INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

SAP GRC Access Control Implementation

Goraksh Shinde[1]

[1]Northeastern University, College of Computer and Information Science
360 Huntington Ave, Boston, Massachusetts 02115, United States
gorakshshinde@ccs.neu.edu, gorakshshinde@gmail.com

Abstract: *SAP GRC Access Control can be implemented to provide Access Management, Risk Management and Audit Management through a common platform and organization can achieve Governance, Risk Management and Compliance through the same. Ultimate aim is to comprehensively use SAP's GRC solutions in GRC Access Control implementation. SAP GRC Access Control provides automated process of detecting, remediating and preventing access control violations across various ERP systems. It also offers robust risk analysis and remediation. SAP GRC Access Control application empowers organization to manage and reduce access risks across the enterprise by preventing unauthorized access and also achieves real-time visibility into access risk management. In this paper, Effective GRC implementation processes and methods will be discussed which addresses all key areas in an organization like finance, people, operations and services.*
Keywords: *GRC, Risk Management, Compliance, Governance, Access Control, Remediation.*

1. INTRODUCTION

Governance, Risk and Compliance are three areas that work together to achieve organizational objectives. "Governance is the combination of processes created by higher management and it deals with the continuous monitoring of implemented processes in order to achieve organizational goals. Risk Management is the analysis and management of risks across the organization. Compliance deals with various rules, regulations, policies and procedures [1]."

Financial regulations like Sarbanes-Oxley (SOX) around the world demands to run business with regulatory compliance and it requires a lot of effort. Increasing compliance and governance needs have mandated a robust method to control and monitor access to systems providing critical financial and reporting data. GRC solutions provides organization with preventive real time approach across different systems and provides faster response to changing business solutions [2].

GRC access control is the improvisation of role based access control; it abandons manual assignment of access through forms or emails and introduces automated access control provisioning system. It also facilitates real time risk simulation and assessment. GRC provides end to end compliance and sustainable prevention of risk violations. Another important factor that goes in the favour of GRC is it demonstrates effective governance of access control across the organization. Business operations access control remains with business heads and business process owners through workflow based access of authorizations that is done after risk analysis and remediation or mitigation of risks.

SOD (Segregation of Duties) is important internal aspect which the organizations need to establish and manage for their ERP applications. The roles and responsibilities should be assigned across an enterprise in such a way that, any individual should not have end to end access rights over any function. The more critical the function is, greater and clearer Segregation of Duties should be. Ideally, single individual must not have authority of creation, modification, reviewing and deletion for any transaction/tasks/resources. Segregation of Duties reduces improper use of materials, money, financial assets and resources. Segregation of Duties streamlines the audits and management review and ensures integrity of financial statements [21].

In particular, SAPs GRC Access Control solution provides automated process of detecting, remediating and preventing access control violations across various ERP systems besides it also offers robust risk analysis and remediation. SAP GRC Access Control gives a comprehensive, cross-enterprise set of access control tools that enable business management, IT security management and auditors to collaboratively define and oversee proper access control. GRC access control solution platform offers great auditing reporting features which can reduce the efforts of internal and statutory audits. Continuous monitoring of controls is important factor in GRC implementation which will help building confidence in an organization about effectiveness of controls [2].

2. NEED FOR GOVERNANCE, RISK AND COMPLIANCE

It has been more apparent that everyone in the typical organization must make more effort to increase the visibility of the risks they manage in their day to day work. Risk impacts the decisions made by every single group in the organization. However, most organizations today are very fragmented, which prevents executives and the board members from understanding and managing the true risk profile of the organization. If a risk management organization does exist, it typically concerns itself with theoretical risk models and analysis of business opportunities. While these are important activities, this practice does not properly account for operational risks which can have a significant impact on the organization. GRC Role based access control ensures operational activities like who can execute specific actions and how. It streamlines global authorization checks and restricts display of the data depending on the user roles. If users of the particular system see only relevant actions then it makes the system user friendly [13].

Without GRC, organization can carry many irregularities and risks. It's difficult for such organizations to be in a legal compliance framework and organization's global

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

risk profile will be incomplete. Security will be very weak in such organizations and data is prone to leakage in there. There will be no transparency at any level in such organizations thus proper security structure should exist and Governance, Risk and Compliance can cover all these issues hence it's the need of an organization to tighten their security. GRC makes the organization more transparent in all the departments like finance, human resources, sales, IT etc. It also helps executives to keep an eye on organizational work more efficiently. With GRC, organization confidence can be increased and it will get reflected in organization's business results.

3. SAP GRC EVOLUTION

GRC Access Control identifies and reduces access and authorization risks across organization to prevent fraud. It also helps to reduce the cost of compliance and control. SAP GRC has improved the access controls and risk monitoring with each version over the years [19].

3.1 Previous SAP GRC Access Control Versions:

1. VIRSA Access Enforcer/Compliance Calibrator 5.2- VIRSA Access Enforcer was used for compliant user provisioning across applications throughout the employee life cycle. It would automate approval processes and enforce mandatory real-time risk assessments prior to provisioning users to enterprise applications [3].

VIRSAs Compliance calibrator was used to analyze the roles of employees who use SAPs ERP system and based on the analysis it would give potential conflicts in the access rights that have been granted [4].

2. GRC AC 5.3- SAP GRC Access Control 5.3 comprises:

1. Compliant User Provisioning - Compliant User Provisioning (CUP) includes access request, access request approval, compliance checks, resolution of access controls and provisioning.
2. Risk Analysis and Remediation - It is used to identify, analyze, and resolve risk audit issues related to compliance.
3. Superuser Privileges Management- It tracks and monitors the activities performed by super users across the system.
4. Enterprise Role Management - Enterprise Role Management (ERM) allows management of enterprise roles with a single unified role repository. Roles can be designed, analyzed, approved and documented within ERM [9].

SAP GRC Access Control 5.3 automates the periodic review of user access by notifying the reviewers with a workflow request. Reviewers can validate roles assigned to users and take the appropriate actions of either confirming or removing user access. All actions are logged and displayed in an audit/status report [5].

3. GRC AC 10.0- SAP GRC Access Control 10.0 comprises:

1. Access Request Management- It set ups the customized multi stage multi path workflows as per the organization requirement.
2. Access Risk Analysis- It is used to analyze the risks and then take the remediation or mitigation option as per the business need.
3. Emergency Access Management- It is used to manage the access required in business critical or emergency situations.
4. Business Role Management-It is an enhanced process for mapping technical access authorizations to business functions [10].

GRC AC 10.0 provides a robust user interface for efficient creation and maintenance of functions, actions, and permissions. It is possible to mitigate risk at the rule level or at the system level in this version [6].

3.2 Current SAP GRC Access Control Version

GRC AC 10.1- SAP GRC Access Control 10.1 provides a feature to define and activate the Org Rules for specific systems only. Using organizational rules in risk analysis can be time consuming especially in batch risk analysis. In most cases, Org Rules only apply to some of the connected ERP systems. By having system-specific Org Rules, only the relevant rules are used for risk analysis resulting in highly improved run times. The access risk root cause analysis remediation view enables easier identification and remediation of access risks. It offers a set of tools for segmenting risk violations to know which risks are needed to target first. Remediation workflow processes can be enabled from the remediation view to ensure that the processing and auditing of remediation activities are followed and tracked. GRC AC 10.1 also puts controls on available reports and dashboards using role based access control [7].

1. Access Risk Analysis (ARA) - It deals with user risk analysis and then remediation and mitigation of those risks depending on the business requirement. Risk analysis can be done on real time environment or in offline environment. Access risk analysis can do the risk analysis at action level i.e. transaction level and also at permission level of objects like permission to create, change or display. Thus identifying risks at different levels is easy. Mitigation controls can be defined and monitored as per the business needs [7].

2. Access Request Management (ARM) - It deals with the business transaction access request in the form of roles and its automated provisioning in the target backend system. The audit logs for each access request are stored in the GRC system which is of great help during external or internal audits. Access request management is the improvisation of role based access control through which role assignment process becomes automated. Access request management also ensures that before access has been granted it has gone under proper technical, functional and business channel. This increases transparency and also deals with conflicting authorizations issue. Thus Automation in access request management helps the RBAC experts to manage the control more efficiently [7].

3. Business Role Management (BRM) - BRM deals with the role management of target system through GRC. One of the great features of BRM is business roles which are created virtually in the GRC portal with their connected backend system's multiple roles can be assigned in

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

multiple target systems at a single time as per the business requirement. This is helpful in cases when through a single request access needs to be granted for two or more systems simultaneously. Person joining is supply chain management requires access of supply chain system as well as his employee portal system and business roles are efficient way to do that. However the role management of backend systems through GRC is complex and needs expertise in both GRC and RBAC to use the same [7].

4. Emergency Access Management (EAM) – This deals with the access required in emergency situations. EAM can be implemented in two ways, centralized emergency access and decentralized emergency access. Centralized emergency access is dependent on GRC system throughout the emergency period whereas decentralized emergency access is not dependent on GRC system all the time throughout the business critical period. Emergency access management has the ability to deeply monitor the activities performed by the Firefighter so that no fraudulent activities are done in the Firefighter period. It also creates special audit reports specific to emergency period [7].

4. GRC IMPLEMENTATION

4.1 Project Plan

Implementation of GRC involves server team, BASIS consultants, business personnel and most importantly GRC consultants who will do the majority of tasks during the implementation. SAP GRC uses a three tier landscape and recommends separate dedicated server for access control components. Server Team and BASIS Consultants will work together to install GRC hardware and components and will make the development, quality and production servers ready for GRC consultants to configure as per the business requirement.

The configuration settings involve integration of GRC with other systems within the organization, Configuration settings of individual components, Client specific workflow design, Segregation of Duties, Risk library design, Mitigation controls design, Organization specific audit reports. Risk library design is the most important part as far as risk management is concerned. Risks for the particular organization are derived from organizational key under which all the risk rules are defined. Workflow design vary as per the business policies for ownership of business processes hence access control workflow needs to be customized in almost all the GRC implementations. Typical GRC workflow involves security team, business process owners, business heads and risk management team [18].

Systems are for the use of employees in the organization thus it is important for them to understand the newly implemented system. Once the technical implementation is completed then we need to carry out the training programs for the users before newly implemented system is released to the users. Go-Live and support activities are equally important as that of implementation phase. Many product bugs are identified and fixed during support phase.

Table 1: Implementation Tasks

No.	Task
1	GRC Access Control Architecture Design
2	Hardware Installation and Configuration
3	GRC Access Control Component Installation
4	GRC Access Control Post Installation Activities
5	Organization specific connector settings
6	Risk Library Design and Configuration
7	Workflow Implementation
8	Component Validation
9	Final Preparation Phase and Testing
10	Training, Go-Live and Support

Source: Siddiqui, Mohammad Imran. 'SAP Governance, Risk and Compliance Overview'. Presentation, Mumbai, India, 2014.

4.2 Implementation Phase

Each organization is different and there is no single approach for GRC implementation, still there are some common challenges that come into picture while implementing GRC solutions. In majority of organizations each business function or unit has its own business processes and its own set of compliance regulations and this makes GRC framework difficult to implement. Sometimes there can be a group of companies working independently under single umbrella and it is not necessary for them to follow the same business processes. In such cases, risk defined for one company may not qualify as risk for other company. Defining separate organizational keys under one GRC platform can be the possible solution in such scenarios. Normalization of risk library, policies, procedures and data classification can be a stern task and thus it is susceptible to errors. Another factor that affects GRC implementation is alignment of regular business operations departments with GRC. Most of the organizations have segregated internal audit department, IT security department, regulatory and compliance department, risk officials. This leads to complexity and the solution on this can be the GRC specialized team that will work concurrently with other business departments to achieve organizational Governance, Risk and Compliance [8].

1. SAP GRC Access Control Architecture Design- SAP GRC access control design depends on usage of master data, transaction usage and the number of employees in the organization. Besides number of target and backend systems for access provisioning, access risk analysis, role generation and superuser privilege management influence the performance of GRC Access Control platform. GRC access control can have its own user database however it is better to have the database updated with HR master user data through which new updates in the user attributes can be pulled in GRC system with proper channel. Identity management is excellent option in this scenario. User data

can be pulled through user directory like LDAP i.e. Lightweight Directory Access Protocol which is synchronized with identity management. LDAP data can be pulled in GRC system through LDAP transaction and query [13].

2. Hardware Installation and Configuration- Hardware installation involves coordinated effort between BASIS (Business Application Systems Integrated Solutions) and GRC experts to determine the required hardware and its sizing. GRC 10.0 landscape will typically have development, quality and production environment with standard ABAP transport functionality. Earlier GRC version like GRC 5.3 did not possess this functionality. GRC server can comprise of cluster environment which is a group of multiple server instances. Cluster environment with its load balancing, offers uninterrupted services and ensures availability, reliability and scalability [11].

3. GRC Access Control Component Installation- Access Control, Risk Management, Process Control are contained in one add-on GRCFND_A. Front end GRC portal will be accessed through web browser and NetWeaver Business Client (NWBC). Plugins like GRCPIERP and SLL-PI can be installed where GRCPIERP is for HR relevant functions like some HR triggers in access control. SLL-PI is for GTS functions to be integrated logistics, HR and finance processes in ERP systems. Non-ERP systems can be connected to GRC through adapters. In GRC 10.1 NWBC is replaced by GRC_POR_1000.The Component installation can be done through transaction SAINT [13].

4. GRC Access Control Post-Installation Activities- This step involves GRC access control configuration settings as it allows you to customize access control suite. It's the most important task in whole GRC access control implementation. Configuration settings are done through SPRO transaction. Configuration parameters require logical thinking while selecting it, as it will impact the whole access control lifecycle. Configuration parameters can be set with respect to specific group or sequentially. Risk analysis, workflow, emergency access, mitigation, role management and change log are some important parameter groups. The values which are set in parameters are going to decide the events and application flow in GRC. GRC configurations can be transported from development to quality and production system through standard ABAP transport system. Apart from parameter settings it also involves end user personalization settings. The application platform will be used by lot of different users like normal end users, business process owners, superusers, business heads, auditors, system administrators and we need to personalize the application as per their needs and make sure no unnecessary information is exposed to certain group of users. There are two ways through which this can be achieved one is web portal customization and second is role based access control in backend GRC box. There will be some predefined roles already available in the system and you can design some more with the help of SAP security role based access control experts to ensure the tight security of GRC portal. Web portal customization can be done through object navigator which is common SAP ERP web service development transactions [13].

5. Organization specific connector settings- Organization can have various systems like employee portal systems, customer relationship management, dealer systems, supply chain systems etc. and it's necessary to put all the systems under GRC for better and streamlined governance, risk management and compliance across the organization. The connection should exist between all ERP, non-ERP and legacy systems. SAP GRC access control has the ability to integrate the ERP as well as non-ERP systems. The integration of the systems can be done through SM59 transaction in GRC backend system. There are different integration scenarios to map the connectors with different applications; scenarios are Authorization (AUTH) scenario, Role Management (ROLMG) scenario, Provisioning (PROV) scenario, Super User Management (SUPM), Automated Monitoring (AM). Thus along with creating connectors through SM59 you need to map them to required applications with different integration scenarios [13].

6. Risk Library Design and Configuration- In business, An SOD risk is present when an employee possesses two incompatible functions, such as "creation of vendors" and "processing of invoices" or we can say Business risk occurs when users have critical privileges such as the maintenance of bank details within a vendor master record. When risk occurs we have two options either to remediate it by removing one of the accesses or mitigating it by accepting the risk under certain conditions. These conditions can be defined as mitigation controls. Mitigation control should be used as the last resort. These are exceptions left over from remediation efforts that have legitimate business reasons for not using segregation of duties (SOD) controls. Risk library is designed under the organizational key. If the multiple entities are running separately under same organization but with complete different structure then separate organization keys can be created for different risk structures as it is not necessary to have that same risks for two different organizations. Rule set is defined and then under the rule set separate risks can be configured. Risk structure in GRC access control is based on functions. If two conflicting functions come with the same user then risk will arise. Conflicting transactions will be put under these separate functions; this is called action level setting. If the risk is coming from the business process permissions like create, change or display then it can be configured under permission level settings. Superusers who works as a facilitator between IT department and various Business departments mostly has the functional knowledge of business processes and technical knowledge up to certain extent. These superusers possess number of critical authorizations but it is needed for their job profile. Thus when it comes to real time risk analysis of such users then it affects the performance of whole GRC system. We can deal with such situation by creating separate critical role for these superusers and define them under critical roles make configuration setting for them so that they will be exempted from real time risk analysis and system performance will remain efficient. This will make the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

GRC system optimized to use. Defining too many risks in the risk library makes it difficult to monitor and also affects the system performance hence the number of defined risks should be less and relevant for the organization. If the number of risks that needs to be monitored are less, it is easy to identify and manage the fraudulent activities within the system. Thus while designing the risk library, input from business functional consultants is necessary like finance consultant, logistics consultant and human resources consultant etc. Multiple individuals from different departments will help to make the risk library concise. Thus it's necessary for GRC experts to understand the business processes to implement the GRC system that is in the best interest of the company and utilizing the GRC platform for organizational well-being [21].

When it comes to audit reports for risks in an organization batch risk analysis is necessary. Batch risk analysis will update the audit reports of risks on dashboard, there are two ways to do this, one is through backend system and another way is to execute the risk analysis through front end portal. One advantage of doing it through backend system is its results can be easily exported to local system as the batch risk analysis result data is huge and exporting it through front end application is tedious task due to limitations of NetWeaver platform. All the result sets cannot be exported simultaneously in NetWeaver which is its drawback [21].

Mitigation controls are effective only till monitoring is done by the responsible individuals else it will just remain as text guidelines in the system. As discussed earlier, mitigation of the risks should be used as last resort. Mitigation is acceptance of risks under certain conditions and whoever business individual is accepting the risk should monitor it periodically through GRC. GRC provides a great monitoring and reporting features on front end application. Risks can be monitored in different ways which are easy for business individuals to understand the same. Mitigation controls should be written in plain text which will make it easier for management to understand the same. Technical language can be easy for security and risk specialists but not management thus mitigations controls and risks needs to be simplified. SAP GRC has different reporting features for the risk analysis ranging from detailed to executive summary format. Mitigation controls are not to remove the risks completely and it's not the aim of risk management but the right aim is to minimize the risks and keep it under acceptable limit [22].

Risk management in GRC is one part to achieve business security; it can also be made more secure by putting an extra control and keeping an eye on critical business processes. Very critical business processes needs to be taken into consideration and then transactions associated with these business processes should be identified. Users having the access of these critical business processes transactions can be reviewed periodically by security teams and reports of those can be sent to business heads for their feedback and actions. This can help the business heads of different departments to easily monitor the critical authorizations within their department.

7. Workflow Implementation- Workflow of the GRC access request is the one thing in GRC implementation that needs lot of critical thinking. GRC access request workflow involves security team, role owners, business heads, risk specialists etc. SAPs GRC access control workflow implementation can be done through SPRO customization. It is called MSMP workflow configuration where MSMP stands for Multi Stage Multi Path. The work flow design involves how the organizational workflow for particular access runs. The reason for mentioning the critical thinking requirement is its multi stage and multi path scenarios. If any of the stage of path goes wrong or remains inconsistent then workflow will fail [12].

There are eight activities through which workflows needs to be defined in SAP GRC access control. These are process global settings, rule maintenance, agent maintenance, variables and template maintenance, path maintenance, route mapping, version generation. There are some pre-delivered processes in the process global settings which generally suffice the requirement for most of the organizations. Some of the processes are access request approval, risk approval, mitigation control maintenance, SOD risk review etc. Process global settings applied for particular process will remain same throughout the other activities for that workflow. Second activity is rule maintenance, different rules on how the workflow should be or what details it should contain can be maintained in rules. There are some pre-defined rules and then the custom rules can be created using the BRF+ i.e. Business Rule Framework. Rules can also be created using different function modules and ABAP class. BRF+ rule is used to fetch the rule results depending on the conditions in the rule, function module based rules and ABAP based rules are coded to output the rule results. Third activity is maintaining agents; agents have the purpose and type assigned to them for certain action. Agent types are notification purpose agent or approval purpose agent etc. Once the agents are maintained we need to design notification templates that the agents will carry. Notification templates will be for approval, rejection, escalation, reminder, new work item, closure etc. Once the notification templates are designed and maintained then the next activity is path maintenance. Here path can be defined as per the business requirement and people responsible for different business access control decisions. Multiple paths and multiple stages as per the different global process can be designed and maintained in path maintenance step. The next activity is route mapping, which request should go to which individual and at what point is decided by the setting in route mapping. This activity defines the mapping between rule results and paths to route the requests to its desired destination. Once the route mapping is completed then the workflow can be simulated for the consistency check and its usable version can be generated. The workflow generated version can be transported to quality for testing the access requests and then after rigorous testing, it can be transported from quality to production [12].

8. Component Validation- Once the configuration settings are done then the components should be validated

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

by subject matter expert of the GRC. All the components needs to be validated if their functioning is correct and aligned with the business requirement. If there are any loopholes in the functioning then it should be rectified in the development and then send to quality for the testing. No changes should be done directly in the production or quality system as it disturbs the cross client synchronization. If even after the proper configuration component is not working as desired, then correction notes may need to be applied for the system [13].

9. Final Preparation Phase and Testing- After validation of all the components, rigorous testing should be conducted on GRC quality system to check all the functionalities and also its performance. Test scripts can be created to check the results. Testing should be done by Testing professionals as it makes the system sound and free from bugs. Once the testing is done, developed and tested version can be transported to the production system. After implementation the thing that consultants usually forget is to change the default password of the users. People are the weakest link in security thus identifying the previous mistakes and learning from those mistakes in future work will tighten belts in security perspective. Thus close all the weak links on GRC system which can make GRC system vulnerable for attacks [13].

10. Training, Go-Live and Support- This is the last step in implementation and does not involve much technical work but the co-ordinated approach to make the system live, train the users, releasing the system for support team is equally important as that of technical implementation. The training programs should be made differently depending on the user profiles. User profiles are different like internal auditors, end users, super users, business heads, role owners, security team etc. Making the user group specific training program will make the go-live period smooth. Most of the times support teams are not the implementation experts thus giving them insights on how the system is implemented will help them in supporting and administering the system for users in a better way.

4.3 Post Implementation Activities

System should not remain stagnant once the implementation is done as changes and updates are available from time to time. It is important to keep the system up to date with patches and security notes. Many of the bugs are identified during support phase hence it is necessary to apply the correction notes. Another important activity is security optimization of the system. In addition to regular audits, security optimization needs to be done on GRC system every year or every six months as per the business load. Security optimization of SAP GRC system involves implementation of RSECNOTES and HOTNEWS which are provided by SAP and sometimes it may require ABAP programming knowledge to implement the same. Security optimization also involves revisiting of all the authorizations within the system and if there are any loopholes then suggesting security plans for them. Security optimized system is less likely to be under attack as optimization will remove the vulnerabilities in the system [23].

5. CONCLUSION

SAP GRC Access control automates the process of authorizations. It derives a competitive advantage from understanding risks and choosing opportunities wisely. SAP GRC reduces the cost and effort needed to proactively prevent risk events and compliance violations and also reduces the unauthorized access risk with centralized monitoring and management. Uniform approach in GRC decreases the cost and effort of compliance, risk and audit programs. Access control increases safety of internal data. SAP GRC Access Control application empower organization to manage and reduce access risks across the enterprise by preventing unauthorized access and also achieves real-time visibility into access risk management. GRC access control covers the access needs, emergency access needs, access risk management and improvises the role based access control. GRC access control streamlines the whole access provisioning and makes it sound from audit perspective. GRC access control implementation fulfils security requirements of the systems within the organization.

REFERENCES

[1]. Reding, Kurt, Urton Anderson, Michael Head, Sridhar Ramamoorti, Mark Salamasick, Cris Riddle, and Paul Sobel. *'Internal Auditing: Assurance & Advisory Services'*. 2nd ed. The Institute of Internal Auditors Research Foundation; 2 Har/Cdr edition Accessed October 9, 2015. ISBN-13: 978-0894136436

[2]. Banzer, Alessandro, and SAP Official. *'Getting Started With SAP Governance, Risk And Compliance Solutions (GRC)'*. Scn.Sap.Com. Last modified 2015. Accessed October 27, 2015. http://scn.sap.com/docs/DOC-8879.

[3]. Baseline. *'Virsa Systems: Control Yourself'*. Last modified 2009. Accessed November 5, 2015. http://www.baselinemag.com/c/a/Projects-Data-Analysis/Virsa-Systems-Control-Yourself.

[4]. Laverdi.com. *'Laverdi - Virsa Access Enforcer'*. Last modified 2015. Accessed November 7, 2015. http://laverdi.com/website/virsa-access-enforcer/.

[5]. Official, SAP. 'SAP GRC Access Control 5.3'. E-book. Version 3.18. SAP AG, 2010. Accessed October 11, 2015. https://websmp207.sap-ag.de.

[6]. Official, SAP. 'SAP Business Objects Access Control 10.0'. E-book. Version 1.0. SAP AG, 2011. Accessed October 12, 2015. https://websmp207.sap-ag.de.

[7]. Official, SAP. 'Master Guide SAP Access Control 10.1'. E-book. Version 1.1. SAP AG, 2011. Accessed October 12, 2015. https://websmp207.sap-ag.de.

[8]. Tero, Vivian. '*The Case for GRC: Addressing the Top 10 GRC Challenges*'. IDC, 2012. Accessed October 14, 2015. https://www.emc.com/collateral/analyst-reports/h11523-idc-case-for-grc-addressing-top-10-challenges.pdf.

[9]. Official, SAP. 'SAP Access Control 10.0 – SAP Help Portal Page'. Help.Sap.Com. Last modified 2015. Accessed October 16, 2015. http://help.sap.com/grc-ac10?current=grc-ac101.

[10]. Official, SAP. 'SAP Access Control 10.0'. Scn.Sap.Com. Last modified 2015. Accessed October 18, 2015. http://scn.sap.com/docs/DOC-8562#section16.

[11]. Official, Oracle. 'Cluster Environment (Sun Java System Web Server 7.0 Update 2 Administrator's Guide)'. Docs.Oracle.Com. Last modified 2015. Accessed October 19, 2015. https://docs.oracle.com/cd/E19146-01/820-2202/gehht/index.html.

[12]. Official, SAP. AC 10.0 Customizing Workflows for Access Management. E-book. Version 2. SAP AG, 2011. Accessed October 26, 2015. https://websmp207.sap-ag.de.

[13]. Official, SAP. *SAP Business Objects Access Control Implementation and Configuration*. E-book. 1st ed. SAP AG, 2011. Accessed November 3, 2015. http://scn.sap.com/content.

[14]. Ertunga, Arsal. *SAP Security: Real-life Attacks to Business Processes*. Hack in Paris. Accessed Nov 15. https://www.hackinparis.com/sites/hackinparis.com/files/arsal_ertunga_sap.pdf

[15]. Rashid, Fahmida. *Majority of SAP Attacks Use One of Three Common Technique.* Security week. Accessed November 29, 2015. http://www.securityweek.com/majority-sap-attacks-use-one-three-common-techniques

[16]. Nunez, Mariano. *Cyber-attacks and SAP Systems*. Black hat Europe 2012 briefings. Accessed December 3, 2015. https://media.blackhat.com/bh-eu-12/DiCroce/bh-eu-12-DiCroce-CyberAttacks_to_SAP_systems-WP.pdf

[17]. Maenkova, Darya. *Chinese attack on USIS using SAP vulnerability*. Seclists.org. Accessed November 27, 2015. http://seclists.org/fulldisclosure/2015/May/64

[18]. Official, SAP. GRC Principles and Harmonization. E-book. 1st ed. SAP AG, 2011. Accessed November 3, 2015. https://training.sap.com/shop/course/grc100-sap-businessobjects-governance-risk-and-compliance-grc-100-principles-and-harmonization-classroom-096-us-en/.

[19]. Protiviti. SAP-Businessobjects-GRC-Access-Control-10.0-Protiviti. E-book. 1st ed. Protiviti, 2011. Accessed November 13, 2015. http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/SAP-BusinessObjects-GRC-Access-Control-10.0-Protiviti.pdf.

[20]. Byrne, Gary. 'Take Our Poll On Version 10.0 Of SAP Business Objects GRC Solutions'. Sapinsider.Wispubs.Com. Last modified 2011. Accessed November 7, 2015. http://sapinsider.wispubs.com/Assets/Blogs/2011/June/Take-Our-Poll-on-Version-10-dot-0-of-SAP-BusinessObjects-GRC-Solutions.

[21]. Siddiqui, Mohammad Imran. 'SAP Governance, Risk and Compliance Overview'. Presentation, Mumbai, India, 2014.

[22]. Siddiqui, Mohammad Imran. 'Mitigation Control-Implementation Approach'. Presentation, Mumbai, India, 2014.

[23]. Official, SAP. 'SAP Security Optimization Services | SAP Support Portal'. Support.Sap.Com. Last modified 2015. Accessed November 9, 2015. https://support.sap.com/support-programs-services/services/security-optimization-services.html#tabSelector#0_2.