ControlPanel GRC®

ControlPanel GRC™ Always Audit Ready™ Series: SAP® Security Vulnerability

Strategies to Prevent SAP Security Vulnerability and Improve Audit Readiness

Strategies to prevent SAP security vulnerability and improve audit readiness

Recently, a company went live with SAP HCM (Human Capital Management). It was discovered the morning of going live that all users had the ability to view confidential employee salary data. The reports to display the data were not easily found and it was not clear if anyone actually ran those reports, but management was appalled by the risk.

The SAP world is littered with similar stories of security gaps and risks. How could that risk have been prevented? What other risks haven't been discovered? Why are there so many vulnerabilities in SAP security?

While being referenced in SAP folklore as an example of an implementation-gone-bad is unsettling, failing an audit due to excessive IT security risks, is worse. SAP security risks have an impact on the internal underpinnings of a company, but they also jeopardize compliance efforts. Even if an enterprise is not subject to external compliance mandates, auditors and executives want to know the state of their SAP security model. How exposed to the potential of fraud or catastrophic error is the company?

This paper will cover 1) why SAP security issues are so prevalent; 2) the major areas of risk to a company; and 3) how an annual "check up"" or vulnerability assessment can help identify and correct issues.

The objective for every company should be to go into an SAP audit confidently, knowing that any security risks or vulnerabilities have been addressed.

Security gone bad

Setting up and testing a proper SAP security model is often looked over and "under engineered" in the original SAP implementation. Why?
Those who have lived through SAP implementations know it can get ugly getting to go live. Too often, the focus is on getting business processes to work and less on mapping access of the related transactions to job roles. For example, in finance, consultants implementing the solution are often consumed by making sure goods received flow through properly to accounts payable. They are likely to overlook whether Gladys or John has a right to process a particular payable.

Even in implementations where setting up a sound SAP security architecture is in scope, too often the focus is on what's known as "positive" security access - whether a user can access the transactions they need to do their job. Less attention is typically given to "negative" security testing, which tests whether a user is prevented from accessing a transaction they have no business executing. For example, a wholesale distributor our company works with discovered a parts picker in their warehouse had been accessing several SAP financial transactions which he had no reason to view. When questioned, he said he was "just curious," but he could have successfully entered fraudulent financial data.

Essentially, SAP implementations too often go live with end users having very broad access to transactions far removed from their actual job functions. Because setting up and testing SAP security was largely looked over in the implementation, the traditional knowledge transfer between the System Integrator (SI) consultant and the internal IT administrator doesn't happen. When the SI consultant leaves, internal SAP administrators are left with a poorly implemented security model and little training to take it from there.

Even more problems occur post-implementation, resulting in further degradation of SAP security controls. The post-implementation problems are focused in three areas:

- Poorly trained SAP security administrators
- Turnover
- Lack of meaningful controls

Poorly trained SAP security administrators

In many companies, the IT helpdesk organization is responsible for day-to-day user add/delete or changes. However, IT helpdesk teams are not usually trained in the applications themselves. SAP support teams are organized by business areas and do not necessarily know technical functions like SAP security authorizations. In many shops, the SAP Basis administrator is also asked to administer SAP security. Having the Basis administrator responsible is also problematic as they don't necessarily know the business implications of giving access to particular transactions.

This constant stream of processing user change requests, often with too little rigor, can create an ever increasingly complex matrix of SAP Roles that become harder and harder to manage. Increasing the number of Roles greatly increases the risk that a combination of Roles can enable one user to access a

combination of transactions to potentially commit fraud. Roles growing out of control also increases the chance that a user might execute transactions outside of their job description or authority.

Turnover

Even in enterprises that did a good job of implementing and maintaining SAP security, turnover in critical staff can create risk. One of the realities of the global recession is that IT organizations have been paired to the minimum. Usually IT organizations are only "one person deep" in many key roles. A void is left with the departure of a key IT resource. The experience and knowledge learned during the original SAP implementation and years of functioning in a role literally walks out the door. Too often, a key resource is backfilled with someone who may be trying hard, but simply doesn't have the experience or training to perform his/her duties at the same level as their predecessor. SAP security administration is a specialized expertise. Without training and experience, it is very difficult for a new employee to properly maintain SAP security. As a result, SAP security tends to degrade under the reigns of a junior resource.

Lack of Meaningful Controls

As mentioned above, SAP security is a specialized expertise. Enterprises rely on their SAP Basis administrators to keep SAP security under control. In addition to all the day-to-day changes and gaps in knowledge that develop over time, an added strain to SAP security controls also arises – audit readiness and compliance.

Publicly traded enterprises have been required under Sarbanes Oxley (SOX) legislation to implement demonstrable controls over access to finance data. This usually means an annual, painful data gathering and reporting process that shows some controls were in place at a given point in time, based on some sampling of data. The focus of these audits in SAP usually center on segregation of duties (SoDs).

Privately held companies may be glad not to have been subjected to SOX mandates, but many do not even have an annual audit to gain some confidence that bad things aren't happening in their SAP systems. A truism is "trust is not a control." Many executives simply don't know the state of their SAP security.

Many enterprises face increasing audit scrutiny. Some are preparing for being acquired or going public. Others start working with a new audit firm or their existing audit firm changes requirements. It can be a nervous time for executives who may have under engineered controls in place in the days before an audit. They simply don't know what is going to be reported.

Major areas of SAP security risk

This paper has covered some major areas stating why there is SAP security risk – under engineered security controls during implementation, poorly trained staff, turnover, and lack of focus on critical compliance controls – and now will shift to understanding what needs constant vigilance to help ensure SAP security issues don't become a problem.

Major areas of risk to a company include:

- Segregation of Duties (SoD)
- Sensitive Authorizations
- Excessive Access
- Sensitive Role and Profiles

SoD risks

SoD risks represent instances where a User or Role has the ability to perform multiple portions of the same business transaction. Companies should understand User/Role risks by business process, Users/Roles with the highest number of risks and the percentage of Users/Roles with risk in your organization.

Sensitive Authorizations

These risks occur when a User or Role has the ability to perform sensitive system functions that should be restricted in production systems. Sensitive Authorization risks represent instances where Transaction and/or Authorization access can impact data confidentiality, integrity or availability. Although it is reasonable that some technical users might require these authorizations in a production system, they should generally not be available to end-users. Companies should understand User risks by User Group and identify Users with the highest number of risks.

Excessive Access

Also known as Critical Transactions, these risks occur when a User or Role has the ability to execute Transactions that are critical from a financial and/or audit perspective. These critical Transactions are normal functions that

are required to run your business. However, because these Transactions have financial and/or audit implications, they should be reviewed for reasonableness to ensure that they are assigned to appropriate Users. Companies should have a good understanding of excessive access risks by User, business process and Role.

Sensitive Roles and Profiles

Sensitive Roles and Profiles represent instances where Users are assigned to Roles or Profiles that are known to contain large numbers of Segregation of Duty, Sensitive Authorization or Excessive Access risks. Assignments to these Roles or Profiles should be monitored separately to ensure they are restricted to appropriate Users.

How to monitor and assess security risk areas

Enterprises who reach a tipping point and want to understand the current state of their SAP security model and vulnerabilities may consider asking their existing staff to conduct a point-in-time analysis. This approach is problematic as existing staff is probably too busy to take on a burdensome, incremental task. In fact, existing staff may be the source of the concerns.

Third party vendors or consultants may offer services to perform a point-in-time assessment. While helpful, these consulting based services can be expensive and still demand an extensive time commitment from internal staff.

Other assessment services exist like Control**Panel**[GRC]'s Security Health Check. These services provide a software based solution that can provide critical insights based on a simple data export, run through a sophisticated software analysis engine and reviewed by a senior SAP security consultants. This approach is cost-effective, minimally disruptive and provides needed critical insights. This approach also provides a perhaps needed layer of "insulation" from internal staff.

Longer term, companies should consider continuous control monitoring (CCM) software. While health checks can detect issues, CCM software helps prevent and detect security vulnerabilities. For instance, CCM would help you assess whether a change was adding risk and let you make changes to prevent those issues.

ControlPanel GRC®

Summing up SAP security issues

SAP, as the enterprise system of record for thousands of companies, is critical to a company's success yet many executives don't know the state of their SAP security. Furthermore, many SAP experts within a company – for a number of reasons – may not know the state of the SAP security risks. However, security risks can result in an incident of theft, fraud or a failed audit. Honing in on SoD, Sensitive Authorizations, Excessive Access, and Sensitive Roles and Profiles risks, can help prevent most common SAP security risks. Companies that perform regular checks, or SAP security "physicals," are the best equipped to manage and prevent risk. Additionally, compliance automation functionality exists, particularly continuous controls monitoring (CCM) that can provide in real-time risk analysis, ensuring a company is aware of risks at any time.

About ControlPanel[GRC]

ControlPanel[GRC™] is a new breed of Governance Risk and Compliance (GRC) compliance automation solutions – one that focuses on rapid implementation, ease of use and broad functionality aimed at making SAP® users Always Audit Ready™. Part of Milwaukee-based SymSoft Corporation, ControlPanel[GRC]'s integrated GRC technology suite addresses the major areas of compliance concerns for SAP users. With more than 60 implementations in over two years, ControlPanel[GRC] has given its clients the ability to confidently satisfy compliance requirements while accelerating workflows that enhance their team's productivity. For more information about ControlPanel[GRC], visit www.ControlPanelGRC.com or call 1-855-MY-CPGRC.

About ControlPanel[GRC]'s Security Health Check

ControlPanel[GRC] Security Health Check

The ControlPanel[GRC] Security Health Check is a risk assessment service that helps identify potential audit risks in SAP. The assessment is for any organization that:

- Uses SAP as the core system of record and is subjected to audits
- Strives to have a customized review of their compliance risk areas
- Wants to know SAP security risks before an auditor discovers them
- Needs to convince senior management of the gaps in the company's compliance program
- Strives to understand strategies and tools needed to overcome potential security risk areas

The ControlPanel[GRC] Risk Analysis Engine

We export a company's security model and run it through the ControlPanel[GRC] Risk Analysis Engine. Within less than two weeks, a comprehensive report that contains over 40 charts and graphs assesses potential and specific risk areas.

The ControlPanel[GRC] Security Health Check report is divided into four sections of analysis – Segregation of Duty risks, Sensitive Authorization risks, Excessive Access risks, and Sensitive Roles and Profiles risks. Each section will indicate where there are low, medium, high and critical risks.
Moreover, the report, which is presented in a one to two hour working session, provides strategies to overcome potential risk areas.

ControlPanel GRC®

Always Audit Ready™

For more information about ControlPanel[GRC], contact us at

1-855-MY-CPGRC www.ControlPanelGRC.com
1201 N. Prospect Ave. Milwaukee, WI 53202