Top 10 SAP audit and security risks

Securing your system and vital data

Prepared by:

Luke Leaon, Manager, RSM US LLP
luke.leaon@rsmus.com, +1 612 629 9072

SAP is a functional enterprise resource planning (ERP) system, with applications and modules that can help manage many facets of a business. The platform is very secure, but with countless options for customization, access levels and permissions, vulnerabilities can appear if the organization is not careful and if a thorough process is not implemented. Companies must know the potential risks to the system to help ensure that it is secure and functioning efficiently.

The current focus of most businesses using SAP is risks related to compliance and securing the system in accordance with regulations such as Sarbanes–Oxley Act of 2002 (SOX) and other regulatory compliance requirements, such as the Health Information Portability and Accountability Act (HIPAA). However, external threats are emerging to systems like SAP that were not significant concerns in the past. Over the last few years, criminals have sought to exploit ERP systems to access information from trade secrets to employee information. The following are 10 common risks that can create vulnerabilities in an SAP system and leave important data at risk.

Inadequate FireFighter controls

The FireFighter function gives certain personnel an elevated level of privileges to make changes in the SAP production system if an issue is discovered. Unfortunately, in some cases, organizations give too many employees that level of access and permissions to make impactful changes, presenting an unnecessary level of risk.
Best practices dictate that a company should divide FireFighter controls into functional areas, instead of granting access to all areas. Don’t give employees “keys to the entire kingdom;” only give them access necessary to do their job.

Base FireFighter access per module or job function, such as FIRE_FLi and FIRE_SD, and never use SAP_ALL, SAP_NEW or equivalents.

Preventive controls include the system requiring approvals before employees can access a FireFighter ID. Ideally, access to FireFighter controls should be time–limited, based on the extent of the necessary work, and transaction codes (T–Codes) should be logged that are executed on those IDs. Organizations can automate the management of FireFighter IDs in a number of ways within SAP, with several versions of GRC and differing abilities to configure IDs. Companies should assign access to individual users and monitor privileged generic or service accounts like SAP* and DDIC, even if they are communication IDs to verify they are not accessed and the FireFighter process is being circumvented.

As a detective control, a company must review logs, but the processes must take place in a timely and thorough manner. Pay close attention to the data to spot unnecessary access; people tend to get caught in a cycle of approving logs without closely reviewing data. The right people must thoroughly review the appropriate information.

Companies should also implement a benchmarking program to view how many people are using FireFighter IDs in a given time frame to spot any inconsistencies. For example, if an organization has 10 people using FireFighter IDs in one month and 50 the next, it needs to investigate further to know why. Companies must also understand if any trends exist with frequent uses (as in a daily); if that’s the case, users’ daily roles may need to be modified, instead of them using FireFighter to accomplish tasks related to their daily job.

Segregation of duties

In many cases, users are able to execute functionality that they should not have access to. Obviously this creates several risks to the business, such as potentially creating a fictitious vendor and processing a payment.

Companies should implement an organization–wide segregation of duties (SOD) matrix, for an enterprise–wide assessment of sensitive functions and incompatible duties. An SOD check during user provisioning is also a best practice as a preventive control. However, SAP is such a complex system that a manual SOD check is difficult, inefficient and is not 100 percent accurate. An automated tool is necessary to perform the assessment; SAP has a GRC module that handles the task effectively, and there are other similar tools available. If a company chooses not to utilize a tool internally, we highly recommend it has their auditors run their automated tool to help assess hidden SOD risks.

Cross–system SODs are also important to reduce risks with conflicting access with other platforms. For example, a company may handle SOD very well within SAP, but someone may perform fictitious processes within a linked human resources (HR) platform. Organizations must instill processes that take all systems that are potentially fraudulent into account.

In some cases, some managers may not know what they are validating. When they go into the system and assess rule sets and potential risks for fraud in the SOD cycle, they must understand the risk, what they are approving and whether a manual control exists to compensate for that risk. Consider the use of role owners as an approval step; their role should be function–based to provide greater accountability. Functional managers need to take ownership of specific roles to manage any changes and the type of access for user provisioning and approval.

Detective controls include providing a periodic review of the SOD, and continuous control monitoring (CCM) can utilize a GRC tool to identify any SOD issues immediately versus raising concerns in the next review. CCM does take some effort to program the SOD rule set into the GRC module. There is some up–front work required, but the subsequent protection level is worth the effort.

Companies must be careful when implementing mitigating controls, including the amount of mitigating controls, as the risk of failure with manual controls is always higher than with reliance on automated controls.

Custom reports, interfaces, conversions, extensions, forms and workflow (RICEFW) object security

Custom objects, such as forms and interfaces, that often drive key business functionality can have security backdoors that create major vulnerabilities. During implementation, companies must include strong change management controls around these objects. Test them appropriately during development and follow SAP–specific methodology to document what they do and specific security measures that are being implemented.

When customizing SAP, many companies are concerned about getting the system up and running, but forget about security. Organizations must have program authorization checks and implement a specific security plan that accounts for customizations. Another best practice when developing custom objects, even during an implementation, is to limit access to key BASIS T–Codes, such as SCC4, SE06, SA38 and STMS, among many others.

A final preventive control is to maintain a comprehensive, updated RICEFW inventory, documenting all custom objects, forms, reports and interfaces. Security audits also make people aware of custom transactions and functionality, providing an inventory of what they do. In addition,
vulnerability assessments can communicate the risks around any customizations. New versions of Solution Manager will allow for the retention of RICEFW customizations linked to actual configuration in SAP.

**Application controls misalignment**

Over time, companies may implement application controls within the SAP system, such as three-way match, opening and closing posting periods and duplicate invoices. The system controls those processes and checks to make sure the necessary elements take place before a process occurs. Unfortunately, the system may not align with a company’s business risks or needs because of changing circumstances, or possibly a good risk assessment was not initially performed. Another potential issue arises when new functions are implemented; new risks may emerge, and controls must evolve with them.

In addition, companies can also overcontrol a system, implementing too many controls and hampering operational efficiency. Companies can be too stringent, but controls must meet the risk appetite.

Preventing the misalignment of controls starts with having a comprehensive, updated risk and controls matrix. In this matrix, key business processes are mapped and risks are identified; subsequently, controls are designed to address these risks.

After mapping risks and controls, SAP functionality must be enabled to enforce controls. However, companies must be careful to establish a rationale for each control and ensure it matches the business strategy and risk appetite.

After application controls are designed, they need to be tested during the implementation phase and then on an annual basis at least to verify the process has not changed and the control remains effective.

**Infrastructure security vulnerabilities**

Infrastructure issues have typically been overlooked in the past, as they were not a key concern. However, as cybercrimes broaden in scope and severity, infrastructure vulnerabilities must take greater precedence. Many issues that most people are unaware of or overlook can have a huge impact. The greatest application-level security in the world can be largely undermined by vulnerabilities lower in the stack.

For example, a layer of SAP configures how different hosts within the SAP infrastructure talk to each other; a normal configuration will have production, quality assurance and test servers. The SAP system trusts those servers, so misconfiguration or lax access controls around system administrator commands could introduce vulnerabilities. Remote function calls (RFCs) enable middle-layer communication within SAP; if someone can exploit those RFCs, they can gain control of an entire system.

Other areas of particular concern include:

- Database security — Particularly system administrator accounts such as “sa” and “sysadmin,” as well as settings for trusted authentication and default application accounts
- Interfaces — Particularly transactional-related data
- Operating system — Pay close attention to typical concerns related to patches, anti-virus, malware, trusting, port vulnerabilities, etc.
- Network — Closely evaluate port management processes

**Contractor and vendor management**

Third-party management concerns are not specific to SAP, but they can cause complications in the environment that management will be responsible for. Many organizations use contractors to perform SAP development or administration and trust those vendors without significant monitoring. Companies should take the same due diligence measures with contractors as they do with employees, if not more stringent measures.

In general, if vendors handle key processes, they should have a service organization control (SOC) report. If a vendor supports any function with financial relevancy, it should have a SOC 1 report. If the SAP system is in a hosted environment, vendors should have a SOC 1, as well as a SOC 2 report. The SOC 2 report provides five trust principles: security, confidentiality, availability, privacy and processing integrity. If the system is hosted, it must be available, and if any outages occur, backup plans should be in place with limited downtime. This information is normally detailed in a contract, but a SOC 2 report actually tests those areas and proves that controls are actually working.

In addition, companies must ensure vendors communicate changes in support personnel; organizations want to limit access to systems to current employees. Vendors’ access levels should be closely monitored, not allowing 24/7, uncontrolled access and issuing individual accounts to track users, rather than a single vendor account.

**User access reviews**

Similar to SOD reviews, a user may have a level of access they never required, or job responsibilities have changed, and they no longer need certain access. However, an SOD review will not find these errors; a separate user access review is needed to help ensure users are entitled to the access they have.

Unfortunately, reviews come with many pitfalls; one is ownership of the process and who conducts the reviews. Access or functional owners must designate and be educated on what they are looking at and doing. Having an effective understanding of what roles actually allow access to, which must be derived from what roles actually are configured with, rather than descriptions, helps prevent excessive access.
Access reviews should be granular, going beyond T-Codes to the authorization object level. One way to accomplish this is to review users and what roles they have on a periodic basis, doing a more detailed review of roles and the assignment of authorization. The process is intensive and requires technical resources, but it does not need to happen as often as a normal access review, and it helps to determine the correct access.

**Interfaces**

System IDs that are used for interfaces typically have elevated access to the system, are not applicable to password configuration settings and could have powerful profiles assigned, such as SAP_ALL. There is a risk that administrators may change the type of account the ID is from a system account to a dialog account, which gives them access to circumvent security controls. This serves as a backdoor manner to circumvent a FireFighter control. It’s critical that end users do not receive accounts noted as System.

Completeness and accuracy of data received is also a key concern for organizations. Institutional Documentation (IDOC) Service is an intermediate document used to facilitate the transfer of data; however, sometimes SAP cannot handle certain IDocs and will create errors. Companies must monitor and assess those errors and correct them so they do not affect financial statements.

New interfaces or changes to existing interfaces need to be accounted for. For example, companies may introduce an additional interface into a system, where a third party interfaces contractor billing data to the system directly. That can potentially introduce a material level of transactions that may require additional procedures to verify the data is accurate.

System and communication accounts, even for interfaces, are typically not evaluated during a standard SOX information technology general controls audit. In addition to a normal audit, a company must take a deeper dive into systems and communication accounts and interfaces to make sure everything is appropriate, and the system is not vulnerable to additional risks.

**Direct data updates**

S_TABU_DIS is an authorization object that may be distributed to many users, allowing for direct access to edit tables (assuming the user has one of the many T-Codes to edit tables directly). Many organizations restrict access by T-Code only, because it is easier, but it potentially allows for many users to have access to the authorization object that could allow for direct editing to tables. Restricting T-Codes only is rarely effective, as there are many T-Codes that can be used to make edits to tables.

Allowing access to other authorization objects that allow for direct execution of programs introduces a risk of direct data updates, as well. Instead of going into a normal transaction screen, a user can execute a program with edit capabilities and perform direct data edits. This is another avenue that presents difficulty of taking a T-Code-only security model.

Like any technology, SAP has bugs and has released patches to fix them. For example SE16N is a table display transaction that can go into edit mode and provide direct data access. SAP released a patch to close up this potential vulnerability, but if a user has Debug access, they can skip over the patch and enter Edit mode. In general, Debug should not be in production, as it can circumvent authorization checks in code.

Authorization groups are a best practice to restrict access to tables. Users can edit data, but only on a specific group of tables. Whenever a new table is made, it must be registered in the TDDAT table to assign it to an authorization group. Custom tables must be registered, and all transactional and security-related tables should have a defined authorization group.

Some functional modules do not perform authorization checks on S_TABU_DIS, presenting another issue. In addition, weak parameter transactions, especially those that are developed, could allow for a user to directly update any table. Another authorization object, S_TABU_NAM, allows organizations to specify tables users have access to. If a user needs direct access to a table, it can be specified in S_TABU_NAM, and the company can control access.

**User admin controls**

A major risk with many SAP systems is ineffective provisioning or changes of accounts and de-provisioning user access controls. As we touched on previously in many cases, approvers may not be knowledgeable about what access they are granting, and access is not role-based, which could result in excessive access.

In addition, some of the technology that has been introduced to automate deprovisioning and provisioning may complicate things and result in security holes that go undetected. Depending on the environment, an identity and access management solution or batch process tied to Active Directory may help to remove and add access. Organizations that rely on automated active directory or HR-based removal introduce the potential for the process to miss users based on poor communication between the different technology and reuse of accounts. Any technology changes and poor administrator practice can render controls ineffective.

Many organizations are automating processes to control access, which is good. However, it is very important for companies to be cognizant of the data sources they use and how changes to access are made. Several possible vulnerabilities can arise, depending on how the company
configures the SAP system, administers access, makes changes to infrastructure and performs identity management, as well as how the platform is communicating. Just because processes are automated does not make them foolproof.

The status of users and the system of record are also major concerns when managing system access. In some cases, managers do not communicate rehired contractors, temporary employees or leave of absences, while some contractors are not in the HR system. Pay close attention to contractors that may be set to expire, as well as potential users with more than one ID and different levels of access.

Other potential control issues include transfers retaining access, users being cloned and giving excessive access, users not named correctly and access not being role-based. Problems can also arise with super-users, when access is not approved or informally given out or when super-users leave. Potential vulnerabilities can arise when account passwords are embedded to processing.

**Conclusion**

In many cases, the SAP system is the backbone of an organization, managing key processes and information. Therefore, companies must implement strategies to know who is accessing specific areas of the system and whether users and third parties have the correct level of access. Proactively evaluating the SAP platform for common risks helps to identify and address vulnerabilities before they can have an adverse effect on data and compliance success.
This publication represents the views of the author(s), and does not necessarily represent the views of RSM US LLP. This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.

© 2016 RSM US LLP. All Rights Reserved.