SECURINFO for SAP
Executive & Analyst Introduction

Integrating SAP Application Security with the Enterprise

Contents

Copyright

Trademarks

Introduction

This paper deals with the Application Security issues faced by SAP customers. The goal of Application Security is to allow personnel to complete their work without having either unnecessary or too much access that could lead to fraud, theft of information or other business vulnerabilities. For example it would not be prudent to allow one person to create a vendor, approve an invoice and print a check. On the other hand, too many persons having access to master data can create integrity issues.

As of July 2002, 19,357 companies in approximately 120 countries run 56,240 installations of SAP® software. Investment runs from $5 million to $1 billion and these new systems are mission critical to the companies' business. In order to protect that investment; security must ensure that the right people have the right permissions to protect the integrity of the information. Not too much, not too little. Most companies experience difficulties with security in their SAP environment. Why? There are many issues but the bottom line is complexity. This complexity combined with a lack of tools in SAP result all too often in a security status that contains many serious but hidden risks.

Securinfo specializes in Information Security and has developed a robust, industry strength solution for use by SAP customers, **Securinfo for SAP**. This unique product simplifies, accelerates and controls the SAP Security Process. The solution captures more than 50 man-years of development and combines the knowledge and experience of specialized security consultants and their customers. Securinfo endeavours to enable customers to make informed decisions about security and therefore this paper sets out the business challenges imposed by integrating SAP Application Security with the enterprise and the alternatives and approaches that should be considered to resolve them for their benefit.

Is SAP Application Security a challenge to your Enterprise?

The issues surrounding the implementation of security on SAP® systems are, generally, not appreciated initially and certainly not well understood. Time and experience quickly change this perception at most SAP customers. Many SAP® systems are being upgraded and extended into even more complex systems as they are prepared to allow interaction with partners and customers using customer relation management systems, and supply chain extensions. Consequently, companies are recognizing the necessity to have more assurance that the right people have the right permissions in these application business systems.

How does an enterprise assess the state of its security? Unfortunately the usual way is from an audit. The auditors deliver a lengthy report identifying loads of risks and issues together with a big bill. Management is often unaware of these issues, because of the lack of reporting and lack of transparency surrounding the security process. Security administrators who can decipher the complex technical jargon usually understand the technical issues, but don't appreciate the business impact. Business personnel likewise are mostly not able to assess their security situation when dealing with a request or approval due to the technical complexity

The question arises "*Why do we have to hear this from the auditors? Couldn't we at least determine this ourselves?*" There are many issues dealt with in this paper however complexity is the major culprit.

How do you resolve the challenge?

Historically, the usual way was with consulting firms, who hire technical administrators in white collars to perform labor-intensive work and deliver a boilerplate solution together with a big bill. And then the auditors

come in again the following year and deliver another lengthy report together with another big bill.

Many organizations are sick and tired of the big bills and having the same issues crop up year after year because the symptoms are being treated instead of the root causes of the problems.

Why can't we get it right ourselves, and then keep it that way?

Again the bottom line is complexity and this paper deals with the specific challenges and sets out how they can be resolved once and for all.

Is there an easy solution?

Securinfo: The Only Complete Solution

Securinfo's solution has been developed with a keen professional eye on addressing all of the issues raised in this document. Securinfo allows security, audit, and business process personnel to apply their knowledge of SAP Authorizations, Control, and Business to help simplify, accelerate and control the security process. Unlike competing products that only solve one aspect of the issue, Securinfo provides one complete solution with a quick ROI for companies moving to role-based security, completing an upgrade, consolidating multiple locations, or redesigning their SAP security.

Securinfo: Simplify the security process

Securinfo achieves this by delivering a standard methodology of "Information Ownership" to the Enterprise.

This "Information Ownership" concept, unique to Securinfo, makes security a Business Issue (not a technical issue), which facilitates awareness and understanding of security across the enterprise and makes business responsible for the design, implementation and ongoing management.

Securinfo: Accelerate the security process

Securinfo supports this methodology with sophisticated software that is very powerful yet extremely easy to use. The software literally empowers non-technical persons in the various discretely accountable areas of the enterprise to be responsible for the design, implementation and ongoing management of security in SAP. This fundamentally changes the way security is dealt with and enables extremely rapid design, implementation and management of security in the SAP environment. Time (and cost) savings approximating 60% - 80% when compared with the best alternatives are to be expected.

Securinfo: Control the security process

Securinfo incorporates clever control concepts that enable the enterprise to design and configure central controls (to meet the enterprise's overall security needs) and decentralized controls (to meet the differing security requirements of the various organizational units.

Once implemented, Securinfo ensures that the state of the security solution remains appropriate from a security perspective whilst meeting the ever-changing requirements of business. All changes are managed with a Change Management module. This is not available in SAP and has long been a requirement of business. Change Management forces compliance with the organization's change policies and procedures before automatically processing the (approved) changes in SAP. This module enables senior management, auditors and other interested parties to quickly obtain the assurance of Data Integrity, Confidentiality and Availability in the SAP system.

And it does all this while delivering full knowledge transfer, thus enabling the organization to bypass the need for expensive third party consultants and achieve the lowest possible cost of ownership. With Securinfo technology, your organization can quickly solve the SAP application security challenge from a business perspective.

Overview

The Gartner Group issued a report in year 2000 projecting that the application security market would evolve into a combination of product and services by the year 2003. Their projection is starting to materialize but the product side has been slower to evolve because of the complexities associated with SAP Application Security.

SAP Application Security was approached no differently from the other systems. In the context of SAP Application Security it was thought that, once initially designed and implemented, there would be very little change associated with a role or profile assigned to a particular person and ongoing maintenance would be easily managed. This simplistic view is now known to be very far from the truth. The industry now realizes that a person's role usually evolves, sometimes quite dramatically, not only as a function of specific tasks that may be assigned to / removed from them on a day-to-day basis but also, and much more often than anticipated, as a function of their general responsibilities within an equally evolving organization. As a result what the person does in the business process is much more dynamic and subject to many more changes than originally assumed.

SAP Application Security is, by its very nature, quite technical so customers have traditionally utilized the services of specialized consultants to help determine requirements, design, implement and administer application security. This usually results in significant expense and extensive projects that deliver centralized methods that are far removed from the individual business processes they are supposed to protect. These methods are mostly not flexible enough to communicate the organization's dynamic requirements across the business to the relevant responsible persons in an efficient manner.

The complexity and pervasion of today's business processes, the dynamic nature of each person's evolving role in the organization and due regard for assigning responsibility to decisions affecting the integrity of individual processes and information generated from them has demanded that business process owners become much more involved in the security process. However, finding ways to involve them and enabling them to communicate, document and effect the security decisions has presented a major hurdle.

The challenge is to empower the organization to take control of the complete SAP Application Security process. This implies developing mechanisms that can, practically, be used by business process owners to manage security and thus the confidentiality, availability and integrity of the information produced by the many SAP supported processes.

Today's world is headlined with banners proclaiming what can happen when risk management is not properly addressed. Although senior executives bear a fiduciary responsibility to safeguard the organization's assets and to minimize the risks that the organization faces, they have often just not been able to evaluate, let alone manage the exposure. Legislation does not provide the answer but, in recognizing this responsibility, is certainly moving closer and providing rules designed to protect the individual, the community, the stockholders and the national interest.

Security Planning

Effective security and data integrity are paramount to every aspect of the business processes supported by SAP. As organizations continue to expand the role of their SAP systems, so their dependence on the confidentiality, availability and integrity of the resultant data increases. We must ensure that their vulnerability does not.

Proper planning is obviously imperative for the various tasks relating to the correct design and deployment of SAP Application Security. Unfortunately experience shows that this critical set of tasks is usually sidelined during SAP system implementations. More frequently we also see that the actual role design and implementation phase is often one of the last action items of an implementation. In these cases it goes without saying that role design is not properly integrated with the risk management process.

There are reasons for this sad state of affairs. It is often not so much due to lack of awareness, the IF or WHY it should be done, as it is due to lack of a method, the HOW it should be done.

A thoroughly planned and executed SAP security implementation should follow a standard methodology with input from many parties. Risk should be evaluated and its management determined and documented on a collaborative basis. Mitigating Controls should be continuously assessed when dealing with role definition and maintenance. Roles should therefore be designed, built, tested, deployed and administered jointly with the collaborative expertise of security professionals, business process owners, user managers, and audit teams.

Unfortunately, without supporting technology, this is not an easy task, especially during a rapid SAP implementation, and usually it simply just doesn't happen this way, because business simply does not have the capacity or the wherewithal to interface all the required persons and skills for each security decision. Some implementations are forced to take an approach of granting broad security access for go-live with the intent to pullback at a future date. Some of the usual excuses in a compromised SAP security environment have been:

- Lack of management awareness.
- Lack of management ownership of risk.
- Lack of a standard security methodology.
- Inappropriate design logic.
- No mechanism available to facilitate communication of business requirements to the technical environment of the security team.
- Volume and complexity of security work underestimated.
- Security work commenced too late – too near go-live – broad security is granted to save time.
- Existing security roles are not aligned or understood by the people managing business processes
- Existing security policies unclear in the definition of controls required by organization.
- Business Process owners not adequately involved.
- Lack of skilled technical personnel.
- Inadequate documentation of risks, controls, and deployed permissions.
- Inadequate time for sufficient testing.
- Inadequate knowledge transfer from external consultants to business.
- Inadequate Change Control policies and procedures for the live environment.

All these and many more are not so much the result of inadequate planning but the lack of a clear method to facilitate the process.

Risk Evaluation

One of the first steps that should be undertaken in any security implementation is a thorough analysis and evaluation of the risks that the business is exposed to in its various SAP supported business processes. Integrating security using the application of SAP technology on an organization's business processes is not a simple task. The nature of enterprise resource planning inherently affects many processes, people and technologies.

Determining the risks associated with business processes, evaluating their eventual likelihood and the impact should they occur and specifying the appropriate responses is difficult. Designing the required mitigating controls, incorporating them into procedures and assigning responsibility for their execution and management is fraught with logistical problems. Providing a mechanism to communicate the actual risk status of the entire organization to senior management is just about impossible.

Management is often just not in a position to make an informed decision.

Consequently, many SAP customers are experiencing increased uncertainties and therefore, escalated concerns over the condition of the SAP security environment and the potential risks faced by the organization. Many SAP customers accept that they have failed to adequately establish the uncertainties, identify the risks and address the security concerns due to the sheer magnitude and complexity of the task.

Complexity

Questions and concerns around SAP security risks are intensified as a direct result of the complexity of the SAP security environment. Factors such as the number of business processes, the volume of underlying transactions, the user population, number of control entities, size of the security team, and employee turnover can greatly influence the complexity of SAP security. With over 55,000 different transactions and literally millions of transaction-field-value permutations, designing and maintaining proper security is an extremely technical and labor-intensive task. The task is complex and labor-intensive; however, business changes are dynamic and mostly require quick and accurate responses. To illustrate, here is a simple (and typical) scenario:

A security professional is asked to add a transaction to a given user. To quickly resolve the issue, the security professional may search for a current profile attached to the user and add the transaction to that profile. However, security changes to a particular profile can have an adverse ripple effect across the organization.

Who made the request? Does that person have the necessary authority? How does this added transaction relate to the overall intent of the profile? Does the originator understand the impact of the change on other users of this profile? Are there any identified business risks associated with this profile? Have any mitigating controls been implemented for the risk? How does this addition impact those risks and controls? Does the change give rise to a conflict with existing defined segregation of duty issues? What other business processes are affected? Does the security professional understand the impact of the change on any associated business risks? How many other users have this profile? Are these users also authorized to receive this privilege? Who is authorized to approve changes affecting all of the affected risks? Have all the necessary approvals been granted? Has the change been properly documented?

Imagine the state of an SAP environment having to make dozens of changes such as this one on a weekly, daily, or hourly basis! It becomes clear that many SAP security systems quickly become unmanageable and get out of control.

.

SAP Functionality

SAP's security architecture was designed for a centralized security approach. This approach assumes that there is a team of highly skilled technical persons responding to ongoing change requests affecting the many and various business processes across the enterprise. All of these changes carry with them the requirement for approval by the affected persons responsible for management of the associated risks and maintenance of the relevant mitigating controls.

Security is much more than just the assignment of authorizations to users, and that is difficult on its own. SAP does not have a practically useable mechanism to manage risk evaluation, control definition, and the assignment of authorizations to users during the implementation process. Furthermore SAP does not have an adequate mechanism that enables business to monitor the existing situation, and initiate Change Requests for approval by the various responsible persons across the various discrete organizational units of the enterprise so as to facilitate ongoing risk management in the live environment.

The SAP customer is left to design, engineer, implement and manage a mechanism to facilitate communication between business and the security team. Unfortunately this has proved to be practically impossible for most SAP customers. One factor is the technical complexity of the applied security and the second factor is the volume of the transactions affecting the many and varied business processes utilized.

Management Review and Audit

As the business environment continues to change, so there is a constant need to re-evaluate each user's role and his/her ability to access sensitive information and perform key business transactions. An understanding of business impacts, internal controls and SAP security technology is imperative to the ongoing evaluation of this dynamic environment.

So how do best-practice organizations manage security risks posed by a complex system? The answer is simple: Follow well-documented procedures and perform frequent monitoring of the system. However, experience shows that its much easier said than done. Investigation reveals that even determining the "what" to monitor can be an extremely complex issue for most SAP customers. Specifically, organizations often struggle to understand which SAP security risks are truly relevant to their environment. Specifying which key business transactions and authorization objects to monitor can be difficult, and identifying which job duties and which roles go together without creating exposures to fraud can be overwhelming. Properly identifying a set of SAP security risks for specific business processes requires a thorough understanding of those business processes as well as technical knowledge of the relevant SAP security technology and knowledge of the internal controls. Organizations having Security personnel or audit staff with this unique blend of skills and knowledge are few and far between, and retaining such unique resources presents them with an even greater challenge.

Generally speaking, the biggest hurdle encountered by SAP customers, which tend to have complex applications of diverse business processes, is to achieve effective collaboration between the technical and business user communities. This hurdle is due to communication barriers imposed by the technical nature of the application security, differences between technical and business terms and inadequate systems to support the communication. The problem is exacerbated further. Even if all relevant SAP security risks can be identified from a business process perspective, it is still very difficult to gather accurate data from the SAP system and present the data to the many different audiences who need to evaluate it in a manner that is both useful and easy to understand.

.

For example, reports obtainable from the SAP system on the authorizations granted to users are just not understood by most business process owners. Such reports are technical and often full of voluminous data that is mostly irrelevant to the control requirements of the specific business process owner performing the inquiry. As a result, the business personnel view this as a security responsibility and do not take ownership of defining and managing the risks associated with the hundreds of business processes that are used by the organization on a day-to-day basis. And these processes and the use thereof continuously changes!

Another example from an audit perspective is Segregation of Duties concerns. It is especially complicated to properly monitor risks caused by assigning dangerous combinations of transactions. Such monitoring requires cross-reference queries that are virtually impossible within the SAP system and very time consuming to execute in any home-grown tool. It is also extremely challenging to arrange results in a standard format where analysis by both technical and business audiences is encouraged. Finally, creating a useable Change Management system that pinpoints changes or relationships to the appropriate personnel for periodic management and audit review is difficult to say the least.

Methodology

All of the above comments point to what probably amounts to the biggest problem that most customers face. How do we go about designing, engineering, implementing and managing SAP Application Security?

SAP does not deliver or recommend a standard method and therefore an enormous amount of time and money is wasted by each and every customer in researching and implementing various methods, many of which are doomed to failure. Even the experts disagree. However, the risk must be managed so we have to start by developing a standard methodology.

Overview

It is apparent from the outset that any solution developed must deal with the technical complexities of SAP, should enhance certain elements of SAP functionality and be flexible enough to cater to the varied control requirements of the enterprise. The solution must encourage business and technical collaboration and must be rigid enough to regulate the fundamental control requirements that organizations *agree should be enforced.*

Existing Solutions?

Organizations should not underestimate the difficulty in creating a solution. At the outset, the complexity and interrelationships might not appear particularly daunting to the people that deal with SAP Basis and security on a day-to-day basis. However, the technical complexity associated with SAP's Security architecture, the difficulty in designing flexibility into a standard methodology to serve many diverse organizations and the challenges in presenting and manipulating relevant data to meet their unique requirements are some of the reasons why there are very few product vendors in this market. Expert systems of this nature require significant expertise, dedication and a big investment in resources to design, develop, and test a product that delivers what the customer wants and needs. To complicate the situation, SAP has continually changed some elements of the underlying architecture in each version from 3.0E to 4.6C. This makes it very difficult for home-grown solutions to keep up as they try to upgrade from one version to another and retrofit their internally developed solutions. Development of an adequately robust product would entail a development time of at least 15 months and a total cost in the order of approximately US$ 10,000,000. And that's assuming the developer sets the objective correctly and knows exactly how to achieve it.

Some software companies, audit firms and even some customers have tried to develop home-grown interim tools that address portions of the business challenges to a greater or lesser extent. As multiple areas are addressed, complexity and the scalability issues associated with a large SAP implementation present more challenges. Products that have failed in this respect are those that add layers to the already complex SAP layers and make it even more difficult to manage the system and related performance issues. Some "point products" have also emerged. These are tools that point to problems, but don't fix them. Audit firms have tools that assist them to compare existing SAP data with sets of pre-defined conflicting transactions and report on the findings. Most of the consulting firms also tend to use these point products. This enables them to fulfil their primary business objective of selling their services to rectify the problems. The scope of these products and their ability to assist the organization with managing its application security is very limited.

Organizations should bear in mind that products that analyze information and do not help eliminate the cause, but rather react after-the-fact, will not help them achieve their objectives. A complete software solution will help the organization identify the risks, design and develop the controls, build and implement the solution and thereafter administer the ongoing security system. The following table shows a comparison of the available solutions:

Security Areas	Securinfo's Solution	Competing Products	Competing Services
Design Methodology	Yes	No	No
Role Development	Yes	No	No
User Assignment	Yes	No	No
Scheduled Reporting	Yes	No	No
Segregation of Duties	Yes	Yes	Yes
Change Management	Yes	No	No
Risk Management	Yes	No	No

Designing a solution

The right place to start is with a list of deliverables that an ideal solution might offer. There are obviously many to consider, and their individual importance tends to vary from customer to customer. The table below shows those considerations that customers often have difficulties with, and would like to see incorporated into an ideal solution:

Deliverables and Requirements on the Wish List		
Standard Approach	**Practical and Sensible**	**Include Best Business Practices**
Incorporate a Project Plan	Facilitate Risk Management	Integrate Risk Management with SAP Authorization Management
Include Configurable Central Controls	Enable Decentralized Data Management (to business persons)	Incorporate Automated Change Management
Integrate with SAP	Offer automatic processing of approved Change Requests	Eliminate central bottleneck of change requests
Facilitate ownership of data	Facilitate ownership of risk	Facilitate documentation
Translate technical issues into business issues	Facilitate Knowledge Transfer	Improve business awareness of security issues
Facilitate Corporate Governance	Facilitate Audit	Offer multi-purpose use (Design, Modelling, Re-engineering etc.)
Easy to implement	Easy to use	Easy to administer
Enhance SAP's functionality	Offer intuitive interfaces	Incorporate standard Naming Conventions
Enables automation of routine tasks	Incorporate Mass Change capability	Support Role & Task based methods
Reduce the likelihood of all errors.	Prevent Segregation of Duty conflicts	Deal with exceptions in a sensible manner.
Offer Cross Module Integration	Offer sophisticated reporting	Incorporate sophisticated security
Contain detailed Online Help	Accelerate the process for additions and changes	Offer good Return on Investment

Collaboration and Participation

One of the problems encountered when designing a solution is how to facilitate monitoring among security, audit and business personnel. In addition each business process may have unique preferences and require specific controls. The active participation of these and other audiences is essential to ensure that the security team communicates with them as their requirements change. In addition, responsibility must be assigned for the various decisions that must be made. If you consider business process owners to be accountable for the results of their actions (and those of people reporting to them) then you must involve them directly in the security process. If you consider security to be an integral part of your business process support and want to use it as a business tool, then it is mandatory to get security into the hands of the business personnel. Having said that, how are you going to get business personnel involved, remembering that they are not technical, not trained in SAP security, are not internal control specialists and may be inclined to think that the IT department is offloading its work onto them? You have to get them involved, so how do you present only the relevant data in business terms as opposed to technical terms? How are you going to make their tasks intuitive and visually compelling in such a manner that encourages them to take ownership of the security system as it applies to their data?

How do organizations decentralize the security process in a manner that ensures that the organization's overall security objectives are still achieved?

This is what takes time and, from a vendor perspective, requires a significant investment in developing a commercially viable solution.

Synopsis

It is clear that the solution must offer all of the various deliverables mentioned above but, most importantly, must simplify and accelerate the security process, otherwise business just won't accept it. Control is essential to maintain the integrity of the security design and keep security permissions aligned with business process changes.

Current State Assessment

Ask yourself some questions:

What Security and Control Strategy did your organization use to design, develop, test and deploy security for the SAP system? Did the strategy provide the components to:

- effectively manage business risk, and
- ensure adequate control processes, procedures, configuration and documentation were created, and
- meet the needs of the enterprise?

The last is the most critical question. A few customers may be able to answer yes close to their go-live date, but most will answer "No" and will always admit there is more work to be done.

To assess the current state, consider the security controls and procedures currently in place at your organization. Also consider the many different audiences that use these controls – SAP security teams, business process owners, SAP Basis professionals, and internal and external audit teams. Investigate the methods used by them to gather and manipulate the required data. Discuss current controls and procedures with all of these groups at a high level.

Realistically, the analysis will generally reveal many SAP security exposures that the organization currently faces and the important need to fill the gaps. The analysis will usually confirm that many audiences don't have the right controls and desperately need security information that is just not available. It will show that there simply isn't a powerful mechanism in place to present the needed security information to business personnel in a meaningful manner so as to enable business to make the right decisions in a timely manner.

Management Buy-in

Decisions affecting security are often difficult to present to Senior Management. The likelihood and impact of threats to the organization's business and actions necessary to address the threats on a proactive basis is difficult to explain when a threat has not occurred. "Everything is fine, we have been making good profits for the past few years. Why should that change?"

There is no doubt that implementing and maintaining security has associated costs. At first this may appear to be a hurdle, however experience shows that a good solution will save money, reduce risks that are sometimes difficult to quantify in dollar terms, and also reduce the costs associated with implementing and administering an inefficient system. To help management evaluate the situation, the following suggestions may help to quantify the business costs and potential losses:

- Find out how much time is spent researching issues and servicing business personnel change requests (customer interviews state it may take up to five hours for researching an issue to find out what changed and or what the impact might be).
- Convert time to $. Once you have estimated the time it should take and the frequency, you can calculate the cost of "controlling" access changes and how much time is really required to get the right business and technical personnel to work through the complexities.
- Try to document the avoidable Costs & Risks. The Computer Security Institute and a recent FBI study on Security points out that the most expensive occurrences are insider threats. The cost of just one occurrence can range from $500,000 to $2.5 million. Taking a risk reduction approach you can add this to your cost avoidance list by reducing the potential for such occurrences and/or reducing the cost of risk management insurance policies.

Securinfo: The Only Complete Solution

Securinfo's solution has been developed with a keen professional eye on addressing all of the issues raised in this document. Securinfo allows security, audit, and business process personnel to apply their knowledge of SAP Authorizations, Control, and Business to help simplify, accelerate and control the security process. Unlike competing products that only solve one aspect of the issue, Securinfo provides one complete solution with a quick ROI for companies implementing SAP, moving to role-based security, completing an upgrade, consolidating multiple locations, or redesigning their security process.

Simplify the security process

Securinfo achieves this by delivering a standard methodology of "Information Ownership" to the Enterprise.

This "Information Ownership" concept, unique to Securinfo, makes security a Business Issue (not a technical issue), which facilitates awareness and understanding of security across the enterprise and makes business responsible for the design, implementation and ongoing management.

Accelerate the security process

Securinfo supports this methodology with sophisticated software that is very powerful yet extremely easy to use. The software literally empowers non-technical persons in the various discretely accountable areas of the enterprise to be responsible for the design, implementation and ongoing management of security in SAP. This fundamentally changes the way security is dealt with and enables extremely rapid design, implementation and management of security in the SAP environment. Time and cost savings approximating 60% - 80% when compared with the best alternatives are to be expected.

Control the security process

Securinfo incorporates clever control concepts that enable the enterprise to design and configure central controls (to meet enterprise security needs) and decentralized controls (to meet the various organizational units' security needs).

The product filters and organizes pertinent information for the business owner, and also prevents inappropriate entries by placing controls over specified key controlling elements like cost centers, or locations etc.. The product also incorporates checks for the organization to avoid segregation of duty conflicts or inappropriate assignments without express approval of the risk by a responsible business person. These responsible persons (we call them Information Owners) know their own areas from a business perspective, understand their own security requirements, are most likely to make informed decisions and are much better placed to ensure that the state of the security solution remains appropriate for the business.

Once implemented, Securinfo ensures that the state of the security solution remains appropriate from a security perspective whilst meeting the ever-changing requirements of business. All changes are managed with a Change Management module. This is not available in SAP and has long been a requirement of business. Change Management forces compliance with the organizations change policies and procedures before automatically processing the approved changes in SAP. This module enables senior management, auditors and other interested parties to quickly obtain the assurance of Data Integrity, Confidentiality and Availability in the SAP system.

Contacts

In addition to product demonstrations to customers, Securinfo offers a “Proof of Concept” to customers who are serious about security. We have regional offices in each continent:

- **Securinfo America**
- **Securinfo Europe**
- **Securinfo Asia-Pacific**
- **Securinfo Africa**

For further information:

please visit us on the web at http://www.securinfo.com

or,

send an email to info@securinfo.com