Top 10 SAP audit and security risks

SAP is a secure platform—but countless options for customization, access levels and permissions, alongside increasing cybersecurity threats—mean vulnerabilities can appear if the organization fails to implement a thorough process for managing them. Thus, companies must be aware of potential risks to ensure the system is secure and functioning efficiently. The focus of most businesses using SAP has securing the system in accordance with regulations such as the Sarbanes-Oxley Act of 2002 (SOX) and other regulatory compliance requirements, like the Health Information Portability and Accountability Act (HIPAA). However, new external threats to SAP have begun to emerge: Over the last few years, criminals have sought to exploit ERP systems in order to access confidential information, from trade secrets to employee information. The following list discusses 10 common risks that can create vulnerabilities in a SAP system and compromise important data.

1. 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 disregard can have a huge impact, as 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, antivirus, malware, trusting, port vulnerabilities, etc.
- **Network**: Closely evaluate port management processes

2. Insecure configuration

Many of the default security settings are not configured properly during the installation of SAP systems, leaving them insecure and highly vulnerable to both internal and external attack. Organizations should therefore keep in mind that configuration is separate from patch management and thus must ensure that the SAP systems are implemented with correct security settings and configuration of the SAP NetWeaver stack at the beginning, which will help avoid costly production server downtime later.

Few examples of areas where insecure configuration can compromise the security of the SAP applications include parameters related to configuration used by RFC connections and gateway and message servers.

3. Lack of patch management

Patch management is critical to supporting the stability and security of your SAP systems through fixing functionality or patching vulnerabilities identified in previous releases. As many organizations migrate their SAP environments to the cloud, patch management has become a more complex process wherein companies are struggling to identify, assess and implement patches on a timely basis.

Some of the challenges that organizations running SAP face while keeping their SAP systems up to date include:

- System administrators who are unaware of existing vulnerabilities and relevant patches required to keep the system stable and secure
- The absence of a patch management strategy required to assess patches based on criticality and applicability
- Testing patches prior to deployment to mitigate unexpected system behavior and downtime

4. Unencrypted interface communications

Communication protocols used by SAP application servers are not encrypted between client/server networks. In addition to encryption, missing mutual authentication mechanisms could lead to network traffic being intercepted by a "man in the middle" attack.

Organizations must therefore consider using security measures such as Secure Network Communications (SNC) in order to encrypt communication between SAP GUI and SAP application servers, as well as RFC communications between SAP servers. Strong authentication mechanisms, including Single Sign-On, also protect communication channels between systems of higher security classification (e.g., production systems) and lower classification systems (e.g., test/development systems).

5. Access control and segregation of duties

Poorly executed SAP application security role design results in unauthorized access, increased potential for fraud in the form of Segregation of Duties (SoD), inefficient access provisioning for end users and increased audit findings/issues. Configuring access controls and roles in SAP applications prevents employees from having access to more data than needed for their job duties and protects against insider threats and the possibility of SoD-related fraud.

Maintenance of the SAP application security role design and its governance, including adequate oversight of the change management process, ensures that the role design remains free of SoDs over a period of time, and thus less vulnerable to internal breaches.

Companies should implement an organization-level 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 not 100% accurate. An automated tool is therefore necessary to perform the assessment; SAP has a GRC module that handles the task effectively; other similar tools are available. If a company chooses not to utilize a tool internally, we highly recommend that they have their auditors run their automated tool to assess hidden SoD risks.

6. Monitoring security events and configuration

Monitoring of privileged user accounts, application configuration, data and databases, and use of logging to evaluate the security events of the organization all help address the risk of vulnerabilities within the SAP system. This also enables the organization to address risks associated with broken access controls while a review of the roles and privileges across the SAP system is performed.

Organizations must establish a security plan and security configuration baseline, prioritize risk management and develop processes to address known vulnerabilities (through patching or configuration changes) and mitigate threats to the SAP environment.

7. System ID security

System and communication IDs often have elevated access to the system, are not applicable to password configuration settings and may have powerful profiles assigned, such as SAP_ALL. Thus, there is a greater risk that a hacker could obtain credentials and utilize the ID to exploit the system.

System and communication accounts are typically not evaluated during a standard SOX information technology general controls audit, so in addition to a normal audit, a company must take a deeper dive into systems and communication accounts and interfaces to ensure everything is appropriately protected so that the system is not vulnerable to additional risks.

8. Custom code security

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

A final precautionary 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 by providing an account of what they do. In addition, vulnerability assessments can communicate the risks around any customizations.

9. Broad administrative user privileges/Excessive emergency access

Many organizations provide elevated access to administrators and/or the IT support team during the time of implementation or during temporary maintenance/troubleshooting of the production systems. Attackers have the possibility of exploiting weaknesses in privileged access security through the use of ransomware attacks or data theft. Loss of privileged access has a high business impact, thus requiring additional measures to ensure its security.

It is recommended that organizations implement multi-factor authentication mechanisms to limit the chances of these privileged accounts being compromised by internal threats or external hackers. Monitoring, logging and review of user activity is another way to ensure privileged access is used responsibly and that any anomalous activity is identified as an indicator of potential cybercrimes.

10. User admin controls

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

In addition, some of the technology that has been introduced to automate provisioning and de-provisioning may complicate matters 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 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 technologies and reuse of accounts. Similarly, any technology changes made under lax administrator practice can render controls ineffective. Many organizations are automating processes to control access, which is good.

However, it is critical for companies to be cognizant of the data sources they use and how changes to access are made. Multiple vulnerabilities can arise from how the company configures the SAP system, administers access, makes changes to infrastructure or performs identity management, alongside 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 leaves of absence, while some contractors are not in the HR system altogether. Pay close attention to contractors who may be set to expire, as well as potential users with more than one ID and multiple levels of access. Other potential control issues include transfers retaining access, users being cloned and given excessive access, users named incorrectly 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.

Operating an ERP system comes with some inherent risks, and SAP is no different. You must pay close attention in order to understand several common threats as well as be mindful not to create additional vulnerabilities. Evaluating and successfully managing these 10 audit and security risks can go a long way in ensuring that your SAP platform and critical data remain secure and continue to function at peak efficiency.

+1 800 274 3978
rsmus.com

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.