives instead of four * No screening in exceptional cases   Former AML Assessment Guidance (V.2.2):   * Additional Requirements extended to Tunisia, Trinidad & Tobago, Sri Lanka |
| 01.01.2019 | Y. Hamm-Dueppe/U. Stach | * Re-definition of risk trigger `corresponding AML law requirements` into `corresponding AML requirements` * Deletion of EX risk trigger within KYC process; corresponding changes regarding especially Shareholder structure and UBO definition:   + 1st level > 25 % shares   + 2nd and following level > 50 % shares * New chap. 2.4.3.1. Documentation of completion: Need of documentation of `disapproval` and `completion under conditions` of KYCs within the KYC Tool * Specification of list categories * Additional Requirements extended to Guyana and Pakistan\*. \*According to DELEGATED COMMISSION REGULATION (EU) 2018/1467 of 27 July 2018 amending the Delegate Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council as regards the inclusion of Pakistan in the table in point I of the Annex (AML very high risk countries) |
| 01.10.2019 | Henning Tabbert | * Revised Approach (Red Flag oriented) * Elimination of country risk due as diligence/KYC trigger (Introduction of chapter C., 2.1., 2.3.3.; 2.3.4.1) |
| 01.01.2020 | Henning Tabbert | * Cash requirements C.1.1. according to GWG changes |
| 01.04.2020 | Henning Tabbert | * Redactional changes in chapter C. introduction, C.1. and C.1.1. * Allocation of responsibilities C.3. * Chapter about AML Red Flags created C.1. * List of AML High Risk Countries included C.1.1.5. * Former separate binding documents for AML Red Flags and AML High Risk Countries abolished |
| 01.07.2020 | Henning Tabbert | * List of AML High Risk Countries C.1.1.5. adjusted: * **Added:** Albania, Jamaica, Myanmar, Nicaragua, Uganda * **Deleted:** American Samoa, Ethiopia, Guam, Libya, Nigeria, Puerto Rico, Saudi Arabia, Sri Lanka, Tunisia, US Virgin Islands. |
| 01.10.2020 | Henning Tabbert | * Chapter C.2. AML DD: Implementation of Fresh Eyes Project changes, Replacement of KYC-Tool process by AML DD process including direct access of Compliance Officers to ORBIS information and flexible factual clarification and assessment in absence of specific legal requirements. Handling of AML Red Flags in relation to German AREs by LC CO IR experts due to particular local law. * List of AML High Risk Countries C.1.1.5. adjusted: * **Added:** US Virgin Islands |
| 01.01.2021 | Henning Tabbert | * List of AML High Risk Countries C.1.1.5. adjusted:   **Deleted:** Iceland   * Legal requirements for Lawyers and other professionals in Germany only added in German Version |
| 01.04.2021 | Koen Miezenbeek | * List of AML High Risk Countries C.1.1.5. adjusted:   **Deleted:** Mongolia |

# 8. Contacts

Compliance Officer

The Compliance Officer responsible for your unit can be found through the following [link](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx).

LC CO IR

[Jürgen Krais](https://scd.siemens.com/luz/IdentitySearch?cn=j%C3%BCrgen+krais&maxanz=50&suchart=schnell&tab=tabs-1), LC CO IR

AML Legal Frame

[Koen](https://scd.siemens.com/luz/IdentitySearch?cn=henning+tabbert&suchart=schnell&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A) [Miezenbeek](https://scd.siemens.com/luz/IdentitySearch?cn=MIEZENBEEK+KOEN+FRANCISCUS+PETRUS+Z0041FAX&tcgid=Z0041FAX&c=DE&o=SIEMENS&ou=LC&l=ERL+M+WVS67&department=LC+CO+RFC+LF&), LC CO RFC LF

AML Processes & Tools / ORBIS

[Ute Stach](https://scd.siemens.com/luz/IdentitySearch?cn=ute+stach&suchart=schnell&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A), LC CO PT CO

AML Risk Management

[Martin Felkl](https://scd.siemens.com/luz/IdentitySearch?cn=martin+felkl&maxanz=50&suchart=schnell&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A), LC CO RFC RC

SFS

For AML of the financial industry, please contact [SFS Compliance](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_organization.aspx).

Germany

For contacts regarding the different obliged parties according to German AML law (GwG) please see [Chapter C. 3.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,C.-Anti-Money-Laundering-(AML),3.-Local-/-sector-specific-AML-requirements)

1. **Counterparts** are defined in detail [here](https://workspace.c6.siemens.com/content/300000007/Compliance%20WebBook/Part%201%20Activity%20Fields/C)%20Anti-Money%20Laundering%20(AML)/_layouts/15/hypernet/custom/link.aspx?bid=00010023&pt=General_x0020Introduction&tt=2._x0020Definitions_x0020and_x0020Abbreviations). Generally, Counterparts involved in business with a **customer** are in the focus of activities fighting money laundering. Payments to suppliers are subject to DAMEX checks aiming at preventing terrorism financing. [↑](#footnote-ref-2)
2. via this [e-mail template](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_CORP_AML/findIT_LC_CO_CORP_AML_9110.msg). [↑](#footnote-ref-3)
3. **Counterparts** are defined in detail [here](https://workspace.c6.siemens.com/content/300000007/Compliance%20WebBook/Part%201%20Activity%20Fields/C)%20Anti-Money%20Laundering%20(AML)/_layouts/15/hypernet/custom/link.aspx?bid=00010023&pt=General_x0020Introduction&tt=2._x0020Definitions_x0020and_x0020Abbreviations). Generally, Counterparts involved in business with a **customer** are in the focus of activities fighting money laundering. Payments to suppliers are subject to DAMEX checks aiming at preventing terrorism financing. [↑](#footnote-ref-4)
4. PEPs are defined in detail [here](https://workspace.c6.siemens.com/content/300000007/Compliance%20WebBook/Part%201%20Activity%20Fields/C)%20Anti-Money%20Laundering%20(AML)/_layouts/15/hypernet/custom/link.aspx?bid=00010023&pt=General_x0020Introduction&tt=2._x0020Definitions_x0020and_x0020Abbreviations). [↑](#footnote-ref-5)
5. See [Chapter C.5.](#_4._Cash_Handling) [↑](#footnote-ref-6)
6. See [Chapter C.1.3.](#_1.4._Letterbox_company) [↑](#footnote-ref-7)
7. Legal representatives are defined in detail [here](https://workspace.c6.siemens.com/content/300000007/Compliance%20WebBook/Part%201%20Activity%20Fields/C)%20Anti-Money%20Laundering%20(AML)/_layouts/15/hypernet/custom/link.aspx?bid=00010023&pt=General_x0020Introduction&tt=2._x0020Definitions_x0020and_x0020Abbreviations) [↑](#footnote-ref-8)
8. See [Chapter C.1.3.](#_1.5._AML_High) [↑](#footnote-ref-9)
9. **Payment:** an amount of money paid, or the act of paying. [↑](#footnote-ref-10)
10. See [Chapter C.1.2.](#_1.4._Letterbox_company) [↑](#footnote-ref-11)
11. See [Chapter C.1.3.](#_1.5._AML_High) [↑](#footnote-ref-12)
12. [↑](#footnote-ref-13)