Identity Management and GRC Trends 2009-2019

September 2008

Martin Kuppinger, Sebastian Rohr
Kuppinger Cole
mk@kuppingercole.de

KUPPINGER COLE

Some guidelines for the Webinar

You will be muted centrally – in case that there is background noise please mute yourself. But: Best is to do nothing – we can control the mute/unmute features

We don‘t record the Webinar

Q+A will be at the end – you can ask questions using the Q+A tool anytime which we will pick at the end or, if appropriate, during the Webinar

We plan to provide a short podcast near-time

Trend Report Identity Management and GRC 2009-2019

Available right now:
www.kuppingercole.com/reports

295 € plus VAT if applicable

Free for customers with an annual subscription of Kuppinger Cole Services

Coming soon: Identity Management Roadmap Report (Webinar: Wednesday, October 8th)

Trends 2009-2019

Short term: 2008-2009

- Current developments – what you should consider for implementation in current projects

Mid term: 2009-2012

- What will happen likely – and what you should keep in mind to define and align your projects for compatibility to the upcoming changes

Long term: 2012-2019

- The larger trends which will affect your IT in the area of IAM and GRC – things that probably will happen but might be delayed or (seldomly) be earlier than expected

Some definitions to start…

Governance	•The rules and control of doings things correctly •IT Governance as part of Corporate Governance •SOA Governance as part of IT Governance
Risk Management	•Managing risks •Operational risks, IT risks,… •Risk definition, measurement, management •Ongoing
Compliance	•Fulfilling regulations •„Checklist" approach •Often recurring, at specific points of time
Entitlement Management	•Managing Entitlements, e.g. Authorizations

Areas to observe: Two dimensions

Function

- Administration, managing identities
- Authentication, SSO, strong authentication
- Access, Authorization, Federation
- Auditing, GRC

Scope

- Internal vs. external users
- Internal vs. external IT
- Infrastructure vs. Applications
- Administrative/IT Level vs. Business/C-Level

Function: Administration Mid term (2009-2012)

Major developments

- **Functional (over-)completeness**: There is an obvious trend of building very complex, feature-rich provisioning solutions which provide not only provisioning functionality, but as well password management, GRC features, and others. The advantage of this approach is that customers can use one product and avoid integration. In some cases, an sophisticated object model with a high consistency of features might be an additional advantage. The disadvantages are expecially still missing features and the complexity of these products, besides some potential inflexibility for integration into existing IT environments and reuse of existing functionalities.
- **Service-orientation**: One of today's threats is the management of more than one provisioning solutions especially in larger corporations or after M&A processes. We expect that there will be solutions which use ESBs (Enterprise Service Bus) approaches and a broader bi-directional support for standard interfaces like SPML to integrate multiple provisioning solutions. This approach isn't likely to fully replace IAM solutions in the mid term timeframe.
- **Modularity**: In contrast to the over-complete solutions, at least some vendors will open up their architecture to integrate external workflows, connectors and so on. That will lead to approaches where for example commonly used workflow tools can be used for provisioning as well. These approaches are pretty interesting for large corporations with well-defined IT infrastructures and high reuse of infrastructure elements.
- **Pre-defined processes**: We expect more vendors to provide best-practice workflows with their provisioning solutions, reducing project costs.
- **Identity bus**: At the end of the time frame there will be first implementations of identity bus approaches, with loosely coupled identity stores instead of today's centralized approaches. Identity bus concepts require fundamental changes in the way identity information is consumed by applications thus that will be more sort of a long term change. The claims-based approach proposed by Microsoft might be one way to implement such an Identity Bus.
- **ITSM integration**: ITSM (IT Service Management) integration will be provided first by vendors with a strong ITSM offering. As a result of growing modularity other vendors will ease the integration with ITSM technologies. Given the fact that we expect a business layer with GRC focus as leading for IAM as well as for ITSM we prefer the latter approach of loosely coupling ITSM and IAM instead of ITSM control of IAM. With ITSM control there are significant shortcomings for more complex requirements in the area of auditing and access management.
- **Entitlement management**: Granular control of entitlements in connected systems will be supported by some vendors at least for selected platforms. In addition, there will be specialized vendors providing more sophisticated solutions for externalizing administration, authentication, authorization and auditing out of applications. That will be covered in the Access/Authorization trends.

Function: Administration Mid term (2009-2012)

Replacements of technologies

- We don't expect that any of the currently used technologies will disappear from the market but expect a growth in „classical" provisioning technologies.
- There will be a spread market with new approaches, very feature-rich provisioning tools and more lightweight provisioning solutions promising a faster implementation and reduced project risks.

IT Impact

- IT shall review and analyze the expected changes and ask vendors on their position towards the different approaches. That will reduce the risk of selecting products which don't fit the customer's strategy.
- IT has to define the interfaces of IAM especially towards GRC and towards ITSM.

Business Impact

- The chosen approach significantly affects the ability of IT to support business requirements, as well in SOA support as with respect to the flexibility of IT for changes. Service-oriented approaches are potentially more capable of reflecting large organizational changes. Modular approaches and ITSM integration serve better for a unique approach to implement request and approval workflows for any type of IT and other infrastructure services.

Function: Administration Long term (2012-2019)

Major developments

- Identity bus: The concept of the identity bus will become a core concept of identity management, providing a more flexible use of identities from different sources.
- Virtualization: A consequence of the identity bus will be that the still existing concept of virtualization will gain momentum. Going beyond today's virtual directory services, there will be virtual views using the identity bus. Another trend, which might be visible in some implementations even in the mid term timeframe will be a more complex approach of virtualization with focus not only on identities but as well on services and other context information.
- Increasing modularity and service orientation: We expect the trend towards modularity and service orientation to become more significant. Products will be split up in functional components supporting the replacement of different parts like the workflow engine, while there will still exist tightly integrated, easy-to-implement products with main focus on the medium-sized businesses. This trend will be supported by a growing number of maturing standards.
- Connector specialists: The trend towards modularity and service orientation together with a broader acceptance of standards like SPML might lead to a market in which some of the vendors focus on their knowledge in building connectors to target systems, providing a much broader range of connectors and a higher degree of connector functionality. On the other hand, there will be more and more standard functionality provided by target systems to integrate with provisioning systems and the identity bus, thus this market segment won't sustain for long. In any case, the ability for granular management of entitlements in the target systems will become standard.
- GRC alignment, business control: The trend towards business control and GRC alignment of identity management, e.g. deriving entitlements from business roles and rules, using a higher degree of automation at today's provisioning layer, will become dominant. That will consequently limit the role of request and approval workflows at today's provisioning layer.
- Master Data Management: For the situations in which virtualized approaches are not suited best there will be a trend towards Master Data Management (MDM), using connectors and standards like SPML for integrating and normalizing identity data out of different sources.

Function: Administration Long term (2012-2019)

Replacements of technologies

- „Classical" provisioning tools: The evolution of Identity Management towards a stronger GRC control layer will lead to a situation where provisioning tools, even with GRC features, will become mainly relevant for the medium-sized business, whilst the relevance in larger corporations will diminish over time. In larger corporations, todays feature-rich, complex provisioning solutions are likely to be replaced by modular, multi-layer approaches with strong use of services and standards at least in the latter part of the time frame.
- Meta Directory technologies: Meta directory services will still be provided by many provisioning tools, but there won't be a market for meta directory tools any more. Even more, the more complex and specific requirements in this area will be overtaken by existing MDM technologies especially in larger organizations.
- Directory technologies: The growing role of standards and approaches like Identity bus and Virtualization will lead to a more distributed approach for storing identity information. In that approach other systems like business systems and databases are more likely to become identity stores instead of today's directories. There will be a market for directories, but with even lower strategic relevance than today. A trend towards integrated virtualization features and service-oriented interfaces in directories might slow down that decrease in relevance.

Function: Authentication Short term (2008-2009)

Status and Changes

- username/password-based authentication is still standard.
- significant growth of Single Sign-On, especially Enterprise SSO.
- versatile authentication (flexible exchange)
- biometrics still weak, will remain in short-term timeframe.
- soft tokens become increasingly

IT Impact

- Single Sign-On has reached a high degree of maturity.
- E-SSO easier to implement.
- strategies for strong authentication, contextual and versatile authentication

Business Impact

- limited to a higher degree of user satisfaction + easy-to-use technologies
- potentially reduced service desk costs
- great potential for improvements in managing risks

Function: Authentication
Mid term (2009-2012)

Major developments

- Context-based authentication
- Versatile authentication: will become standard,
- Federated authentication: a major element of auth strategy
- Online identity providers:
  more due to relevance of federated authentication,
- Soft tokens: will be enhanced
  for strong online businesses authentication

Function: Authentication
Mid term (2009-2012)

Replacements of technologies	•soft-tokens will replace most non-established approaches •classical smartcards: will be replaced by more flexible approaches
IT Impact	•Vendor selection: rate vendors with focus on concepts of context-based authentication •Strong online authentication: will become a realistic opportunity •Strong and flexible authentication: IT has to support this!
Business Impact	•Risk management: most relevant Authentication can be granted based on the risks identified

Function: Access/Authorization Short term (2008-2009)

Description

- Access and Authorization deals with providing access to information for authenticated users. That includes the area of federation as an approach which separates administration and authentication from authorization. Thus federation is covered as well from the authentication as authorization perspective in this report.

Status and Changes

- Convergence of Web Access Management and Federation: The current trend to integrate federation functionalities in web access management solutions will remain strong. We expect that federation vendors will either become acquired or provide more advanced web access management features in their products whilst web access management vendors will increase their federation support and eventually will integrate separate federation products.
- Entitlement Management: The management of entitlements, e.g. authorizations on the system level, will become more important but with a limited support for target systems and a limited granularity in the short-term period.
- Network-based access management: Some few vendors start to provide access control functionality on the network layer. There might be some more offerings and a broader recognition of these approaches, even while we don't consider them to be strategic at that point of time.
- Privileged account management: Even while this can be discussed as well in the context of administration or authentication, we observe this trend mainly as an access management issue, providing controlled access to privileged functions in systems. There is a strong pressure with many specialized vendors providing point solutions. We expect a significant increase in this market.
- SOA Security: The awareness of SOA security will increase significantly, but will be adressed at the beginning mainly with additional layers providing by SOA security solutions. We don't recommend that approach but prefer more tightly integrated approaches, but consider them to be valid for current implementations due to the leak of a broad availability of more comprehensive technologies which provide end-to-end security.

Function: Access/Authorization Short term (2008-2009)

IT Impact

- Layered approach: With new approaches like federation and network-based access management and IRM at least at the horizon IT organizations have to rethink their access management strategies, focusing on a layered approach which consists of few managed layers (firewalls, access controls at system level, network level authorization,…) and a clear definition of which of these approaches shall be used for which use cases and application types.
- Federation strategy: A federation strategy which includes the user-centric approaches has to be defined. This especially has to address the application development, providing federation-ready applications.
- SOA Governance and security: A strategy for governing SOA applications and a consistent approach for SOA security has to be defined. That includes the definition of application security infrastructures and a strategy for externalizing administration, authentication, and authorization out of the application code.

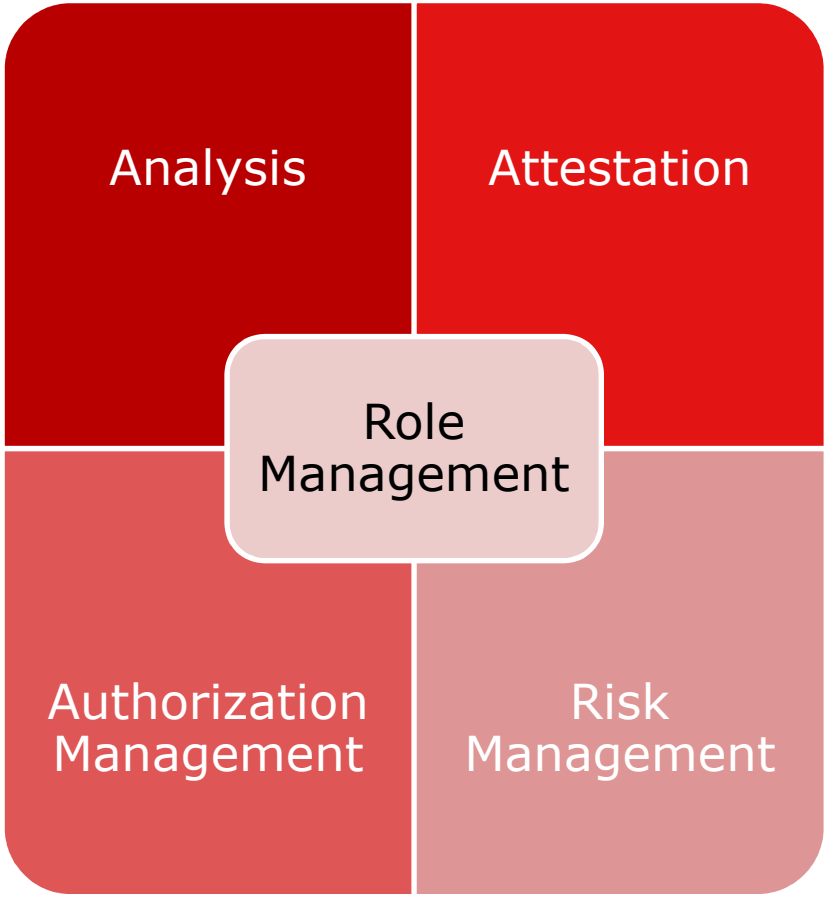
Function: Access/Authorization Mid term (2009-2012)

Major developments

- Fine-grain Entitlement Management: signifcant improvements stronger standards support and mature implementations
- Claims-based approaches:
  approach to become important in the context of the identity bus
- Integrated privileged account management:
  will become a standard feature
- Fine-grain service authorization:
  A granular service authorization will become more frequent
- Context-based authorization:
  decides per application or even per application feature whether access is granted
- Externalization:
  will gain momentum significantly

GRC:
Business Control for IAM

- The new, evolving GRC market segment
- That‘s were many of today‘s tools fit in
- GRC – the layer above today‘s IAM
- But: No successful GRC without strong IAM foundation

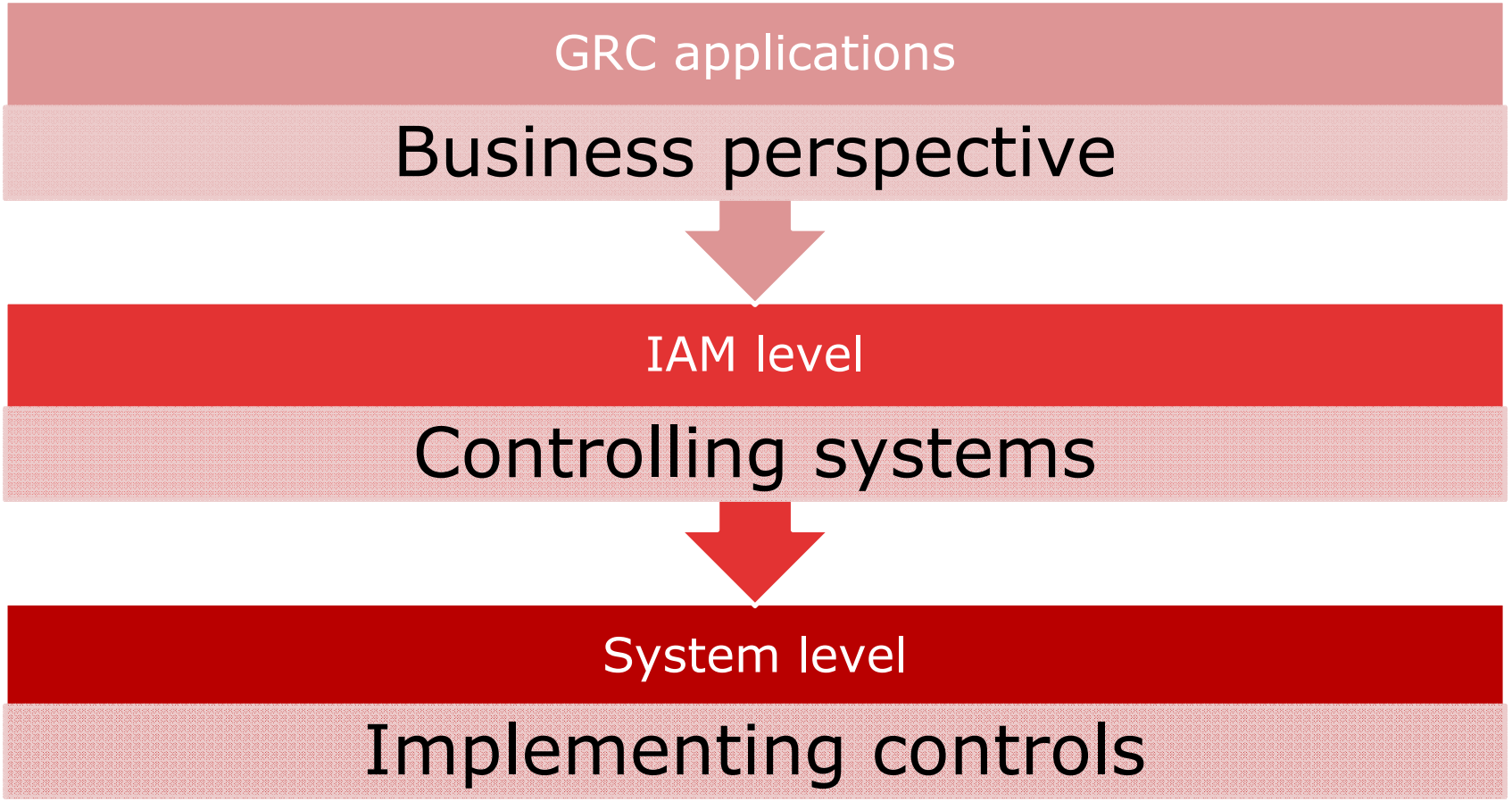


Function: Auditing/GRC Mid term (2009-2012)

Major developments

- GRC/SIEM integration: The integration of IT GRC and SIEM will take place over time, given the fact that a complete IT risk management and auditing/analysis requires a complete view, including security information and events. In the mid-term time frame that might be done mainly by building suites with some degree of integration, but we expect to observe some fully integrated products.
- Auditing/GRC standards: The current lack of standards in Auditing and GRC will be adressed. Current initiatives like for Role exchange standards will provide results, additional initiatives for example for audit log interface standardization are likely to happen. By the end of the mid-term time frame we expect a significant number of standards for interoperability with the different elements in a GRC framework.
- Maturity of GRC solutions: GRC solutions, as well for IT GRC as Enterprise GRC, will become more mature, providing a pretty complete set of functionalities at least delivered by some few of the vendors. Features like comprehensive access control databases which provide detailed historical information about access control down to the system level will be part of some offerings.
- Integration between enterprise and IT GRC: There will be more advanced, probably somewhat standardized integration points between IT GRC and the business-level, e.g. Enterprise GRC.
- Tighter integration with provisioning solutions: IT GRC solutions will provide tighter integration with provisioning solutions, having the provisioning systems act as tool for interfacing the target systems. That will lead to a higher degree of business control and less control provided at the provisioning layer.
- Platform approach: In general we expect that there will be a trend towards a platform approach for GRC, making point solutions for specific regulations or specific requirements like attestation obsolete.

Layered approach



Scope:
Internal vs. external users

Short-term (2008-2009):

- Threat of managing internal and external users is understood whilst many of the technologies in place doesn't support this in a sufficient manner.
- Federation technologies and Web Access Management in combination with Virtual Directory Services appear to be the preferred approach for short-term solutions.

Mid-term (2009-2012):

- The perimeter will slightly disappear, with more and more business processes integrating business partners and customers. IT has to reflect this change.
- Flexible approaches like Federation together with user-centric technologies and the support of external Identity Providers will gain momentum.
- There will be a growing number of offerings for managed identity services, with focus on external users.
- The concept of the Identity Bus and a stronger virtualization of digital identities will add to this.

Long-term (2012-2019):

- Exchangeable, cross-platform and cross-organization authorization policies will add to this.
- Several technologies like strong mobile authentication, context-based authentication and authorization and Identity Bus plus claims will be in place supporting all types of use cases for internal and external users in a consistent manner.

Events 2008/2009

Governance, Risk & Compliance Forum 2008
November 18/19, 2008, Frankfurt / Germany

Enterprise Identity Management Best Practices
November 26/27, 2008, Munich / Germany

SOA Governance Best Practices
October 13, 2008, Stuttgart / Germany

Outsourcing Strategies, SaaS & Cloud Computing
October 14, 2008, Stuttgart / Germany

Eurasia Identity Management Conference 2009
February 11 – 13, 2009, Istanbul / Turkey

European Identity Conference 2009
May 5 – 8, 2009, Munich / Germany

Contact: bb@kuppingercole.com

More about the IAM and GRC Trends

Report

- 295 € plus VAT if applicable
- Available for annual contract customers

Individual analyst briefings

- Individual briefings (pay-per-use) – contact sales@kuppingercole.com
- Free for annual contract customers depending on contract type

Individual Consulting, Research, and Evaluation

IAM Strategic Advice package – contact sales@kuppingercole.com

Other services included in the annual contracts

- Monthly newsletter, 16 pages, PDF with briefing
- Event tickets and more…

Questions and Answers

Ask your questions

Enter them into the Webinar tool

We will unmute you when picking your question