COURION™

IDENTITY AND ACCESS GOVERNANCE

Buyer's Guide

TABLE OF CONTENTS

Purpose of this Guide 1

Identity and Access Governance 2

IAG as Part of Identity & Access Management 4

Feature Tables:

- Role Definition 7
- Access Requests 11
- Access Approvals 15
- Access Certifications 18
- Audits and Compliance Analysis 21
- Identity and Access Intelligence: Monitoring and Analysis 24
- Solution Deployment and Integration 29
- Summary of Tables 32

Appendix 33

For More Information 34

PURPOSE OF THIS GUIDE

Welcome to the Courion Identity and Access Governance Buyer's Guide.

This guide is designed to help you define requirements for an Identity and Access Governance solution for your enterprise.

It can also help you select a short list of vendors for evaluation, and compare Identity and Access Governance products during an evaluation process.

Our Approach

The material in this guide is organized around the core tasks of Identity and Access Governance (IAG) and the people who perform them. It examines the features and functions of IAG solutions needed to:

- **Define roles and the access permissions associated with them,** a task typically performed by IAM analysts, resource owners and business managers. (In this guide we will use "IAM analysts" as shorthand for IAM project leaders and security professionals responsible for managing IAM activities. "Resource owners" will refer to line-of-business and IT staff responsible for managing access to applications, databases and other resources.)
- **Request access to applications, systems and resources,** an activity carried out by business managers on behalf of their reports, and by a wide variety of employees and other system users for themselves.
- **Approve access requests,** typically performed by business managers and resource owners.
- **Certify the appropriateness of access** to sensitive systems, applications and data, tasks performed by business managers, resource owners and auditors.
- **Manage risk and verify compliance with government, industry and corporate policies,** tasks belonging to auditors and compliance officers.
- **Use Identity and Access Intelligence tools to analyze usage, uncover vulnerabilities, identify policy violations, respond to attacks, remediate problems and reduce risks.**
- **Deploy IAG solutions** and integrate them with other identity management and security products.

The opening sections provide a brief overview of Identity and Access Governance (IAG), and place IAG solutions in the context of Identity and Access Management as a whole.

[1] Examples from real Identity and Access Management buyer's guides.

The remaining sections are designed so that evaluation team members can work with representative "subject matter experts (SMEs)" in each category (business managers, system users, compliance officers, etc.) to assess how an IAG solution can help them do their jobs better and meet organizational goals.

The feature tables can be used to capture assessment data during feature reviews, vendor demonstrations, proof-of-concept tests, reference calls, and other evaluation activities. The tables are laid out so you can use the rating system of your choice, and there are spaces for comments and assessments by section. If you want to modify or expand the tables, you can download them in PDF or Excel format from the Courion web site Resources section at ***www.courion.com.***

In this guide we try to apply the same practical, business-friendly design principles used in Courion's products, avoiding platitudes ("Today's business world is changing rapidly, and so are your IAM requirements") and dense feature descriptions ("Has a workflow that seamlessly integrates with SAP and Oracle ERP, and fine-grained separation-of-duties checking with flexible exception-handling methods [Yes/No]").[1]

Talk with Us

Our consulting team and partners can answer your questions, demonstrate Courion's solutions, help you conduct a proof-of-concept, generate a business case, or assess access risk. We would also like your feedback on this guide. Please contact us at ***info@courion.com***

IDENTITY AND ACCESS GOVERNANCE

Functions of Identity and Access Governance

Today, the field of Identity and Access Governance covers four main components:

1. Processes to certify that existing permissions are appropriate and in conformance with corporate policies.
2. Processes to audit identity and access processes and results, demonstrate controls, define policies about who should have access to what resources (governance), prove compliance with regulatory requirements and company standards, and remediate any issues uncovered.
3. Processes to define roles and to request and approve access to data, applications and other information technology resources.
4. Monitoring and analysis tools to detect vulnerabilities, assess risk, and improve compliance with requirements and standards.

The original focus of IAG was on the first two components, especially on tools to certify permissions and to help auditors and compliance officers reduce audit costs and document compliance.

However, it was soon recognized that these four areas are reinforcing. Organizations that have reliable processes to request and approve access make fewer errors, and therefore expend less effort on certification, auditing and remediation. Organizations with identity and access intelligence tools can monitor changes for policy violations, track trends and identify vulnerabilities, allowing them to respond to problems faster.

In fact, comprehensive IAG solutions provide value in many areas by:

- Improving the productivity of managers by simplifying identity and access certification processes
- Saving time for employees by speeding up the process to request and receive access to resources (especially when the request system is integrated with automated provisioning)
- Providing more data to speed up audits and reduce the high cost of regulatory compliance
- Reducing vulnerabilities and decreasing the risk of data breaches and the loss of customer and employee information and intellectual and financial property
- Improving risk management
- Deterring policy violations by employees and other insiders

At the same time, IAG solutions help enterprises address some of their most pressing human and technology challenges: increasing numbers and types of technology users (employees, contractors, business partners, customers), multiplying applications and devices (including employee-sourced devices encouraged by "BYOD" policies), growing regulatory requirements, pressures for better risk management and security, and tight limits on budgets and staffing.

Tasks and People

Figure 1 shows some of the major tasks involved in Identity and Access Governance, and the people who typically perform them.

The feature tables section of this guide uses these task areas to organize its list of desirable features and functions, to make it clear how those features and functions relate to specific people doing specific jobs.

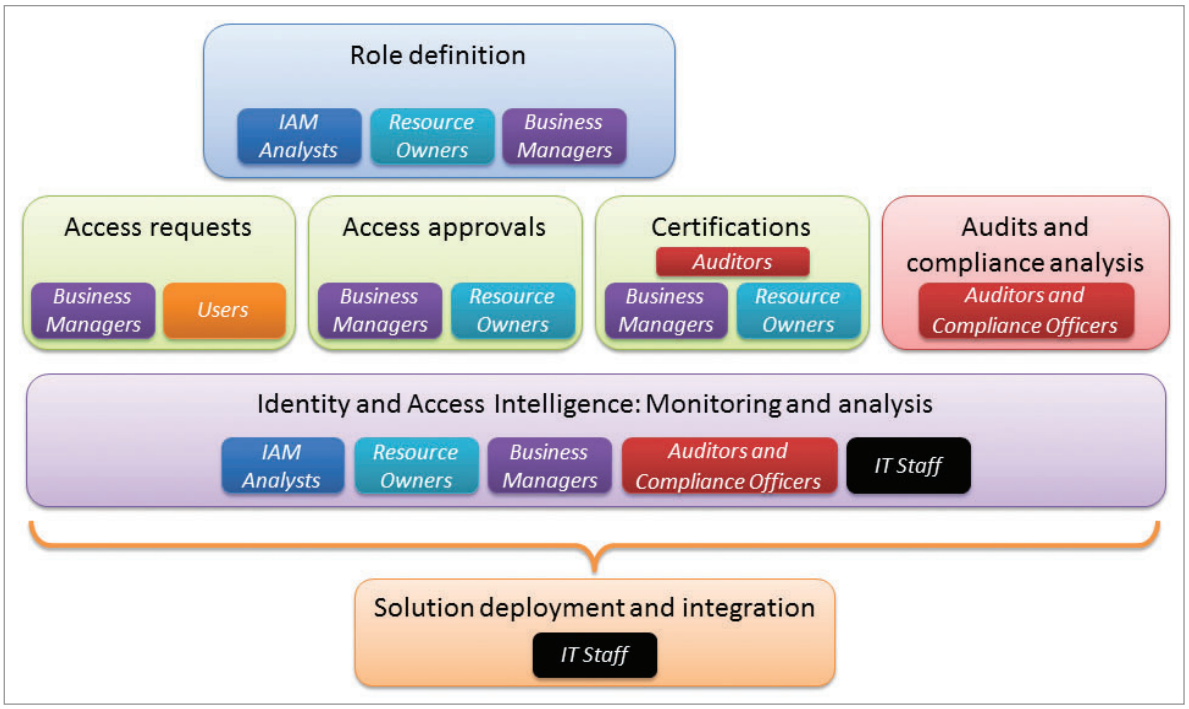


Figure 1: IAG tasks, and the people who perform them

IAG AS PART OF IDENTITY & ACCESS MANAGEMENT

Broadly speaking, today's state-of-the-art Identity and Access Management systems cover three primary areas of functionality: Governance, Provisioning, and Intelligence.

Governance systems provide processes to request, approve and certify access to applications and IT resources, and tools to document compliance with government regulations, industry standards and corporate policies.

Provisioning systems automate the provisioning and de-provisioning of access to applications and IT resources, and manage access through users' lifecycle with the organization. Key IAM functions such as password management, advanced authentication and single sign-on are sometimes considered as part of provisioning and life-cycle management, and sometimes as separate entities (but are in any case outside of the scope of this guide).

Identity and Access Intelligence systems provide tools to continuously collect, monitor and analyze large volumes of identity and access-related information, combining data not only from Governance and Provisioning systems, but also from security products and other external systems. Identity and Access Intelligence products are often designed so they can be used with either a governance system, or a provisioning system, or with both.

In fact, Identity and Access Intelligence tools should be seen as an integral part of any Identity and Access Governance implementation. This guide discusses functionality that is typically available in governance systems and in Identity and Access Intelligence tools when they work together. Figure 2 illustrates this approach, and lists the products from Courion that fall into those areas.

A brief overview of the Courion products is provided in the appendix.

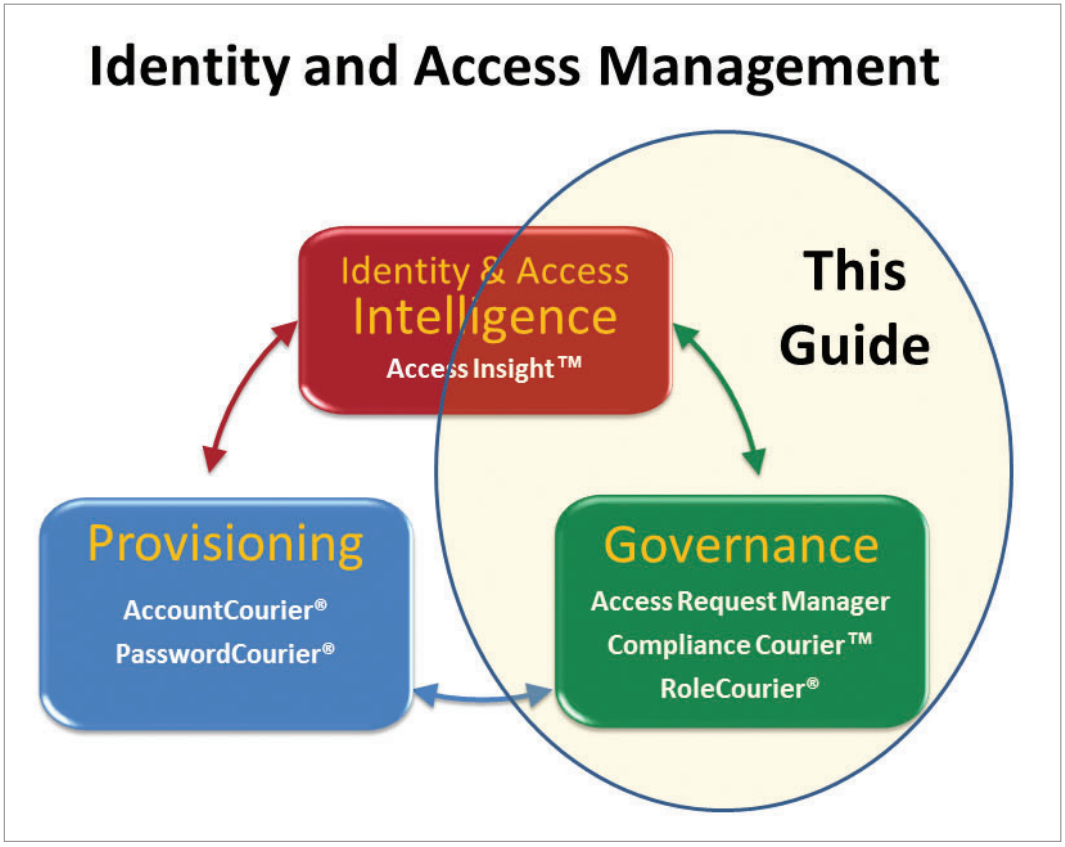


Figure 2: The three main areas of Identity and Access Management, with products from Courion. The Courion products are modular and can be implemented in any combination.

Feature Tables

ROLE DEFINITION

Primary participants: IAM analysts, resource owners and business managers

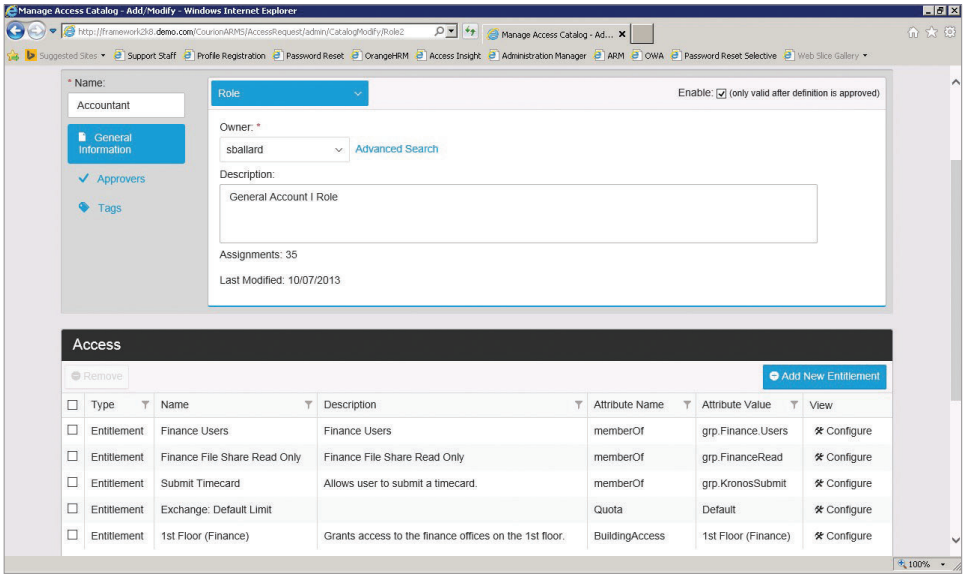
An Identity and Access Governance solution should make it as simple as possible for IAM analysts, resource owners and business managers to define roles and the access permissions that are associated with them.

People should be able to use business terminology, not technical jargon, to identify roles and permissions. This allows business managers and business users to participate fully in defining roles, and later in requesting, approving and certifying access.

It should be easy to create simple roles at first, then refine, enhance and expand them over time. That allows organizations to start using the system quickly while continuously improving efficiency and accuracy.

It should be possible to define permissions that (a) accurately reflect the legitimate needs of system users, and (b) do not provide unnecessary entitlements that could jeopardize security and privacy. To achieve these objectives, analysts, resource owners and business managers should be able to:

- Create very granular entitlements, for example permission to make AP inquiries against a specific accounting package, to use a specific computing resource like SharePoint or Internet access, or to acquire an asset like a laptop with a 17" screen.
- Create roles that include combinations of permissions, such as an "Accountant" role that includes permissions to make deposits, reconcile bank statements, create purchase orders, make AP inquiries, etc.
- Create groupings that combine roles, for example a "Senior Accountant" role that includes permissions assigned to the "Accountant" and "Level 2 Manager" roles.
- Model new roles by comparing specific permissions from existing roles (Courion calls this "intelligent modeling").



Roles can combine permissions to perform specific actions on target resources

Most individuals will have diverse access requirements, based on their function, location, management level, and application needs. Therefore people should be able to find appropriate entitlements and roles by using search and filtering techniques with a catalog of roles. They also should be able to classify and tag roles so people making access requests can find the right ones to request, and so approvers can determine the most appropriate roles for specific system users.

The system should be able to accommodate both:

- A "bottom up" approach: See what permissions people have today and assemble roles based on those observations.
- A "top down" approach: Create roles based on an analysis of what is likely to work best in the environment, and test those.

System users should be able to define policies, for example Separation of Duties (SoD) policies that prevent the same person from taking potentially damaging actions like creating vendor accounts and authorizing vendor payments.

Role definition and refinement can involve many people, including IAM analysts who know best practices for designing roles, "resource owners" responsible for applications, databases, and other IT services, and business managers who understand the responsibilities of employees performing specific jobs. Therefore the system should have mechanisms to manage who can define, change, disable and delete specific roles.

The systems should create a complete audit trail of every action related to defining, modifying and deleting roles.

There should be "out of the box" or easily managed integration with provisioning systems, directories and applications, so role-related information from those systems is available.

There should be integration with Identity and Access Intelligence tools so analysts can assess roles after they have been created. For example, if a report or query shows many users with the same role requesting an additional account or entitlement, then that account or entitlement can be added to the role. Conversely, if there are entitlements that nobody with the role uses, these should be removed from the role definition.

Integration with Identity and Access Intelligence tools also allows role-related information to be analyzed and used for governance, compliance, incident response and other purposes.

Role Definition	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Use a single interface to manage access to a wide array of business resources, including applications, networks, IT accounts, local, remote and cloud-based systems, locally installed, client/server and cloud-based applications, LAN, wireless and Internet connectivity services, physical assets such as laptops and smartphones, and software licenses.		
Define roles using business terminology (not technical jargon)		
Assign a user friendly name to roles (for searching and filtering)		
Add a user friendly description to roles		
Define roles based on individual, granular entitlements (e.g. read-only access to a specific database)		
Define roles based on groupings of existing roles and entitlements		
Define roles based on titles or departments (e.g. Accountant, Vice President, IT Contractor, Sales, Customer Service)		
Define roles based on applications or IT resources (e.g. Microsoft Office, Salesforce.com, Network Access, Laptop User)		
Clone roles from existing roles		
Model new roles based on existing roles (add/subtract)		
Model new roles based on existing user access (add/subtract)		
Create an entitlements “catalog” of available entitlements and roles		
Use searching and filtering to identify relevant roles in the catalog		
Assign tags to roles, and use tags for searching and filtering in the catalog		
Allow users to use the catalog to define new roles combining groupings of existing entitlements and roles		

Role Definition	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	**Option X**
Define Separation of Duties (SOD) and other access-related policies (e.g. the same user cannot have permissions to make deposits and reconcile bank statements)		
Run new polices against existing roles and policies to flag policy violations		
Set administrative policies about who is allowed to define roles (e.g., anyone, only managers, only Human Resources staff, only designated individuals for each department)		
Limit permission to change a role definition to a designated "role owner" or "resource owner"		
Require that changes to a role definition be approved by one or more specified individuals in addition to the role owner		
Disable roles temporarily		
Display role usage statistics, such as when a role was last modified and the number of times it has been assigned to users		
Obtain role and user information from provisioning systems (integration)		
Export role and user information to directories, applications, analytic tools and other external systems (integration)		
Create a complete audit trail of all actions related to role creation, definition, modification, deletion and approvals.		
Overall assessment for Role Definition		

Comments:

ACCESS REQUESTS

Primary participants: Business managers, employees, contractors and other system users

An Identity and Access Governance solution should make it as simple as possible for managers to request access permissions for direct reports, and for employees, contractors and other system users to request access for themselves.

People should be able to use business terminology, not technical jargon, to find relevant roles and understand the related entitlements. People should find appropriate entitlements and roles by using a role catalog with search and filtering techniques, and by using tags for searching and filtering.

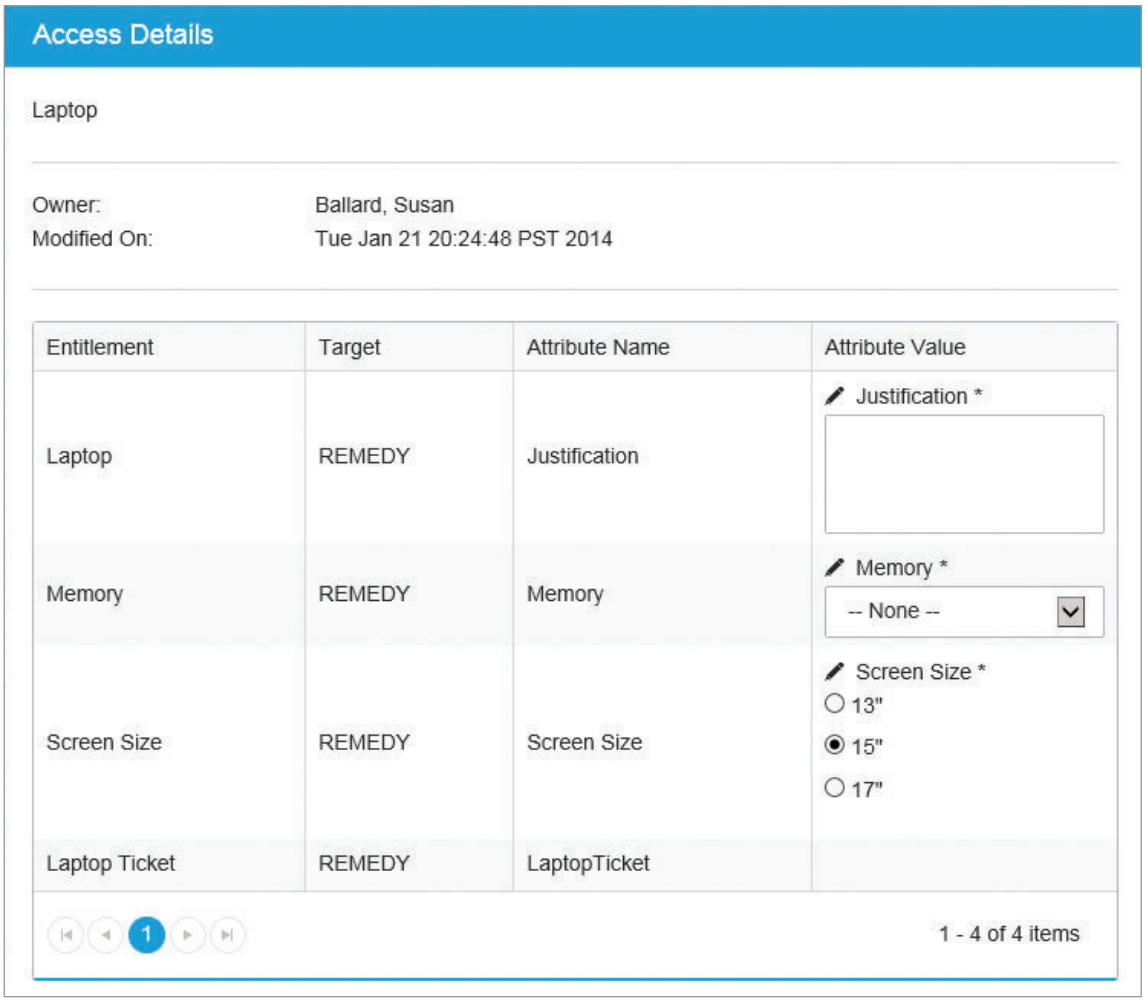
It should be possible to allow some people to request permissions for everyone in the organization, and to limit other people to making requests for specific groups, or only for themselves.

It should be possible to restrict requests based on policy, and to filter roles and entitlements based on related criteria. For example, a member of the finance staff might be restricted to requesting entitlements related to finance, and would be able to apply a filter in the role catalog so that it would display only those entitlements.

Some applications and resources may involve options that do not affect security or governance; there should be a mechanism to allow people to request these options without creating many separate roles. For example, it should be possible to have a single role called “Laptop” with a choice of memory and screen size options. That is more efficient than creating separate resources called “Laptop, 8MB memory, 13in screen,” “Laptop, 8MB memory, 15in screen,” “Laptop, 16MB memory, 13in screen,” etc.

The systems should create a complete audit trail of every action related to requesting, approving and granting access.

This functionality is complementary to provisioning. Provisioning systems automate the process of requesting and granting access, especially when people enter and leave the organization. Some provisioning systems have front-end interfaces with the same features described here. But an access request tool can be used as part of an Identity and Access Governance solution without a provisioning system. It can be used in conjunction with one, especially if the provisioning system front end lacks key features or is hard to use.



There should be a mechanism to request options without creating separate roles for every combination

Access Requests	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Request permissions for direct reports		
Request permissions for self (self-service)		
Request permissions for a specific list of users		
Request access to a specific list of resources, such as applications		
Request permissions based on existing roles and groupings of roles and entitlements		
Select options relevant to a specific resource (e.g. have one resource called “Sales Laptop” with a dynamic form to choose memory and screen size options)		
Use a role catalog with searching and filtering to quickly find and request relevant roles and entitlements		
Use tags for searching and filtering in the catalog		
Use “bulk provisioning” to request one set of roles and entitlements for multiple direct reports, or for a list of users		
Ability to delegate access requests (e.g., the director of a department can delegate to a manager the right to make access requests for all members of the department)		
Validate access requests against defined business policies and flag violations		
When policy violations are flagged, allow requesters to override the policy through an exemption request		
Share access request information with provisioning systems (integration)		

Access Requests	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Export access request information to Identity and Access Intelligence tools so they can identify suspicious activities and policy violations (integration)		
Create a complete audit trail of all actions related to access requests		
Overall assessment for Access Requests		

Comments:

ACCESS APPROVALS

Primary participants: Business managers and resource owners

An Identity and Access Governance solution should provide simple, efficient processes for business managers and resource owners to process access requests.

In this context “resource owners” are line-of-business or IT staff responsible for controlling access to applications, databases and IT services. They are the people who, along with business managers, understand what types of access users need to perform their jobs, and what entitlements can be given without compromising security, privacy rules and corporate policies.

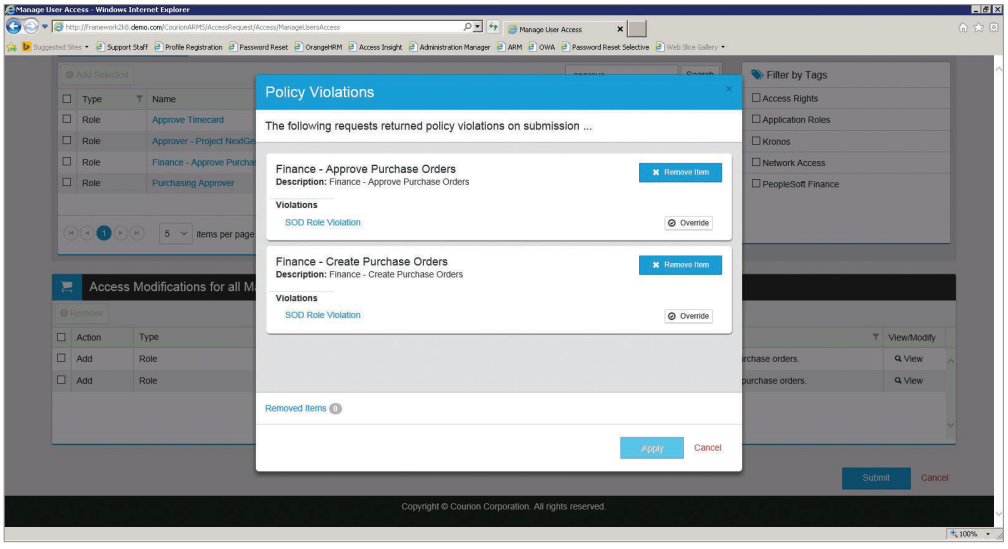
Business policies may require multiple approvals for some requests. The solution should enforce these policies, for example by requiring approval from the requester’s immediate manager and department head, or from a manager and the “owner” of the requested resource.

The solution should provide an intuitive interface, so approvers can assess individual requests efficiently and manage dozens of requests each day.

The solution should alert approvers to potential policy violations.

Busy or absent approvers can be a bottleneck, preventing users from accessing resources needed for their work. To address this issue, the solution should provide reminder and escalation procedures to alert approvers and to allow higher-level managers or appropriate colleagues to step in.

The system should create a complete audit trail of every action related to approving access requests.



The solution should alert approvers to potential policy violations

Access Approvals	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Assign approvals to business managers and resource owners		
Require multiple approvals (e.g., a manager and a resource owner, or two levels of management)		
Provide approvers with a list or inbox showing all waiting approval requests		
Provide approvers with a detailed view of new access requests		
Alert approvers to potential policy violations (e.g. the same user cannot have permissions to make deposits and reconcile bank statements)		
Approve or reject individual line items in each request		
Option to require a comment for each line item rejected		
Delegate all requests to another manager or resource owner for a specified time period		
Send email notifications of approvals and rejections to requesters		
Optionally send email notifications of approvals and rejections to requesters' managers and other interested parties		
Send email reminders of pending requests to approvers		
Send email notifications to approvers' manager if no action taken after a specified time (e.g. no action 2 days after the request)		

Access Approvals	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Escalate approval to approvers' manager if no action taken after a specified time (e.g. no action 3 days after the request)		
Create a complete audit trail of all actions related to access requests		
Overall assessment for Access Approvals		

Comments:

ACCESS CERTIFICATIONS

Primary participants: Business managers, resource owners and auditors

An Identity and Access Governance solution should make it easy to initiate certifications, and should provide simple, efficient processes for business managers and resource owners to perform them.

In this context “resource owners” are line-of-business and IT staff responsible for managing access to applications, databases and IT services.

The solution should be able to support both comprehensive certification efforts (e.g., certifying access for all members of a department) and micro-certifications (certifying access for a single employee after a policy violation is detected).

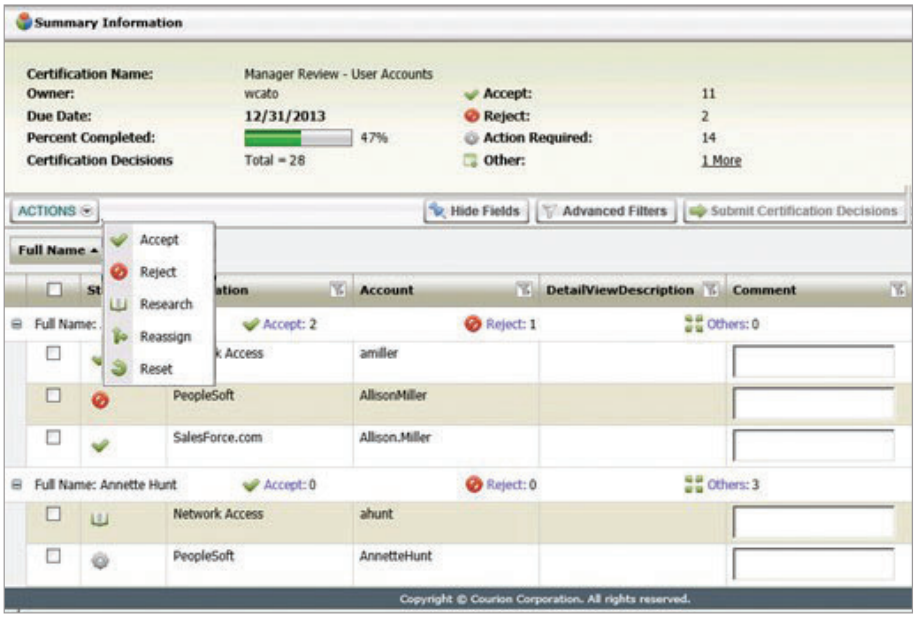
Certifiers should be able to assess exactly what access is available to current users. They should be able to accept and reject individual instances of access rights, perform additional research, and reassign certifications to another appropriate manager or resource owner.

The system should give certifiers visibility into issues like excessive access rights and the violation of separation of duties and other policies.

To allow certifiers to process dozens or hundreds of decisions efficiently, the solution should provide an intuitive interface and features to allow decisions to be applied to multiple requests in one step.

The solution should provide reminder, escalation and delegation procedures to alert certifiers and to allow higher-level managers or appropriate colleagues to step in.

The system should create a complete audit trail of every action related to certification processes.



Certifiers should be able to accept and reject permissions, perform additional research, and reassign certifications to others

Access Certifications	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Initiate certification reviews manually		
Initiate certification reviews based on events (e.g. identification of policy violations)		
Provide certifiers with a list or inbox showing all waiting certification requests		
Provide certifiers with a detailed view of current levels of access for each user		
Alert certifiers to potential policy violations (e.g. the same user cannot have permissions to make deposits and reconcile bank statements)		
Approve or reject individual line items in each certification		
Option to require a comment for each line item rejected		
Give certifications a “Research” status if investigation is required		
Reassign individual certifications to another manager or resource owner		
Delegate all certifications to another manager or resource owner for a specified time period		
Give each certifier a dashboard showing total number of certifications completed and outstanding, in total and broken down by certification type		
Show each certifier the total number of certifications he or she has accepted and rejected, and the number accepted and rejected for each user, each role, and each application or resource		
Send email notifications of certification results to users		
Optionally send email notifications of certification results to managers and other interested parties		

Access Certifications	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Send email reminders to certifiers of incomplete certifications		
Send email notifications to certifiers' manager if no action taken after a specified time		
Escalate approval to certifiers' manager if no action taken after a specified time		
Create a complete audit trail of all actions related to certifications		
Overall assessment for Access Certifications		

Comments:

AUDITS AND COMPLIANCE ANALYSIS

Primary participants: Auditors, compliance officers and risk managers

An Identity and Access Governance solution should capture every action related to creating, defining, modifying and deleting roles, to requesting and approving access, and to certifying permissions.

Standard reports should show actions related to access requests and approvals and certification reviews.

It should be easy to export all of this data to spreadsheets, databases, reporting tools and other systems so that auditors and compliance officers can use the information to verify compliance with regulations and corporate policies.

An Identity and Access Governance solution should also go beyond basic reporting by incorporating intelligent analytics. For example, an organization should be able to look at activity for accounts that are certified but have no log-ins or activity. They should be able to improve risk assessment, for example by determining which orphan accounts represent the highest risk and need to be addressed first. Analytics can also be used for better trend analysis, for uncovering subtle policy violations, and for tracking the organization's overall compliance posture. Capabilities like these are covered in the "Identity and Access Intelligence" section of this guide.

Audits and Compliance Analysis	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Capture all actions related to creating, defining, modifying and deleting roles, and for approving modifications to roles		
Capture all actions related to requesting access and approving access requests, including reassigning and delegating approvals		
Capture all actions related to certifications, including initiating certifications and approving and rejecting permissions		
Capture all identified policy violations		
Capture all data needed to support audits related to SOX, GLBA, HIPAA, PCI DSS, UK Data Protection Act and other government regulations and industry standards		
Capture data showing performance against key metrics (e.g. time to disable accounts of terminated employees, percentage of permissions certified quarterly)		
Reports showing access request and approval actions		
Reports showing access requests and approvals by target system and by resource		
Reports showing access requests and approvals by user accounts		
Reports showing certification review actions and results		
Export data to spreadsheets, databases and reporting tools for analysis and reporting		
Export data to Identity and Access Intelligence tools for data mining and sophisticated analyses		

Audits and Compliance Analysis	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Overall assessment for Audits and Compliance Analysis		

Comments:

IDENTITY AND ACCESS INTELLIGENCE: MONITORING AND ANALYSIS

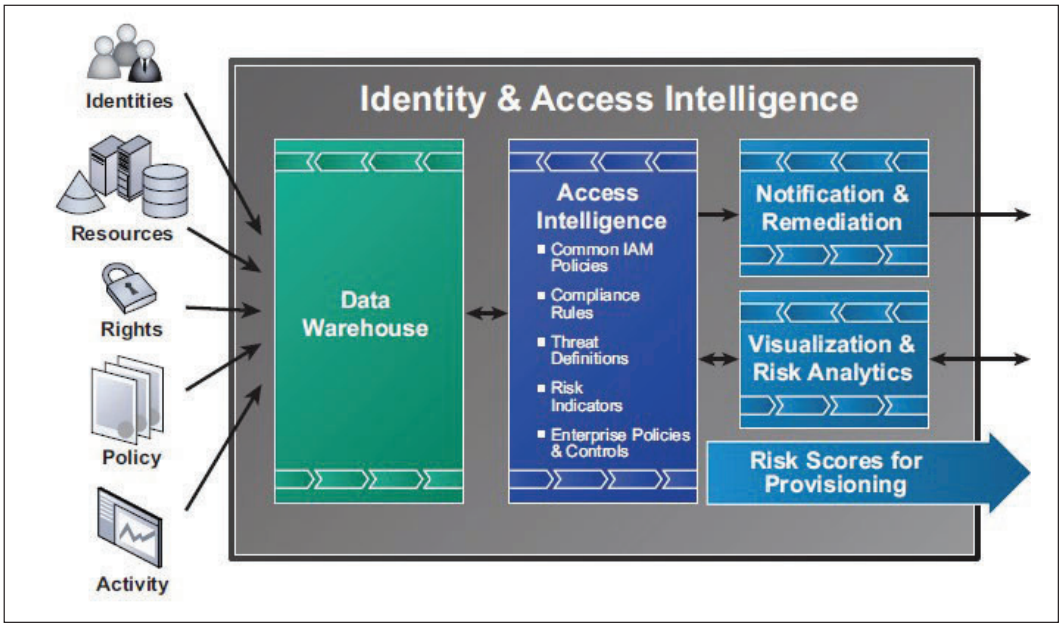
Primary participants: IAM analysts, resource owners, business managers, auditors, compliance officers and IT staff

Identity and Access Intelligence (IAI) goes beyond reporting to add two critical capabilities to Identity and Access Governance solutions:

1. Continuous monitoring, to detect access issues and policy violations quickly (rather than waiting weeks or months for certification reviews).
2. "Big data" and advanced analytic tools to process and interpret massive volumes of identity and access data, to identify vulnerabilities and subtle policy violations.[2]

Identity and Access Intelligence tools can be used by almost all of the individuals discussed in this document.

The basic components of an Identity and Access Intelligence system are shown in the diagram below.



Overview of an Identity and Access Intelligence System

[2] Enterprises today can easily generate billions of data points related to identity management. These include data about identities, resources, rights, policies, and identity and access-related activities. An organization with 1,000 system users, 5,000 user accounts and 1,000 entitlements would need to keep track of 5 billion combinations (1,000 x 5,000 x 1,000), and that figure doesn't include actions performed by those users. Identity and Access Intelligence solutions need data warehousing tools to process those volumes of information, and business intelligence and data visualization tools to help pinpoint meaningful details. For more information see the Courion white paper *Identity and Access Intelligence: How Big Data and Risk Analytics Will Revolutionize IAM.*

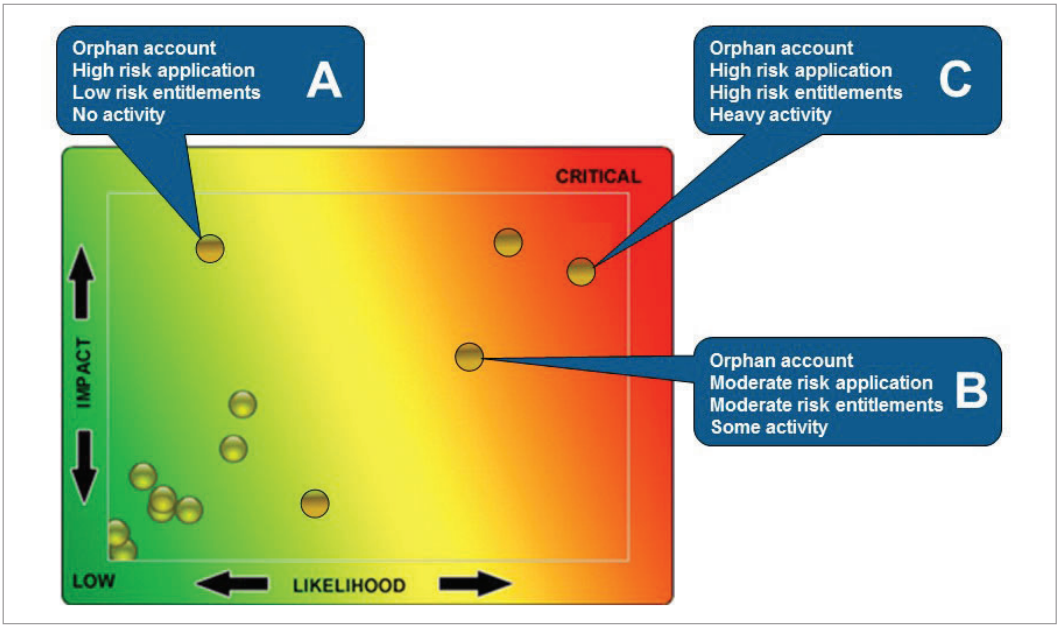
Many types of identity and access-related data from many types of systems and devices are collected continuously in a data warehouse. This data is analyzed with reference to policies, compliance rules, threat definitions, and risk indicators.

When issues and policy violations are identified, either they are automatically remediated, or relevant managers and resource owners are alerted so they can take action.

Sophisticated data visualization and risk analytic tools can be used to find patterns in complex data, identify vulnerabilities, and pinpoint policy violations. With conventional reporting tools, many of these would remain hidden, or would have been detected only after incidents had already occurred.

An Identity and Access Intelligence system can make it much easier to uncover vulnerabilities and risk factors like:

- Orphan accounts
- Rights granted via inherited permissions and nested groups
- Individuals whose access rights significantly exceed norms for people in their jobs
- Abnormal numbers of rights granted by exception, or outside the approved corporate workflow



Advanced analytic tools like heat maps help users uncover subtle policy violations and correctly prioritize risks

Data visualization tools can help viewers assess what issues should be the highest priority based on multiple criteria. In the "heat map" example on this page, an automated analysis shows that orphan accounts B and C should be addressed before orphan account A. Although account A involves the highest-risk application, accounts B and C involve higher-risk entitlements and more activity, and therefore represent more serious risks that should be addressed first. It would be extremely difficult, if not impossible, to attain this insight with conventional reports.

Additional uses of Identity and Access Intelligence tools include:

- Alerting security analysts, anti-fraud groups and incident response teams to "privilege escalation" and other symptoms of persistent threats and other attacks.
- Tracking positive and negative trends.
- Analyzing massive amounts of identity and access data against policies and company-defined models of activity patterns.
- Performing "what-if" analysis of the impact of policy changes.

Identity and Access Intelligence tools can be a critical part of provisioning as well as Identity and Access Governance solutions, but here we will focus on uses for governance.

Identity and Access Intelligence	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Provide out of the box connectors and collectors to gather data continuously from enterprise directories, governance solutions, policy creation tools, security products and other data sources		
Gather information from sources of unstructured data (e.g. file shares) as well as sources of structured data (data bases)		
Provide ETL (extract, transform and load) and data warehouse tools to transform information from disparate systems into a common format so it can be correlated and analyzed		
Provide “Big data” business analysis capabilities to correlate millions or billions of identity-resource-permission relationships		
Detect orphan accounts		
Detect violations of Separation of Duties (SoD) policies		
Detect individuals with permissions associated with former positions		
Detect factors associated with vulnerabilities, such as shared passwords, weak passwords and very old accounts		
Detect rights granted through exceptions or outside the approved workflow (“out of band”) and trigger reviews by resource owners		
Detect excessive numbers of accounts or permissions granted by an administrator or other privileged user		
Detect individuals with rights in excess of those in the same department or with similar roles		
Detect rights granted via inherited permissions and nested groups		
Detect risk indicators, such as privileged accounts created and deleted within a short period, or multiple failed logins followed by a successful login		

Identity and Access Intelligence	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	**Option X**
Provide graphs and reports to highlight sources of risk (e.g. individuals who deviate from group norms or cause the most policy violations)		
Provide heat maps and other analysis and visualization tools to identify high-risk and recurring policy violations		
Automatically initiate de-provisioning actions when dangerous activities are detected		
Automatically initiate certifications when suspicious activities or permissions are detected		
Automatically initiate certifications when risk levels change		
Alert administrators, managers and compliance officers when policy violations are detected		
Alert administrators, managers and compliance officers to “privilege escalation” and other symptoms of persistent threats and other attacks		
Track positive and negative trends in access requests and policy violations		
Performing “what-if” analyses of the impact of changes (e.g. the number of people or accounts that would be affected by modifying a policy)		
Overall assessment for Identity and Access Intelligence		

Comments:

SOLUTION DEPLOYMENT AND INTEGRATION

Primary participants: IT Staff (administrators, operations, applications, etc.)

An IT organization should be able to deploy an Identity and Access Governance solution in a short time frame, without needing to install complex new infrastructure or acquire new skills. Fast deployment lowers implementation costs and starts generating value for the enterprise sooner.

Ongoing administration should be straightforward, to minimize the burden on the IT staff.

Identity and Access Management systems need to interact with a wide variety of external systems, to share information about users, roles, access activities, security events and other data. Do-it-yourself integrations with these systems can be very costly to code and maintain, and working on them can delay implementation. Therefore it is very advantageous if the solution can be integrated with a very wide range of systems and applications using out-of-the-box connectors supported by the vendor.

There should also be tools to facilitate the rapid development of custom connectors when out-of-the-box solutions are not available.

Solution Deployment and Integration	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Intuitive tools for installation and configuration		
Little or no requirement for programming skills to install and configure		
Run on industry-standard web and application servers so no specialized installation or management skills are required		
Lightweight infrastructure (e.g. no need to install middleware or an enterprise directory)		
Ability to extend the database schema of the solution to hold additional types of information from integrated systems such as business applications and security products		
Modular design – solution modules can be deployed in whatever order provides the quickest benefit to the business		
Out-of-the box connectors to enterprise directories and access control systems (e.g. Microsoft Active Directory, LDAP, Open LDAP, IBM RACF, Sun Directory Server, CA-ACF2)		
Out-of-the box connectors to systems with industry standard operating systems (e.g. Red Hat Linux, SUSE Linux, IBM AIX, IBM z/OS, HP-UX, Solaris)		
Out-of-the box connectors to business applications (e.g. SAP, PeopleSoft, Oracle E-Business Suite)		
Out-of-the box connectors to databases and collaboration products (e.g. SQL, MySQL, Oracle Database, Microsoft Exchange, Novell GroupWise, IBM Lotus)		
Out-of-the box connectors to SIEM, DLP and other security products (e.g. RSA Authentication Manager, RSA SecurID, Citrix SSO, Imprivata OneSign, RSA DLP Suite, RSA enVision, McAfee ePO, Symantec Data Loss Prevention)		

Solution Deployment and Integration	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Rapid development kit (RDK) to integrate the solution with other systems when out-of-the-box connectors are not available.		
Overall assessment for Deployment and Integration		

Comments:

Summary of Assessments by Section	Scoring (Yes/No, High/Med/Low, 1-5 scale, other)	
	Courion	Option X
Role Definition		
Access Requests		
Access Approvals		
Access Certifications		
Audits and Compliance Analysis		
Identity and Access Intelligence: Monitoring and Analysis		
Solution Deployment and Integration		
Overall assessment		

Comments:

APPENDIX: OVERVIEW OF COURION PRODUCTS

Governance

Access Request Manager Courion's access request solution provides intuitive, easy to use processes for authorized users to create, review and approve access requests.

ComplianceCourier® Courion's access certification and compliance management solution provides organizations the ability to automate the verification and remediation of access rights. It extends the responsibility and accountability for compliance to the most appropriate resources, enabling business users to monitor and enforce access to sensitive data and other vital corporate assets. Powerful analysis tools provide a visually rich interface that makes it easier to monitor compliance and reduce enterprise risk.

RoleCourier® Courion's role lifecycle management solution automates role creation and ongoing role management, enabling organizations to effectively align business roles with IT accounts and access rights. RoleCourier's unique hybrid approach combines "top-down" role design and "bottom-up" role mining to create a platform for robust long-term role lifecycle management that flexibly adapts to today's changing business environment.

Identity and Access Intelligence

Access Insight® Courion's Identity and Access Intelligence solution applies predictive analytics to manage business, people, asset and security risks, automatically creating near-real-time graphical profiles of the most critical security risks to information, as part of a total Identity and Access Management strategy.

Provisioning

AccountCourier® Courion's user provisioning solution enables enterprises to fully automate new hire, promotion/transfer and termination processes. With its flexible workflow engine and ability to connect to multiple authoritative sources, AccountCourier provides a common access management environment for both IT accounts and physical assets.

PasswordCourier® Courion's password management solution enforces consistently strong password policies and enables users to instantly and securely reset their own passwords on enterprise systems, applications, and Web portals. Transparent synchronization lets users use one password to access multiple systems, improving convenience, enhancing security, and increasing adoption. Multiple self-service entry points are available, such as Web, desktop PC, voice authentication, IVR, or via support staff.

FOR MORE INFORMATION

For information on these Courion products, please visit **www.courion.com** or contact your Courion representative or reseller.

About Courion

With deep experience and more than 600 customers managing over 10 million identities, Courion is the market leader in Identity and Access Management (IAM), from provisioning to governance to Identity and Access Intelligence (IAI). Courion provides insight from analyzing the big data generated from an organization's identity and access relationships so users can efficiently and accurately provision, identify and minimize risks, and maintain continuous compliance. As a result, IT costs are reduced and audits expedited. With Courion, you can confidently provide open and compliant access to all while also protecting critical company data and assets from unauthorized access. For more information, please visit www.courion.com or read http://blog.courion.com.

World Headquarters
COURION CORPORATION
1900 West Park Drive
Westborough, MA USA 01581
Phone: +1 508-879-8400
Toll-free: 1-866-COURION

APAC
COURION IT PRIVATE LTD
305, Pride Purple Accord,
S. N. 3/6/1 Baner Road,
Pune, Maharashtra, India 411 045
Phone: +91(20) 6687-9100

COURION™