Spring 2006

The Sox Compliant Sap Security Implementation

Michael Candelaria
Regis University

Regis University
School for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

The SOX Compliant SAP Security Implementation

by

Michael Candelaria
michael.candelaria@sap.com

A Project Report submitted in partial fulfillment of the requirements for the degree of
Master of Science in Software and Information Systems

School for Professional Studies
Regis University
Denver, Colorado

April 24, 2006

Acknowledgements

I would like to recognize the following people for their contributions:

Colin Norton, Senior Consulting Manager – SAP America, Inc., for the financial support throughout the degree process.

Darl Kuhn, Affiliate Professor, Regis University, Oracle DBA and my project advisor, for providing technical, intellectual advice and review of this project.

Philip Nightingale, SAP Security Manager – KBR, for guidance and technical critic on my first professional paper and the introduction to the world of IT audit and control.

The SOX Compliant SAP Security Implementation

By

Michael Candelaria

April 24, 2006

The reality of the Sarbanes-Oxley Act, is that it is among the most visible and far-reaching regulations that organizations face today. Failure to comply can result in significant loss of market capitalization and shareholder trust, as well as criminal liability for corporate executives. In this thesis the author focused on the implementation of SAP security software including the development of several ongoing production environments that will have a formalized security strategy to achieve SOX compliance.

Spacely Chemicals, just as many other SAP customers understands the importance of SOX compliance. In the past Spacely Chemicals has not implemented the appropriate policies to enforce procedures within the business that would easily allow for IT controls and audit of the existing SAP R/3 application.

This thesis includes the SPACELY Chemicals implementation of the latest suite of SAP applications. SAP is complex software that offers many levels of security design and control options. It will also cover procedures for securing SAP systems and their external interfaces, focusing primarily on scenarios for user and role maintenance. It discusses user maintenance procedures and documented for issues relative to requesting changes to user access because of job change, project responsibility change and employee or contractor terminations. In addition, role maintenance procedures are documented including the security architectural role strategy, naming conventions and procedures for identifying ownership and approvals for all security components. Both user maintenance and role maintenance procedures pay particular attention to ensuring the requirement for segregation of duties (SOD) and SOX compliance is not jeopardized.

The application security implementation will be outlined and defined through appropriate controls such as policies and procedures. The procedures for managing the level of access granted to users and managing the level of access in job roles must be outlined through policies as well. By following the guidelines and recommendations from the Control Objectives for Information and Related Technologies (COBIT®), the SAP applications discussed in this thesis will help SAP customers meet and maintain SOX compliance.

Table of Contents

Table of Figures

This page was intentionally left blank

1 Introduction

To protect the identity of the actually company referred to in the thesis, the student will use the fictitious name Spacely Chemicals.

1.1 Problem Statement

SAP is the world's largest business software company and is the recognized leader in providing collaborative business solutions for all types of industries and for every major market. SPACELY Chemicals, just as many other SAP customers is searching for the most cost effective way to obtain and maintain compliancy with the Sarbanes-Oxley Act (SOX).

The Sarbanes-Oxley Act was created as a direct result of corporate governance failures caused by the lack of controls and appropriate corporate ethics. SOX requires the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) to sign a certification of their companies' financial reports. The management team performs assessments of the companies existing internal controls and report their findings. Both corporate management and executives must report all known deficiencies and acts of fraud immediately to be in compliance. In addition, the organization needs to develop and implement a methodology to capture any anonymous complaints from the company's employees, i.e., whistle-blower.

The implementation of a SAP Security Project at SPACELY Chemicals will consist of the development of several ongoing production environments that need to have

a formalized security strategy to achieve SOX compliance. How best can this be achieved?

1.2 Thesis Statement

By following the guidelines and recommendations from COBIT®, the Control Objectives for Information and Related Technologies, as built around the internal controls framework outlined and defined by COSO the Committee of Sponsoring Organizations of the Treadway Commission, a SAP application can meet and maintain SOX compliance for Information Technology.

1.3 Purpose of the Project

The purpose of this project is to provide a logical, repeatable, and auditable set of processes to ensure that proper sets of checks and balances are maintained in the SPACELY Chemicals SAP landscape to ensure SOX compliance. These processes apply to the Security Administration Team, user administration and the security controllers, which will be described in detail.

SPACELY Chemicals will be implementing the latest suite of SAP applications, i.e., Customer Relationship Management (CRM), Supplier Relationship Management (SRM).

1.4 Mechanics of the Paper in Support of the Thesis

This paper will flow in a systematic order that will allow the reader to use the paper as an implementation tool for SAP applications. The paper will identify roles and

responsibilities of the security team responsible for SOX compliance of the SAP application from an IT perspective. In addition, an overview of SAP security and the "What's" of SAP security will be provided. This information is presented in a framework outline

1.5 Barriers

SAP is a very complex product that offers many complex levels of security design and control options. To provide SPACELY Chemicals with maximum control flexibility with minimum support effort the functional description of the Three Tiered security role strategy that will be used in SAP R/3 – enterprise resource planning, BW – business information warehousing, CRM – customer relationship management, SRM – supplier relationship management, XI – exchange infrastructure, XMII – manufacturing integration and intelligence, and other system landscapes must be outlined and defined through appropriate controls, such as policies and procedures. The procedures for managing the level of access granted to users, and managing the level of access in roles within SPACELY Chemicals must be outlined through policies as well.

In the past SPACELY has not implemented the appropriate policies to enforce procedures within the business that would easily allow for IT controls and audit of the existing SAP R/3 application. With the implementation of SAP applications, a business culture change is about to take place. As with any change people will question your motives and criticize your approach. These barriers can be a difficult to circumvent.

1.6 Scope

This project covers procedures for securing SAP systems and their external interfaces, focusing primarily on scenarios for user and role maintenance.

- User maintenance procedures are documented for issues relative to requesting changes to user access because of job change, project responsibility changes, and employee or contractor termination.
- Role maintenance procedures are documented including the security architectural role strategy, naming conventions, and procedures for identifying ownership and approvals for all security components.

Both user maintenance and role maintenance procedures pay particular attention to ensuring the requirement for segregation of duties (SOD) and SOX compliance is not jeopardized.

This project will not cover other IT security issues such as operating system, database security, and single sign-on (SSO).

2 Review of Literature and Research

2.1 Definition of terms

TERM	DEFINITION
Authorization	Controls what is allowed when the user gets to a transaction (such as report all data for specific cost centers).
Business Process Master List (BPML)	Microsoft Excel worksheet containing a representation of the R/3 business processes and transactions defined in the project scope.
End User	A user that is not responsible for SAP system administration, system configuration, system support, or system development
Firefight Role	A role that allows direct functional and or configuration change in the system, this role is only assigned during a production down situation and must receive proper authorization and be audited during the period of assignment.
Inherited Access	A user has more than one job role and a transaction from one role has too much functionality because it interacted with an authorization from another role.
Online Analytical Processing (OSS)	On-line Service System that helps in users to get fast and effective help from SAP. The user may log-in to OSS system to find a possible solution for a 'bug'. Get the patch, if any, download and apply to correct the problem.
Profile Generator	A tool that simplifies role creation, by first selecting transactions for a role, and automating the addition of authorizations needed for those transaction codes (T-Codes) into roles.
Role, Composite	A role that has a list of other derived or master roles, to simplify role assignments to user (i.e. 1 composite role instead of several individual roles). These are not used for SPACELY Chemicals end users since it complicates problem analysis.

TERM	DEFINITION
Role, Derived	A role that references a Master Role, and inherits the Master's authorizations, except for organizational field values. Therefore, these are 'organizational specific' variations of the master. Examples would be a project specific variation of the Project System Accountant role.
Role, Display	A role with all the non-sensitive display and reporting transactions needed for an application. A user may have 0 to many roles in this tier.
Role, General	A role with transactions needed by all SAP users. All users will be given this role.
Role, Job	A role with all the transactions a user needs to perform their job (not counting transactions from general or core roles). A user should typically just have 0 to 1 of the roles in this tier. More than 1 role adds complexity to managing Segregation of Duties risks, and to problem analysis and resolution.
Role, Parent or Master	Any role that doesn't reference another role
Roles	A container to assemble groups of authorizations needed for specific transactions. SAP role types are: Master, Derived, and Composite.
Sarbanes Oxley (SOX)	Periodic assessment and enforcement of system controls.
Security Controllers	People that have any tasks or responsibilities in User Maintenance requests and Role maintenance procedures, across many SPACELY Chemicals organizations. Examples are Role Owners, Auditors Control Compliance Monitoring, etc.
Segregation of Duties (SOD)	Combinations of transactions and authorizations that greatly increase the risk of misusing SPACELY Chemicals resources for personal gain.
Sensitive Object	Are objects that have an unusual amount of risk and therefore must be more tightly controlled, with specific rules around their utilization in roles.

TERM	DEFINITION
Service User	A user type in the SAP system that does not observe the password expiration rule and can be used as a communication or dialog user. This user type should not be used.
Three Tier Role Strategy	Strategy for deciding what transactions and authorizations to group together into roles. Role tiers are General, core and job role.
Transaction (T-code)	A technical identifier for specific processes in SAP. These control where a user can go in SAP (such as to create vendors, or run a specific report).
User	A person that accesses SAP
User Master	Records in SAP that contains information about a user (including name, password, type of user, role assignment, etc).
Userid	Typically the network ID that is used as a unique identifier for a user

2.2 SAP Security Overview

SAP security works by first creating users, and then assigning roles. When the user attempts to sign on to SAP, the User Masters are checked to ensure that the user exists and has the correct password, and is not locked or past their validity date.

Then, as the user attempts to navigate in SAP, appropriate checks are done along the way to ensure they have the authorizations needed to execute their task. This is accomplished by looking at the authorizations from roles assigned to the user.

Since many users are assigned the same role, corrections to a role will apply to all users assigned the role. You cannot add transactions or authorizations directly to a user; they must be added to roles.

To build a role, begin with adding transactions to the role using the profile generator tool. Then the tool gathers the authorizations associated with those transactions into the role and allows the security administrator to adjust the values that are checked. This is extremely complex and requires specialized training and experience.

Maintaining roles in SAP also requires a lot of interaction between security administrators that are trained in SAP security tools and the business functional experts that understand the business processes and security requirements. Additionally resources that actually know specific end users and their job responsibilities, Internal Audit and the Controller need to be involved to assist in addressing business risk issues including SOD risk and access to sensitive data. Therefore, much collaboration is required to get the right content in roles, assigned to the right users.

2.3 Research Methods Used to Investigate the Problem

Problem investigation started because of the initial shortcomings identified in the audit performed by Ernst & Young. IT security was consulted to aid in the resolution of these findings. The student working on the project performed a security assessment focusing on business practices, security controls policies, procedures, the R/3 application itself and current IT audit practices. The requirements from the auditors were analyzed to associate the SOX requirements to the COSO control framework.

2.4 Project Relevant Literature and Research

Research was performed online using the Internet, by downloading guides, white papers, and attending an online SOX Security school that is offered at

SearchSecurity.com. The student was able to identify the organizations, i.e., COBIT®, COSO and the literature such as (possible i.e. lookup) ISO17799, BS7799 that currently exist and relate directly to security controls, policies and procedures.

2.5 Summary of Project Known and Unknowns

The projects known are the requirements from audit and available resources. The unknown is how the IT SAP application security team can best assist the business in achieving and maintaining SOX compliance in the current R/3 system and the new SAP applications to be implemented.

2.6 Contribution the Project Will Make

This project will provide the documentation for the CRM, SRM and other SAP application implementations at SPACELY Chemicals to ensure SOX compliance. Additionally it is this student's belief that the approach and framework can be re-used at other customer sites to guide them in a SOX compliant implementation.

3 Methodology

3.1 Formats for presenting results/deliverables

The results will be presented in the document itself as flow diagrams, Microsoft ® Excel work books, forms built with Microsoft ® Word and Microsoft ® Visio diagrams. A Microsoft ® PowerPoint presentation will be used to deliver the project overview.

3.2 Resource requirements

Resource requirements are identified by specific tasks and the number of hours to complete the associated task. Therefore the use of a excel spreadsheet is most appropriate for this project. (Refer to Appendix A)

3.3 Review of deliverables

Project deliverables will include:

- This document that can be re-used as a SAP Security Policy and Procedures template for SAP customers
- List of Sap monitoring procedures
- PowerPoint presentation to accompany the document focusing on highlights, procedures and methods
- Use Case diagrams and Flow Charts to visually aid in procedural steps
- An appropriately implemented SOX compliant SAP security system

3.4 Specific procedures

This project followed the following specific procedures:

- Identification of specific roles and responsibilities
- Strategies for role and user maintenance
- Standards for reviewing SOD issues

3.5 Outcomes

This project has provided a working security policy and procedures document for the Information Technology department for the current and future SAP projects. Identifying the roles and responsibilities allowed the organization to better understand how they will contribute to the over all success of the project.

Creating the resource requirements spreadsheet has allowed us to staff appropriately, manage the workload, and hopefully stay within budget.

4 Project Dynamics

4.1 How the project began

The SOX Compliant SAP Security Implementation began as a direct result for the need of the current R/3 environment to become SOX compliant, as well as the future implementation projects.

4.2 How the project was managed

The project is being managed using an excel spreadsheet to identify specific tasks. The time it will take to complete the task in employee work hours is identified, the tasks are then mapped to an individual. The use of a excel spreadsheet allows for a cumulative total of hours needed by workweek in the month, this has allowed us to manage our people resources effectively.

4.3 Significant events/milestones in the project

The most significant project milestone was obtaining buy in from the business leads regarding their ownership of the business roles. Originally the business leads were not accountable for authorized assignment of the business roles to end-users.

4.4 Changes to the project plan

At this point there have been no project plan changes.

5 Roles and Responsibilities

5.1 Security Administration Team Leader

The Security Administration Team leader is responsible for producing the security plan and obtaining approval from the SPACELY Chemicals organization. The leader will then execute the plan and insure the job roles are defined and that the security administration team will implements them. The leader will coordinate the activities of various groups and meeting internal controls requirements and documentation for SOX relative to security. The leader reports progress to the project team(s).

5.1.1 Security Administration Team

Responsible for gathering and reviewing requirements from the role owners and developing roles per SPACELY Chemicals approved procedures. And, validation in the development phase of SOD and SOX compliance along with monitoring of the production clients for compliance and security issues. They are also responsible for ensuring user administration policies and procedures are adhered to.

5.1.2 Role Owners

Role Owners are functional experts appointed by the business and are responsible for gathering the information about individual business processes, determining the jobs involved and ensuring the resulting roles will be SOD and SOX compliant. They will map the processes to SAP transactions for each job and submit this to the security team

for role updates. Role owners are also responsible for verifying security requirements are met by testing the security roles. Responsibilities include:

- Represent the business
- Make security rules
- Owners are identified for each major object involved in security including
    - Roles
    - Transactions
    - Tables
    - Document types, etc
- Role owners
    - Consolidate business unit requirements
    - Evaluate business unit requirements to facilitate job standardization where

5.1.3 Security Controllers

5.1.3.1 Controllers Office

Responsible for ensuring corporate compliance with legal and best practice rules concerning the security of corporate assets. Responsibilities include:

- Legally liable for controls
- Primary decision maker on controls
- Determine acceptable levels of risk for business
- Approve Security Controls
    - Validate Owners and Role approvers

    - Approve Security Policy and Procedures
    - Approve Security Architectural strategy
    - Approve SOD management tools
- Approve SOD's to be allowed and the mitigating controls for them
- Insure compliance with Sarbanes Oxley (SOX) and other laws
- Approve modifications to SOD rules based on auditor risk assessments

5.1.3.2 Audit

The audit department's function is to verify compliance with laws and internal controls rules. Responsibilities include:

- Identify risks or criminal activities
- Provide the controller with security risk assessments
    - Evaluate Role Owner and Role approver strategy
    - Evaluate Security Policy and Procedures
    - Evaluate Security Architectural Strategy
    - Evaluate SOD management tools
- Evaluate allowed SOD exceptions and mitigating controls for them
- Evaluate compliance with SOX and other laws
- Evaluate custom transactions for risk assessment as to
    - Sensitivity of data and appropriate ownership
    - SOD, proposing SOD rule updates as appropriate
- Conduct audits to validate security controls

5.1.3.3 Government operations compliance

Ensure compliance with Canadian and American governmental requirements.

5.1.3.4 Approvers

Appointed to approve the assignment of roles to users:

- Approve access for their area of responsibility
- Validate requests against SOD matrix
- Monitor role assignments for their area of responsibility

6 Strategies

6.1 Role Maintenance Strategy

6.1.1 Three Tier Security Role Strategy

There are multiple ways to approach the issue of user access administration in SAP, and to successfully create a security strategy, implement, and administer it over time. After careful evaluation, SPACELY Chemicals has selected a Three Tier Security Role Strategy, which will utilize the functionality of SAP's Profile Generator tool to facilitate the design and creation of Security roles.

In this approach, tier one is the General access role. This role includes authorizations that all SAP users will require, such as access to spool files and to online help, etc.

Tier two is the Display tier for non-sensitive display and reporting access per functional area. These are typically the largest volume of transactions, and least risk. The Display roles are intended for all users working in the functional area. A large number of users will only have General and Display roles.

The third tier is the job role based tier and is the most critical to control. The intent is that one of these roles is built based on the job role the user performs for SPACELY Chemicals. Every attempt should be made to limit a user to one job role. Exceptions will occur at small business units where individuals perform multiple job

functions. This job role should include everything a user needs to do their job that is not already covered by the General and Display roles.

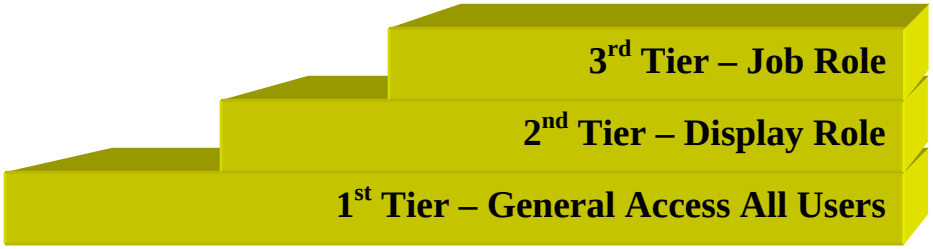

Figure 1: Three-Tier Role Strategy

For the implementation of this Three Tier process, people knowledgeable in SAP and SPACELY Chemicals business procedures should be appointed as SPACELY Chemicals Business job role owners.

Role owners are responsible for getting transactions in scope and determining which roles perform these transactions. Additionally, they need to determine how the transactions need to be secured in each role. They provide these requirements through procedures to the Security Administration Team who construct the roles. They are also responsible for ensuring the roles meet their requirements, and approving transports to the production environment.

6.1.1.1 General Access Role

Provide access to common transactions for any user logging on to the SAP system. The Security Administration Team owns this role. Some examples of these activities are access to print, online help, SAP office, etc. This avoids duplicating these same transactions in every job role throughout a landscape. Changes here affect all users, reducing the administrative load for the Security Administration Team, and speeds up response time to users.

6.1.1.2 Display Access Role

The Display Access Role provides all display and reporting access for a specific SAP module. This allows role changes that affect a complete functional group, for example Accounts Payable (AP), to be made in one place rather than requiring modification of multiple roles. Going forward, as new releases are implemented, this functional level should remain stable since only job roles will need to be created unless new display functionality or reports are introduced. Testing time will also be reduced since the access in the functional and organization levels will already be known so that only the interactions between this and the new job role access must be tested. All authorizations in display roles must be restricted to display only.

In addition, it is extremely important that no SOD transactions are added to display roles, even if the authorizations are restricted to display. The best prevention is by not having the create transaction, regardless of underlying authorizations as the user may inherit update access from their job role.

6.1.1.3 Job Role Access

These roles should have all transactions and authorizations needed for a specific job. Security Administration will build the roles, and the job role owners will ensure the roles are tested prior to moving them to production and assigning them to users. Any transaction with change, sensitive transaction, or company-specific access is placed in these roles.

The job-based roles will facilitate role assignments to positions in SAP's HR organizational structure rather than directly to users at some future date. Users assigned

to positions in HR organizational structure would then inherit the authorizations for the role that is assigned to their position.

Position based role assignment alleviates the control issue of user administration being notified of job changes. However every employee in the organizational structure should have a position.

6.1.2 Derived roles

Derived roles will only be used on display or job roles. These roles have the identical transaction and general authorizations as their master. Each derived role is an organizational specific variant of the master where only the organizational authorization fields may be changed. (e.g. Company, Cost Center etc).

6.1.3 Composite Roles

Composite roles are only used for support team and fire fight roles. No end user production composite roles will be created as this adds unnecessary increased complexity.

6.1.4 Generating Configuration roles from the Implementation Guide (IMG)

Configuration roles will be built per major application area, such as Financial (FI). The technique will be to pull transactions into the role menu from an IMG project that has the appropriate nodes selected, and then remove any inappropriate authorizations (such as security or basis transactions)

6.2 User Administration

User administration strategy will follow these principles:

- Minimal Privileges – users will only be granted the privileges they need to complete their job functions
- Need to Know – all user access must be approved by the appropriate individual(s), obviously the requestor and approver can not be the same
- Segregation of Duties – no user may obtain access that will cause a segregation of duties violation

6.3 User Authentication

External and internal users will authenticate themselves before access to any SAP application systems will be granted; refer to the USE Case Model below.

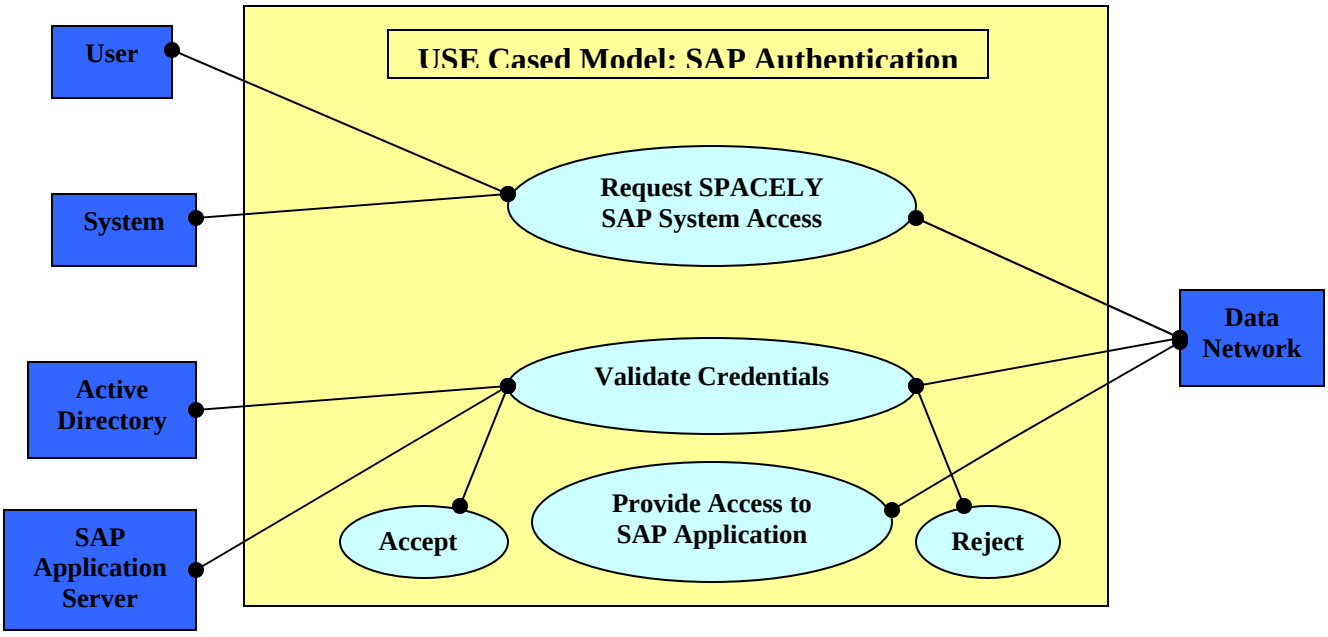

Figure 2: Authentication Case Model

6.4 User Access

User access to the SAP systems has to be approved before access can be granted. In the development systems a single approver is required while in the production system a two-tier approval system will be employed. Every role has a role owner and they are responsible for selecting appropriate approver(s) for access to their role(s). With the implementation of the Three Tier role architecture users will generally have three roles each. There will be some exceptions to this.

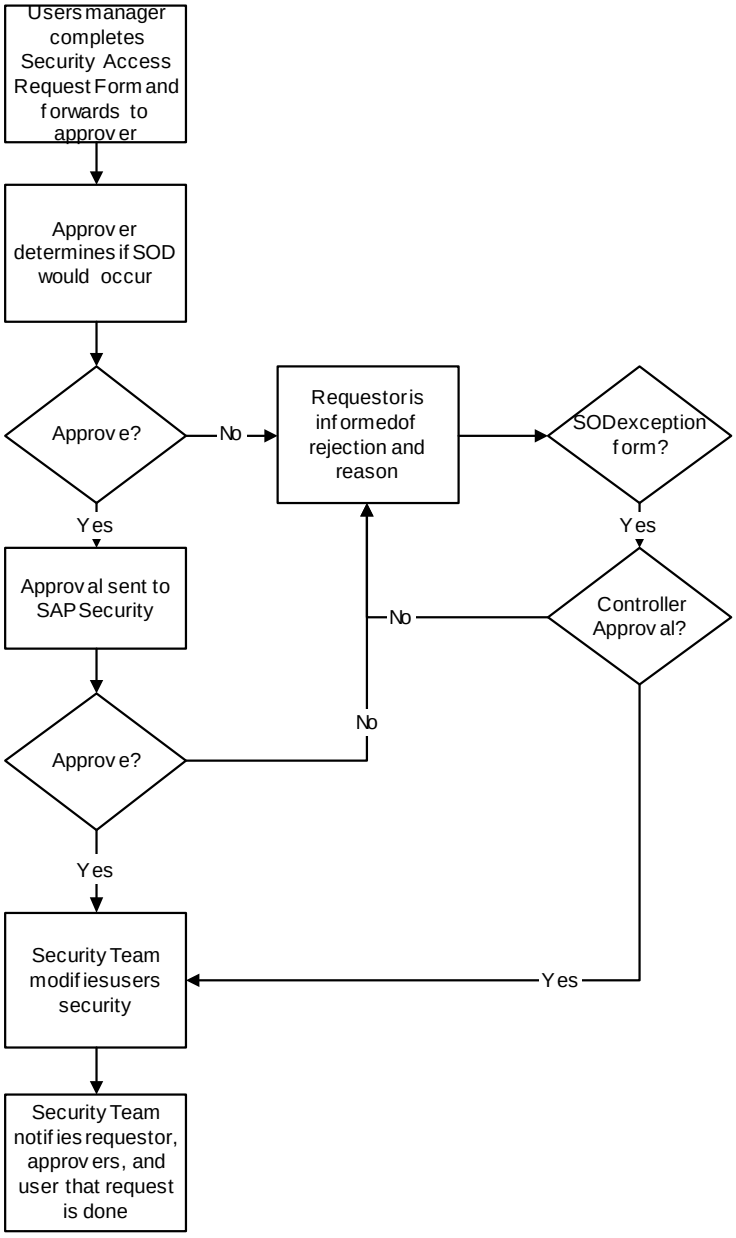

Figure 3: User Request Diagram

6.5 Temporary Access

The User maintenance transactions have functionality to accommodate temporary users and short-term job assignments of permanent users by creating a validity period for the user's access. An example of when an expiration date is useful in this strategy would be in the case of a user transitioning from one functional job role to another. When the expiration date on a role is reached the system automatically deletes the old job role from the user. When the expiration date on a user is past they will no longer be able to log on to SAP. The access request process will include procedures for assigning roles and users for limited periods.

7 Business Practices

7.1 SAP Security Administration

SPACELY Chemicals Business Practice

SAP Security Administration

Date: February 9, 2006	**Reference No.:**

PURPOSE:
This business practice defines security administration pertaining to the SPACELY Chemicals SAP systems.

SCOPE:

This document will address security administration for all SAP applications.
The document will not address security administration for any other applications, i.e., Microsoft Outlook.

BUSINESS PRACTICE:

SAP security administration will adhere to the following:

- Use the 3 – tier architecture for security role development
- Role naming standards
- Appropriate business owner approvals for all security entities
- Management of transaction code relationships to authorizations via SAP authorization tools
- Role change controls requiring testing prior to implementation of roles

DEFINITIONS: (if applicable)

Role – a collection of system transactions to perform a work task(s).

REFERENCES: (if applicable)

- **Corporate Policy**

Type text here.

REVISION SUMMARY: (if applicable)

Type text here.

APPROVED BY: Name and Title	**DATE**:
Supersedes:	

Figure 4: Security Administration Business Practice

7.2 SAP User Accounts

SPACELY Chemicals Business Practice	
SAP User Accounts	
February 9, 2006	**Reference No.:**

PURPOSE:
This business practice defines the level of security pertaining to the SAP user accounts.

SCOPE:
This document will address user administration for all SAP applications.
The document will not address user administration for any other applications, i.e., the SPACELY Chemicals network.

BUSINESS PRACTICE:
SAP user accounts will be assigned upon completion of the appropriate approved access request. User accounts, both production and development, will adhere to the following:

- SPACELY CHEMICALS naming standards.
- Password rules and restrictions, to include a minimum of 6 characters, and two of the following:
  - A special character, i.e., $,#,@.
  - A numeric value, i.e., 1, 3,6,7,8…..
  - A alpha character, i.e. a,b,c…. note SAP passwords are not case sensitive
- Roles assigned to user only after appropriate approval.
- Validation period(s) of user and role assignments based on:
  - User status, Managers discretion, Termination dates., User type
- SAP security team will enforce employee termination and emergency account lock downs relating to hostile and/or disgruntled employee behavior directly.
- All non SPACELY CHEMICALS employee dialog user accounts will be created with an expiration date.
- All dialog accounts will be subject to a time forced password change.
- 3rd party users must execute a non-disclosure agreement before access is granted.
- All dialog accounts for non-employees must have an expiration date. This includes: Contactor accounts, 3rd party accounts, and Test accounts.

The use of access to SAP by an individual will be governed by the corporate code of conduct and this business practice. Any violation of these rules can result in disciplinary action up to and including termination of employment. Any of the following acts will be considered a violation:

- Use of available access for which you have not been given permission to use. That is, if you have the access this does not give you the right to use it.
- Sharing your password or in any way allowing another individual to use your SAP log on account.
- Use of SAP access to misappropriate corporate tangible or intangible assets.
- Retrieving personal data of other individuals unless this is an integral part of your job.
- Knowingly withholding information concerning violation by others of this business practice.
- Using SAP access to distribute or cause to be distributed information or comments of an offensive nature.

REFERENCES: (if applicable)

REVISION SUMMARY: (if applicable)
Type text here.

APPROVED BY: Name and Title	**DATE**:
Supersedes:	

Figure 5: User Account Business Practice

8 Procedures

8.1 Role Administration

8.1.1 Role Naming Convention

The purpose of a good role naming convention is to facilitate analysis, problem resolution, and consoles by identifying:

- System
- Ownership
- Type of role such as job role, display roles, derived roles etc.

Although SAP allows 30 characters for role names single roles will be restricted to 10 positions because profiles are restricted to 10 positions and must be named as close to the role name as possible.

8.1.2 Role Name Construction

Roles names will be in the following format:

1st position will identify the type of role:

V – Display roles

D – Derived roles

J – Job roles

F – Firefight roles

T – Temporary roles

Z – Non-production roles

2nd & 3rd positions will identify the application:

R3 – ERP Centralized Component

BW – Business Information Warehouse

CR – Customer Relationship Management (CRM)

SR – Supplier Relationship Management (SRM)

SE – Supply Chain Management (SEM)

4th & 5th positions will identify the functional area or module:

FI – Finance

AP – Accounts Payable

AR – Accounts Receivable

CO – Controlling

MM – Materials Management

LO – Logistics

SD – Sales & Distribution

HC – Human Capitol Management

PS – Project System

PP – Project Planning

QA – Quality Assurance

EC – Enterprise Controlling

CA – Cross Applications

BC – Basis Components

6th position will be a delimiter _____

7th thru 10th positions will identify a abbreviated description of the role:

ACCT – Accountant

CLRK – Clerk

ADMN – Administrator

Examples:

JR3GL_ACCT for General Ledger Accountant
JR3CA_SPRT for cross application support
FR3HR_FIRE for HR Fire Fighter

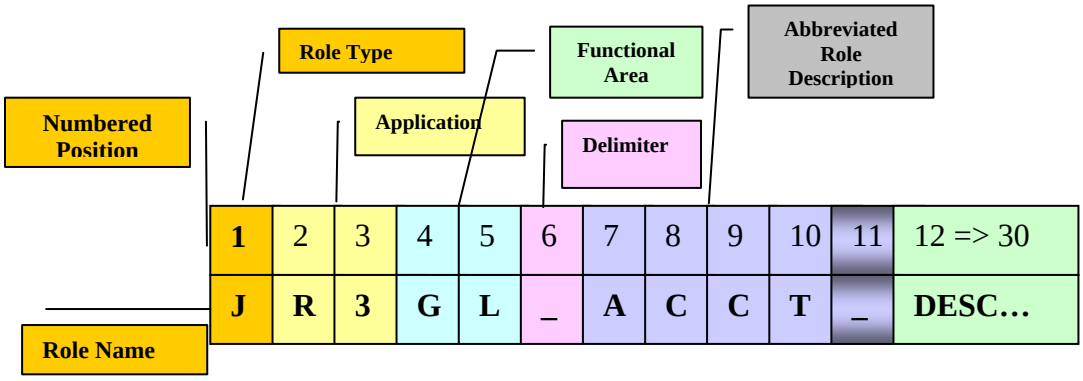

Figure 6: Role Naming Convention

8.1.3 Role Design

The role design strategy must be scalable for all various size SAP implementations. The primary difference in role design between large and small SAP implementations is the utilization of SAP's Solution Manager.

Larger SAP implementations define the business processes in scope via Solution Manager. At the end of the Blueprint phase of a project, a Business Process Master List (BPML) is generated from Solution Manager. This is simply a spreadsheet that gives a

hierarchy of business processes in scope, and the SAP transaction code for those processes.

All SAP role designs must begin with a listing of transactions in scope, whether it is the BPML spreadsheet generated from Solution Manager or a manually created spreadsheet for smaller implementations.

It is common to separate these spreadsheets by primary functional areas (such as Accounts Payable, General Ledger, Project Systems, Procurement, etc) since role owners typically are responsible for all roles for their functional area, but occasionally they must involve transactions (and therefore owners) from other functional areas.

From these spreadsheets, role owners must determine the jobs that will perform each of these transactions, and mark them appropriately in columns added per job needed. This is referred to as role mapping.

For Three-Tier architectural strategy, the role owner must simplify role mapping by populating general role and display role columns first. Then only map the remaining transactions into job role columns, and submit the spreadsheet to Security Administration per the Role Maintenance procedures.

	A	B	C	D	E	F	G	H	I	J	K
1	Tcode	Tcode Description	C:CALLUSER	C:APDIS000 AP DISPLAY CORE	J:APCHK000 AP CHECK PRINTER	J:APCLK000 AP CLERK - TC	J:APCLR000 AP CLEARING	J:APMGR000 AP SUPERVISOR / MANAGER	J:APPSP000 AP PAYMENT SPECIALIST - TC	J:APPWR000 AP POWER SUPPORT USER	J:APSPC000 AP SPECIALIST - TC
2	AUTH_DISPLAY_OBJECTS	Display Active Authorization Objects	1								
3	BWSP	SAPoffice: WWW	1								
4	BWWI_EXECUTE	Executing a work item (WEBgui)	1								
5	F.15	ABAP/4 Report: List Recurr.Entries		A				1			
6	F.41	A/P: Open Items		1				D			
7	F.56	Delete Recurring Document						1			1
8	F110	Parameters for Automatic Payment							R		
9	F-21	Enter Transfer Posting						1			
10	F-30	Post with Clearing						1			1
11	F-31	Post Outgoing Payments							1		
12	F-41	Enter Vendor Credit Memo				1					
13	F-42	Enter Transfer Posting						1			
14	F-43	Enter Vendor Invoice				1					
15	F-44	Clear Vendor					1	1			
16	F-47	Down Payment Request				1					1
17	F-48	Post Vendor Down Payment				1					1

Figure 7: Business Process Master List

After the roles are built, mass changes can be indicated to security by using:

- A to indicate transactions to be added to a role
- D to indicate transactions to be removed from a role
- R to indicate that a transaction has additional special requirements that are included in the comment attached to the cell

8.1.4 Role Maintenance

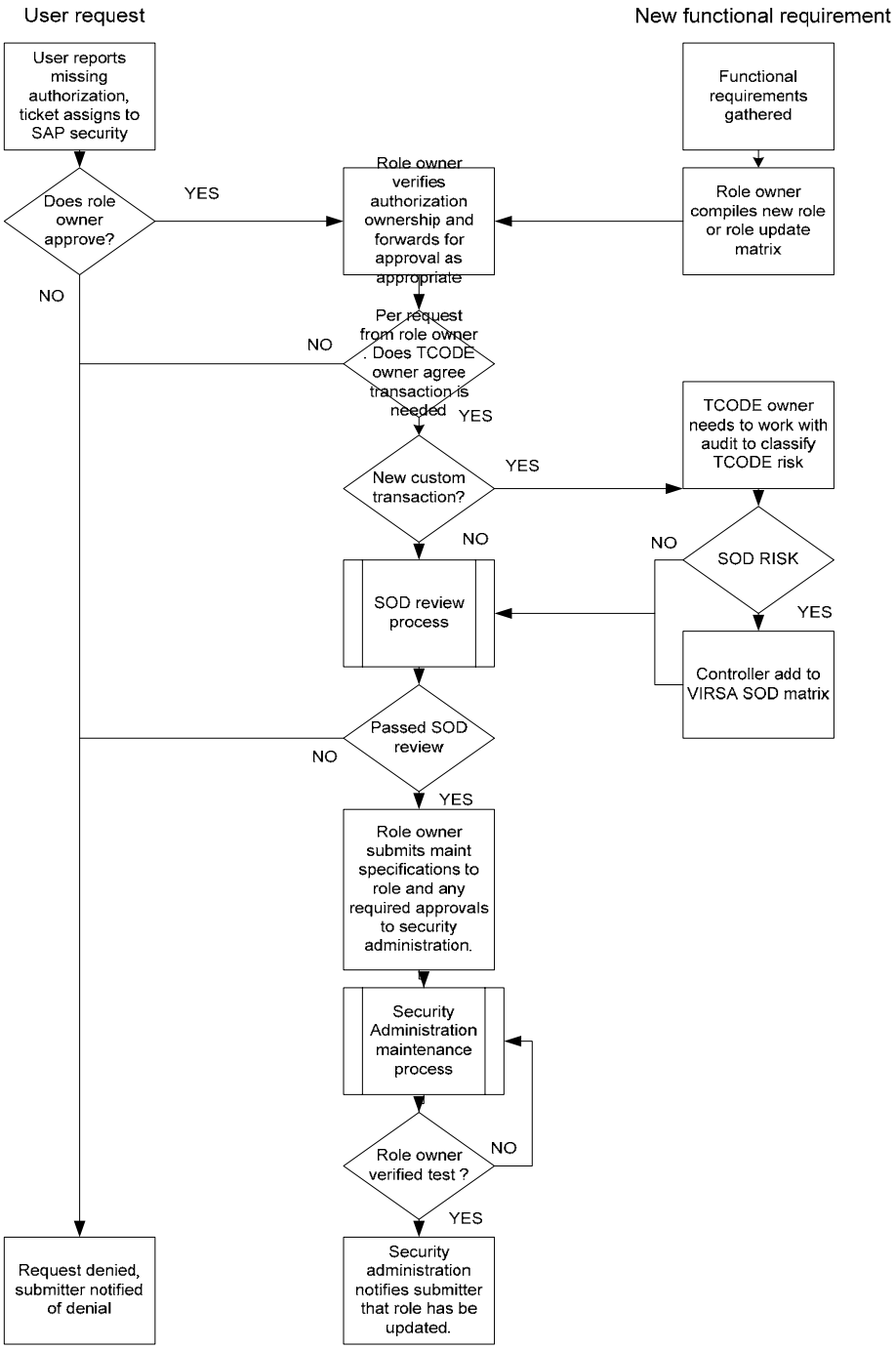

Figure 8: Role Maintenance Flow Diagram

8.1.5 Security Role Administration Maintenance

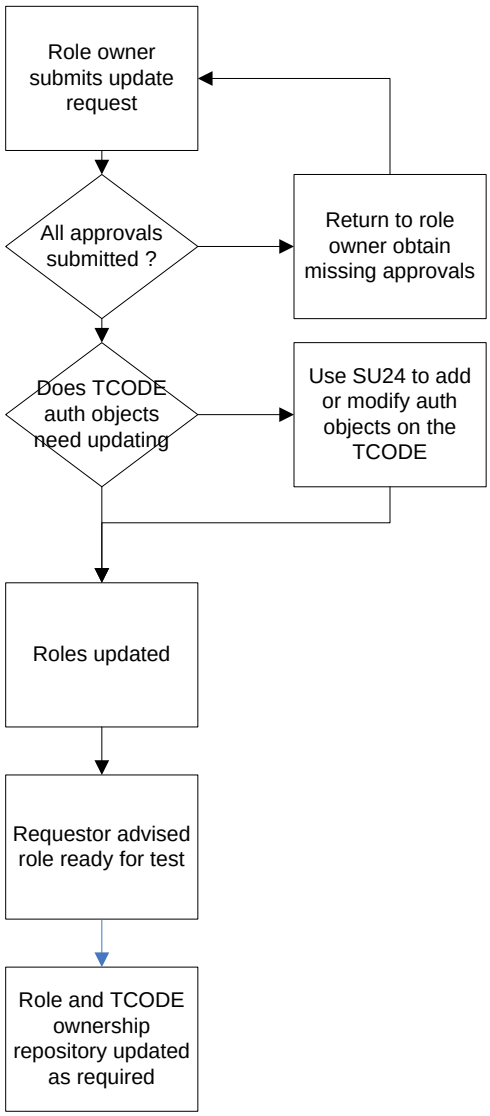

Figure 9: Security Role Maintenance Tasks Flow Diagram

8.2 User Administration

8.2.1 User Naming Convention

The purpose of a good user naming convention is to easily identify the individual or entity having the access. SAP allows up to 12 characters for an SAP ID.

- For employees or contractors (i.e. those who have access to the SPACELY Chemicals intranet) the network ID will be used for the SAP ID. These are generally 7 characters in length.
- For SAP connections in reference to an SAP Online Service System (OSS) note analysis or fix OSS followed by the last 6 numbers of the OSS note (e.g. OSS065231).
- For SAP access for easily watch 'SAP' followed by the 6 numeric date granted in the format yymmdd (e.g. SAP041105).
- For other service vendor access, a 3-character vendor identifier followed by an individuals or problem case identifier.
- 3rd party access, a 3 character entity identifier followed by up to 9 character identifier for the individual.

8.2.2 User access request process

8.2.2.1 Internal user request for production access

The user's manager sends the appropriate request form to the role approver for approval; it is the role approver's responsibility to check for SOD violations. Refer to the following flow diagram.

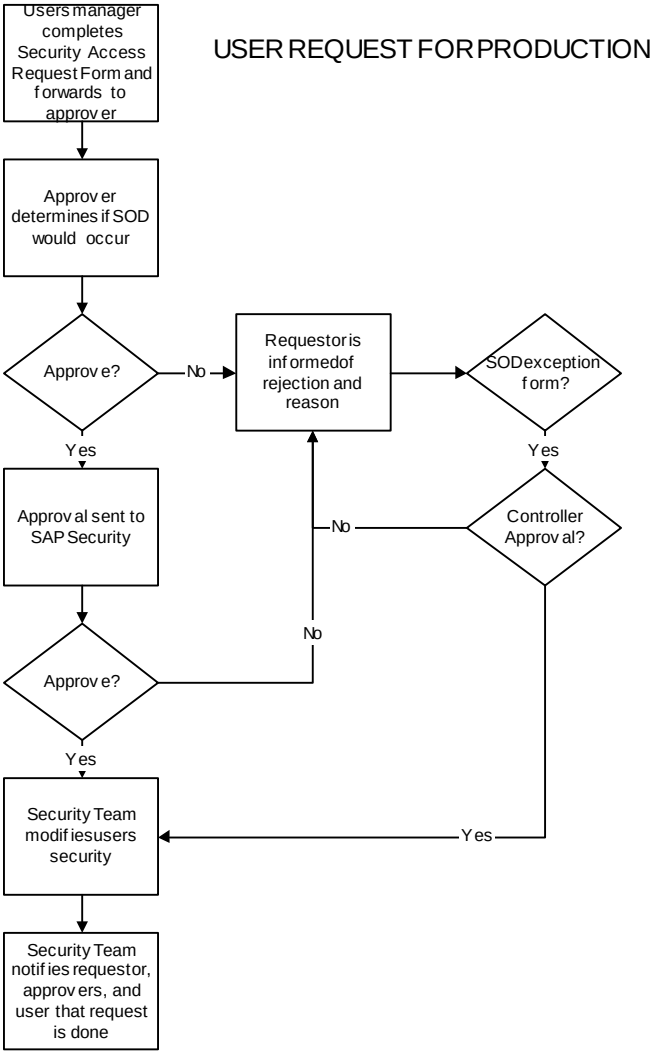

Figure 10: Production Access Flow Diagram

8.2.2.2 User Fire Fight access request

Fire Fight is assigned as an additional role to an existing account with appropriate prior approval.

8.2.2.3 Internal user request for development / test access

- User's supervisor retrieves current soft copy of development access request form.
- Supervisor fills out the form with all the users' information. If the user is not a SPACELY Chemicals employee an effective to date is required.
- If supervisor is not a development or function lead the form should be passed to a functional lead for approval. If the supervisor is a functional or development lead no further approval is required.
- Form to be e-mailed, by the approver, to the security administration team for processing.
- Security administration will send to the user their password when the account(s) have been created.

8.2.2.4 Online Analytical Processing (OSS) connection request

This is for a request for SAP to access our system to research a problem that has been submitted through SAP's OSS system. All OSS problems should be submitted via OSS1 and NOT web access OSS. The security administration team will set up the user ID and communicate it back to SAP; basis will open up the OSS connection into the client.

- User sends a request to open the OSS connection to both security administration and basis. The request must include the following.

    - OSS note number
    - Client access is needed for
    - Duration access is needed (max number of days)
    - Functional area access needed, we will assign full access in the requested functional area. Request for SAP_ALL will be rejected.

- User must request and make sure the OSS is set to customer update. Security has to use this to enter the ID and password.
- Basis will open the OSS connection.
- Security will copy the template OSS user for the requested functional area to a new user. The user ID will be 'OSS' followed by the last 6 numbers of the OSS note.
- Expiration date on the OSS user ID to be set in accordance with the requested duration.
- Security will go into the OSS note and update the system, user ID and password on the OSS note for the SAP analyst.
- Security will e-mail the requestor when this is complete.

8.2.2.5 3rd party access request

- Non disclosure agreement must be executed by either
    - The individual requesting the access to cover just their access
    - The company doing business with SPACELY Chemicals to cover all of their employees
- Copy of the signed agreement to be forwarded to the Security Administration team for a permanent record
- SPACELY Chemicals representative who are responsible for the SPACELY Chemicals relationship with the 3rd party must fill out and forward an access request form to the appropriate role approver(s). One per individual, group, shared or generic accounts is not permitted. An e-mail address MUST be provided for the user.
- Role owner either:
    - Approves the access, ensures there is an end date on the request form, and forwards the form to Security Administration department for processing.
    - Rejects the request and inform the requestor of the action.
- Security administration will create the account as requested and forward the password to the user at the e-mail address supplied.

8.2.3 User Access duration

SAP allows for the creation of user accounts with an expiration date. This should be used on all non-employee dialog accounts.

8.2.3.1 Accounts that do not require an expiration date

- Employee user accounts
- System and CPIC accounts
- Batch users

8.2.3.2 Accounts / roles requiring expiration and durations

- Consultant user accounts, max duration number of months.
- SAP support OSS accounts, max duration number of days.
- SAP early watch (SAP system monitoring) accounts, max duration number of days.
- Other vendor support accounts max number of days.
- Fire Fight role access, end of following business day unless extended approval is obtained.
- 3rd party accounts max 6 months.

8.2.4 User termination process

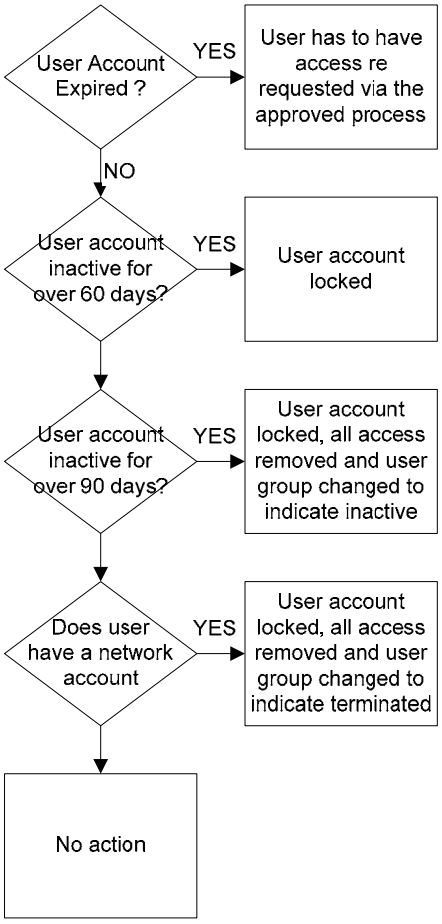

Figure 11: User Termination Process

8.3 Approver Verification Process

8.3.1 Ownership Administration

8.3.1.1 Ownership Concept

SAP Security controls is a significant portion of Sarbanes Oxley compliance and protecting the business owners from inappropriate and excessive risks. Security

Administration is not knowledgeable enough to make decisions for the business as to what constitutes acceptable risk levels. Therefore, business owners or their representatives must be selected for SAP security roles, and transaction codes.

As part of the Role Administration Procedures, new roles and transactions will be assigned an owner and the controller's office representative will verify that the owner is appropriate. These owners are documented, and Security Administration will ensure that appropriate permissions for role changes are obtained from these owners.

Over time, Role Owners may change jobs, terminate, etc. and therefore no longer serve as owners or representatives for the business. Due to the responsibility and accountability of these owners for all changes to security roles, it is necessary to have documented procedures for managing when these owners must be changed.

8.3.1.2 Ownership Change

Separate forms will be created for ownership changes, one for Role Owner and one for Transaction Owner. The form may be completed by business managers, or by current role or transaction code owners. Upon completion, the form must be forwarded to the Controllers office for approval. The Controller's office will forward approved forms to SAP Security. Upon receipt of the form, Security Administration will update the Ownership Database

8.3.2 User Role Approver Administration

8.3.2.1 User Role Approver Concept

As stated previously, SAP Security controls are a significant portion of Sarbanes Oxley compliance and protecting the business owners from inappropriate and excessive risks. Since Security Administration is not familiar with all employees in SPACELY CHEMICALS and the jobs they perform, business owners or their representatives must be selected to determine if SAP Access requests are appropriate.

This responsibility includes validating that the combined role assignments for a user won't result in Segregation of Duties risks to the company. It also includes verification that roles that are created specifically for an organization is only given to people that should have access to that organization.

Periodically per SOX requirements, role approvers will evaluate the users assigned to the roles they are approvers for, and validate that access to those roles is still appropriate.

Due to the responsibility and accountability of these role approvers for all changes to user access, it is necessary to have documented procedures for managing when user role approvers must be changed.

8.3.2.2 User Role Approver Change Procedure

A form will be created for User Role Approver changes; the form may be completed by business managers, current User Role Approvers, or by the controller's office.

Upon completion, the form must be forwarded to the Controllers office for approval. The Controller's office will forward approved forms to SAP Security. Upon receipt of the form, Security Administration will update the User Role Approver Database.

8.4 SAP Security Transport Process

1. On receipt of approved request, work with the role owner or their designate to change the role(s).
2. If the requestor is able to test in the development system, get them to test as far as they can before releasing the transport.
3. Create transport request form for the basis team to move transport to QA.
4. Once transport is in QA requesting testing.
5. If test fails.
    a. Make corrections to the role.
    b. Return to item 2.
6. If test passes and you have all approvals from the role owner to move to production:
    a. Update the target client in the R/3 transport request form.
    b. For standard promotion to production:
        i. Security will contact security team lead or their designate by e-mail, including the role owner's approval, to approve the transport move to production.

ii. Approval will be sent via e-mail to the basis team.

iii. QA to Production transports will be processed at 3 pm daily.

iv. Once transported the basis team will move the form to the 'transported to production' folder.

c. For emergency promotion to production (i.e. before the 3 pm daily transport):

i. User has to get emergency transport approval from a department director.

ii. The identified department manager will e-mail their approval to SAP Basis and Security Teams.

iii. The basis team will transport to production.

iv. Once transported the basis team will notify everyone

d. For promotion to production during a mandatory freeze we will follow guidelines set by management.

e. Once the transport is in production forward the e-mail to the role owner informing them of the move.

f. File the final e-mail in the appropriate mail folder.

8.5 SOD Review

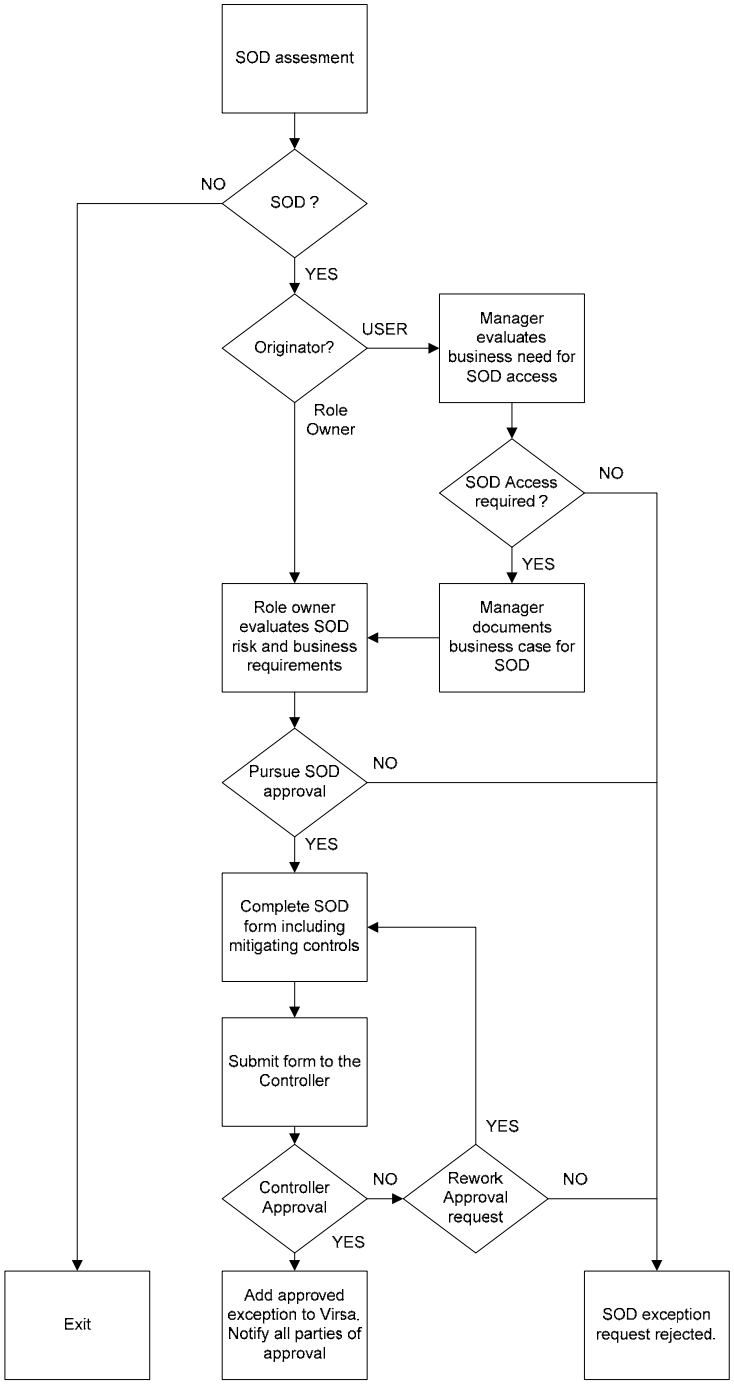

Figure 12: SOD Review Process

8.6 SOD Management

Segregation of Duties management is a key internal control that requires certain types of transactions to remain segregated therefore performed by separate individuals. The *Generally Accepted Account Principles* (GAAP) require that an internal control structure be in place to ensure that errors or irregularities are prevented or detected on a timely basis by employees in the normal course of business. Segregation of duties (SOD) is an internal control intended to prevent or decrease the occurrence of errors or inappropriate transactions. Ensuring different functions of a process area are properly separated so that no single individual is in a position to both cause and conceal errors and irregularities. SOD conflicts and violations will be managed by the following criteria:

- Assessment – Assessing your current situation by identifying your SOD violations
- Mitigation – Mitigating your exposure by addressing your SOD violations.
- Prevention – Preventing generation of new SOD violations by proactively checking for conflicts or violations before implementing security requests.

8.7 Security on Call Procedures

- First the user must contact the support help desk this includes support users. No one is to contact the security team on call directly. During certain integration tests limited direct access may be arranged with the functional manager.
- Help desk will evaluate the urgency of the issue with the user and escalate it if needed. Generally, only production system emergences or test system access for a production break/fix will be considered an emergency. The following are not generally considered emergencies:

- Test user set up.
- Assigning display roles.
- Test system request unless to correct production break/fix or security coverage has been pre arranged for an integration or end user test.

- After creating a ticket and assigning to the security team the help desk is to send an e-mail with the issue to the security team mail box then phone the on call analyst. On call schedule with phone number will be forwarded to the help desk weekly.

8.8 Monitoring Procedures

Monitoring is the ongoing and recurring review of the activities performed to follow the procedures that have been established to mitigate a business risk, the security team will perform monitoring activities as indicated further in this section. As an audit is the independent and formal review of the activities performed. Audit reports its findings on how well or not the procedures were followed, an audit is conducted by a external party.

SAP monitoring procedures include not only monitoring transactions executed by the SAP security team but also monitoring of SAP security team activity.

8.8.1 System Configuration Monitoring

- System parameter settings, appropriately controlled passwords including minimum length, expiration and excluded words.

- System change settings that do not allow changes to configuration or development in production, and do not allow production to be overwritten.
- System settings show that no extra clients have been created in production.
- Communication between systems is secured.

8.8.2 Role Monitoring

- Temporary roles are named correctly, and are only assigned to end users with an expiration date. They are removed from the system when they are no longer required.
- Roles that are not assigned to anyone within twelve months are removed from the system.
- Approvals for role changes are randomly verified.
- SAP delivered roles are not generated and not assigned to users.

8.8.3 User Access Monitoring

- Terminated or expired users have their access removed.
- Inactive users are locked and eventually have their access removed.
- Approvals for user changes are randomly verified.
- Approvals for Firefight access are randomly verified.
- System and batch user-ids are verified and secured.
- Users are verified for SAP license purposes.
- Reports are sent to role owners or approvers to validate users assigned to any sensitive roles.

8.8.4 SOD Monitoring

- Segregation of Duties rules and exceptions to those roles, with mitigating controls documented, are documented and made readily available. Reports are distributed to appropriate people to validate SOD rules are valid and violations to the rules are addressed.

8.8.5 Critical and Sensitive Authorization Monitoring

- Critical authorizations are defined, and reports sent to their owners to review utilization in roles and for users assigned to those roles. The owners may identify roles or user changes that may be needed. Examples include the ability to:
    - Perform system administration tasks (create printers, create batch jobs, maintain system settings and connections, etc.)
    - Perform security administration tasks (maintain roles and users)
    - Perform master data maintenance tasks (maintain vendors, customers, accounts, cost centers, profit centers, etc.)
    - Perform financial closing tasks
    - Perform Human Relations tasks
    - Perform Payroll tasks
    - Perform development tasks

8.8.6 Firefight Monitoring

- It is the responsibility of the person approving firefight access to monitor that only appropriate transactions were performed against appropriate data.

9 Audit Practices

The security team will provide internal and external auditors access to the production environment for business, system and tax audits. Internal auditors will be assigned audit roles to enable access to system audit table and authorizations. The security team will configure system-auditing tools, i.e., Audit Information System, system log.

9.1 Audit Information Services

Audit Information Services (AIS) will be implemented to provide auditors the following information if needed:

- Application logging – to capture the progress of the execution of an application
- Workflow executions – captures cross-application process not captured by application logging
- Change documents logging – to audit the change documents themselves
- Table data logging – to log changes of sensitive or critical tables that are typically subject to audit
- Change & Transport System (CTS) logging – changes created via CTS are stored in the CTS and TMS logs.

9.2 System Log

SAP systems record all system errors and user locks due to failed logon attempts in the system log. Security team will provide the appropriate profile parameter settings to the Basis team for location and size of system logs.

9.3 Security Audit Log

SAP systems have the functionality to configure security filters that record specific activities such as:

- Successful and unsuccessful dialog logon attempts
- Successful and unsuccessful RFC logon attempts
- RFC calls to function modules
- Successful and unsuccessful transaction starts
- Successful and unsuccessful report starts
- Changes to user master records
- Changes to the audit configuration

If the security audit log is activated the security team will ensure no personal information that might be protected by data protections regulations is compromised.

Appendix A: Resource Requirements

Microsoft Office
Excel Worksheet

Appendix B: Sample User Change Request Form

SAP PRODUCTION ACCESS REQUEST

REQUESTOR		
Name ***Must be line manager for user needing access***	**Phone**	**Date**
USER		
Network id **Job title** ☐ **Create** ☐ **Change** ☐ **Delete**	**Start date** **End date** *Required for contractors, not to exceed 6 months*	
Last name	**First name**	

Send completed form to approver listed for selected roles.
Use subject SAP PRD ACCESS, and marked importance high.
SAP security will only accept forms from Approvers.

SECURITY ROLE SELECTION

See the Security Role Narratives for more information about what access these roles provide

Accounts Payable *Approvers:*	**Project Systems** *Approver:*
Add/Delete - Roles	Add/Delete - Roles
☐ / ☐ Display - DIS	☐ / ☐ Display - DIS
☐ / ☐ Clerk - CLK	☐ / ☐ Sensitive Display with Labor - SEN
☐ / ☐ Manager - MGR	☐ / ☐ Project Controls Administrator - CAD
☐ / ☐ Payment Specialist - PSP	☐ / ☐ Project Controls - PCN
☐ / ☐ Check Printer - CHK	☐ / ☐ Project Controls Manager - PCM
☐ / ☐ Specialist - SPC	
☐ / ☐ Clearing Matching Transactions - CLR	

Comments:

Appendix C: Sample Fire Fight Form

PRODUCTION FIREFIGHT ACCESS REQUEST

REQUESTOR			
Last Name *User needing access*	**First Name**	**Phone**	**Date**
USER			
Network id	**Company**	**Start date**	**End date**
		More than 24 hours must be approved by Will Kizer, Phil Nibert or Gabe Rodriquez	
SYSTEM SUPPORT *Send form to any approver from list below requested role. You cannot approve yourself.* ***CALL IF URGENT, ESPECIALLY IF AFTER HOURS!***			
☐ PRD FIREFIGHT – **CMP_FIREFIGHT** People names go here			
☐ SRP FIREFIGHT – **CMP_FIREFIGHTSRM**			
SECURITY ADMINISTRATION USERS ONLY			
System: ☐ PRD ☐ SRM ☐ BW SECURITY – **R3SCADM / R3CA911** (to be added by the security team after approvals) **Detailed reason (Business case, etc) for needing Firefight Access:**			
Approvers must forward (not Reply) their approval:			

References

British Standard. (2002, September). *BS7799-2:2002: Information Security Management Systems With Guidance For Use.*

IT Governance Institute. (2003). *IT Control Objectives For Sarbanes-Oxley*.

SAP NetWeaver®. (2006). SAP Library. < http://help.sap.com/saphelp_nw04s/helpdata/en/e1/8e51341a06084de10000009b38f83b/frameset.htm