4. Outgoing and incoming payments

Outgoing and incoming payments can involve risks for Siemens, inter alia, from an anti-corruption or anti-money laundering perspective.   
The former Compliance High Risk Payment Process (not to be confused with Payment Alerts from Finavigate® - refer below) is discontinued effective 1st of October 2020. The abolishing of the process is possible as the existing processes from other Governance Owners adequately cover the requirements without the necessity for additional standard Compliance payments controls. Nevertheless, awareness of Outgoing / Incoming Payments is essential for a comprehensive Compliance risk identification, assessment and potential local mitigation.

Therefore, in the event of elevated Compliance risks, local mitigating measures should still be implemented e.g. payment blocks for high risk third parties / transactions, monitoring of manual / non-ERP payment processes.

In the following chapters, you will find an overview about the tasks of Corporate Compliance involvement as well as the obligations of Compliance Officers and their contribution in the main processes associated with payments.

## 4.1. Outgoing Payments

Corruption is covered by the Siemens Compliance System very prominently regarding benefits by Siemens ([Chapter A.1.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,A.-Anti-Corruption,1.-Gifts-and-Hospitality)), Sponsoring, Donations and Memberships ([Chapter A.2.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,A.-Anti-Corruption,2.-Sponsoring,-Donations,-Memberships)) as well as Facilitation Payments ([Chapter A.3.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,A.-Anti-Corruption,5.-Facilitation-Payments)). Also, the Business Partner process ([Chapter A.4.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-1-Activity-Fields,A.-Anti-Corruption,3.-Cooperation-with-Business-Partners)) relating to corruption via third parties is well known.

Furthermore, CF F process Control Over Funds (CoF) ([[Siemens Circular 208 “Treasury Transactions in the Company"](https://regulations.siemens.com/content/sc/208/en))](https://regulations.siemens.com/content/sc/208/en) and SOP SCM process Purchase-to Pay (P2P) [([Siemens Circular 130 “Compliance in the Purchasing Process – Purchase-to-Pay (P2P) Control Framework”](https://srs.siemens.cloud/#/c/sz89wk))](https://regulations-admin.siemens.com/content/sc/130/en) also aim at the prevention of corruption.

### 4.1.1. Involvement of Corporate Compliance

Corporate Compliance is involved in the following committees and processes as described in this Chapter as laid out below.

P2P Process Committee:

The **P2P Process Committee** serves the alignment and close collaboration of the relevant corporate functions (i.e. SOP SCM, CF F (Treasury), CF R (Accounting), LC CO, CF R/IC, CF A CA, SOP IT). LC CO is represented by LC CO RFC. The committee meets approx. three times per year and aligns inter alia the:

* P2P alert criteria (see [here](https://intranet.for.siemens.com/cms/050/en/processes/jobrole/Pages/purchase-to-pay.aspx) under the tabs “Preventative Controls” and “Detective Controls”),
* SCM Vendor Dashboard flags ([Chapter 3 of the SCM Vendor Dash Board Assessment Guide](https://wse04.siemens.com/content/P0003122/Vendor%20Dashboard/Support_Trainings_official/SCM%20Vendor%20Dashboard_Intro_and_Assessment_Guide.pdf)),
* CoF (Control Over Funds) / CoP (Central Routing of Payments) methods, and
* discusses risk trends / emerging risks in relation to payments.

High Risk Payment Scoring Committee:

The **alert monitor** of **Finavigate®** as part of the **Control over Funds (CoF)** process identifies critical payments based on defined alert criteria (e.g. High-Risk Payments, such as non-standard payments methods, e.g. cash, cheques and Suspicious Outgoing Payment). CF F (Treasury) and LC CO decide on the alert criteria at the annual **High-Risk Payment Scoring Committee**. LC CO is represented by LC CO RFC.

Central Compliance Monitoring by LC CO RFC

Outgoing payment risks are part of **LC CO RFC RC central monitoring activities.** Key elements of central monitoring activities are an aggregated risk analysis based on the following information sources to identify and assess “unusual” transactions, contexts and developments over the course of time.

* Alert Monitoring in Finavigate®
* Finance Cockpit incl. non-preferred payment methods, such as
  + Non-ERP-system based check payments
  + Other manual outgoing payments
  + Direct debit by third parties
  + Cash withdrawals and transfers
* P2P Control Framework
* SCM Vendor Dashboard

Further details about these measures as well as central monitoring activities will be implemented in Chapter K.1 on Compliance Risk Assessment.

### 4.1.2. Involvement of Compliance Officers

Operational Compliance Officers are involved in the following processes: P2P - Continuous Control Monitoring Alert (CCM), SCM Vendor Dashboard and Payment Alerts from Finavigate® (CF F / HoA).

#### 4.1.2.1. P2P - Continuous Control Monitoring Alert (CCM)

CCM alerts are flagged by local Supply Chain Management as “**Key Alert**” following evaluation when a deliberate or fraudulent rule breach is suspected. These Key Alerts are required to be evaluated by the responsible “[CCM Local Monitoring](https://wse04.siemens.com/content/P0003122/P2P_Purchasing_Governance/P2P%20Purchasing%20Control%20Framework/2.%20P2P%20Role%20Model%20and%20Responsibilities/P2P_Purchasing_Role_Model.pdf)” which is generally the responsible **Compliance Officer** to get a reasonable second review to decide, if the incident is confirmed or not.   
In order to address the identified compliance incidents, all Key Alerts closed with status “Incident Confirmed” will be addressed to further stakeholders, such as Management (e.g. CFO) and the responsible **Compliance Officer** to initiate an investigation as Compliance case according to the role of the “[CCM Local Monitoring](https://wse04.siemens.com/content/P0003122/P2P_Purchasing_Governance/P2P%20Purchasing%20Control%20Framework/2.%20P2P%20Role%20Model%20and%20Responsibilities/P2P_Purchasing_Role_Model.pdf)”, as described P2P Purchasing Role Model.  
It is recommended that a local **P2P Control Board** is established in order to ensure the structured and regular, at least quarterly coordination of relevant user functions (i.e. Supply Chain Management, Treasury, Accounting, **Compliance Officer**, R/IC, CF A) and the level of **Siemens entities**. The board analyzes patterns and developments for its entity also in comparison with other AREs.

#### 4.1.2.2. SCM Vendor Dashboard

For the **SCM Vendor Dashboard** application (also see [Chapter H.2.4.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-2-Business-Perspective,H.-Compliance-in-Business-Processes-and-Projects,2.-Compliance-in-Procurement,2.4.-Vendor-Dashboard)) SOP SCM bi-quarterly (Q2 and Q4) identifies suppliers for a detailed assessment based on the defined red-flag criteria. The suppliers with the highest number of red-flags are selected in general for the assessment by SOP SCM. The responsible **Compliance Officer** will be involved / contacted by SOP SCM according to [Chapter 4.8 of the Vendor Dash Board Assessment Guide](https://wse04.siemens.com/content/P0003122/Vendor%20Dashboard/Support_Trainings_official/SCM%20Vendor%20Dashboard_Intro_and_Assessment_Guide.pdf) for the:

* Pre-alignment of Top supplier selection
* Verify about already existing investigations / clarifications
* Support of transaction deep dive in case of possible fraud incidents
* Receive possible fraud cases or other violations of Siemens Circular 226 and drive further compliance internal investigation / clarification
* Approve final assessment conclusions e.g. in cross-functional P2P Control board

#### 4.1.2.3. Payment Alerts from Finavigate®

Alerts of individual outgoing payments with higher risk characteristics are generated in alert monitor from Finavigate® on corporate level.  
If a Siemens entity is not able to use the alert monitor from Finavigate® for all outgoing payments an individual setup of local controls has to be defined and agreed by CF F CMP.

High Risk Payment / Suspicious Payment Alerts

The responsible **Head of Accounting (HoA)** assess the Payment Alerts as generated by the Outgoing Payment Alerts monitor in Finavigate®. If the HoA doubts that the payment complies with legal requirements, has been correctly executed on basis of a legitimate liability and/or Siemens internal regulations, then the HoA should refer the payment to the local responsible **Compliance Officer** for further assessment.   
Payment Alerts can come form a) before final payment run execution in Finavigate® (known as **Suspicious Payment**) and b) after final payment run execution in Finavigate® (known as **High Risk Payment**) alerts.

Cash Alerts

At the first level, the responsible **HoA** assess each detective post-payment **Cash Alert** generated by the Finavigate® Outgoing Payment alert monitor in order to check why the Cash Alert was generated and to ascertain, if it is reoccurring.  
In case of reoccurring Cash Alerts i.e. two or more Cash Alerts within one fiscal year, then the **HoA** has to assess the reason why Cash Alerts are recurringly generated and, in accordance with CF RIC PCMB 3.2.3.3-19, inform the responsible **Compliance Officer** appropriately. The Compliance Officer should assess whether additional risk mitigation measures, in alignment with the HoA, are necessary.

## 4.2. Incoming Payments

From an Anti-Money Laundering (AML) perspective, we should be aware of incoming payments that would trigger 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-(AML),1.-AML-Red-Flags)).

Insofar, a respective application is in development to support German AREs regarding their specific local law requirements.

## 4.3. Training & Supporting Material

[Siemens Circular 208 (Treasury Transactions in the Company)](https://regulations.siemens.com/content/sc/208/en)

The circular (“Treasury Guideline”) establishes amongst other things detailed, binding objectives, principles and mainly central controls (Control over Funds (CoF)) for bank accounts and payments (including cash payments).

[Siemens Circular No. 130 (Compliance in the Purchasing Process – Purchase-to-Pay (P2P) Control Framework)](https://regulations-admin.siemens.com/content/sc/130/en)

The Purchase-to-Pay (P2P) Control Framework is a company-wide rule set comprising compliance-related controls for the purchasing process, along with the corresponding regulations, remediation measures and obligatory procedures to be instituted throughout the company.

## 4.4. History of changes

|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Major changes of binding content** |
| January 1, 2019 | Dieter Heinke (LC CO OC CCF) | First release through the Compliance Handbook based on Siemens Circular SC No.226 “Global Compliance”. |
| April 1, 2020 | Dieter Heinke (LC CO RFC RC C) | Deletion of CRB Q 3 references |
| October 1, 2020 | Dieter Heinke (LC CO RFC RC C) | New title of the Chapter (formerly high risk payment)  New Chapter structure regarding outgoing and incoming payments with specific focus on involvement of Corporate Compliance and obligations resp. contribution of Compliance officers |

## 4.5. 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).

Corporate Governance Owner

The contact person for Outgoing Payments is:

[Dieter Heinke](https://scd.siemens.com/luz/IdentitySearch?cn=Dieter+heinke&suchart=schnell&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A) (LC CO RFC RC C)