Day&Zimmermann
We do what we say.®

Policy 1329: Segregation of Duties Conflict Resolution
Policy No.: 1329
Responsible Officer: Senior VP Finance and CFO

1.0 Scope

The Day & Zimmermann Group, Inc. and its subsidiaries and affiliates.

2.0 Purpose

The purpose of this policy is to establish the Company's position regarding the clearance and mitigation of segregation of duties (SOD) conflicts within the Company's ERP system (i.e. SAP).

3.0 Definition

SOD refers to an internal control concept that a single person does not have the ability to perform incompatible and critical functions within the IT environment. If such controls are not in place, it allows for intentional or unintentional errors in the processing of the associated data. Properly designed and operating SOD controls discourage fraud and other malicious practices. Segregation of duties is an important component of a properly designed and effectively operating internal control environment.

4.0 Policy

All high and medium risk SOD conflicts created as a result of SAP transactions assigned to employees must be cleared or mitigated in accordance with the guidelines provided in this policy.

The Company's staff function and business units must clear or mitigate SOD conflicts recognizing the need to protect assets, manage access to information, and improve the quality of controls over business critical information (i.e., financial, operational, regulatory, personal, etc.). The following are examples of SOD conflicts:

- A buyer in Corporate Purchasing who has the ability to create and process a Purchase Order can also pay a vendor thus creating the risk of fraudulent or inappropriate purchases.

- An accountant in Corporate Accounting can both create and approve a journal entry thus creating the risk of inappropriate and or inaccurate accounting records.

- An employee who can request a wire transfer can also release the wire transfer thus creating the risk of inappropriate or fraudulent transfer.

- An employee who can set up a vendor can also process payments to vendors thus creating the risk of inappropriate or fraudulent payments.

4.1   Clearing or Mitigating SOD Conflicts

Managers' internal work procedures should include controls designed to prevent and detect fraud or inadvertent errors that may occur regarding the integrity and/or processing of business critical data. Accordingly, the following procedures must be followed in assigning SAP transactions to employees:

4.1.1 When a new employee or an existing employee needs access to SAP transactions to perform their job responsibilities, the employee's manager will request IT Security to assign those transactions to the employees.

4.1.2 The IT Security will assign the requested transactions in groups of transactions called User Roles in accordance with its internal protocol. The IT Security will analyze the requested transactions through software called Compliance Calibrator. This analysis will reveal SOD conflicts, if any, in the assigned transactions. If an SOD conflict is identified through this analysis, the following procedures will be followed in clearing or mitigating the SOD:

a. If the SOD conflict is due to a transaction used by the employee, then the manager/supervisor should see if the employee's job responsibilities can be re-assigned so that the SOD conflict causing transaction can be removed from the employee and the conflict can be cleared. If that is not possible, the SOD conflict must be mitigated in conjunction with the appropriate controller and the mitigation must be documented and approved in accordance with the requirement in the SOD Risk Mitigation form. (Exhibit A)

b. If the SOD conflict is due to a transaction that an employee does not use, then the manager should work with Corporate IT Security to determine if the transaction is used by anyone in the Company. If the transaction is not being used by anyone in the Company, it can be removed from the User Role and thereby eliminating the SOD conflict. If that is not possible, the SOD conflict must be mitigated in conjunction with the appropriate controller and the mitigation must be documented and approved in the SOD Risk Mitigation form.

c. In mitigating the risks, the following prioritization can be used:

Priority should be given to clearing or mitigating those Medium and High risk SODs which impact the following areas:

- Revenue cycle
- Journal entries
- Protection of assets
- Ability to procure goods and services
- Ability to receive goods and services
- Ability to pay or change invoices
- Ability to enter contracts
- Ability to change billing rates
- Ability to change employee wages
- Ability to add vendors

5.0 Responsibility

5.1 All managers and supervisors are responsible for:

a. Ensuring that the employees reporting to them do not have SOD conflicts as a result of SAP transactions assigned to them.

b. Ensuring that SAP transactions are removed from an employee when the employee leaves the Company or moves to a new position within the Company.

c. Seeking assistance or guidance from IT Security or their Controllers, as needed, in ensuring that SOD conflicts within their organization are cleared or mitigated using the SOD Risk Mitigation form.

5.2 Corporate IT Security is responsible for:

a. Monitoring SOD risks using Compliance Calibrator when SAP transactions are requested for employees by their managers during initial assignments and or subsequently because of changes in responsibilities.

b. Alerting appropriate managers and their Controllers when an SOD conflict is revealed during initial assignment of SAP transactions and or during subsequent assignments as a result of changes in job responsibilities.

c. Ensuring that no transaction combinations with SOD conflicts are assigned to employees unless approved by the appropriate Controller and accompanied by a documented and approved SOD Risk Mitigation form.

d. Sending quarterly reports to the Controllers informing them about the SOD conflicts with the employees in their areas.

5.3 The Corporate Controller, the SSO Controller, and the Business Unit Controllers are responsible for:

d. Ensuring that all Medium and High risk SOD conflicts are cleared or mitigated within their organizations within 30 days of receiving the SOD reports from IT Security per Section 5.2.b. above by following up with the managers of the employees with SOD conflicts.

e. Reviewing the quarterly SOD reports received from Corporate IT Security per 5.2.d. above to assess whether or not employees with transactions causing SOD conflicts continue to need to have those transactions and that there are appropriate mitigating controls if such transactions must be retained.

5.4 The Senior Vice President of Finance and the CFO is responsible for the overall administration of this Policy.