

Access Control 5.3

Implementation Roles and Responsibilities



Applies to:

Access Control 5.3

Summary

GRC Access Control identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. This document is a partner to the integrated project plan and lists the roles identified there, as well as the corresponding responsibilities.

Authors: Lori Donnelly, Janet Tran
SAP GRC Customer Advisory Office

Created on: January 2009

Version 2.0

Typographic Conventions

Type Style	Description
<i>Example Text</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
Example text	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

Icons





Icon	Description
	Caution
	Note or Important
	Example
	Recommendation or Tip

Table of Contents

- 1. Management Overview 4**
- 2. Project Roles and Responsibilities..... 4**
- 3. Related Content 6**
- 4. Copyright 7**

1. Management Overview

This document identifies selected responsibilities typically owned by each role specified in the *SAP GRC AC 5.3 Integrated Project Plan*. It is not an all-inclusive list, but is intended to represent types of activities that are commonly performed by team members. This document may be used to identify individuals and teams to participate in your AC 5.3 implementation project.

2. Project Roles and Responsibilities

Listed below are the roles identified in the Access Control (AC) integrated project plan. All team and management members are also participants in the change management process, when necessary.

The following abbreviations are used for the capabilities of AC.

CUP	<i>Compliant User Provisioning</i>
ERM	<i>Enterprise Role Management</i>
RAR	<i>Risk Analysis and Remediation</i>
SPM	<i>Superuser Privilege Management</i>

Roles appear in alphabetical order.

Access Control Administrators: One or more person(s) responsible for the configuration and administration of the AC system's four capabilities. They are commonly members of the organization's IT security team (all capabilities) or the IT functional team (ERM, RAR). Tasks include, but are not limited to, the following:

- Primarily responsible for application administration
- Participate in defining the implementation strategy
- Assist in determining an integrated AC master data strategy
- Review related SAP Notes
- Validate AC system requirements
- Complete the Post-Installation Checklist
- Validate system installation and configure each capability
- Assist in validation of system configuration
- Create/validate master data
- Responsible for user administration

Access Control Business Team: One or more person(s) responsible for insuring critical business requirements are met. This involves defining relevant risks, roles, provisioning process and remediation strategy. The team members are commonly end users, super-users, Business Process owners and Business Process analysts. Tasks include, but are not limited to, the following:

- Define the use of Access Control and the system functionality requirements
- Determine an integrated AC master data strategy
- Assist in configuring Access Control
- Assist with validation testing with focus on meeting business and audit requirements
- Assist in identifying the AC approval and remediation processes including approvers of risk definitions, role definitions, user provisioning, and mitigating control assignments.
- Assist in delivering the project's communication plan
- Responsible for developing and delivering the training plan

Access Control Client Project Manager: The client's or customer's project manager who is responsible for the overall project success. He/she is also the primary communicator of the project status to management. Tasks include, but are not limited to, the following:

- Lead the definition of the implementation strategy
- Ensure critical business requirements are met by the AC implementation
- Assist team with requirement clarification and issue resolution
- Develop and deliver the communication plan
- Ensure deliverables are met
- Conduct post go-live review

Access Control Functional and Technical Consultants: Provide Access Control expertise and assist project teams in different areas, as needed. They assist with project implementation and issue resolution which includes, but is not limited to, the following:

- Assist in defining the implementation strategy
- Assist in defining the system landscape strategy
- Assist in defining the user management strategy
- Assist in defining risks, security roles and mitigating controls
- Perform testing and validate system configuration
- Provide guidance to Access Control project team, as required.

Access Control Technical Team: This team is responsible for all Access Control technical tasks pertaining to the technical infrastructure and Basis/DBA tasks. This team may be made up of one or more resources and are also represented in the project plan as the **Infrastructure Team** and the **Basis/DBA Team**. Tasks include, but are not limited to, the following:

- Review software and hardware requirements
- Review related SAP Notes
- Participate in defining the system landscape strategy of AC
- Participate in identifying the target systems and minimum Basis requirements for AC RTAs
- Participate in defining the user management strategy
- Complete Technical Checklists
- Validate NetWeaver environment
- Deploy and install AC 5.3 application components on NW server

Audit / Internal Control Team: Liaison between external auditors and owners of the risk definitions. Tasks include, but are not limited to, the following:

- Affirm that access management processes meet audit requirements
- Assist in identifying risks prior to AC implementation and afterward on an on-going basis
- Assist with validation testing with focus on meeting audit requirements
- Assist in delivering the project's communication plan

Management Team: Participants in go-live activities. They are liaisons between the project team and the end-users of the application. They provide management support in the following areas:

- Deployment of the training plan
- Delivery of the communication plan
- Resolution of project issues
- Deployment of the roll-out plan
- Project go-live
- Provide post go-live feedback

3. Related Content

[AC 5.3 Integrated Project Plan \(Adobe Acrobat\)](#)

[AC 5.3 Integrated Project Plan \(Microsoft Project\)](#)

[Getting Started with GRC Access Control](#)

[SAP Preferred Practice site for GRC Access Control](#)

4. Copyright

© Copyright 2009 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided "as is" without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

SAP NetWeaver "How-to" Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.