Global Information Assurance Certification Paper

Lori A. Kirk
GSEC Version 1.2f (Amended August 13, 2001)
Securing Information within SAP v4.6b

The following thoughts and best practices are the end result of an upgrade, experience with the necessary clean up after the cutover and review of best practices offered by third parties. In our upgrade, we implemented some additional levels of security from both a technical and process perspective. During the months that followed, we learned what mistakes and omissions we made as well as some things that we had implemented very well. We are currently working to tighten security on an on-going basis and have limited the enterprise's exposure to a manageable acceptable level. This practical is not intended to focus on the technical aspects of creating security access for users but rather on the implications on designing a loose, difficult to manage security environment. Accordingly, the technical discussion will be limited and at a fairly high level. Although the specifics in this discussion are directed to SAP, the premise can be applied to any software system.

One of the critical components of keeping a company's information secure is to ensure that employees are only able to view or change the financial, production, sales or master data necessary to perform their duties. User access to view or manipulate key data inappropriately presents a risk to the enterprise if the data is misused or causes actions to be taken that are unnecessary. Since data and processes are linked within one system in an Enterprise Resource Planning (ERP) environment, there are inherent risks that users will be able to access more information than they were able to access in the legacy systems previously used by most companies. Legacy systems offered controls over data simply because the sales, production and financial information was often on completely separate systems and users were only allowed access to the system necessary to perform their assigned tasks. Failure to appropriately restrict access to data may affect the data integrity and impact subsequent decisions based on that data.

As an ERP system, SAP can be used to link all facets of the organization together. A basic example of an ERP system can start with an order being placed. Once the order is in the system, the finished goods are automatically verified and, if necessary, a production order can be initiated to complete the customer's order. If a production order is initiated, raw materials can be reserved and an order placed with the supplier to replenish the stock on hand if the production order caused the stock on hand to fall below a pre-specified minimum level. Once the sales order is complete and shipped to the customer and the raw materials are ordered, accounting entries can be made to accurately reflect the activity in the corporate records. A customer invoice and payment for materials can be made automatically if the system is set up to do so.

Process Design

SAP may be best used in a process-centered organization. Process centered

organizations deliver the best value to the customer and enable the organization to outperform its competitors. One of the reasons a process centered organization can outperform competition is that the organization has analyzed the processes necessary to deliver product to customers as ordered, order product from vendors and track those transactions in the accounting records so that customer invoices and vendor payments are accurate. The newly designed processes retain only the value-added tasks and eliminate those that do not serve a purpose. By eliminating non value-added tasks, the employees are more efficient and can provide better service to their internal and external customers. There may also be cost savings associated with fewer employees or expansions into new areas by refocusing the efforts of existing employees.

In order to be effective and accurate, processes must be designed across historical organizational boundaries. Process teams must be developed which consist of enterprise experts in their respective sub processes. The process teams are responsible for defining the most effective process and identifying the tasks necessary to complete their process, whether it is order fulfillment, asset management or quality control. The enterprise experts should be assigned to the implementation project on a full-time basis until it is complete. This reduces the amount of catch-up that must be performed and ensures that the experts are able to focus completely on the project.

All employees in the organization must understand how performance of their assigned tasks impacts other employees within their process and the impact their process has on others within the organization. By providing employees with the process information, the enterprise is increasing the risk that those same employees will be able to obtain and understand information they may not have been aware of while using a legacy system. Access to the additional information makes employees more autonomous and better equipped to make independent decisions but also substantially increases the company's risk that the information will be used in an unauthorized manner.

SAP is one of the most complex ERP systems in use globally. It offers a multitude of options to limit the activities employees can perform or information they can access without negatively impacting their ability to perform their assigned tasks. In order to enable system users access to perform their jobs, the enterprise must understand what their jobs are and the processes employees follow to successfully complete their tasks.

In an upgrade or implementation of SAP, one of the most critical, and often overlooked, aspects is the impact that security will have on the final process design. The process teams are responsible for identifying the tasks necessary to complete their process and the most effective way to perform those tasks. As they identify the tasks, they also need to specify exactly how each activity should be transacted within the system. In SAP, each activity is called a transaction and each transaction has one or more transaction codes associated with it. The process teams must be able to identify the necessary transaction codes in order to build the security access assigned to users. Assigning transaction codes to users allows them to perform their assigned tasks. In

order to create a control-focused security design, the process experts must understand and implement internal controls and actively question requests for additional information or transaction codes. They must understand the risks to the organization associated with allowing users too much access to critical data.

The time allocations to the process and security design phases are consistently under budgeted by project teams. The time allocated and thought involved in developing the security design will have a long lasting and significant impact on the success of the implementation.

The process and sub process teams should also divide the transactions between themselves and retain 'ownership' of those transactions. For example, it may not be appropriate for the order entry sub process to include transactions that are specific to the shipping sub process within their process and user access design. The shipping sub process has the responsibility to ensure that all of the shipping transactions are performed according to their design and applicable training and if they allow another process to assign the transactions without their approval or knowledge, the entries may not be entered correctly or contain all of the information that is required to actually ship the product to the customer. Each process or sub process should have the authorization to refuse the use of one of their transactions to another process' security design although they can allow it if they so choose. The processes, sub processes and security teams must work closely together to make sure the out-of-process transactions in the security designs have been reviewed and approved by the process which 'owns' the transaction.

Security Design

The process teams should have a vision of the final security access design desired by the enterprise. There should be an emphasis placed on defining the enterprise security design well in advance of actually creating the security access. Without an end-design in mind, the process teams could take widely divergent paths and impact enterprise security without being aware of the exposures being put into place until the testing phase or after implementation. Redesigning security after implementation is time and cost intensive.

Since SAP is an integrated system, there will be overlap between most of the processes and sub processes within the enterprise. A weak design in one process or sub process may compromise a stronger design when assigned to users. SAP operates on the principle of greatest authorization meaning that the user will be able to access data according to the most permissive authorization assigned to their user ID rather than limiting access to the least permissive authorization. Enterprise management should provide guidance to the process teams on at least a high level to ensure that all process teams take a consistent approach. Management should provide input into the security design in areas such as:

- Organizational restrictions, such as limitations at the plant level;
- User access to direct table queries;

- Limitations around reporting capabilities; and
- Functional restrictions such as material types.

At a high level, the basic premises underlying SAP security are that user access to data is governed by the transaction codes and the related authorization objects required to process the transactions that are assigned to their user ID. Every transaction code requires at least one authorization object to process within the system. Without the transaction code, generally the user cannot even access the initial processing screen. This is considered the first level of security – by not allowing a user access to the transaction, you have effectively limited his ability to process data within the system. The authorization objects can be used to implement additional levels of security, such as limiting the user to a specific plant or company code. The authorization objects actually determine the level of access a user will have within the transaction code.

The transaction codes and authorization objects are assigned to 'Activity Groups'. Activity groups contain one or more transactions and related authorization objects depending on the purpose of the activity group and how it fits into the overall security design. Activity groups can be assigned to 'Composite Activity Groups'. The composite activity groups can hold one or more activity groups depending on the overall security design. Users can be assigned access at both the activity group and composite activity group levels.

Each of the process teams should know and be required to comply with the enterprise security design in order to limit 'permission creep'. 'Permission creep' occurs when the user is assigned two or more transactions that share authorization objects and one or more of the authorization objects allow access in excess of the user's needs. For example, the enterprise design may require that receiving clerks only be allowed to receive materials at their specific plant. If one of the authorization objects required to process the transaction code used to receive raw materials allows all plants or plants in addition to the user's location, the user will be able to enter a goods receipt at any of the allowed plants. 'Permission creep' is a known risk associated with the SAP security environment.

Internal Controls

An effective SAP Security implementation incorporates an internal control perspective into the process-designed activities. Once the process has identified the related tasks that a user is intended to perform on a daily basis, or the job responsibilities, they should communicate with the internal controls group to determine whether any segregation of duties issues exist within each newly defined activity group or composite activity group.

The internal controls group is responsible for identifying conflicts between assigned tasks. Each organization will need to develop its own sets of conflicts depending on the critical business processes performed. There are generally some standard

guidelines such as limiting a single users' ability to ship and write-off product or create and pay a vendor but often the conflicts are specific to the activities performed within the organization. There may be some conflicts that are discussed, understood and accepted by the organization but they should be well documented and approved by management.

The process teams also should provide the internal controls group with a summary of typical users. For example, a typical receiving clerk may be assigned certain activity groups in order to be able to perform receiving clerk tasks or defined job. The internal controls team must be able to review the typical security access assignments in order to assess the exposures the enterprise may have after users are assigned all of the activity groups necessary to perform their job.

By reviewing every layer of the security design, the internal controls team can limit the segregation of duties conflicts that will be built into the activity groups, composite activity groups and jobs. After the job responsibilities are modified to correct any internal control concerns, the security team should build the approved activity groups and composite activity groups to be assigned to users.

Security Creation

The security team, in conjunction with the process and other technical teams, should be responsible for identifying key transactions and authorizations that need to be closely monitored. Many transactions within SAP are used for technical purposes, such as for database management or for technical development that should not be assigned to the general user population. The security team should review all of the transactions submitted for inclusion in the various process jobs to ensure there are no technical transactions included. Additional approval should be obtained from the technical teams if a process does request one of these transactions.

There are also powerful authorization objects that should be actively tested and scrutinized prior to adding them to an activity group. In security table SU24, the security team can inactivate key authorization objects so they will not be automatically added to the activity groups when using the SAP tool Profile Generator. These authorization objects should be identified through discussion with the process and technical teams. The authorization objects that are considered critical may vary at every enterprise depending on the activities performed. Some companies may consider the ability to create master data to be one of the most critical functions or they may consider direct table change a high-risk activity.

Based on the discussions with the process, technical and security teams, the authorization objects should be identified and inactivated before any activity groups are created. Inactivating the authorization objects will ensure that the activity groups are fully tested before they are assigned to users. The testing will allow the authorization objects to be added to allow the user to perform the transactions as intended but not grant any additional access. By requiring testing to be performed, the security team

can ensure only the most specific values are included in the authorization objects, thereby limiting 'permission creep' to the extent possible.

Once the activity groups are created, they should be assigned to test IDs and the process teams should perform positive testing to make sure the activity groups are functioning as designed. A key aspect to testing that is often ignored is to perform negative testing as well. Negative testing ensures that the test ID cannot perform a function that was not intended. For example, if the enterprise design is to limit by plant, the process team should negatively test each activity group to ensure that it only allows processing at the specifically identified plant.

After each activity group has been thoroughly tested, the process teams must identify the activity groups that will be assigned to every user in the system. In many cases, a user will perform more than one job. If users are to be assigned multiple activity groups, the internal controls team should again review the assignments for segregation of duties issues. They can also identify potential control concerns such as incompatible job assignments, which do not cause specific segregation of duties concerns but may present internal control concerns that should be addressed by the organization. Negative testing should also be performed when users are assigned multiple activity groups to ensure the user has not unintentionally been assigned more access than intended.

All of the components of the security design and creation and the user assignments should be documented and approved to provide a baseline for the access assigned as of the implementation date.

Training

Users must be properly trained so they know how to enter the data into the SAP system. A data entry error can flow all the way through an ERP system and negatively impact data integrity and the decisions made based on that data. Each organization must determine the best way to train its users and ensure every end-user has completed at least the minimum training requirements.

Security Maintenance

After the implementation, there has to be a documentation tool to track and obtain approval for changes to the user access and the activity groups. If the enterprise is going to maintain tight control over the access that users have within SAP, there must be a rigid approval process for any changes to the activity groups. Activity groups are assigned to numerous users and any change made to the activity group will impact the access allowed to all of the users with that activity group. The process teams still retain ownership to the activity groups created to perform the tasks within their process. They also retain ownership to the transactions that pertain to their process.

The security team is the main point of contact when a process wants to make a

change to their activity group. One of the first checks that should be made is whether that process owns the transaction or not. If it does not, the appropriate approvals must be obtained and documented prior to adding the transaction to the activity group. Since changes to activity groups will have an impact on every user with that activity group assigned to their user master record, each change must be assessed for compliance with the enterprise security design.

All changes must be tested in a development or quality assurance system to validate the change is working exactly as intended and negative tested to make sure that it doesn't allow more access than intended. Even with the negative testing, there may be 'permission creep' because the process team cannot test every combination of that activity group with others as they are assigned to users in the system. The change to the activity group should be reviewed for segregation of duties issues. If it is not reviewed prior to making the change and a conflict is built into the activity group, all users assigned the activity group will now have the conflict.

Changes to user access should also follow a strict approval process. As a user requests access to a specific transaction, the security team should determine which activity group contains the transaction. Once the activity group is identified, the security or internal controls team should perform a segregation of duties analysis to verify there will not be any additional segregation of duties issues when the access is assigned to the user. If there are no additional issues or concerns, the user's request should be forwarded to the appropriate approver for the activity group. Once the approval is obtained, the security team can assign the additional access to the user.

On a regular basis, the internal controls team, internal audit or external audit should review the security design and user access from an overall perspective. Since many of the changes to activity groups may be made without an overall review of the impact on the users assigned the activity group, the internal control environment may degrade over time. As the environment degrades, users will be allowed more access to data than they actually need. A looser security environment will eventually erode the enterprise's ability to keep its information secure and accurate.

Sources

[1] Hammer, Michael. Beyond Reengineering. New York: Harper Collins Publishers, Inc., 1996

[2] ASAP World Consultancy. Special Edition Using SAP R/3: The Most Complete Reference. Que Corporation, 1996. 743 - 780

[3] SAP AG, "Data protection and security in R/3", R/3 note no. 30724
URL: http://www.ciudadfutura.com/sap/sap/oss/0030724.htm (September 6, 2001)

[4] CIO.com, "Does ERP Build a Better Business?" February 15, 2000
URL: http://www.cio.com/archive/021500_excerpt.html (September 21, 2001)

[5] Foster, L. Annette and Herndon, Billy T. "Implementation of a Reengineered Procurement Process at Duke University, Using Technology and Work Process Redesign". 1997
URL: http://www.educause.edu/ir/library/html/cnc9708/cnc9708.html (September 6, 2001)