

Segregation of Duties

This is a case assignment that develops both the theoretical base for segregation of duties and then illustrates how this is accomplished in a highly integrated computerized enterprise business environment. The authorization system within the SAP ERP system is used to illustrate the implementation of segregated duties.

Product

SAP ERP
GBI
Release 6.04

Level

Undergraduate
Graduate

Focus

SOD Internal Controls
Roles Based Authorizations

Authors

Nancy Jones
Jim Mensching

Contributors

Dawna Drum
James Marlatt

Version

1.0

MOTIVATION

This scenario deals with examining the business functions involved in selling goods to another company (B to B sales) and the authorization and access controls that should be in place in order to safeguard the company's assets and the integrity of the company's financial records.

PREREQUISITES

Before you use this case study, you should be familiar with navigation in the SAP system.

You should also be familiar with basic internal controls.

NOTES

This case study uses the Global Bike Inc. (GBI) data set, which has exclusively been created for SAP UA global curricula.

Assignment Overview

The scenario starts by describing the business process and designating a series of tasks used to complete the process. There are four steps to the scenario.

Part 1: You will be provided with some risks associated with the business process and will be asked to determine appropriate controls to mitigate those risks. You will also be asked to assess additional risks associated with this business process.

Part 2: Using the risk analysis as a base, you are to then examine the assigned positions within the organization to be sure that there is adequate segregation of duties without incurring excess personnel costs.

The next two steps constitute the second part of the assignment.

Part 3: You must develop an authorization matrix that specifies the extent of computer access for each of the employees designated in the previous step. This step is a way of transitioning from a paper-based environment to a highly integrated computerized environment that is typically used in business.

Part 4: The last part of the assignment involves examining the SAP authorization system where you will see how to establish rules that enforce segregated duties. This part of the assignment uses data from the SAP ERP IDES system to illustrate the security configuration in an ERP system.

Security and Information Assurance

GBI is very concerned about security and information assurance. Due to the passage of the Sarbanes-Oxley law, GBI realizes that solid financial accounting controls are extremely important for the corporation. Originally GBI had an open security model in which the computer system users were only restricted from doing specific functions if it was obvious that an access authorization presented a security risk or an information assurance risk.

GBI realizes that a closed security model must now be adopted. A closed security model grants access to users based on the business function for which they are responsible; that is, a user is only allowed access to the functions of the system that they need to do their job. A closed security model is much more difficult to enforce than the open model. It is necessary to determine exactly what functions a user should be allowed and restrict the user to only those authorizations.

Determining the authorizations is not as easy as one might think. If we issue too many authorizations to a user, then we open the door to the risk of loss of control over our financial transactions, which could lead to errors or fraudulent or criminal activity. If we restrict the authorizations too much, then the controls become disruptive and the users cannot do their jobs. The ideal situation is for the user to have only the needed authorizations and nothing more. That is one objective of this assignment.

Segregation of Duties

The traditional way of analyzing whether there is adequate segregation of duties in a predominantly manual accounting system is to classify duties as to their responsibility with respect to the following four duties (sometimes only the first three duties are used):

- Authorization of the transaction

- Recording of the transaction
- Custody of assets involved in the transaction
- Independent verification and reconciliation of the transactions.

In theory, separate individuals should be granted each of these responsibilities. If this is the case, this “segregation of duties” introduces a series of checks and balances that help to assure the proper handling of the transaction. Of course, employee collusion could circumvent the segregation of duties controls.

In a computerized environment, some of these four responsibilities are done by the computer. With highly integrated computer systems, routine transactions may have all of the functions completed within the computerized system with little human intervention. Hence in an integrated computer environment, it is necessary to introduce additional concepts with respect to segregated duties. This involves enforcing access restrictions within the computer system. By not allowing access to specific data in the transaction, the system restricts an individual from involvement in various parts of the transaction. This enforces a segregation of duties within the computer system.

Determined by the way the application system is designed, user access can be limited by preventing the individual from executing specific functions within the system or by limiting access to the data stored in the system. Well-designed systems enable both functional restriction and data access restriction.

For most business applications, it is easiest to think of the documents involved in the transaction and restricting access to these documents. Access to the documents can be classified in the following manner:

- Create authorization – the user can create a new document and store that document on the system
- Read authorization – the user has access to the document in order to see / display its contents
- Update authorization – the user can change or edit an existing document – this authorization allows the user to void a document, but it does not allow a user to create a document or delete a document
- Delete authorization – the user can eliminate the document from the system – this is an authorization that should be used sparingly since it eliminates the transaction
- Authorize authorization – the user can signify that the document is authorized and should go on to the next step of the process

By issuing multiple access authorizations, the role of the user in the transaction can be well regulated. For example, a person responsible for authorizing the payment of a check will be given Read and Authorize rights to the supporting documents, but definitely none of the other rights. Having Create, Update, or Delete rights would allow this person to commit fraud by falsifying the documents used to verify proper payment, because they can both authorize and record the transaction. For example, the amount of the invoice and the payee could be altered with the money going to the person authorizing the payment instead of the entity that should be receiving the funds.

Risk Assessment and Other Controls

An organization must do a detailed assessment of the risks involved with any business process and then determine the likelihood of that risk occurring and the severity of the risk if it should occur. These factors will then be used to decide what controls should be implemented in order to mitigate the risk. While segregation of duties is an important control, it, like all controls, will not eliminate risks. No control is perfect in that it can completely eliminate a risk. Hence, it is necessary to have layers of controls. This concept of layered or multiple controls is termed **defense in depth**. The idea is to have a series of controls so that if one control fails to prevent or detect a problem, the other controls are in place to supplement the protection.

Company Background

Global Bike Inc., (GBI) is a world class bicycle company serving the professional and “prosumer” cyclists for touring and off-road racing. GBI’s riders demand the highest level of quality, toughness and performance from their bikes and accessories.

Product development is the most critical element of GBI’s past and future growth. GBI has invested heavily in this area, focusing on innovation, quality, safety and speed to market. GBI has an extensive innovation network to source ideas from riders, dealers and professionals to continuously improve the performance, reliability and quality of its bicycles.

In the touring bike category, GBI’s handcrafted bicycles have won numerous design awards and are sold in over 10 countries. GBI’s signature composite frames are world-renowned for their strength, light weight and easy maintenance. GBI bikes are consistently ridden in the Tour de France and other major international road races. GBI produces two models of their signature road bikes, a deluxe and professional model. The key difference between the two models is the type of wheels used, aluminum for the basic model and carbon composite for the professional model.

GBI’s off-road bikes are also recognized as incredibly tough and easy to maintain. GBI trail bikes are the preferred choice of world champion off-road racers and have become synonymous with performance and strength in one of the most grueling sports in the world. GBI produces two types of off-road bike, a men’s and women’s model. The basic difference between the two models is the smaller size and ergonomic shaping of the women’s frame.

GBI also sells an accessories product line comprised of helmets, t-shirts and other riding accessories. GBI partners with only the highest quality suppliers of accessories which will help enhance riders’ performance and comfort while riding GBI bikes.

For purposes of this assignment, we will focus on the process involved in sales of in-stock, standard, off-road bicycles. GBI uses an open invoice system to bill its customers; that is, the customer is billed and must pay for each order separately as opposed to the customer being billed periodically for all orders made during that period (usually referred to as cycle billing).

Standard Product Sales Business Process

Tasks within business processes may vary considerably depending on the level of automation and the associated technology. For instance, in a manual system, the task of recording a transaction may be accomplished by either entry into a journal or by the “filing” of a copy of a multi-copy form. In an

automated system, “recording” entails the “filing” or storage of the transaction in the AIS. This is sometimes accomplished by pressing a “save” button after entering the transaction into the system. The order of the tasks will also differ depending on the extent of automation within the system.

Assume that GBI is currently working with a manual system. The company uses the following 26 steps when they sell standard goods to the customers:

1. A customer sends a purchase order for off-road bicycles to a GBI employee.
2. A GBI employee compares the customer’s purchase order to determine if the customer’s master data is in the system and is correct.
3. If the customer master data is not in the system or is incorrect, then the master sales and distribution data (such as company address, contact person, phone numbers, etc.) for the customer is entered by a GBI employee.
4. If the customer master data is not in the system or is incorrect, then the financial data (such as banking information and GBI reconciliation account number) for the customer is entered by a GBI employee.
5. If the customer master data is not in the system or if the customer would like to change credit terms or limits, then a GBI employee checks the credit rating of the customer and assigns a credit limit and credit terms.
6. A GBI employee checks inventory availability.
7. If the customer can be extended credit and inventory is available, a GBI employee creates a sales order.
8. A GBI employee creates an order acknowledgement and sends it to the customer.
9. A GBI employee records the sales order.
10. A GBI employee creates a picking ticket to fill the customer’s order.
11. A GBI employee picks the goods (the bicycles) from the picking ticket.
12. A GBI employee creates a packing slip and a mailing label.
13. A GBI employee puts the packing slip into a reinforced packing container with the goods, seals the container and adheres the mailing label to the container.
14. A GBI employee moves the goods from the inventory control area to the shipping dock.
15. A GBI employee creates a shipping manifest.
16. A GBI employee places the goods to be shipped on the truck.
17. A GBI employee gives the shipping manifest to the truck driver.
18. A GBI employee creates a shipping document to show that the goods have been shipped.
19. A GBI employee records that the goods have been shipped.
20. A GBI employee creates an invoice with a remittance advice and sends it to the customer.
21. A GBI employee receives the payment from the customer with the returned remittance advice.
22. A GBI employee records the payment from the customer.
23. A GBI employee takes all of the payments for that day and makes up a deposit slip for the bank.
24. A GBI employee deposits the cash in the bank.
25. A GBI employee records the bank deposit.
26. A GBI employee reconciles bank deposits with the cash receipts on a daily basis.

Important Note – You are not allowed to change the above business process. That is, you cannot add, delete or modify any of the steps above.

Part 1 – Risk Analysis and Control Implementation

In this part of the assignment you will be given some risks involved with the sales transaction and determine what controls can be used to mitigate those risks. You will also have to analyze the business process to determine additional risks involved in the process. In order to give you a little assistance, we will give you a list of controls from which you are to select to mitigate the risk. Here are the controls that you are to select from:

1. Segregation of duties. **Note:** If you give this answer, you must state what duties should be segregated with comment like: ‘Segregation of _____ Duties from ____ Duties’; ‘SOD: segregate _____ from _____’)
2. Using sequential prenumbered documents
3. Matching the customer’s purchase order with the sales order, shipping document and invoice to be sure the transaction is complete and no duplication occurs
4. Physical security – for example, security cameras, security personnel and limiting access to certain areas
5. Reconciling the bank statement with the record of the deposits
6. Cancelling documents after they are completed – for example, marking a sales order as “shipped” when the goods are sent to the customer
7. Having management periodically check the work of employees
8. Doing a periodic count of inventory to reconcile the records with the actual amount in inventory
9. Firing and prosecuting employees found defrauding the organization
10. Having customers send payments directly to a lock box at GBI’s bank.

You are to:

- Analyze each of the following risks
- From the above list determine the **THREE best** controls that can be used to mitigate the risk.
- Explain in detail how the chosen control would mitigate the risk.

The following is an example of a risk and the possible controls.

RISK: GBI invoices a customer multiple times for the same sales order.

CONTROL 1: Implement Control 3 - Matching the customer’s purchase order with the sales order, shipping document and invoice to be sure the transaction is complete and no duplication occurs. Doing this type of checking would verify whether or not these transactions have already been completed, so that a duplicate invoice is not sent.

CONTROL 2: Implement Control 6 - Cancelling documents after they are completed – for example marking a sales order as “shipped” when the goods are sent to the customer. This would also include marking the sales order as “invoiced” when the customer is billed.

CONTROL 3: Implement Control 7 - Having management periodically check the work of employees. This is an additional check to be sure the two controls above are implemented by the employees.

Required Activities

Following are the situations for which you are to determine which of the above ten controls should be implemented. You are only allowed to select the THREE controls that you think will best mitigate the risk. Be sure to explain how each control will help to mitigate the risk. Be sure to use the same format as the example above.

RISK 1: Employees in the shipping department steal goods from the company inventory while picking goods for shipment to a customer.

CONTROL 1:

CONTROL 2:

CONTROL 3:

RISK 2: The employee making the bank deposit alters the deposit slip and keeps some of the cash that was to be deposited in the bank.

CONTROL 1:

CONTROL 2:

CONTROL 3:

RISK 3: A GBI employee creates fake sales returns and issues cash refunds even though no goods were purchased by the customer and no goods are returned. The GBI employee pockets the money from the refund.

CONTROL 1:

CONTROL 2:

CONTROL 3:

RISK 4: The employee that picks and packs the goods is lazy and uses the picking list as the shipping report even though some of the items were not available and weren't included in the shipment.

CONTROL 1:

CONTROL 2:

CONTROL 3:

RISK 5: An employee that receives customer payments commits lapping fraud by diverting a payment from the customer's account and concealing it by posting payment from a different customer to the account.

CONTROL 1:

CONTROL 2:

CONTROL 3:

To follow up you need to:

- Identify three additional risks that you think could be serious problems for GBI.
- Using the same format as above, determine the three controls that can be used to mitigate the risk you developed. The three controls you use can be taken from the ten controls stated above or you can use controls other than the ten described above.

In this part of the assignment you will be graded on the importance of the risk to GBI and the appropriateness of the three controls you employ to mitigate the risk.

RISK 6:

CONTROL 1:

CONTROL 2:

CONTROL 3:

RISK 7:

CONTROL 1:

CONTROL 2:

CONTROL 3:

RISK 8:

CONTROL 1:

CONTROL 2:

CONTROL 3:

Part 2 – Assignment of Duties

In this part of the assignment you are to determine whether GBI has effectively assigned its employees to each of the 26 sales tasks listed above. That is, you must assess whether GBI's SOD constitutes good control – control that is not too expensive or overburdening, but protects the company from fraud and errors. You may reassign tasks to each of the employees listed or assign tasks to other GBI employees not currently involved in the sales-to-cash process. Hint: It may be helpful to reference the risk assessment you completed in part 1. By assessing whether specific risks are reduced by segregating certain duties, this can help you analyze incompatible tasks.

For example, even though the first two tasks are stated as if they are done by two different people, they could be done by only one employee without violating SOD. So with respect to these tasks, the present GBI assignment of duties is not a problem and doesn't need to be changed. However, if these tasks were in conflict, then you must reassign the conflicting tasks and fully explain why there was a conflict and how your reassignment resolves the problem. This should be done for each of the above 26 tasks with the consideration that the company wants good control procedures, but also wants the minimum number of employees involved so that the cost of operations can be minimized. You must also take into consideration operating efficiencies; that is, will the document and order processing disrupt business activities or make job completion particularly onerous or cumbersome? Also, GBI is large enough that one employee would not have to do incompatible or illogical tasks. For example, a warehouse employee handling goods would not also handle cash even though these are both custody of asset functions. The background and training for a single employee to do both of these tasks would have to be too broad. Put in different terms, the question you need to ask is if your task assignments also make good business sense.

The following Job Assignment Matrix shows how tasks in the 26 step sales-to-cash business process are currently assigned to the following roles.

Sales Representative needs to have personal contact and form a relationship with the customer. That means that tasks 1, 2, 5, 7, 9, 23 and 24 need to be done by the sales representative.

Accounts Receivable handles technical tasks. Hence, accounts receivable has task 8.

Sales Support Staff has the primary job of making the sales representatives more productive. They are tasked with doing the routine jobs that could be done by the sales representatives, but can be more efficiently done by support staff at a lower cost. With this in mind, the sales support staff is responsible for tasks 3, 4 and 10.

Inventory Clerk needs to anticipate what orders are coming in from the customers and also needs to pick and pack the goods and then get them ready for shipping. So the inventory clerk does tasks 11 through 16.

Shipping Clerk takes care of loading the truck with the goods and the related paper work. That means that the shipping clerk does tasks 6 and 17 through 21.

Billing Clerk processes the documentation dealing with the customer. The billing clerk does tasks 22, 25 and 26.

All of these assignments are shown on the following task matrix.

Task Assignment						
	Sales Rep	Sales Support Staff	Accounts Receivable	Inventory Clerk	Shipping Clerk	Billing Clerk
1. A customer sends a purchase order for off-road bicycles to a GBI employee	√					
2. A GBI employee compares the customer's purchase order to determine if the customer's master data is in the system and is correct.	√					
3. If the customer master data is not in the system or is incorrect, then the master sales and distribution data for the customer is entered by a GBI employee.		√				
4. If the customer master data is not in the system or is incorrect, then the financial data (such as banking information and GBI reconciliation account) for the customer is entered by a GBI employee.		√				
5. If the customer master data is not in the system, then a GBI employee checks the credit rating of the customer and assigns a credit limit and credit terms.	√					
6. A GBI employee checks inventory availability.					√	

Task Assignment						
	Sales Rep	Sales Support Staff	Accounts Receivable	Inventory Clerk	Shipping Clerk	Billing Clerk
7. If the customer can be extended credit and inventory is available, a GBI employee takes the customer's purchase order and creates a sales order.	√					
8. A GBI employee creates an order acknowledgement and sends it to the customer.			√			
9. A GBI employee records the sales order.	√					
10. A GBI employee creates a picking ticket to fill the customer's order.		√				
11. A GBI employee picks the goods (the bicycles) from the picking ticket.				√		
12. A GBI employee creates a packing slip and a mailing label.				√		
13. A GBI employee puts the packing slip into the reinforced container with the goods, seals the container and adheres the mailing label to the container.				√		
14. A GBI employee moves the goods from the inventory control area to the shipping dock				√		

Task Assignment						
	Sales Rep	Sales Support Staff	Accounts Receivable	Inventory Clerk	Shipping Clerk	Billing Clerk
15. A GBI employee creates a shipping manifest				√		
16. A GBI employee places the goods on the truck to be shipped				√		
17. A GBI employee gives the shipping manifest to the truck driver					√	
18. A GBI employee creates a shipping document to show that the goods have been shipped					√	
19. A GBI employee records that the goods have been shipped					√	
20. A GBI employee creates an invoice with a remittance advice and sends it to the customer					√	
21. A GBI employee receives the payment from the customer with the returned remittance advice					√	
22. A GBI employee records the payment from the customer						√
23. A GBI employee takes all of the payments for that day and makes up a deposit slip for the bank	√					
24. A GBI employee deposits the cash in the bank.	√					

<i>Task Assignment</i>						
	Sales Rep	Sales Support Staff	Accounts Receivable	Inventory Clerk	Shipping Clerk	Billing Clerk
25, A GBI employee records the bank deposit.						√
26. A GBI employee reconciles bank deposits with the cash receipts on a daily basis.						√

The 'Part 2' tab of the Submission Template contains the information from the above matrix. To this spreadsheet add any of the following roles that you feel are necessary to accomplish appropriate segregation of duties controls:

- Receptionist
- Secretary
- Mailroom Clerk
- Warehouse Assistant
- Treasury Clerk
- Treasurer
- Accounting Manager
- Controller
- Office Manager
- Maintenance Supervisor
- Others you determine

Now reassign tasks, where appropriate to mitigate any known Segregation of Duties risks. You can reassign tasks to any of the employees listed in the original matrix or assign tasks to other GBI employees not currently involved in the sales-to-cash process (the new roles from above that you are adding to your spreadsheet).

Hint: It would be helpful to reference the risk assessment you completed in part 1.

Part 3 – Authorization Matrix

The analysis in parts 1 & 2 implies that actual paper documents are being produced in order to complete the sales transaction. For most companies this is an invalid assumption since most of the steps in this type of transaction are computerized.

For this part of the assignment you need to determine the level of computer authorization each one of the people that you assigned tasks to in part 2 should have in order to properly complete their tasks. Hence, we want you to develop a closed security model in which you determine what computer access authorizations each one of the people in the sales-to-cash business process should be granted.

To properly organize your analysis you should place the results of this part of the assignment into an authorization matrix (See Part 3 tab in the submission template). Along the top of the matrix put each of the roles involved in the sales activity (those people from step 2, above). Down the left-hand side are the electronic documents involved in the process. The cells of the matrix should be filled with the symbol for the type of access that person should be allowed. The possible access types and their corresponding symbols are:

C – Create authorization – the user can create a new document

R – Read authorization – the user has access to the document in order to see its contents

U – Update authorization – the user can change, edit, or void an existing document

D – Delete authorization – the user can eliminate the document from the system

A – Authorize authorization – the user can signify that the document is authorized and should go on to the next step of the process

The electronic documents listed on the left-hand side of the matrix are:

- Customer general sales master data – The general customer master data such as name, address, contact information, etc.
- Customer financial master data – Confidential customer data such as bank accounts, credit card information, etc.
- Customer credit master data – Confidential customer data dealing with credit status
- Credit authorization – The documentation stating the credit limits and credit terms for each customer
- Sales order – The internal order that is used to start the process of delivering the product to the customer
- Sales order acknowledgement – Copy of the sales order or similar document sent to the customer to confirm the agreed upon sales terms
- Picking ticket – Internal document used in pulling the desired products off the shelf in order to deliver them to the customer
- Packing slip – Listing of goods in the shipment (usually included with the respective goods)
- Shipping manifest – Listing of goods, quantity, and sometimes weights and volume of the packages in the shipment, usually carried by the transporting company's employee
- Shipping report – Internal report of the goods shipped out
- Invoice – The billing information to be sent to the customer
- Record of payment from customer – Record of the cash received
- Bank deposit slip – Record of deposit of the cash into the bank

- Bank statement – Document showing transactions recorded in GBI’s account by the bank

For example, the employee doing the pre-sales and sales (steps 1 and 2) might have the following entries in the matrix:

Document\Person	Sales Employee	Person 2	Person 3 ...
Customer general sales master data	C, R, U		
Customer financial master data	R		
Customer credit master data	R		
Credit authorization	R		
Sales order	C, R, U, A		
Sales order acknowledgement	R		
Picking ticket	R		
Packing slip	R		
Shipping manifest			
Shipping report	R		
Invoice	R		
Record of payment from customer	R		
Bank deposit slip			
Bank statement			

Based on the information in the matrix, the sales employee can create, read and update a customer’s general master data. The sales employee can create, read, update, and authorize a sales order but cannot delete the sales order document. The sales employee can only read the customer financial and credit master data. The sales employee can read the credit authorization, sales order acknowledgement, shipping report, invoice and the information on payment by the customer, but

can't create, update, delete or authorize any of these. For all of the other documents, the employee has no authorizations.

It is your job to determine the people involved in the process (you already did this in part 2), place their names along the top of the matrix and then fill in the authorizations they should be granted with respect to each of the documents.

Part 4 – Implementation in an ERP System

In the final part of the assignment you will be examining the authorization process in the SAP system and compare those authorizations with the matrix you completed in part 3 of this assignment.

SAP enforces a very strong security policy. Every time an SAP transaction is executed, the user's authorizations are checked against that transaction to be sure that user is authorized to take the specific action. If the authorizations properly check, then the transaction proceeds. Otherwise, the user is informed that they are not authorized to execute the transaction and the process is terminated.

One of the strengths of the SAP authorization policy is the granularity of the security. This granularity extends to not just finely defining the types of business transactions the user can execute and the privileges allowed, but also the business objects that the user can process. For example, the authorizations can be granted to allow reading of the data in a document for a specific transaction, but not the ability to create a new document or change an existing document for that same transaction. Also, the SAP authorization system can restrict the specific document the user can access. For example, the user may be allowed access to retail customers, but not wholesale customers. Or the user may be allowed access to customers in the western United States, but not in the eastern United States.

While the SAP system is based on profiles, authorizations, authorization objects and fields, the users are categorized by their role in the organization. Hence, the role a user plays in the organization dictates what authorizations that user is granted. This is a strong form of authorization control since when an employee changes jobs, the authorizations can be changed immediately so that the employee can do the tasks of the new job, but also the authorizations associated with the old job are removed from the system for that employee.

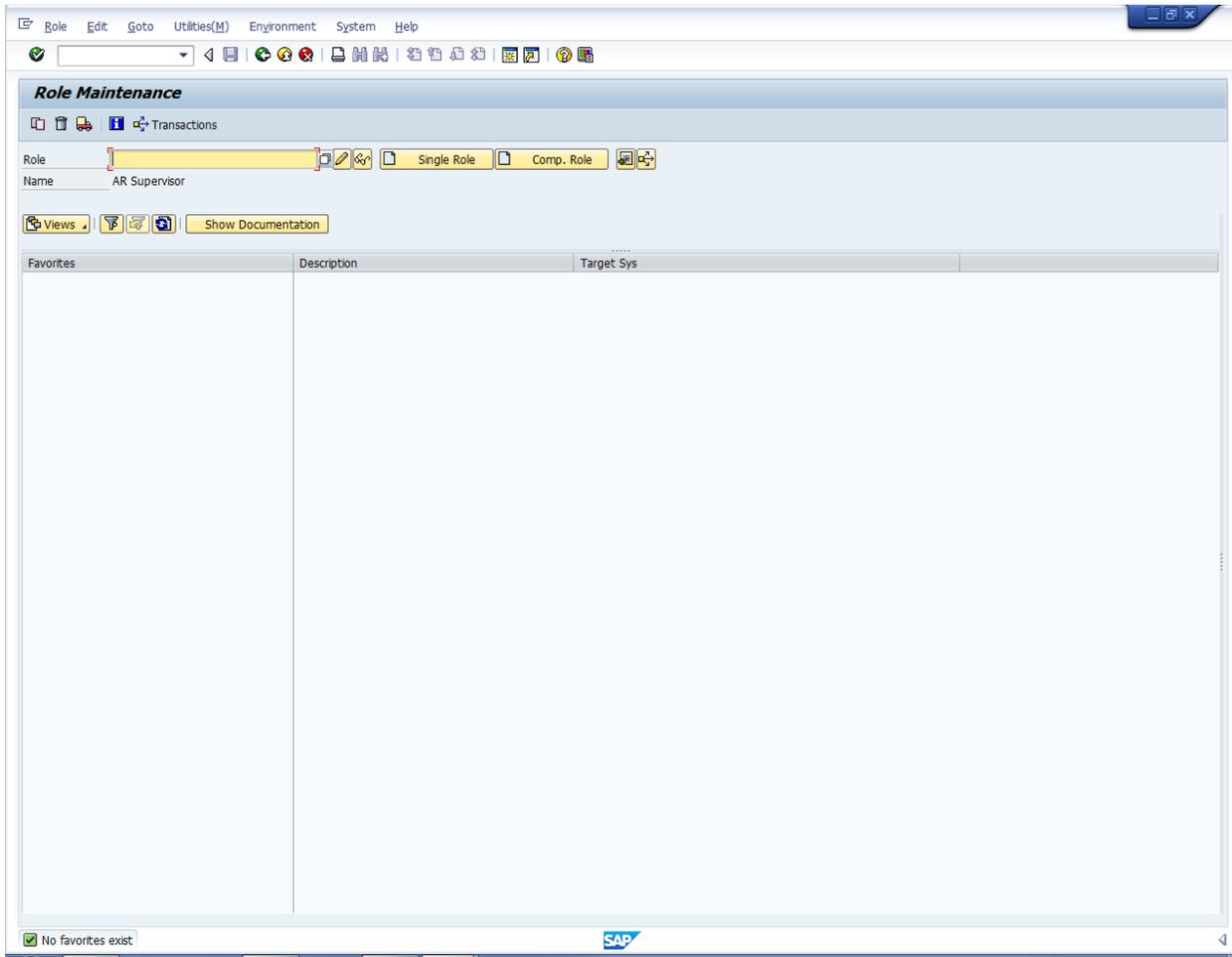
SAP groups authorizations together using a profile. A profile can contain many authorizations or it can contain additional profiles. Hence, the role that we are looking at is also termed a profile.

An SAP authorization is composed of a series of authorization objects.

In the following, we ask you to examine some of the roles that are already defined in the system and investigate how SAP assigns authorizations based on these roles.

To access the predefined system roles, log into SAP using the same SAP system you used in previous assignments and then take the following path:

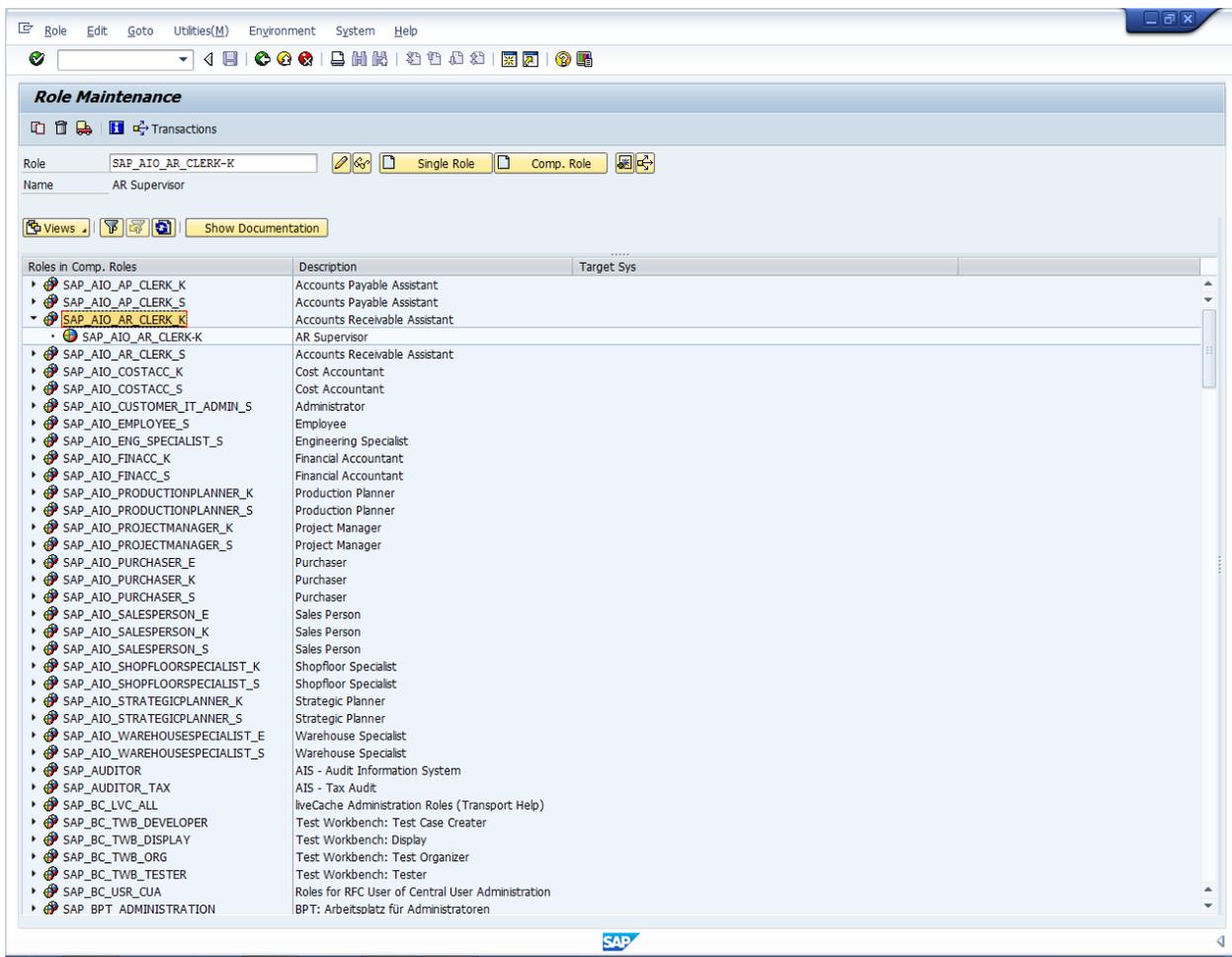
Tools -> Administration -> User Maintenance -> Role Administration -> Roles {PFCG}



In the Role Maintenance screen hit the Views button and select *Roles in Comp. Roles* (this means you wish to view the roles that belong to a composite role, i.e. a group of roles).

This displays all of the system roles available and the sub-roles under those roles.

Expand the A/R clerk role (*SAP_AIO_AR_CLERK_K*) by selecting the right facing triangle.

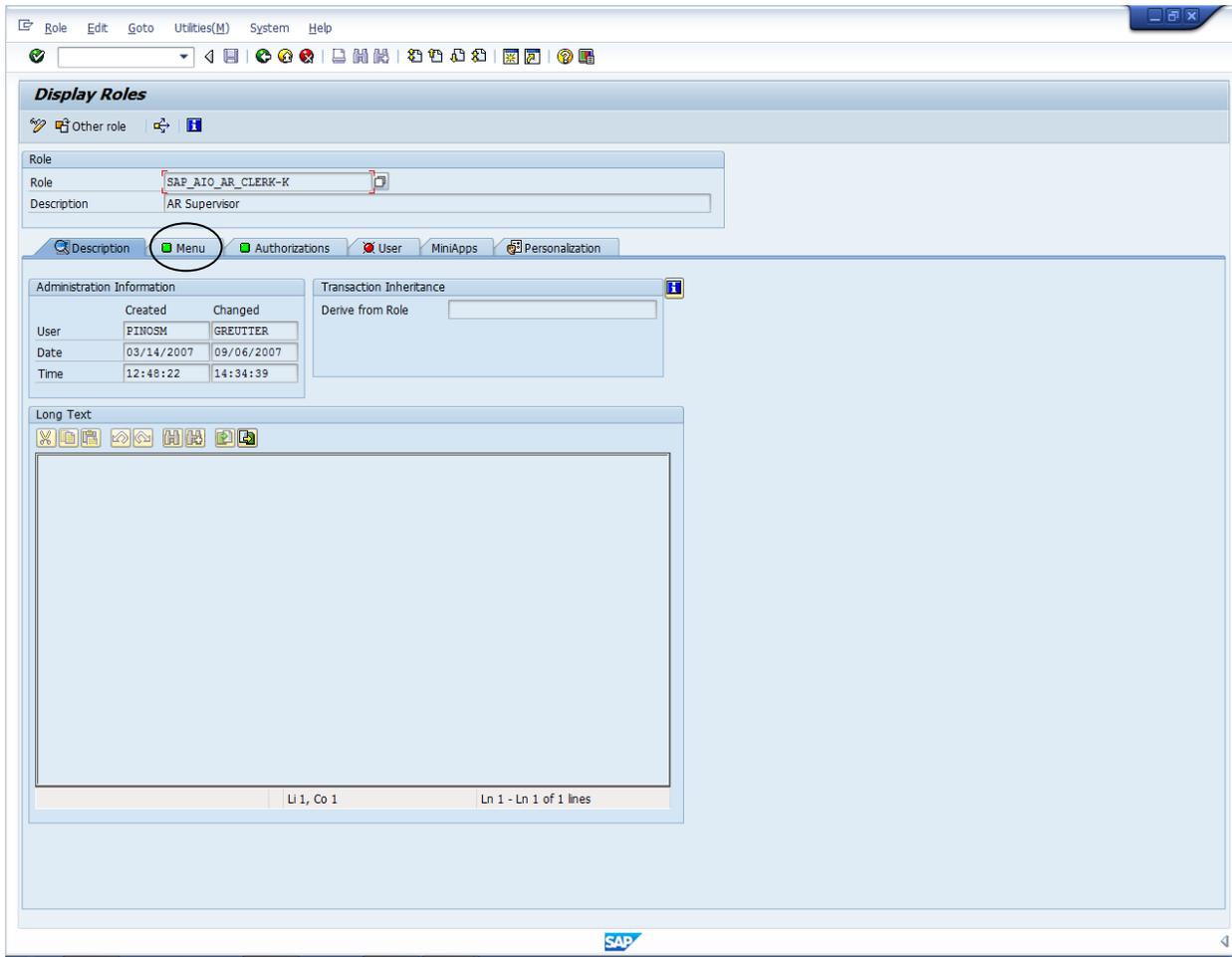


Highlight the A/R Supervisor, (*SAP_AIO_AR_CLERK-K*) role and click on the *Display Role* button (the icon with the eye glasses).

The screenshot shows the SAP Role Maintenance interface. The role 'SAP_AIO_AR_CLERK-K' is selected and highlighted in yellow. The 'Display Role' button, represented by an icon of eye glasses, is circled in red. The interface includes a menu bar (Role, Edit, Goto, Utilities(M), Environment, System, Help), a toolbar with various icons, and a table of roles.

Roles in Comp. Roles	Description	Target Sys
▶ SAP_AIO_AP_CLERK_K	Accounts Payable Assistant	
▶ SAP_AIO_AP_CLERK_S	Accounts Payable Assistant	
▼ SAP_AIO_AR_CLERK_K	Accounts Receivable Assistant	
• SAP_AIO_AR_CLERK-K	AR Supervisor	
▶ SAP_AIO_AR_CLERK_S	Accounts Receivable Assistant	
▶ SAP_AIO_COSTACC_K	Cost Accountant	
▶ SAP_AIO_COSTACC_S	Cost Accountant	
▶ SAP_AIO_CUSTOMER_IT_ADMIN_S	Administrator	
▶ SAP_AIO_EMPLOYEE_S	Employee	
▶ SAP_AIO_ENG_SPECIALIST_S	Engineering Specialist	
▶ SAP_AIO_FINACC_K	Financial Accountant	
▶ SAP_AIO_FINACC_S	Financial Accountant	
▶ SAP_AIO_PRODUCTIONPLANNER_K	Production Planner	
▶ SAP_AIO_PRODUCTIONPLANNER_S	Production Planner	
▶ SAP_AIO_PROJECTMANAGER_K	Project Manager	
▶ SAP_AIO_PROJECTMANAGER_S	Project Manager	
▶ SAP_AIO_PURCHASER_E	Purchaser	
▶ SAP_AIO_PURCHASER_K	Purchaser	
▶ SAP_AIO_PURCHASER_S	Purchaser	
▶ SAP_AIO_SALESPERSON_E	Sales Person	
▶ SAP_AIO_SALESPERSON_K	Sales Person	
▶ SAP_AIO_SALESPERSON_S	Sales Person	
▶ SAP_AIO_SHOPFLOORSPECIALIST_K	Shopfloor Specialist	
▶ SAP_AIO_SHOPFLOORSPECIALIST_S	Shopfloor Specialist	
▶ SAP_AIO_STRATEGICPLANNER_K	Strategic Planner	
▶ SAP_AIO_STRATEGICPLANNER_S	Strategic Planner	
▶ SAP_AIO_WAREHOUSE SPECIALIST_E	Warehouse Specialist	
▶ SAP_AIO_WAREHOUSE SPECIALIST_S	Warehouse Specialist	
▶ SAP_AUDITOR	AIS - Audit Information System	
▶ SAP_AUDITOR_TAX	AIS - Tax Audit	
▶ SAP_BC_LVC_ALL	liveCache Administration Roles (Transport Help)	
▶ SAP_BC_TWB_DEVELOPER	Test Workbench: Test Case Creator	
▶ SAP_BC_TWB_DISPLAY	Test Workbench: Display	
▶ SAP_BC_TWB_ORG	Test Workbench: Test Organizer	
▶ SAP_BC_TWB_TESTER	Test Workbench: Tester	
▶ SAP_BC_USR_CUA	Roles for RFC User of Central User Administration	
▶ SAP_BPT_ADMINISTRATION	BPT: Arbeitsplatz für Administratoren	

On the Display Roles screen select the *Menu* tab.

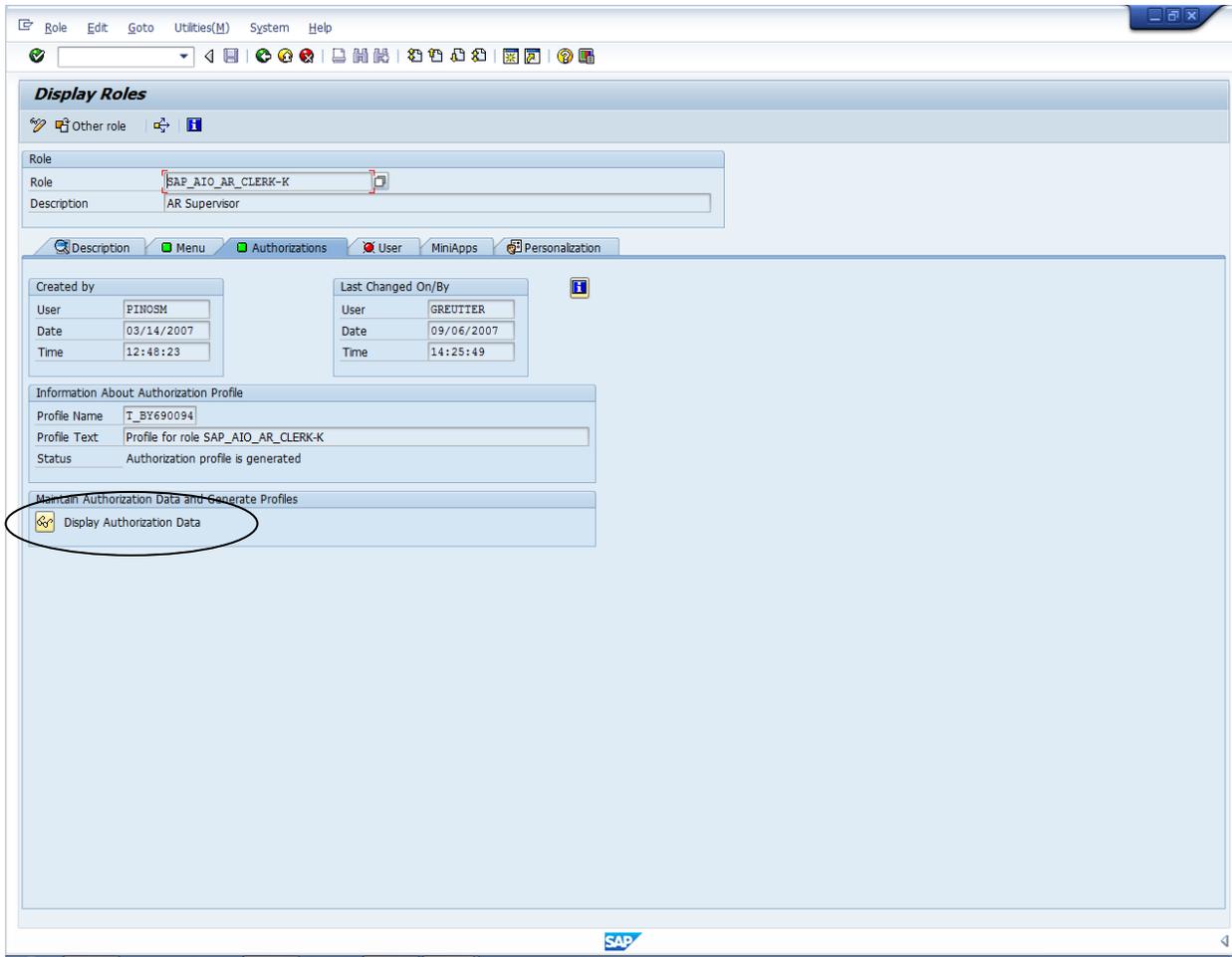


Expand the menu list. This shows the transactions that this authorization allows the user to do (the technical term is that this is a User Menu). In order to provide additional control, a user could be shown only the user menu and not even be allowed to see the general SAP menu that you normally see when you first log into SAP. However, a user menu does not restrict the actual transactions the user can execute, only those that they know about. This is sometimes termed an ignorance control.

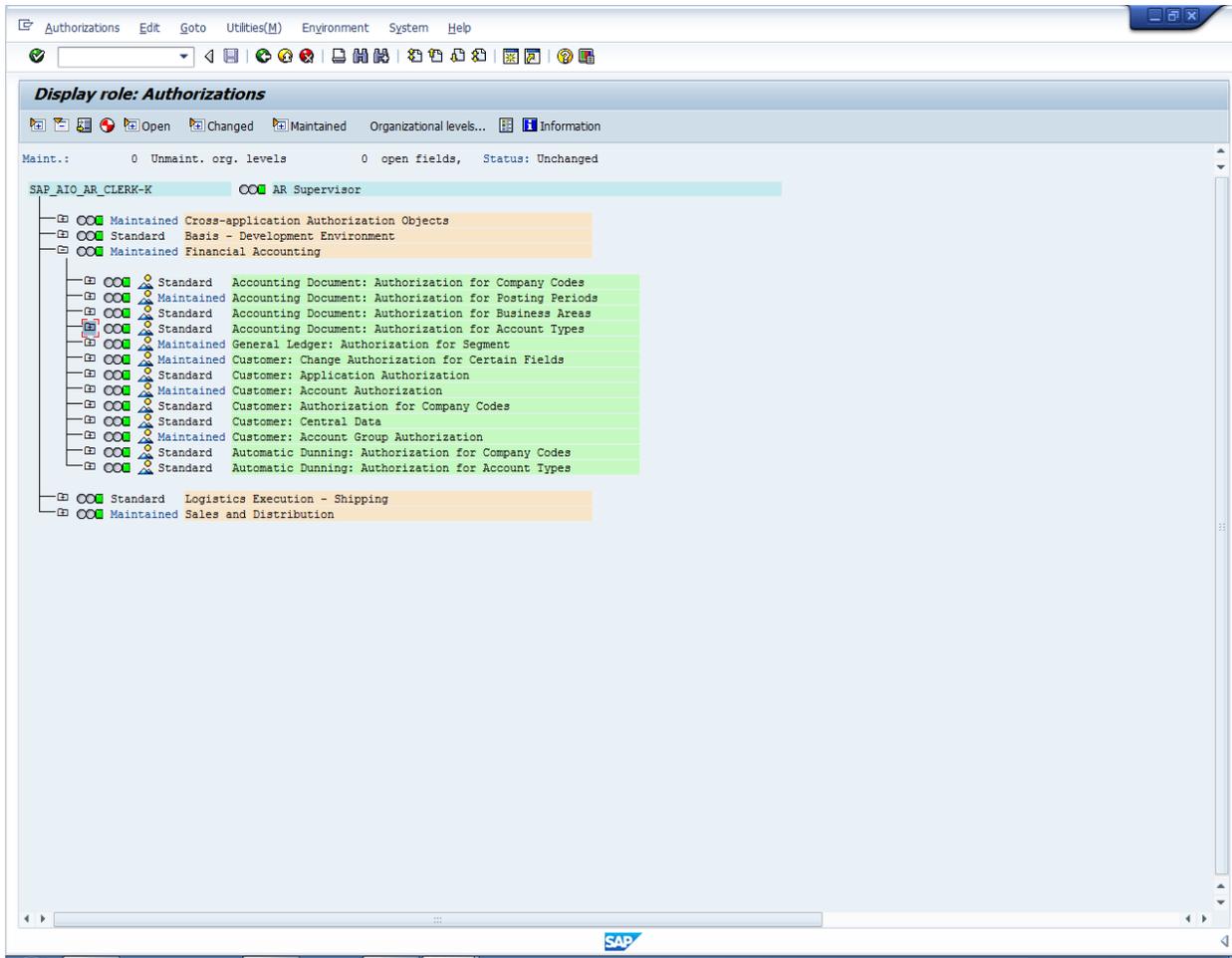
Question 4.1: Explain the logic behind an ignorance control. If this was the only control for a specific set of risks, do you think that it would be an effective control? Explain your answer.

Question 4.2: Choose one of the tasks under the Periodic and Closing Activities and explain what the task is.

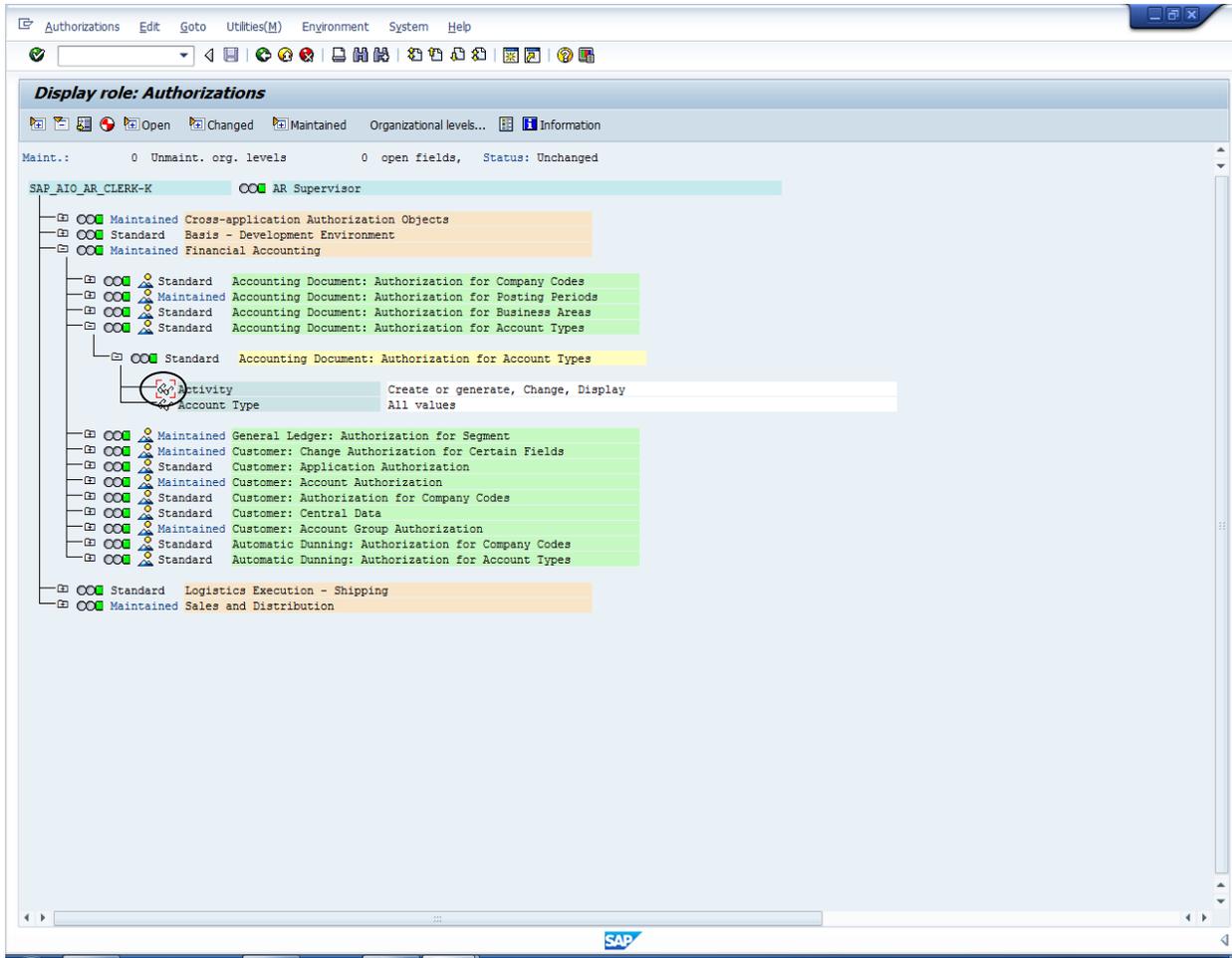
Now go to the Authorizations tab. Click on display authorizations data.



Expand the authorizations matrix in the Financial Accounting area by clicking on the plus sign to the left of the role. Explore the various authorizations for the AR Supervisor role.



Choose and expand the Standard Accounting Document: Authorization for Account Types.
Click on the view details icon (the eyeglasses icon) to the left of Activity.

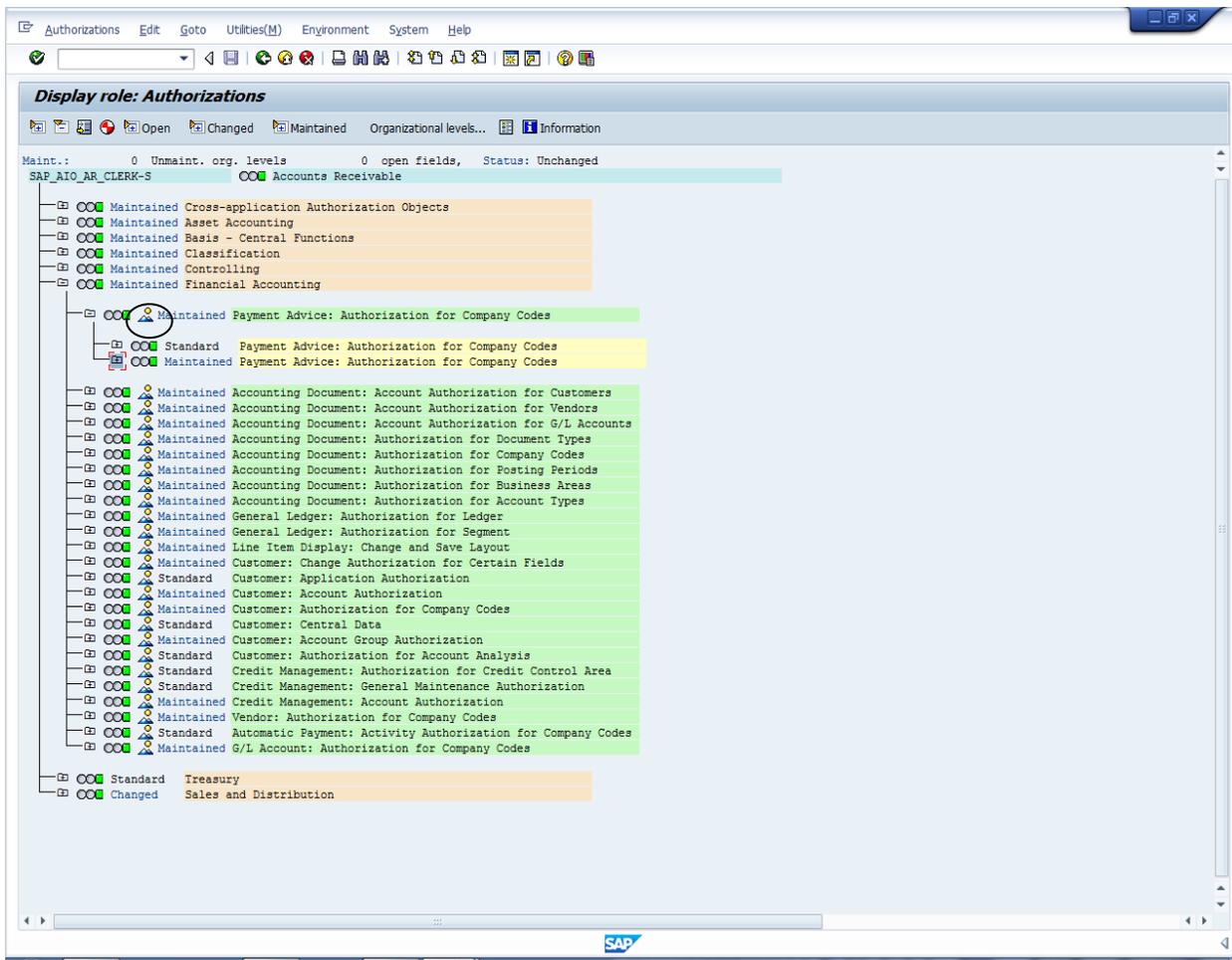


Question 4.3: What authorizations does the AR Supervisor not have for Account Types? Why do you think the AR Supervisor would be restricted from these authorizations for this accounting document?

Using the preceding steps, look at the authorizations for the role AR Accountant *SAP_AIO_AR_CLERK-S*.

Question 4.4: What activities and authorizations differ between the two roles?

For the AR Accountant role, expand the Financial Accounting authorizations table and click on the overview icon (the mountain) to the left of Payment Advice Authorization for Company Code.



Question 4.5: What is the transaction code and activity description related to the authorization?

Question 4.6: Based on your examination of the SAP roles and authorizations, can you tell what a person's job title and responsibilities might be for each of these profiles? Explain.

So far we have only looked at preconfigured SAP roles. For most companies the assignment of responsibilities to their employees can be different from that of the standardized roles that SAP provides. That means that it would be the responsibility of the user authorization and security group to customize the roles provided by SAP. As you might imagine, this is not a simple task. The authorization matrix that you developed in step 3 of this case could be used to develop the necessary authorizations for each role.

When users are first assigned roles, there is a good chance that the proper authorizations were not granted for the users to accomplish their jobs. In this case, the transaction being executed will fail authorization check. The user authorization and security group must then investigate why the transaction failed. This may sound like a daunting task, but there are tools that can be used to simplify the process. Here is an example that we want you to try.

Get to the roles screen by the following path:

Tools -> Administration -> User Maintenance -> Role Administration -> Roles {PFCG}

Enter TESTROLE in the *Role* screen field. Under the *Role* pull down (at the top of the screen) select

Create -> Role

Question 4.7: What happened? Why?

Now enter the following into the transaction entry box (top of screen to the right of the green check mark):

/OSU53

This allows you to analyze why the transaction failed authorization. Briefly analyze why the previous transaction failed.

This ends the assignment.

NOTE: An abbreviated version of this assignment has been provided for you to turn in your answers for grading. The abbreviated document is called “EX4 SOD Submission Template.xlsx”.