RAC/M
IDENTITY

GIA SIMPLIFIED

Achieve compliance, reduce costs and risks

Organizations are increasingly challenged to demonstrate full control over access management.

RAC/M Identity™ is a simple and effective IAM solution that enables organizations, large and small, to understand and manage the complex relationships between users and their access to physical and IT resources located on-premises or in the cloud.

RAC/M Identity™ is the cornerstone on which to build an IAM practice that can turn your most daunting challenges into a competitive advantage. These challenges include lack of resources, limited budgets, strict timelines, and rapid transformation fueled by the accelerating adoption of cloud computing and the Internet of Things.

RAC/M Identity™ also addresses one of the most difficult challenges faced by IAM programs - ensuring sustainability of the IAM practice by maintaining senior management commitment and addressing the challenges of skilled labor shortages and retention.

To this end, OKIOK's offer includes three levels of service: an on-premise version that you manage and operate, a managed, Software as a Service (SaaS) version that you operate, and a fully managed services version (IDaaS), whereby day-to-day operations are handled by OKIOK resources. This approach completely eliminates the costs and hassles associated with implementing and maintaining an infrastructure and managing and operating an IAM solution.

In addition, the solution monitors and reports on the maturity and effectiveness of key IAM processes, allowing management to assess progress made and opportunities for improvement.

Simplify your identity and access governance program

As organizations grow, understanding who has access to what and maintaining control become increasingly complex due to challenges such as fragmented user populations, a complex and rapidly changing technology landscape and inconsistent management practices.

By simplifying identity governance, RAC/M Identity enables organizations to quickly obtain and demonstrate control over access to critical information as required by various regulatory frameworks such as GDPR, SOX, PCI, NERC, HIPAA, etc.

Reduce your costs with RAC/M Identity as a Service (SaaS)

You can realize substantial cost savings and avoid maintaining highly trained staff by deploying RAC/M Identity as a service. RAC/M Identity as a service is deployed in a dedicated cloud space, eliminating the need to build, manage and support a costly and complex infrastructure onsite, while OKIOK provides day-to-day management services such as backups, monitoring, updating, upgrading and security patching.

Eliminate the cost and hassle of hiring and retaining staff with RAC/M Managed Services (IDaaS)

RAC/M Identity as managed services enables your organization to realize even greater benefits by allowing you to focus your most valuable resource, human capital, on mission-critical, value-added tasks.

RAC/M Identity as managed services provides you with maximum benefits by eliminating day-to-day operational tasks, which are handled by OKIOK's expert resources. In this mode of operation, specific resources are assigned to your company and work in symbiosis with your teams to ensure a maximum level of service.

Low code – No code

The future is low code, the whole industry is talking about it. The RAC/M Identity solution provides substantial savings in deployment efforts by avoiding customization and coding through the configuration of pre-built business logic modules and the use of standardized, yet flexible, approval and provisioning workflows.

Get results fast

RAC/M Identity is built around a data repository that provides a complete view of all accounts, accesses and rights held by all users on all relevant assets. Near real-time reconciliation of the repository with all identity sources and target systems, whether on-premises or cloud-based, combined with powerful analysis and reporting capabilities, provides immediate visibility. The repository allows for immediate detection and remediation of risky situations as well as the rapid initiation of periodic access reviews, improving the maturity and efficiency of IAM processes.

Reduce your risk

Risk is reduced by continuously identifying and remediating risky situations such as orphaned or malicious accounts, as well as quickly revoking unnecessary access when people leave the organization or change roles. In addition, periodic access reviews allow asset managers and owners to validate access to critical resources and eliminate unnecessary access.

Optimize user experience

RAC/M Identity optimizes user experience and productivity by providing single sign-on (SSO) with Active Directory domains and SAML federated identity providers as well as a self-service portal, customized to your preferences, that allows key operations such as access requests, approvals, and access reviews to be performed from any device with a compatible browser.

A different approach, focused on concrete results

RAC/M Identity differs from traditional identity governance and administration (IGA) suites in that it is delivered as a complete service offering, supported by a proven, risk-free, deployment methodology.

Our approach focuses on building a solid foundation of enhanced identity and access management governance and processes, which is a prerequisite for automated provisionning.

In fact, IAM projects often stumble when they aim to hastily automate IAM processes without gaining a clear understanding of existing, often obscure, practices or taking the time to clean up access data and establish a clear, shared vision of goals.

RAC/M Identity puts forward the establishment of a clear identity governance strategy, tailored to the real needs of your organization, by providing you with the critical expertise and support that will allow you to achieve it. This approach will enable you to, among other things:

- Quickly understand your organization's identities and access rights structure across integrated identity sources, target systems and applications.
- Identify and revoke unnecessary identities and accounts.
- Manage employee, privileged user, contractor, and external user accounts.
- Manage service, shared, generic and technical accounts.
- Assign owners, approvers, reviewers, and trustees to assets, accounts, and roles.
- Define a structured access model based on business and application roles and assignment rules.
- Define, monitor, and enforce segregation of duties (SOD) rules to prevent fraud and error.
- Implement a flexible access certification process for identities, roles, rights, and segregation of duties conflicts.
- Promote self-service access management and password resets through automated approval workflows.
- Automate the arrival, departure, and movement of users by automatically provisioning and de-provisioning accounts, group members and rights in connected target systems.
- Provide all required artifacts to support compliance and audit requirements.
- Automatically generate metrics to maintain executive support for the IAM program.

Flexibility by configuration *Low code – No code*

RAC/M Identity easily adapts to any technological and business context by integrating with existing systems and business processes through the configuration of a rich set of integrated business logic modules. To reduce integration time and effort, RAC/M Identity can handle any type of reference data representing your organizational structure, workflows, nomenclature, or business logic. The user experience can be enhanced by customizing forms and screen labels to match your organization's nomenclature. This approach eliminates costly customization efforts, reduces deployment costs, and delivers better results faster.

Unlimited data model

A key feature of RAC/M Identity is the ability to dynamically extend the data model to represent and manage any number of specific attributes populated from your data sources. These extended attributes are defined by you and can be attached to data elements such as identities, roles, accounts, groups, and organizations. These extended attributes can be invoked just like standard attributes to further define business logic or filter search results.

Fast and convincing results

Every RAC/M Identity implementation begins with the mapping, consolidation, and analysis of identity data. These first steps catalyze an organizational transformation that brings immediate and lasting improvements to information access management practices. In fact, RAC/M Identity has enabled our customers to analyze, detect and revoke unnecessary accounts and rights within days of implementation.

Powerful matching algorithms

Real-world identity data is never clean, complete, or reliable. Ask anyone who has tried to manually match multiple accounts to unique identities. To solve this challenge, RAC/M Identity includes a set of powerful matching algorithms.

These algorithms allow users to quickly solve many complex matching conditions such as:

- Name collisions
- Spelling mistakes
- Alternative spellings
- Different order of naming components
- And several others.

The matching logic can be iteratively refined to a very high level of automated matching, depending on the quality of the source data. The remaining unmatched accounts or identities can be matched manually with the help of the included tools.

Role mining and modeling

RAC/M Identity includes powerful role mining and modeling tools.

The identities and assets to be analyzed can be determined using filtering rules. These rules can be based on any relevant characteristics to determine the identities and assets to be analyzed. Mining algorithms automatically identify common access rights and permissions that can be assigned to roles. This is the bottom-up method.

Roles can also be defined in a top-down manner, allowing role engineers and experts to determine exactly what rights should be granted.

The combination of bottom-up and top-down approaches is a powerful and flexible feature supporting a two-tier role model where business and application roles can be dynamically assigned by assignment rules and policies.

Dynamic role assignment significantly reduces operational effort. Roles can also be statically assigned to specific members.

Integration capabilities

RAC/M Identity integrates easily with virtually any identity source and target system. It does so with Identity Connector Framework (ICF) connectors and flat file collectors. These connectors, along with the required business logic, are built into many predefined templates for applications and systems such as Active Directory (AD), LDAP directories, SQL databases, AS/400, SAP BW, SAP IDoc files, as well as for cloud applications such as Office 365 and ServiceNow.

This flexible architecture allows RAC/M Identity to easily adapt to any existing and future technical environment.

Risk reduction

RAC/M Identity reduces attack surfaces by systematically eliminating unnecessary accounts and rights, controlling over-privileged accounts, performing near real-time reconciliations between identity sources and all target systems, formalizing access request approval workflows, and enabling periodic and ad hoc reviews.

Two editions for maximum scalability

RAC/M Identity is available in two editions allowing maximum scalability for organizations of any size.

The RAC/M Identity Governance Edition enables the implementation of an identity repository to perform access reviews to quickly meet regulatory or contractual requirements.

The Premium Edition includes all the features of the Governance version but adds self-service and automated provisioning using ICF connectors.

Governance

- Complete visibility of entitlements
- Access reviews & recertification
- RBAC/ABAC access models
- Flat files

Premium

- Complete visibility of entitlements
- Access review & recertification
- RBAC/ABAC access models
- Self-service
- Automated processes
- ICF connectors
- Flat files

RAC/M Identity's unique identity governance model as managed services and low total cost of ownership make it a viable solution when other IAM solutions are too costly or cannot meet functional requirements. RAC/M Identity is designed to manage an unlimited number of identities in complex scenarios involving both external users and your employees, across all your information systems.

USER EXPERIENCE

Features	Benefits
Web Interface	Administrators can easily perform all configuration and management tasks from any browser.
Responsive web interface	Tasks such as access reviews, access request approvals and notification responses can be performed from any supported browser and mobile device.
Fully customizable integrated self-service portal	Access requests and tasks such as approvals and access reviews can be performed by end users, managers, super users, and certifiers through the included self-service portal, customizable to your colors.
Integration with ticketing solutions	The solution allows you to open and manage tickets in ITSM ticketing solutions such as ServiceNow™ and others.
REST and SOAP APIs for administrative functions	Self-service and administration functions can be automated or performed by applications via REST and SOAP APIs.
Customizable user interface	The user experience can be enhanced by customizing the user interface to match your organization's specific colors and nomenclature.

CAPABILITIES

Features	Benefits
ICF bi-directional connectors for integration of identity sources and target systems	IBi-directional integration of virtually any target system, SaaS application or identity source, such as: •Active Directory •LDAP directories •SQL Databases •SAP BW •SAP IDocs •Windows servers 2008/2012/2016 •NIX servers (*Linux/Unix) •Microsoft Graph API (Office 365, Azure, etc.) •AS/400 •Any target system, SaaS application or identity source via a scripting connector
Unidirectional collectors	One-way collectors can import and process data from any identity source, target system or application that can export access data to a flat file such as CSV, XLS, XLSX, IDOC, etc.
Automated matching algorithms	Automated matching algorithms Several automated matching algorithms such as soundex, multiple soundex, permutations as well as flexible business logic allow for a high rate of account to identity matching without user intervention.
Manual matching interface	Remaining accounts and identities can be manually matched using a variety of powerful tools.

RAC/M IDENTITY

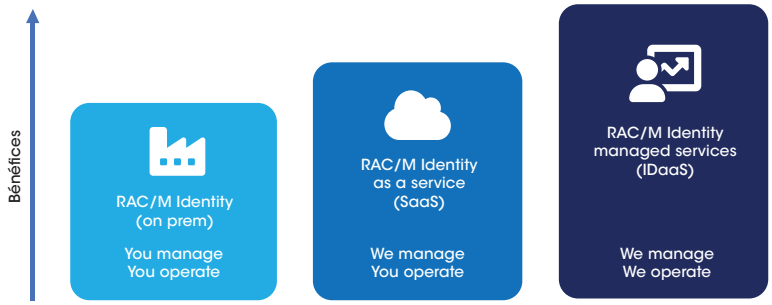
Features	Benefits
Account categorization and categories	Account processing and categorization allows for efficient tracking and control of all types of accounts, including personal, generic, technical, privileged and others.
Role mining and modeling	Roles can be extracted from existing access by mining using powerful filtering rules for assets and identities. Roles can also be modeled and built manually (RBAC).
Dynamic and static role assignment	Roles can be assigned automatically based on rules and attributes (ABAC). Roles can also be statically assigned to specific identities.
Repository reconciliation	The repository is automatically kept in full synchronization with all identity sources and target systems and applications, providing complete and reliable identity and access visibility.
Configuring business logic elements	Allows for much faster results by eliminating time-consuming programming and scripting.
Metrics, dashboards, and overviews	Provide immediate visibility into the effectiveness and efficiency of IAM processes and the status of the repository. Insights provide immediate visibility into risky situations prioritized by criticality for rapid resolution.

Features	Benefits
IAM Program Health Index	Maintains management support and commitment to the IAM program by expressing the maturity and effectiveness of key IAM processes through a single indicator for benchmarking and monitoring IAM posture.
Customized display	Optimizes the user experience by providing a view of the management console that is tailored to the user's responsibility and privilege level.
Comprehensive reports	Allows for powerful analysis and reporting from a multitude of built-in reports. Custom report generation is also available.
Flexible access review campaigns	Fully configurable campaigns and tracking workflows allow the campaign manager to apply sound governance by focusing on critical resources and ensuring timely execution of revisions. Automated queries ensure that corrective actions are taken quickly throughout the campaign.
Synchronization of passwords	Password changes can be propagated from Active Directory to compatible target systems.

Operating models

RAC/M Identity™ is available in three operating models for maximum flexibility:

- RAC/M Identity on site (on site)
- RAC/M Identity as a Service (SaaS)
- RAC/M Identity as a managed service (IDaaS)



	ON SITE	SERVICE MODE (SaaS)	MANAGED SERVICES (IDaaS)
Hardware and software requirements	Please contact an authorized OKIOK dealer for the latest requirements.	No hardware or software requirements. Infrastructure hosted in a dedicated Microsoft Azure tenant. Connectivity with your network provided by VPN.	
Subscription model	Annual, depending on the number of identities. Includes a limited pre-production environment		
Management activities •Sizing & workload management •Availability and performance monitoring •Upgrades, patches and updates •Backups & disaster recovery •Investigation of operational issues •Assistance for integrating of target systems	Performed by you	Performed by OKIOK	Performed by OKIOK
Operating activities •Identity and account matching •Follow-up and resolution of anomalies •Drilling and role modeling •Definition of SOD policies and rules •Definition and execution of access reviews •Application and system integration	Performed by you	Performed by you	Performed by OKIOK
Client software requirements	Windows: Microsoft Internet Explorer 11, Microsoft EDGE, recent versions of Firefox and Chrome Mac OS X: Safari, Opera, any compatible browser		

Please contact an authorized reseller for more information and pricing.

OKIOK

OKIOK is a leader in the field of information security. Since 1973, the company has distinguished itself through the excellence of its products and the high quality of its services. OKIOK offers a wide range of integrated solutions designed to meet the needs of organizations of all sizes.

www.okiok.com | info@okiok.com | 1 877 561-1681

Revision date: February 2022