A Segregation of Duties Case Study in the Purchase-to-Pay Process with an SAP Example

Volume 2, Number 1
2007
page 1 – 21

Nancy Jones
California State University, Chico, njones@csuchico.edu, (530)898-4832
Jim Mensching
California State University, Chico, jmensching@csuchico.edu, (530)898-6405

Abstract

With the advent of legislation dealing with financial responsibility and information assurance, the topic of segregation of duties has gained additional importance. Recent studies have found that segregation of duties is one of the areas in which companies have frequently disclosed material internal control weaknesses under reporting requirements of the Sarbanes-Oxley Act of 2002. 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 R/3 system is used to illustrate the implementation of segregated duties in one type of ERP system. There are four steps to the case: assessing risks of the business process, defining positions within the organization to handle a set of defined tasks, developing an authorization matrix for designated employees, and examining the SAP authorizations system.

Keywords
Keywords Segregation of duties, expenditure cycle, SAP user authorizations, risk assessment, access control matrix

A teaching note is available for use with this case. If you are member of the AIS Educator Association, please go to http://www.aiseducators.com and follow the links for the AIS Educator Journal. If you are not a member of the Association, please contact the author directly at the address provided above to obtain these materials. Please provide a means for verifying your credentials as a faculty member so that we may protect the integrity of the solutions materials.

INTRODUCTION

With the advent of legislation dealing with financial responsibility and information assurance, the topic of segregation of duties has gained additional importance. Recent studies have found that segregation of duties is one of the areas in which companies have frequently disclosed material internal control weaknesses under reporting requirements of the Sarbanes-Oxley Act of 2002 (Ge & McVay 2005).

While segregation of duties has traditionally been an important area of internal controls, the new COBIT guidelines stress this as a separate detailed control objective (COBIT V4.1 2007). In addition, small business and not-for-profit organizations have also experienced many problems due to a lack of segregation of duties (Hodges 2002; Lenk & Donnelly 1998). Accounting information system textbooks spend a good amount of time dealing with this subject (Romney & Steinbart 2006; Gelinas, Sutton & Hunton 2005).

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 R/3 system is used to illustrate the implementation of segregated duties in one type of ERP system.

We have found that students struggle with applying SOD concepts, especially within a highly integrated computerized environment such as that found in most large organizations that use ERP systems. During the semesters we have used this assignment,

we observed that by the end of the course, students have a better understanding of the SOD concepts than students in previous semesters where the case was not used.

Because this case is presented prior to class discussion of business cycles, it also acts as an introduction to the transactions common to the expenditure cycle. Specifically, the case deals with buying goods from another company (B to B activity) 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. There are four steps to the case.

Step 1: The student is asked to assess the risks involved in this business process. Risks should include possible errors, lost opportunities, fraud, etc. We specifically limit the risk discussion to a narrow band of threats since addressing other threats such as system and interface point threats makes the problem much more complex. For example, system threats are covered in detail in the COBIT standard. However, COBIT is well beyond the scope of this assignment and is actually only covered in a very cursory manner in the entire course. Interface considerations are also complex topics that can only be addressed during and after coverage of the business cycles.

This assignment involves the purchasing cycle. The company conducts four different types of purchase transactions: inventory, fixed assets, contract services, and routine goods and services. We chose to use the purchase of routine goods and services for this activity as it is a simpler process as compared to the other types of purchasing transactions. In addition, many of the risks to this type of purchase can be addressed by segregation of duties, which is the purpose of this activity. In contrast, purchase of inventory introduces a level of complexity to the case we feel inappropriate for students at this stage in their first AIS course. The case strives to focus the student on segregation of duties rather than sorting through the intricacies of inventory management, production scheduling, and distribution. Purchase of fixed assets and purchase of contracted services also are somewhat less easily understood by undergraduates as these are generally non-routine transactions.

Step 2: Using the risk analysis as a base, the student is to then define positions within the organization to handle the defined set of 28 tasks within the business process and assign the specific tasks to the individual personnel in such a way that there is adequate segregation of duties without incurring excess personnel costs. As an alternative to having students define personnel and job assignments, a substitute Part 2 is offered in the Appendix to this document. The modified assignment gives students information about employees currently responsible for the 28 tasks within the business process and asks them to analyze any SOD risks and reassign tasks to minimize the identified risks.

Step 3: The student must then develop an authorization matrix, which specifies the extent of computer access for each of the employees designated in the previous step. This step transitions the student from a paper-based environment to an integrated computerized environment that is typically used in business and prepares the student for step 4 of the assignment which illustrates how an authorization matrix could be used to create a security role in the SAP system.

Step 4: Using the student's understanding of the authorization matrix developed in step 3, the last part of the assignment involves examining the SAP authorization system where the student will see how to establish rules that enforce segregated duties. This part of the assignment uses data from the SAP R/3 IDES (Internet Demo and Evaluation System) to illustrate the security configuration in an ERP system.

PURCHASE TO PAYMENT CASE STUDY

Company Background

The Acme Company is a large automotive secondary market manufacturer. The automotive secondary market involves manufacture of after-market parts for many different brands and models of automobiles. For example, if your car needs a replacement muffler, starting motor, generator, etc. then you have the choice of buying the part from the original manufacturer (OEM), which is usually expensive, or from a secondary market manufacturer, usually substantially less expensive.

Acme has manufacturing plants located in Detroit Michigan, Newark New Jersey and Oakland California. It also has distribution warehouses in seven cities in the U.S., two in Europe, one in China, three in Japan, one in Mexico and two in South America.

Acme has a centralized purchasing system that is located in the headquarters in Detroit. The procedure that is followed to acquire materials and supplies varies with the type of goods that are being purchased. There are four categories of goods and services that are acquired. They are:

the goods and services that are used for production of the products that the company produces,

the acquisition of the fixed production assets,

services that involve contract negotiation,

the goods and services that are acquired for the normal support of the general operations of the firm.

Examples of the each of these categories follow. The first category of acquisitions includes the raw materials and subassemblies used for producing the finished goods. This includes metal castings, various grades of wire, bulk plastics for injection molding, oils and lubricants and many other similar products. The ordering of this category of goods is initiated by the inventory control personnel. This ordering activity must be coordinated with the planned production activity and the projected sales and marketing activity.

The second category of acquisitions involves the ordering of heavy production equipment such as serialized machines, turret lathes, pneumatic presses, and other similar production equipment. The initiation of the ordering of these types of goods is done by the production engineers. This activity is coordinated with the long-term strategic production plans (included in the capital budgeting process) and the research and development engineers.

The third category of acquisition involves contracting of services. For example, all maintenance and service contracts for equipment fall under this category. In addition, contracts for consulting and outsourcing services are also included in this category. These transactions involve quite a bit of legal contract negotiation and hence Acme has a staff of lawyers that are involved in these transactions.

The last category of acquisitions includes the office supplies that are used by all support personnel, computer equipment and supplies, and similar items. This activity is originated by individual employees.

Since the business processes are different for each category, each of the four above categories has a separate area within the centralized purchasing organization that deals with the acquisition of those goods and services. In this assignment, you are only asked to examine the business process and controls involved in the fourth acquisition category.

Acquisition Business Process

The company uses the following steps to acquire goods for their employees:

Ordering Goods:

An Acme employee determines that there is a need for goods in order to do their job.

An Acme employee fills out a purchase requisition form for the desired goods.

An Acme employee signs the purchase requisition and submits it to another Acme employee.

An Acme employee approves the purchase requisition.

An Acme employee sends acknowledgement and disposition of the requisition back to the originating employee, (if the requisition wasn't approved, the process stops here).

An Acme employee submits the approved purchase requisition form to centralized purchasing and other appropriate people.

An Acme employee records the purchase requisition information.

An Acme employee determines the appropriate product to order.

An Acme employee determines the appropriate vendor to order from and checks to see if the vendor's master data is in the system and is correct.

If the vendor master data is not in the system or is incorrect, then an Acme employee confirms the master data and payment terms with the vendor and enters the master data into the system.
An Acme employee consolidates purchase requisitions and creates a purchase order.
An Acme employee sends the purchase order to the vendor and other appropriate people.
An Acme employee receives an order acknowledgement from the vendor.
An Acme employee records the purchase order information.

Receiving and Storing Goods:

The vendor ships the goods with a packing slip to the destination on the purchase order and an Acme employee receives the goods at the receiving dock at our location.
An Acme employee counts the goods in the shipment.
An Acme employee removes the packing slip from the box and sends it to the appropriate people.
An Acme employee fills out a receiving report that has details on the time of the arrival and the items received.
An Acme employee records the packing slip information.
An Acme employee records the receiving report information.
An Acme employee passes the goods on to the designated recipients.
An Acme employee who requested the goods receives the desired goods.

Paying for Goods:

The vendor sends the invoice and remittance advice for payment and an Acme employee receives the invoice and remittance advice.
An Acme employee compares all of the documents for the order (that is, a voucher package is compiled).
An Acme employee approves payment of the invoice.
An Acme employee creates the payment check.
An Acme employee sends the payment check and remittance advice to the vendor.

Verification:

Periodically an Acme employee verifies all of the documentation to be sure that the transaction has been handled correctly.

Security and Information Assurance

Acme is very concerned about security and information assurance. With the recent passage of the Sarbanes-Oxley law, Acme now realizes that solid financial accounting controls are extremely important for the corporation. Originally Acme 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. For example, the system administrators knew that normal business users should not be allowed to create new user accounts or to add new tables to the database. Hence, these authorizations were restricted to system administrators and application developers. However, for most business transactions, it was thought that restricting access was not necessary. In fact, the philosophy was that the more access an employee had, the more they would learn about the system and hence the more useful they would be to the company.

Acme 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. Of course, 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 risk 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 or non-integrated accounting system is to classify duties as to their responsibility with respect to the following four duties (sometimes textbooks only discuss the segregation of the first three duties). Execution of the transaction is assumed to occur within any of the first three duties:

Authorization of the transaction

Recording of the transaction

Custody of assets involved in the transaction

Auditing or reconciliation of the various aspects of the transaction (Reconciliation of accounts is the duty sometimes unaddressed by textbook authors discussing SOD. However, many others recognize the importance of segregation of the reconciliation function from the other three. Additionally, in our experience, all but the smallest of businesses commonly segregate the reconciliation duties from authorizing, recording, and custody duties. The additional segregation of duties obviously provides for stronger internal control.)

In theory, separate individuals should be granted each of these responsibilities. If this is the case, this introduces a series of checks and balances that help to assure the proper handling of the transaction. Of course, employee collusion could circumvent these 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 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 that the accounting system generates documents for each step of a transaction. In SAP, each step of a transaction generates a document and all documents in a transaction scheme are linked together by the unique document numbers. 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

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 audit trail of the transaction

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

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

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.

The first step in doing an analysis of the segregation of duties should involve a detailed assessment of all of the potential risks involved in the transaction. This means that it is necessary to fully understand the business transaction. While most people think of criminal activity when they initially think about risk analysis, it is only one aspect of analyzing risk. Studies have found (Gelinas 2005, 235, Romney 2006, 145) that a majority of problems arise from non-fraudulent sources such as errors in processing, lost transactions, delayed processing, poor record keeping, etc. Doing a comprehensive risk analysis enables the development of strong internal controls to mediate these risks. Segregation of duties is one of the key internal controls in mediating risks since it reduces the probability of fraud and also introduces checks and balances into a system, thereby reducing the chance of processing errors.

The Information Systems Audit and Control Association defines risk as

> Risk is the possibility of an act or event occurring that would have an adverse effect on the organization and its information system. Risk can also be the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. (ISACA, 2002)

Risk is normally analyzed by looking at the two factors of risk – threats and vulnerabilities. A threat is the probability someone or something can in some way damage, corrupt, or defraud a system. Threats are a result of actions and can be intentional or unintentional. For example, a very liquid and valuable asset, such as cash, has a high threat level with respect to theft because it is a very desirable target for dishonest people since it is so marketable. At the same time, a fixed asset such as a building has a much lower threat level with respect to theft, since it would not be as easy for dishonest people to convert the building to their use.

Vulnerability deals with the opportunities inherent in something that allows for that item to be damaged, corrupted, or defrauded. If a company was to leave its cash lying on a desk open to all employees and customers, this would make it very vulnerable. However, locking the cash in a vault and restricting access to the vault greatly reduces the vulnerability. Vulnerability is usually something that a company can control, since vulnerabilities can be reduced by introducing additional internal controls, while threats are substantially less controllable. The product of the probability of all of the threats and all of the vulnerabilities is the risk to a specific operational system.

Part 1 – Risk Analysis

You are to assess the risks involved in the purchase transaction. Since you are not familiar with the controls used by the company in this case, we are asking you to only assess the threats to the system and are not asking you to assess the vulnerabilities. With respect to the threats, you are to determine if the source of the threat is external, coming from outside of the company or internal, coming from a source within the company. For example, an error can originate outside of the company, such as the vendor sending us the wrong goods, but most errors would originate within the company. Under each category (External Threats, Internal Threats) you are to list the individual types of threats and then determine if the specific threat could be mitigated by enforcing segregation of duties (SOD). If you believe that SOD mitigates the risk, then you need to state how it does.

In a normal business assessment of risk, the next step would be to assess the vulnerabilities and then suggest internal controls that could be used to mitigate each of the threats. In this case, we are only concerned with the segregation of duties control.

Please use the format in Exhibit I to present your risk analysis:

Exhibit I – Format for Risk Analysis

Risk Analysis

External Threats:	**Mitigated by SOD?**
The vendor sends the invoice for the incorrect amount	No
…	
Internal Threats:	
The Acme employee creates the payment check for the incorrect amount	Yes, because of additional checking
…	

Part 2 – Assignment of Duties

In this part of the assignment, you are to determine who in the organization should be doing the 28 purchasing tasks that are listed above. That is, you must assess what constitutes good control – control that is not too expensive or overburdening, but protects the company from fraud and errors. So you have to state who would be doing each of these tasks. Hint: It will be helpful to reference the risk assessment you completed in part 1. By assessing if specific risks are reduced by segregating certain duties, this can help you analyze incompatible tasks.

For example, even though the first three tasks are stated as if they are done by three different people, they could be done by only one employee. So your answer would be that the employee doing the purchase requisition activities should do tasks 1 through 3 and give a brief explanation of why the consolidation of these tasks are not in conflict with good control procedures. This should be done for each of the above 28 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? Note: You may find it helpful to assign your employees job titles rather than just generic labels such as “employee 1” or “employee A”.

Part 3 – Authorization Matrix

The analysis in parts 1 & 2 implies that actual paper documents are being produced in order to complete the purchasing 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 designated 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 purchasing business process should be granted for each document.

To properly organize your analysis you should place the results of this part of the assignment into an authorization matrix. Along the top of the matrix you should put each of the people involved in the purchasing activity (those people from step 2, above). Down the left-hand side you should put 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

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

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

The documents that are to be listed on the left-hand side of the matrix should be:
Purchase Requisition
Purchase Order
Packing Slip
Receiving Report
Vendor Invoice
Payment Voucher
Check for Paying Vendor

For example, the employee doing the purchase requisition (steps 1, 2 and 3) might have the following entries in the matrix in Exhibit II:

Exhibit II – Authorizations Matrix

Document\Person	Employee needing goods	Person 2	Person 3 …
Purchase Requisition	C, U, R		
Purchase Order	R		
Packing Slip			
Receiving Report	R		
Vendor Invoice	R		
Payment Voucher			
Check for Paying Vendor			

Hence, the employee needing goods can create, update, and read a purchase requisition. This employee can only read the purchase order, the receiving report and the vendor invoice. For all of the other documents, the employee has no authorizations. You should note that this employee cannot delete or authorize any documents.

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 to achieve proper segregation of the authorization, recording, custody and audit reconciliation duties and allow efficient completion of the process.

Part 4 – Implementation in SAP

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 the 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 security. This granularity extends to not just finely

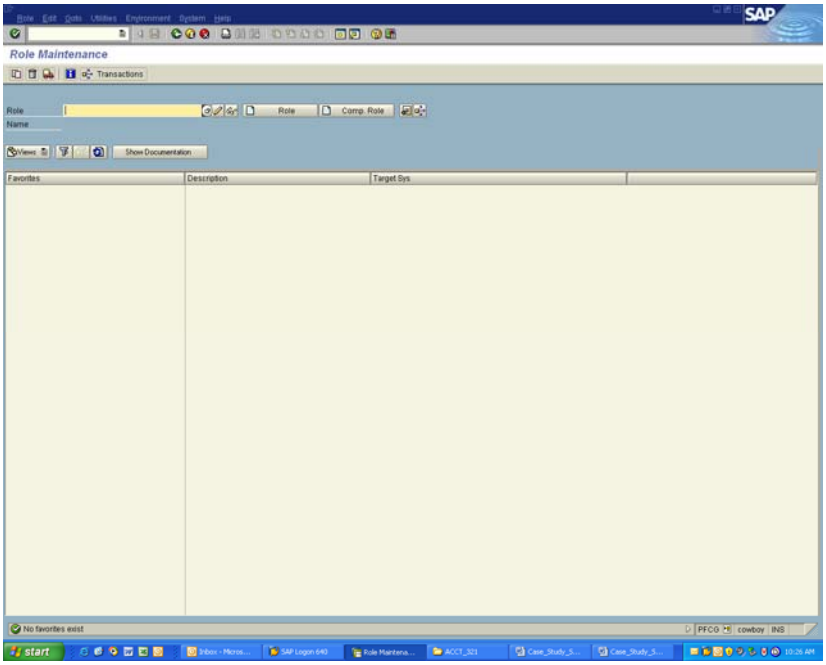
defining the types of business transactions the user can execute and the privileges allowed, but also the business objects that the user can process. For example, the authorizations can be granted to allow reading of the data in a document for a specific transaction, but not the ability to create a new 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 (all these will be explained in a little bit), 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.

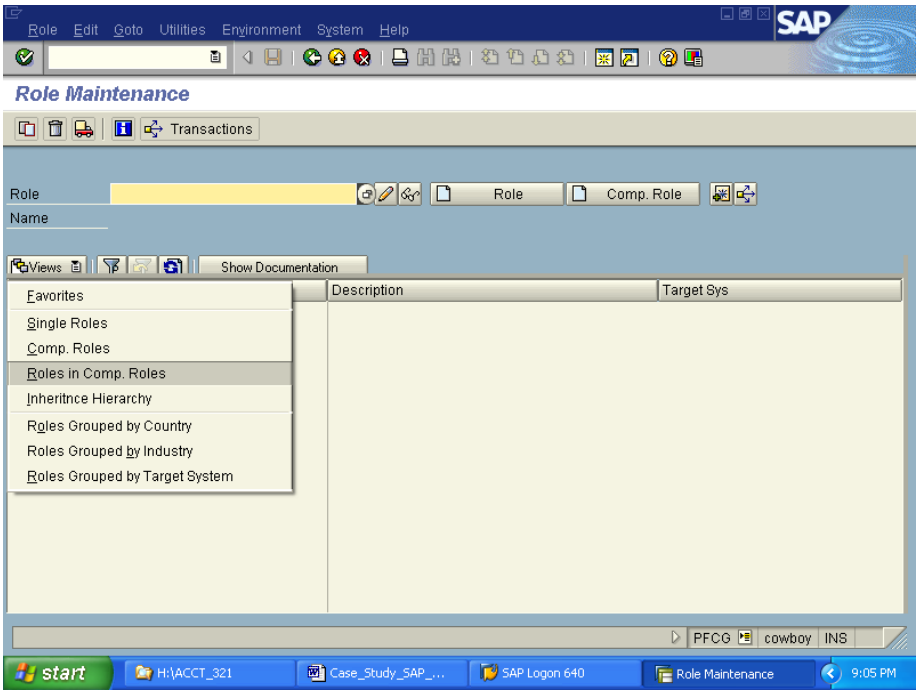
In the following, we ask you to examine some of the roles that are already defined in the system and investigate how SAP assigns authorizations based on these roles.

To access the predefined system role, log into SAP and then take the following path:

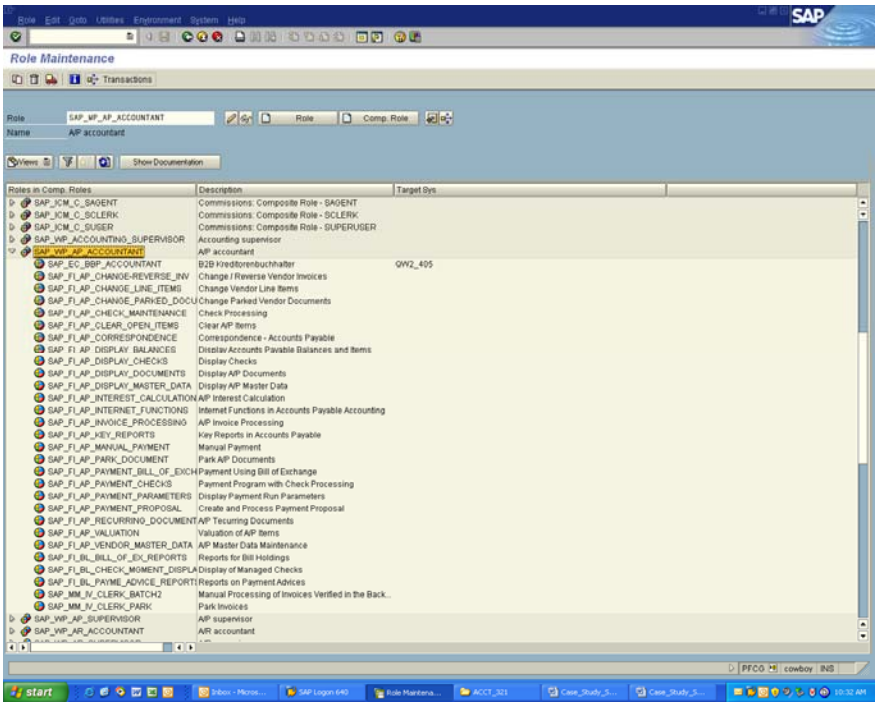
Tools -> Administration -> User Maintenance -> Role Administration -> Roles



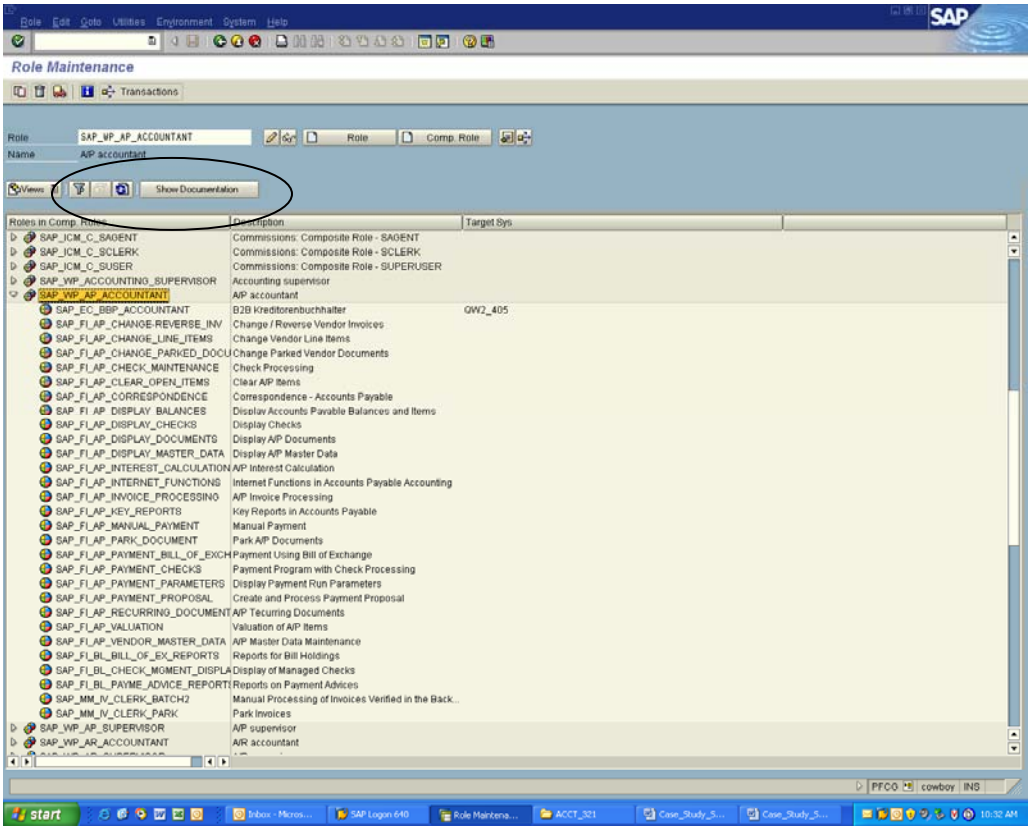
In the Role Maintenance screen, hit the Views button and select *Role in Comp. Roles* (this means you wish to view the roles that belong to a composite role, i.e. a group of roles).



This displays all of the system roles available and the sub-roles under those roles.
Expand the A/P accountant role (*SAP_WP_AP_ACCOUNTANT*) by selecting the right facing triangle.

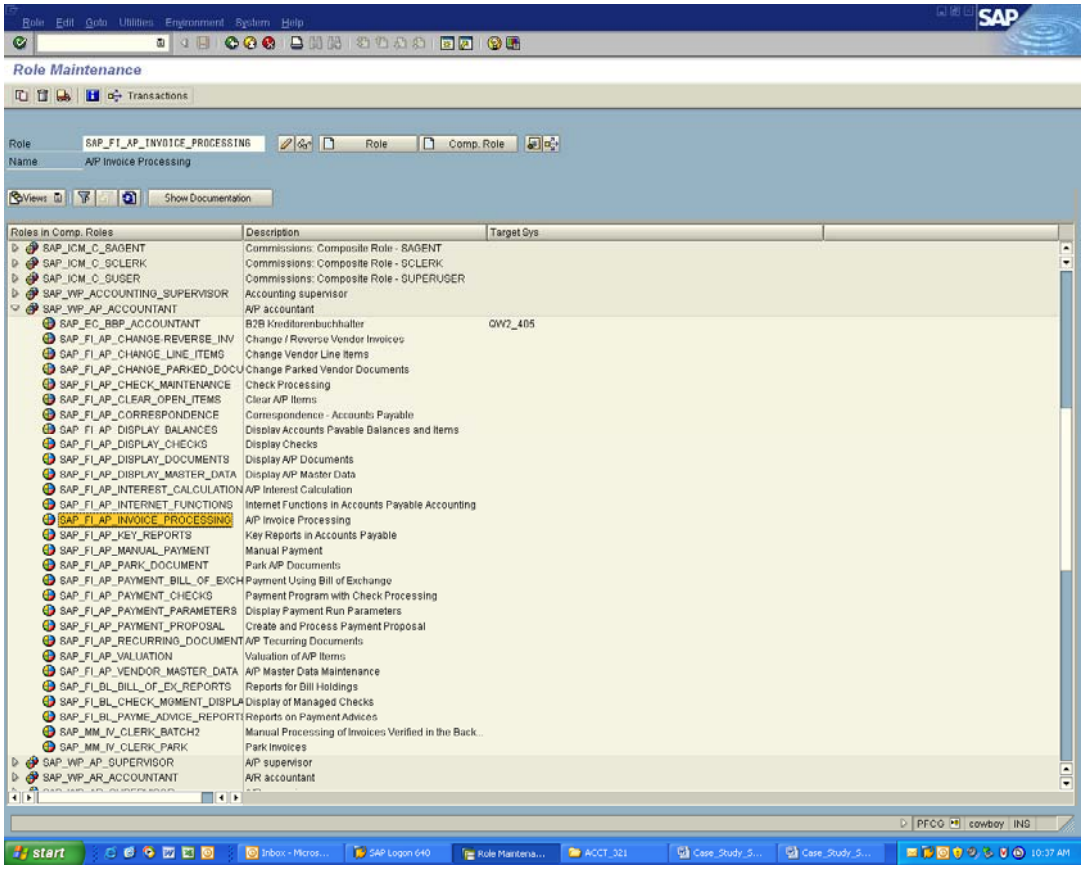


Now highlight the A/P accountant role and hit the *Show Documentation* button.



Question 4.1: Be sure to read this documentation. Write a short summary (in your own words) about what the role entails (Remember, cutting and pasting is cheating). What are this person's job functions?

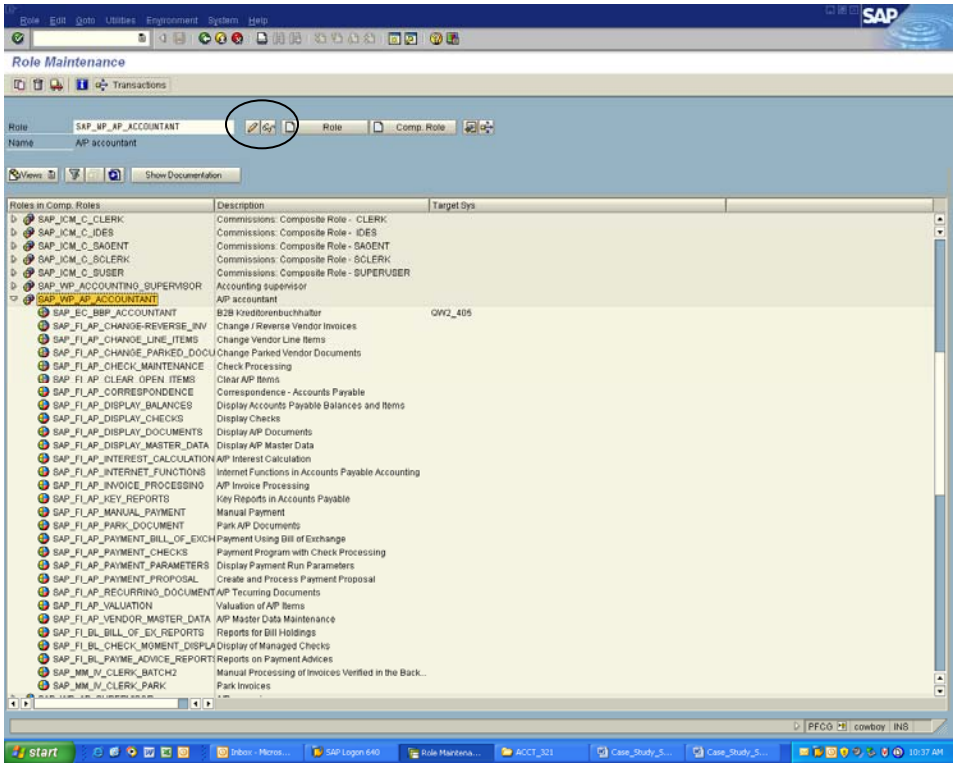
Highlight A/P Invoice Processing (*SAP_FI_AP_INVOICE_PROCESSING*) and read that documentation.



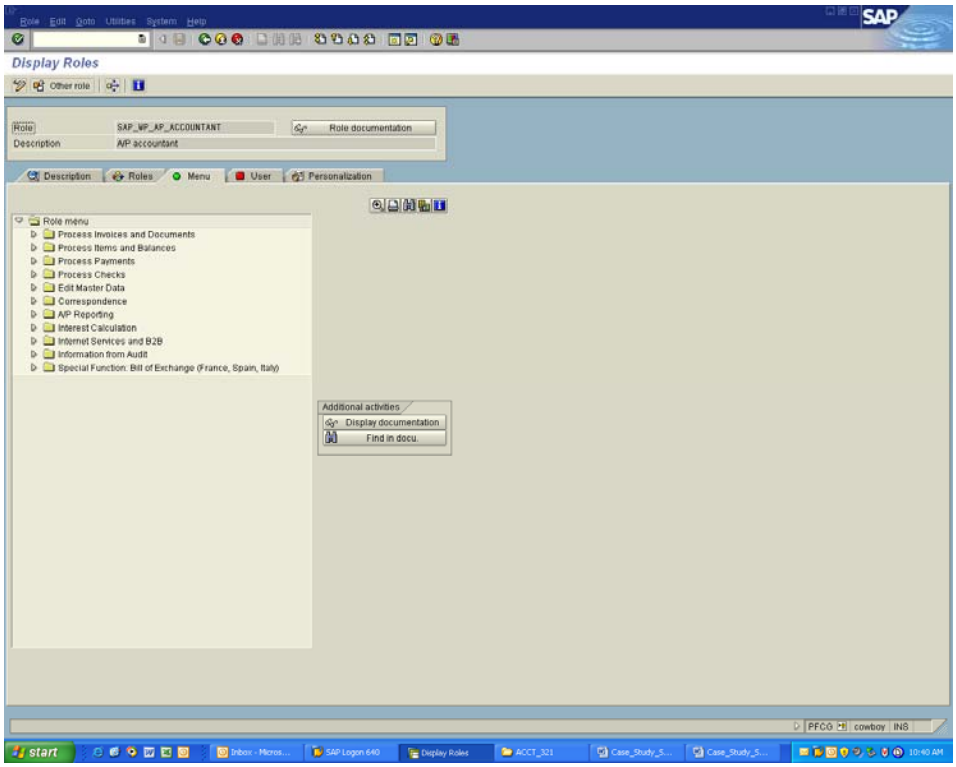
Question 4.2: Under what circumstances would you issue the A/P Accountant role to an employee?

Question 4.3: When would it be better to just issue the A/P Invoice Processing role to an employee rather than the A/P Accountant role?

Highlight the A/P accountant role and hit the *Display Role* button (the icon with the eye glasses).

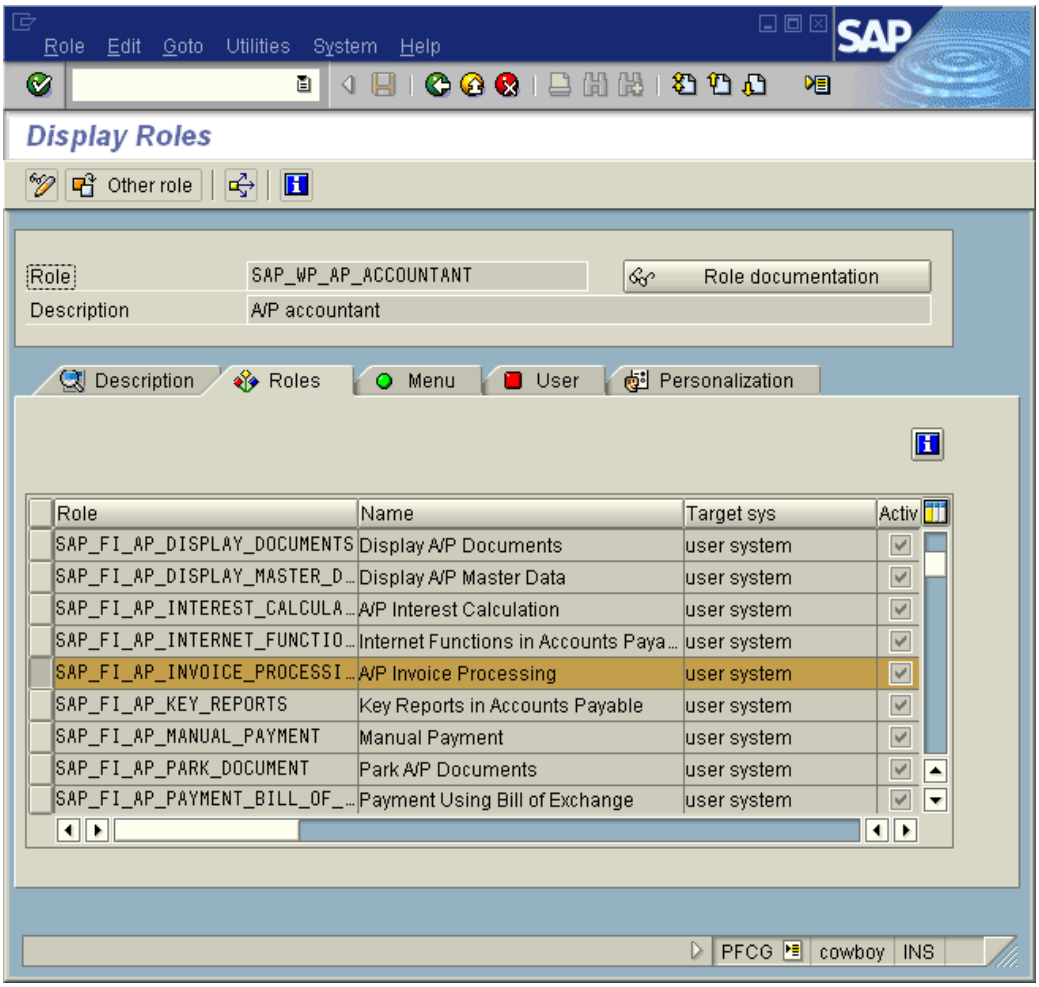


On the Display Roles screen select the *Menu* tab.



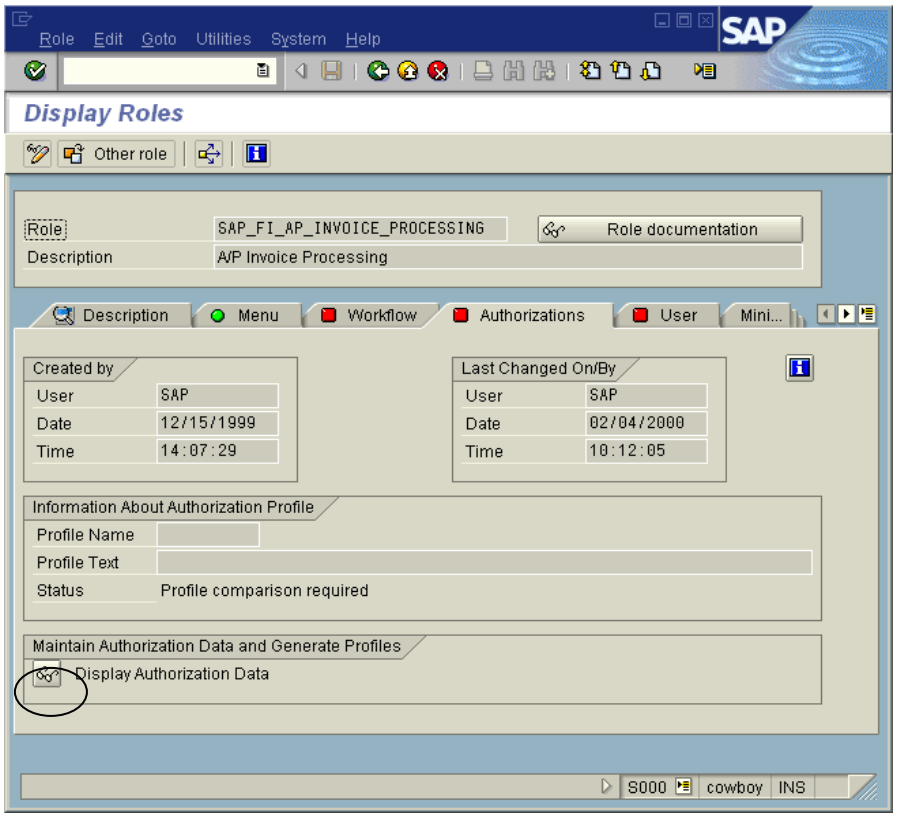
Question 4.4: What does this allow the user to do? In other words, what are the user's job functions?

Now go to the *Roles* tab and select the *A/P* Invoice Processing line and highlight it (use the left-most button). Double click on this role.

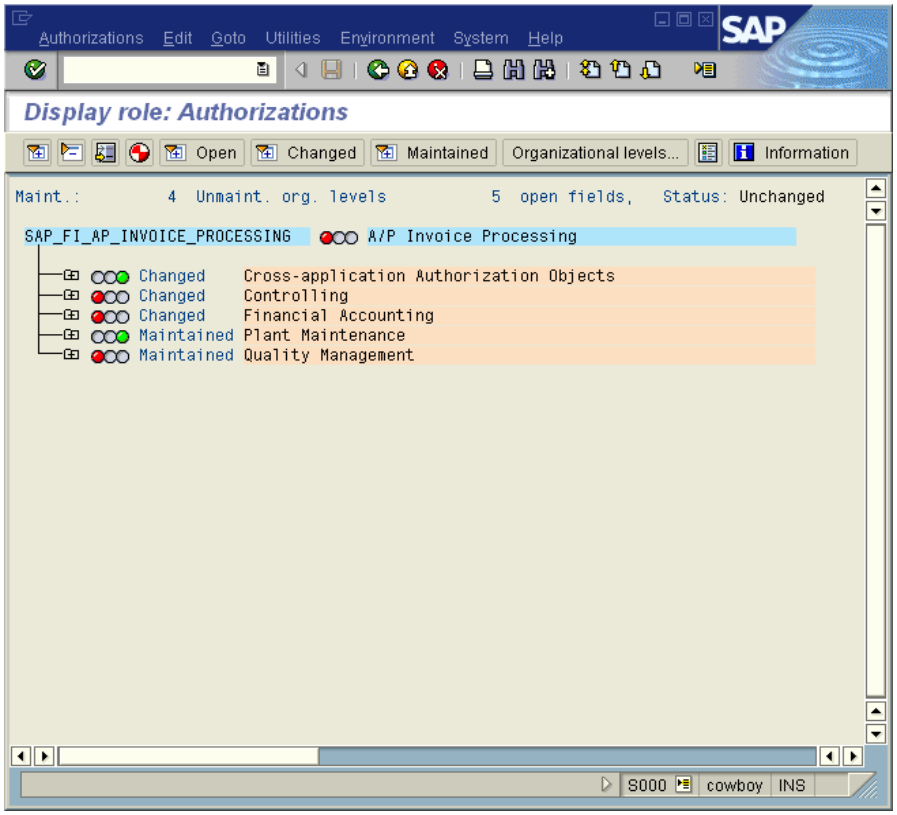


Question 4.5: A new session is started. Examine the *Menu* tab again. What has changed?

Now select the Authorizations tab and under Maintain Authorization Data and Generate Profiles hit the Display Authorization Data (the eye glass icon).



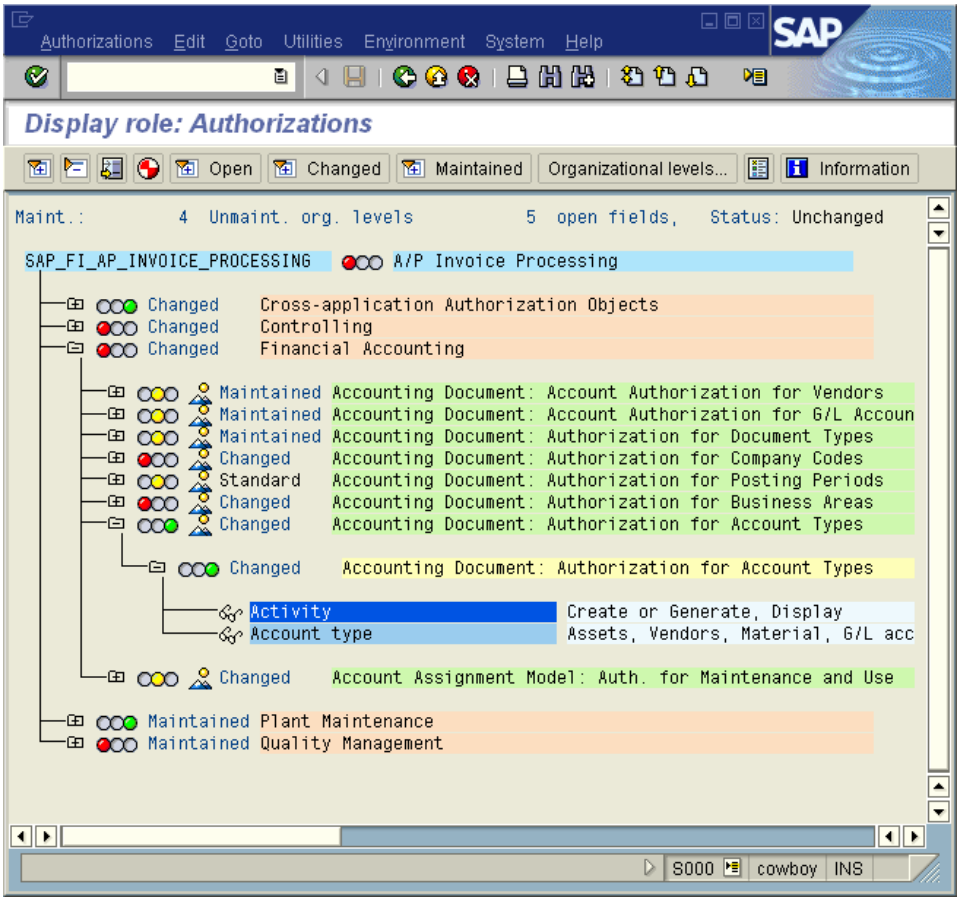
This brings you to a screen that shows the authorizations that are granted for the role.



SAP groups authorizations together using a profile. Hence, 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. Click on the plus sign next to *Financial Accounting* and this expands the tree and shows the authorization objects under the *Financial Accounting* authorization. Then expand the *Accounting Document: Authorizations for Account Types* authorization object.



This shows the fields that can be assigned values for this authorization object.

Question 4.6: What does the *Activity* field allow the user to do? What activities is the user not allowed to do? Explain the reasoning behind this configuration. (Hint: double click on the values to see all values allowed.)

Question 4.7: Now look at the *Account Type* field. What is the purpose of this field? Can you explain how the values could be changed in this field under different business circumstances?

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.

Generally, the person that specifies the authorizations is not allowed to program the authorizations and the person activating the

authorizations should be an entirely separate individual. The testing of the authorization can be done by the person who specified it, but it is best if this task is done by a separate test team. The issuance of authorizations is done by a security specialist and the authorizations are issued to work positions (i.e. jobs) and not individuals. Human resources will then assign individuals to work positions and the employee will then obtain the authorizations because of his or her job. Thus, company accountants should not actually implement a control plan in the ERP. This would be done by a security officer or at the very least a system administrator (COBIT V4.0 control objective DS5.3). To allow the company's accountants access to security assignments is a serious IT control weakness.

Question 4.8: Why would it be better to base and issue security authorizations to a specific work position and not directly to the person doing the work?

When users are first assigned roles, there is a good chance that the proper authorizations may not be 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. In fact, many companies find that authorization problems are a major issue when an ERP system goes live. It may sound like a daunting task to solve these types of problems, 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

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

Create -> Role

Question 4.9: What happened? Why?

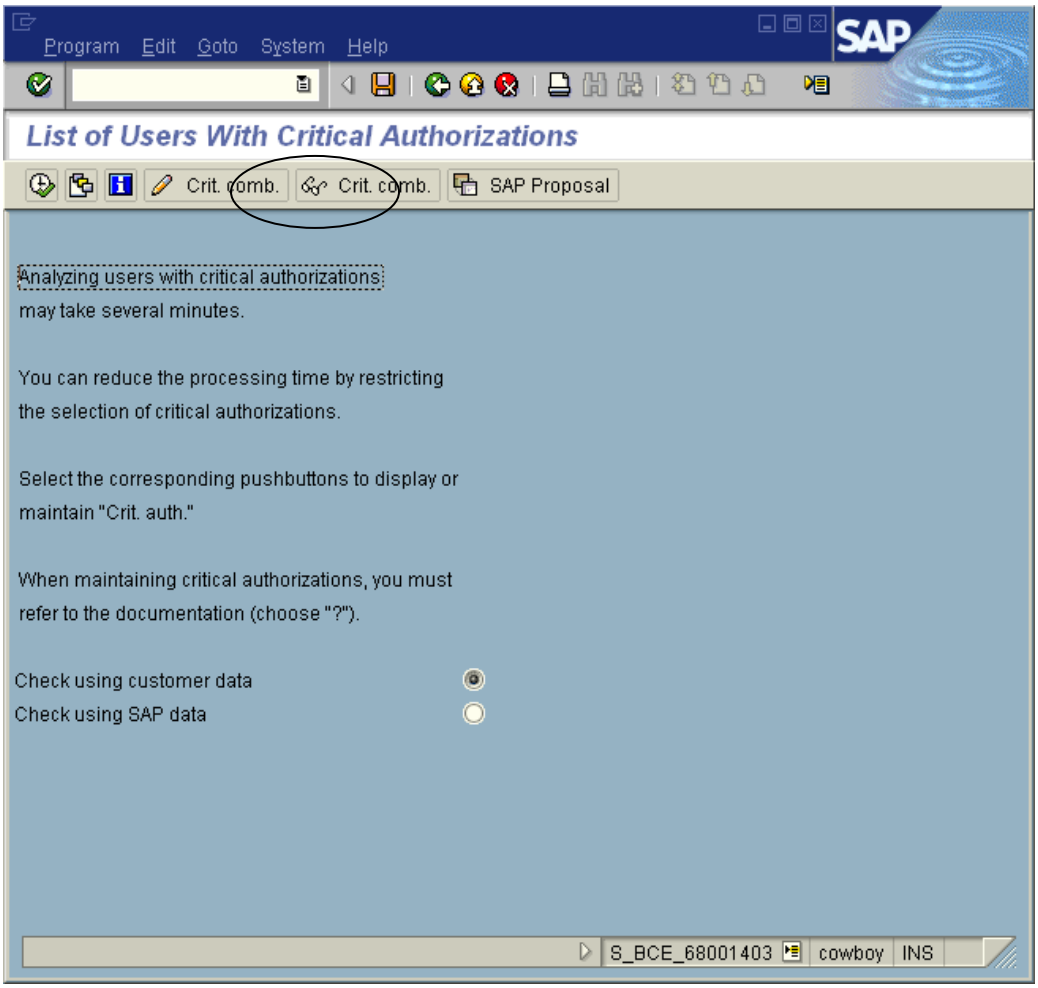
Now enter the following into the transaction entry box (top of screen to the right of the green check mark):

/OSU53

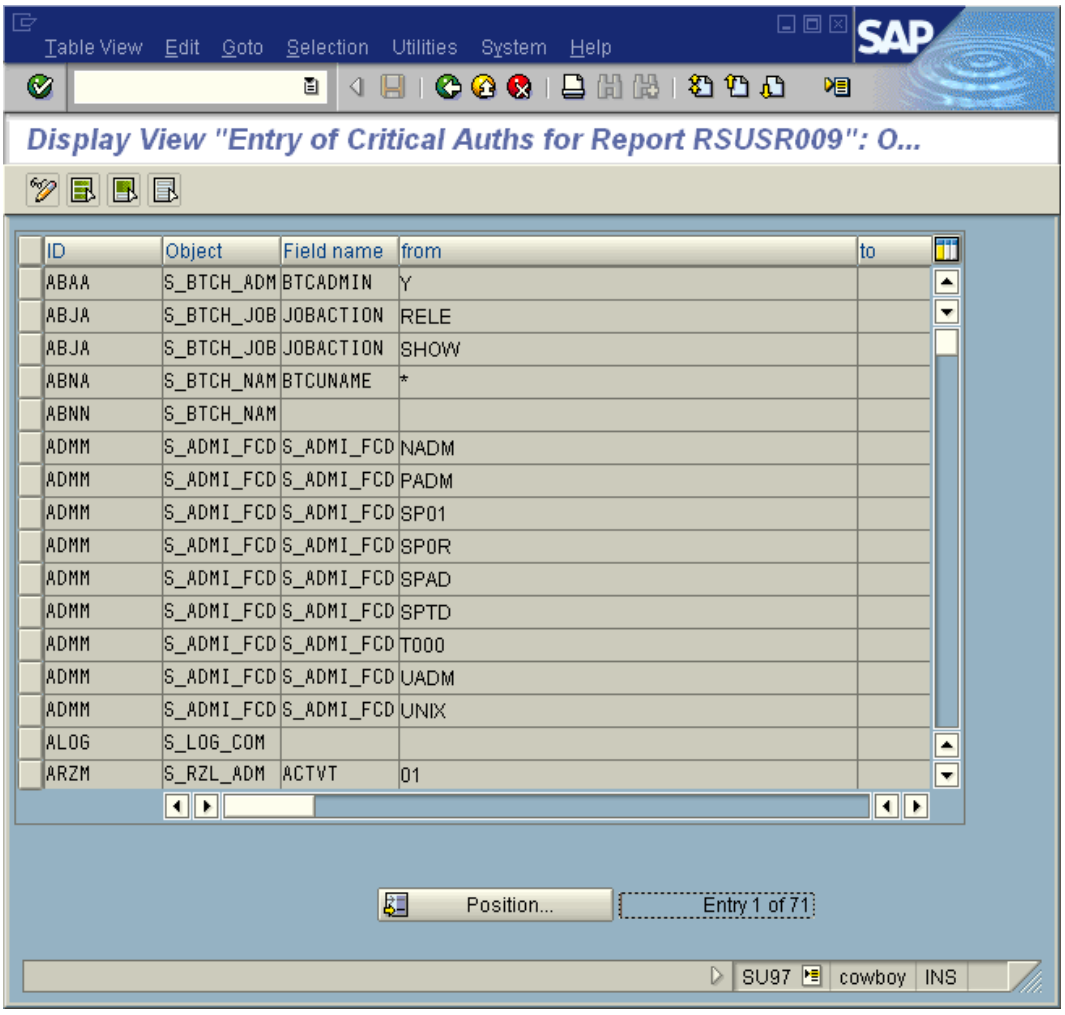
Question 4.10: This allows you to analyze why the transaction failed authorization. Briefly analyze why the previous transaction failed. Why don't you as a user have authorization to do this?

SAP also provides the capability of analyzing profiles and roles to see if they assign incompatible privileges to the people granted these authorizations. The user can define a series of authorizations which are defined as critical authorizations. Then specific users (or all users, if desired) can be checked to see if they have been issued any critical authorizations.

You can view the critical authorizations from transaction code S_BCE_68001403. View the critical authorizations by selecting the eye glass icon.



This displays the definitions of the critical authorizations.



Your system has only default critical authorizations that are predefined by SAP. These deal primarily with system administration functions. However, companies would also want to define authorizations that deal with incompatible duties such as recording transactions and authorizing those same transactions.

The capabilities of the standard SAP system to detect possible SOD problems is limited in that it can only analyze critical authorizations after they have been issued to users. There are third party products (such as Virsa) that do this analysis on roles and profiles before they have been issued to the users. This type of analysis is beyond the scope of this assignment.

This completes the case.

CONCLUSION

This is a substantial student assignment in which the student must spend a good amount of time dealing with each step of the problem. Unlike many accounting problems, the students will produce different correct answers. We provide an instructor's guide for this problem that presents a set of solutions and also discusses different approaches that can be used with respect to offering the case as an assignment.

References

Ge, Weili, and Sarah McVay. 2005. The Disclosure of Material Weaknesses in Internal Control after the Sarbanes-Oxley Act. *Accounting Horizons* 3 (Sep 2005): 137-159.

Gelinas, Ulric, Steve Sutton, and James Hunton. 2005. *Accounting Information Systems.* 6: Thomson Southwestern.

Hodges, Peter. 2002. In Suspicious Circumstances. *The British Journal of Administrative Management.* Jul/Aug2002: 33-34.

Information Systems Audit and Control Association (ISACA). *IS Auditing Procedure P1: IS Risk Assessment Measurement.* 2002.

IT Governance Institute. *COBIT Version 4.1*. 2007

Lenk, Margarita, and Bridget Donnelly, Bridget. Instructional Case: Community Outreach. *Issues in Accounting Education.* 13 (Feb. 1998). 173.

Romney, Marshall, and Paul Steinbart. 2006. *Accounting Information Systems.* 10: Pearson Prentice Hall.

Srinidhi, Bin.1994. The Influence of Segregation of Duties on Internal Control Judgments: Professional Adaptation. *Journal of Accounting, Auditing & Finance* 3 (Summer1994). 423.

Appendix – Alternate Part 2

Part 2 – Assignment of Duties

In this part of the assignment you are to determine whether Acme has effectively assigned its employees to each of the 28 purchasing tasks listed above. That is, you must assess whether Acme'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 Acme employees not currently involved in the purchase-to-pay process. Hint: It will be helpful to reference the risk assessment you completed in part 1. By assessing if specific risks are reduced by segregating certain duties, this can help you analyze incompatible tasks.

For example, even though the first three tasks are stated as if they are done by three different people, they could be done by only one employee. So your answer would be that the employee doing the purchase requisition activities should do tasks 1 through 3 and give a brief explanation of why the consolidation of these tasks are not in conflict with good control procedures. This should be done for each of the above 28 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?

The following paragraphs describe Acme Company employees who are currently involved in the purchase-to-pay cycle. Keep in mind that the tasks described below are not the only tasks these employees are responsible for, but are those within our 28 step purchase-to-pay cycle. Of course there are other individuals employed by Acme as well. Some additional Acme employees include: Receptionist, Secretary, Mailroom Clerk, Warehouse Assistant, Treasury Clerk, Treasurer, Accounting Manager, Controller, Office Manager, Maintenance Supervisor, and others. You might also find it helpful to refer to the Job Assignment Matrix at the end of this section in order to understand how the tasks are currently assigned. You will want to duplicate the matrix format when you complete this part of the assignment.

Any Acme Employee can determine a need for goods, complete a requisition and submit it to his or her Supervisor for approval, (tasks 1 through 3).

Department Supervisor will make sure that requested purchases are appropriate, within company policy, and within departmental budget constraints and approve the requisition. The Supervisor then sends acknowledgement back to the originating employee, determines the appropriate item to order, sends the requisition to purchasing, and enters the requisition into the information system (tasks 4 through 8). When the goods arrive, they are delivered to the Department Supervisor for distribution to the originating employee. This is thought to be the most efficient means of distributing goods and allows the Supervisor to double check to be sure the right goods have been ordered and received (task 22).

Buyer determines which vendor to purchase goods from, based on cost and quality parameters. If the vendor is already in the company's information system, the Buyer checks vendor information for accuracy and completeness and makes any corrections necessary to the master data. If Acme has not purchased from this vendor before, the Buyer acquires all the necessary information to approve and enters the vendor into the computer system and then updates the master data in the system. The Buyer then consolidates the purchase requisitions, creates and records a purchase order to the designated vendor, and sends it to appropriate parties (tasks 9 through 12 and 14). When the vendor invoice arrives at Acme, it is given to the Buyer to verify pricing and quantities (task 23) and is then passed on to Accounts Payable.

Purchasing Clerk receives the order acknowledgement from the vendor and notifies both the buyer and the warehouse (task 13).

Shipping & Receiving Clerk receives the goods when they arrive at Acme's loading dock and passes them on to the Warehouse Clerk (task 15).

Warehouse Clerk counts the goods, pulls the packing slip from the package, sends it on to Accounts Payable, records the receipt of the goods in the information system, and passes the goods on to the Department Supervisors (tasks 16 through 21).

Accounts Payable receives the purchase requisitions, purchase order, and vendor invoice from the Buyer and the packing slip and receiving report from the Warehouse Clerk and compiles a voucher package. If quantities and pricing match, payment is approved. Accounts Payable then writes a check for payment and sends it to the vendor. Once a month, Accounts Payable is required to reconcile the subsidiary payable accounts with the general ledger and perform a review of the documents to be sure everyone is in compliance with procedures (tasks 24 through 28).

Job Assignment Matrix - Acme Purchase to Payment Cycle								
		Any Acme Employee	Department Supervisor	Purchasing Clerk	Buyer	Shipping & Receiving Clerk	Warehouse Clerk	Accounts Payable
1. An Acme employee determines that there is a need for goods in order to do their job		√						
2. An Acme employee fills out a purchase requisition form for the desired goods		√						
3. An Acme employee signs the purchase requisition and submits it to an Acme employee		√						
4. An Acme employee approves the purchase requisition (if it isn't approved, the process stops here)			√					
5. An Acme employee sends acknowledgement and disposition of the requisition back to the originating employee			√					
6. An Acme employee submits the approved purchase requisition form to centralized purchasing and other appropriate people			√					
7. An Acme employee records the purchase requisition information			√					
8. An Acme employee determines the appropriate product to order			√					
9. An Acme employee determines the appropriate supplier to order from and checks to see if the vendor's master data is in the system and is correct.					√			
10. If the vendor master data is not in the system or is incorrect, then an Acme employee confirms the master data and payment terms with the vendor and enters the master data into the system.					√			
11. An Acme employee consolidates purchase requisitions and creates a purchase order					√			
12. An Acme employee sends the purchase order to the vendor and other appropriate people					√			
13. An Acme employee receives an order acknowledgement from the vendor				√				
14. An Acme employee records the purchase order information					√			
15. The vendor ships the goods with a packing slip to the destination on the purchase order and an Acme employee receives the goods at the receiving dock at our location						√		
16. An Acme employee counts the goods in the shipment							√	
17. An Acme employee removes the packing slip from the box and sends it to the appropriate people							√	
18. An Acme employee fills out a receiving report that has details on the time of the arrival and the items received							√	
19. An Acme employee records the packing slip information							√	
20. An Acme employee records the receiving document information							√	
21. An Acme employee passes the goods on to the designated recipients							√	
22. An Acme employee who requested the goods receives the desired goods			√					
23. The vendor sends the invoice and remittance advice for payment and an Acme employee receives the invoice and remittance advice					√			
24. An Acme employee compares all of the documents for the order (that is, a voucher package is compiled)								√
25. An Acme employee approves payment of the invoice								√
26. An Acme employee creates the payment check								√
27. An Acme employee sends the payment check to the vendor								√
28. Periodically an Acme employee verifies all of the documentation to be sure that the transaction has been handled correctly.								√