

Future proof IAM and GRC Optimizing your investments

Martin Kuppinger, Kuppinger Cole
mk@kuppingercole.com

May 5th, 2009

Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

10 Top Trends 2009

GRC as the
Business
Control Layer
for IAM

Growing
Maturity of
Identity 2.0
Approaches

Multi-purpose
Cards gain
Momentum

Context and
Versatility
become Reality

More IAM and
GRC for the
Cloud

Portable
Identity
Information for
Social Networks

GRC going
beyond IAM

First Impacts of
new Electronic
Passports/ID
cards

Increasing
Service
Orientation in
IAM and GRC

Privacy is back
– and there are
more Solutions

Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

Observations 2008

GRC

GRC became a core topic

The need for a platform approach, beyond point solutions, is more and more understood

IAM-GRC as core market segment

Attestation and SoD policies, controlled by roles, as major approach

Risk management support still missing

Observations 2008

IaaS, Cloud, Metasystem,...

Still few offerings for IaaS, but some new providers in the market

Increasing support at least for SAML by SaaS providers

Clear trend towards using „cloud“ services

Identity Metasystem, claims, and user-centric becoming more prominent – but still pretty immature

Federation still a slow growing market – but it isn't a technical issue anymore

Observations 2008

Authorization Management

Authorization Management understood as a threat – the ACL level is too complex to manage

SharePoint Security (access controls) as a specific field, strong increase

New approaches for managing authorizations are appearing – network-level, externalization of authorization decisions,...

GRC authorization management as a trend

Observations 2008

Market

Market situation

- Many vendors were extremely successful, impressive growth rates – even in the last few quarters
- Many new vendors appeared
- Some interesting acquisitions
- GRC vendors with biggest growth rates

Market approaches

- GRC as entry point
- First vendors with focus on easy-to-use, quick-start solutions with focus on mid-sized business (500 to 5000 IT workers)

Expectations 2009

Market

No one really knows ☹️

Currently, the IAM and GRC markets appear to be still solid

GRC initiatives are inevitable – not „even“, but „especially“ in the crisis

We expect an increasing number of service offerings (IaaS, Cloud)

Expectations 2009

GRC

Integrated Risk Management:
Understanding that IT risks and
operational risk can't be managed
separately

Moving beyond IAM-GRC: GRC
platforms start to support more than
IAM controls

Expectations 2009

„Classical“ IAM

More GRC features

Some new vendors with strongly service-oriented approaches to appear, focus on workflows

Some vendors will move towards access policy management as core feature

Expectations 2009

Application Security

Externalization will gain momentum

„Geneva“ and related approaches (e.g. STS, claims,... from other vendors and for other platforms) will become popular rapidly

Vendors will start to rethink their authorization approaches at the application level

Expectations 2009

Identities in the cloud

More offerings to be expected – IaaS with provisioning, strong authentication, federation brokers, SSO for SaaS, and more

More support for externalization of IAM (not GRC yet) in SaaS offerings

First strategies for the cloud will be built – how to manage identities and access in an environment where services might be moved to the cloud, to other providers, or back and where users are increasingly mobile?

Key initiatives in IAM and GRC

Build on what you have...

GRC: Implement the business control layer for IAM – and more (with „more“ maybe in the future, but part of the concept)

Authorization: Define an authorization strategy

Cloud: Define your strategy for an IT world with no clear borders between internal and external IT

Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

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

Short term (2008-2009)

Description

- Administration focuses on the management and storage of identity information

Status and Changes

- Currently specific directory technologies are mainly used for storing identity data, whilst the management is done using local interfaces of these tool, specific tools for directory management, and structured, process oriented approaches based on identity provisioning technologies.
- There will be no significant short-term changes, even while provisioning will become more important even in medium-size companies. The more fundamental changes discussed in the mid-term view will take place only in selected early-starter companies.
- There are, at least with the release of Microsoft ILM 2, no more pure meta-directory products on the market. All product with a history as meta-directory service (e.g. synchronization) functionality now support provisioning features like workflows, whilst any provisioning product can be used to create meta directories (e.g. centralized, combined identity data stores).

Function: Administration

Short term (2008-2009)

IT Impact

- IT shall especially focus on the mid-term trends because they will influence the way provisioning is done today. There is no direct IT impact by short term trends.

Business Impact

- No significant business impact.

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.

Function: Administration

Long term (2012-2019)

Major developments

- 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, today's 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: Administration

Long term (2012-2019)

IT Impact

- Reuse: IT shall focus on the reuse of technologies like MDM, eventually connectors, and workflow engines. That allows an easier IT management. Workflows, for example, might be managed by existing Business Process Management tools and methodologies. That is important in the context of IT Governance, because managing many things in a consistent way provides a higher degree of control.
- Structurization of infrastructure: Given these changes, a clear structure of the IT infrastructure with defined roles for GRC, ITSM, and other elements is required. That has to include application architecture and development, because especially the concept of the identity bus will influence SOA security significantly.
- Strategic approach: Companies have to decide on a strategic approach. Whilst the focus on modularity, reuse and a GRC control layer is relevant to larger organizations as well as companies in heavily regulated industries, the medium-sized business will probably focus more on integrated solutions which provide GRC and provisioning functionality and which aren't too complex.

Business Impact

- Increased business control: The overall trend is a stronger business control, automating business rules and roles down to the entitlement level. Thus, changes in business will be reflected immediately by changes in the target systems.
- Business agility: The concepts of the identity bus and of virtualization will greatly enhance business agility, enabling a fast integration of new internal and external identities in a managed way.

Function: Authentication

Long term (2012-2019)

Major developments

- Federation as standard: Federation will become the standard approach for authentication, splitting up between authenticating systems (Identity Providers) and relying systems (Service Providers). Identity Providers will have to provide strong and flexible authentication approaches.
- Strong mobile authentication: Even while there will be more mobile devices supporting strong authentication even in the short-term and mid-term period, we expect a strong increase and strong authentication support becoming standard for mobile devices not before 2012-2014.
- Context-based and versatile as standard: The trend towards context-based and versatile authentication will lead to mature solutions, becoming standards around the beginning of the long-term time frame.

Replacements of technologies

- Existing strong standard authentication technologies: We don't expect a replacement of established technologies like OTP (One Time Password) or Smartcards but a diminishing strategic relevance in the context of versatile authentication approaches, because up then different technologies can be used for different types of devices, user groups and use cases. The focal point will be the authentication platform instead of a singular authentication technology.
- Existing SSO technologies: Existing SSO technologies will remain important even while federation will become dominant, because they will be used to support existing legacy applications without federation support.
- Kerberos: Kerberos might become less relevant even in Intranet environments with federation as the more flexible approach, which can be easily used as well beyond the perimeter of an organization.

Function: Authentication

Long term (2012-2019)

IT Impact

- Platform approach: The approach of flexible authentication platforms with support as well for context information as for versatile authentication and thus the flexible use of different authentication technologies.
- Federation as core approach: Federation shall be used as standard approach, dividing authentication and authorization. Investments in other approaches are considered to be tactical, not strategic.

Business Impact

- Business agility: Any of these changes will enhance business agility by providing the ability to integrate any group of internal and external users in a controlled manner, supporting strong authentication technologies.
- Risk management: Using strong authentication in a flexible way as well supports risk-oriented approaches for building business applications.

Function: Access/Authorization

Long term (2012-2019)

Major developments

- Information rights management standardization: The current lack of standards for interoperability of different IRM implementations and easy implementation of IRM functionality in applications will be solved. We expect standard initiatives in the mid-term time frame but broad scale adoption to happen not before 2012-2014. Given these changes, IRM will become a standard approach of access management and will at least partially replace system-level ACLs which address access management only for stored information in specific systems.
- Full federation support in SOA infrastructures: SOA infrastructures will provide full federation support, probably implement as feature of containers and available for any single web service. Thus, a granular authorization within web services will become much easier to implement than it is today.
- Policy-based business-driven entitlement management: Entitlement management will become fully policy-based and business-driven, improving the ability to manage entitlements using business rules, roles and other business-related controls.

Function: Access/Authorization

Long term (2012-2019)

Major developments

- Distributed authorization policies: Beyond XACML as a basic standard we will observe a trend towards distributed authorization policies which can be used across systems. That will ease a consistent entitlement management for heterogeneous applications as well as a consistent management across the boundaries of organizations.
- Standards and system-level functionality for privileged account management: Privileged Account Management will be part of operating systems as well as other systems, eventually based on new standards. Ancient concepts like root accounts will probably be replaced in next-generation systems.
- Granular context-based authorizations: Context-based authorization will become more granular, with integration features to applications allowing a fine-grain control about what can be accessed from which context.

Function: Access/Authorization

Long term (2012-2019)

Replacements of technologies

- System-level ACL management: Today's system-level ACL management where a large part of IT administration efforts is spent will be replaced in large parts by higher-level controls and IRM. That has to be considered when defining access management strategies.
- SOA security solutions: We expect that standalone SOA security solutions will be replaced at least at the end of the long-term time frame by integrated security support and end-to-end security in SOA infrastructures, even while they will be in place for a long term for – at the end of the time frame – then legacy SOA applications with outdated security concepts.
- Stand-alone privileged account management: Stand-alone solutions for privileged account management will be replaced by functionality integrated in provisioning solutions and especially provided at the system level.

Function: Access/Authorization

Long term (2012-2019)

IT Impact

- Focus on business control: Business control of entitlements is a major trend. Thus, investments shall focus on this instead of point solutions which might be outdated within a relatively short period of time.
- Consistent access control approaches: The ability to implement consistent access controls at few layers will increase significantly. These approaches shall be implemented, providing a better manageability and a higher level of control.
- Distributed authorization management: In that context, distributed authorization management will become reality, with policies which can be used across different heterogeneous systems as well as a broad support for business-driven entitlement management.

Business Impact

- Risk management: A consistent strategy for access control and authorization provides tighter, consistent manageability and auditability of information access, thus providing the basis for reducing business and IT risks.
- Business control and agility: Approaches which will work in centralized environments allow faster adoption of security settings in target systems, thus supporting a fast reaction to changes in business requirements.

Function: Auditing/GRC

Long term (2012-2019)

Major developments

- Maturity: With the major developments likely to occur in the mid-term time frame, the longer term evolution will mainly build upon this, providing more mature solutions. We don't observe entirely new trends in the long term timeframe.
- Tighter integration: In all areas, e.g. IT GRC/SIEM or IT GRC/Enterprise GRC, we will observe tighter integration of different offerings.
- Operations management and risk management: It is likely that there will be a tighter integration of operations management and risk management, with risk management invoking operations management tools in the case of detected risks.

Replacements of technologies

- SIEM and BSM GRC approaches: The expected integration of SIEM into IT GRC and the role of GRC as controlling layer above the entire IT infrastructure will lead to replacements of existing, limited SIEM and BSM GRC approaches. Overall platform approaches appear as a more valid strategy.

Function: Auditing/GRC

Long term (2012-2019)

IT Impact

- Focus on business control: Business control of entitlements is a major trend. Thus, investments shall focus on this instead of point solutions which might be outdated within a relatively short period of time.
- Platform approaches: Platform approaches will be at the center of GRC solutions, thus decisions have to be made for the choice of platforms. That should keep in mind that GRC should address the entire IT infrastructure and not be limited to specific parts like ITSM or core business systems like ERP.
- Layered approach: We expect a layered approach with Enterprise/IT GRC as control infrastructure above the IT infrastructure layer, moving many controls to the higher level and more automation at the infrastructure level.

Business Impact

- Again, the business impact will be the same as in the short-term and mid-term time frames.

Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

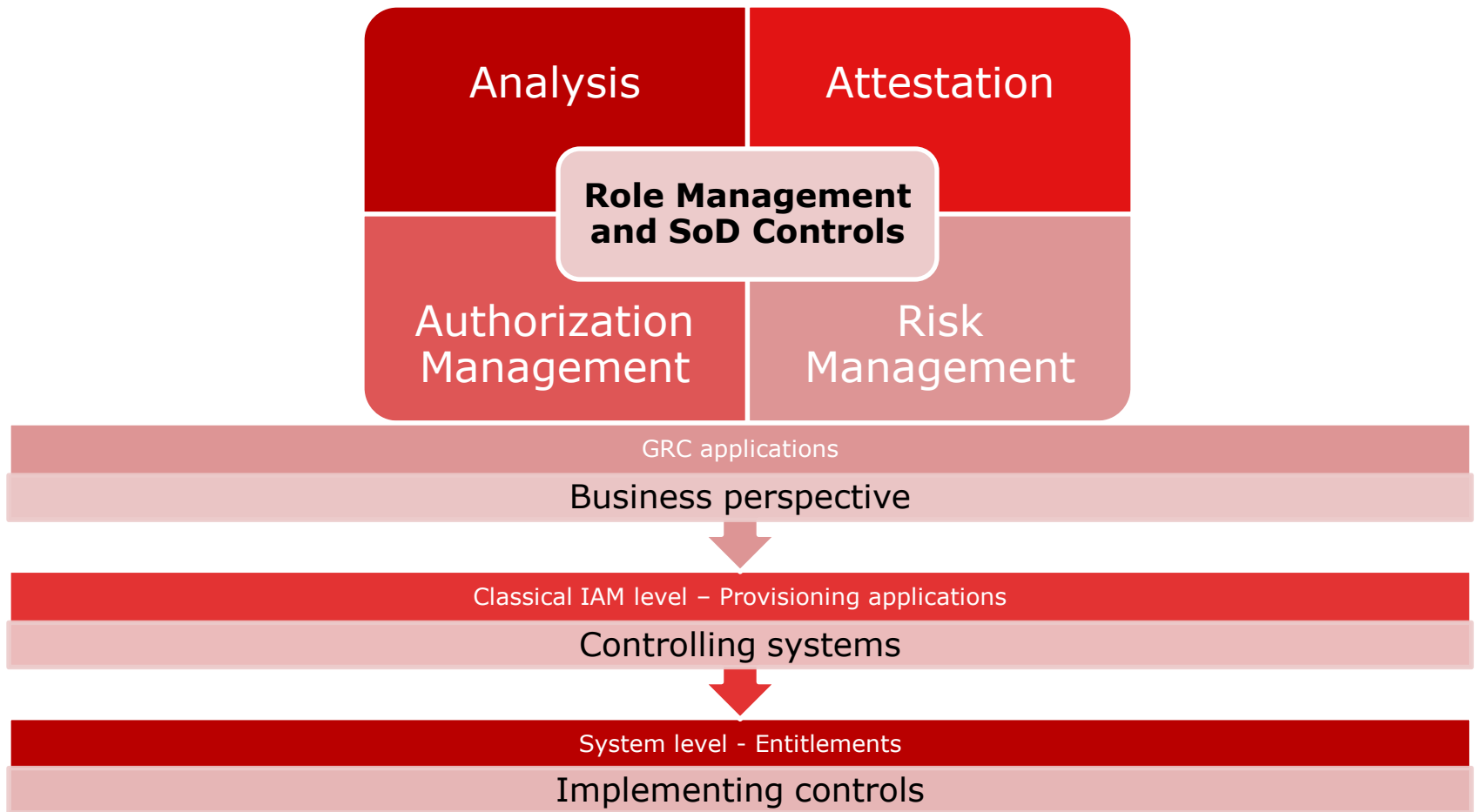
The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

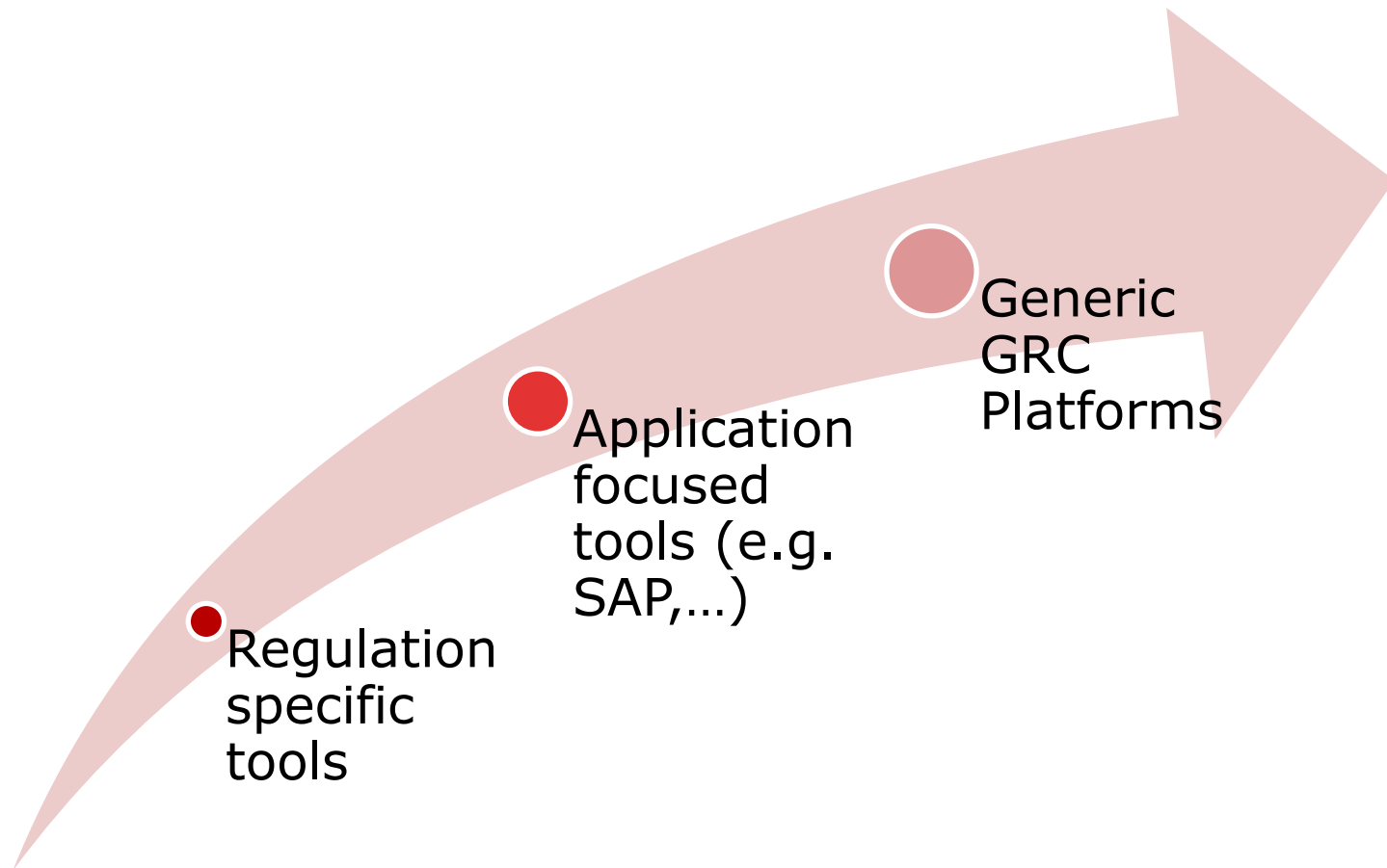
IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

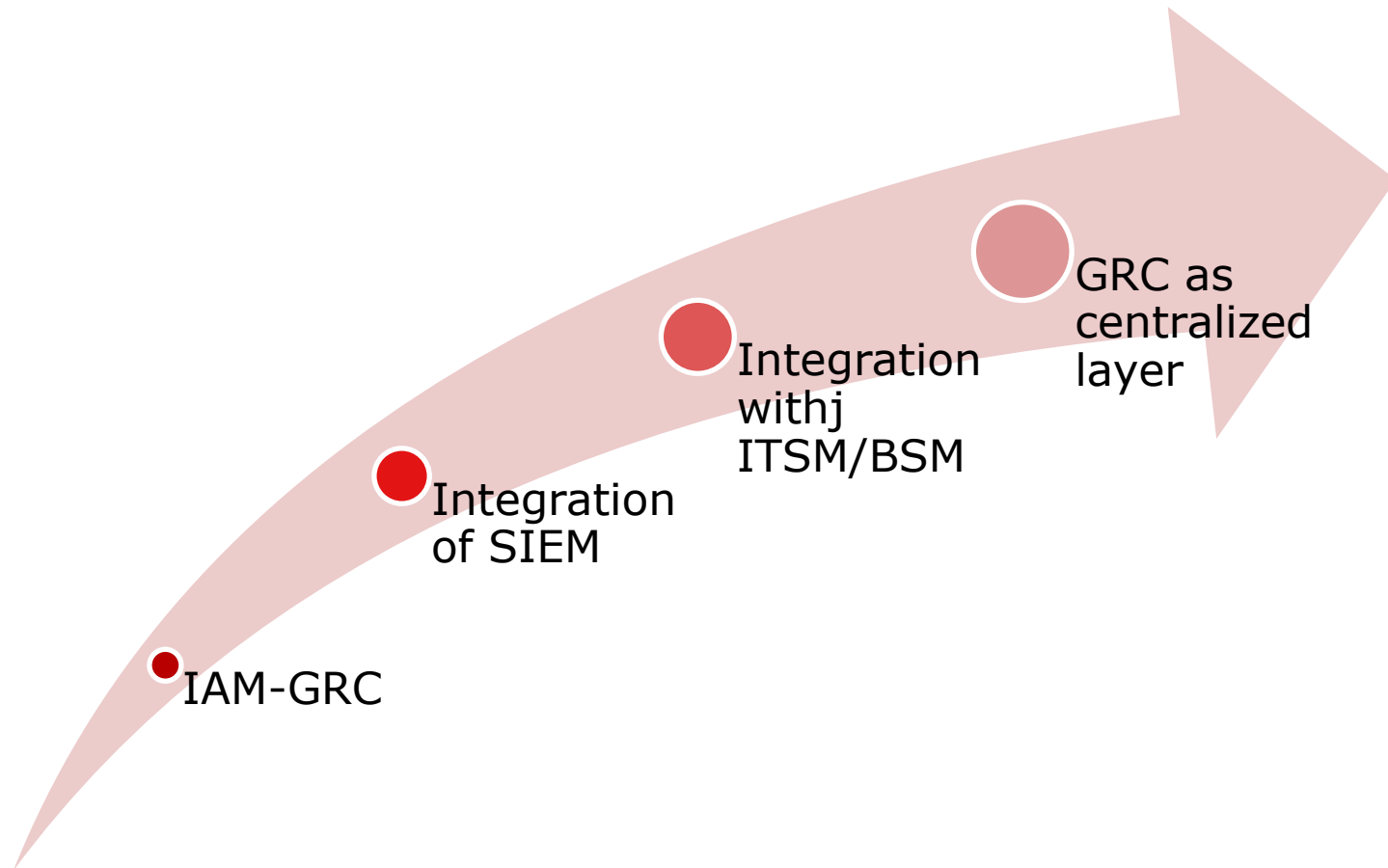
GRC: Business Control for IAM



GRC Market: Moving towards platforms



GRC Platforms: Beyond IAM-GRC



Enterprise Risk Management vs. IT Risk Management

Enterprise Risk Management:

- Example: Operational Risks in Brokerage
- Solution: amongst others, SoD rules
- SoD rules are implemented at the IT level

IT Risk Management:

- Example: Risk of missing de-provisioning and resulting orphaned accounts, thus risk of illegal access and information theft
- Solution: Identity Lifecycle Management
- The risk is not an IT risk, it affects operations

Integrated Risk Management

The diagram features a central red circle labeled 'Integrated Risk Management'. Two arrows point towards this central circle: a dark red arrow from the left and a light red arrow from the right. The left arrow originates from a red rounded rectangle containing text about Enterprise Risk Management. The right arrow originates from a light red rounded rectangle containing text about IT Risk Management. A thick red horizontal bar is positioned above the diagram area.

Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

Virtual Corporate Business Card

Information Card

- Managed or self-issued
- Digital identity card for users

Virtual Corporate Business Card

- Managed Information Card
- Generated from Active Directory or any other identity provider

Usage

- Registration of employees
- Business processes – with process controls delivered via attributes (claims)

What is the Identity Metasystem?

A “system of systems” designed to solve several *fundamental* identity problems

A single Identity model that works across different systems and applications

The foundation for Identity for the future (starting now!)

Based on wide industry consensus and many contributions from a wide range of people

- Kim Cameron’s “seven laws of identity”
- WS-* industry specifications

Why do we need an Identity Metasystem?

For Enterprises:

- Many incompatible systems, little interoperability
- Collaboration and outsourcing of applications and processes is difficult, businesses are held back, not enabled by technology

For Users:

- Users have little control over how their identity information
- The Internet is a notoriously unsafe and scary place with many identity traps and mines

How does the Identity Metasystem solve these problems?

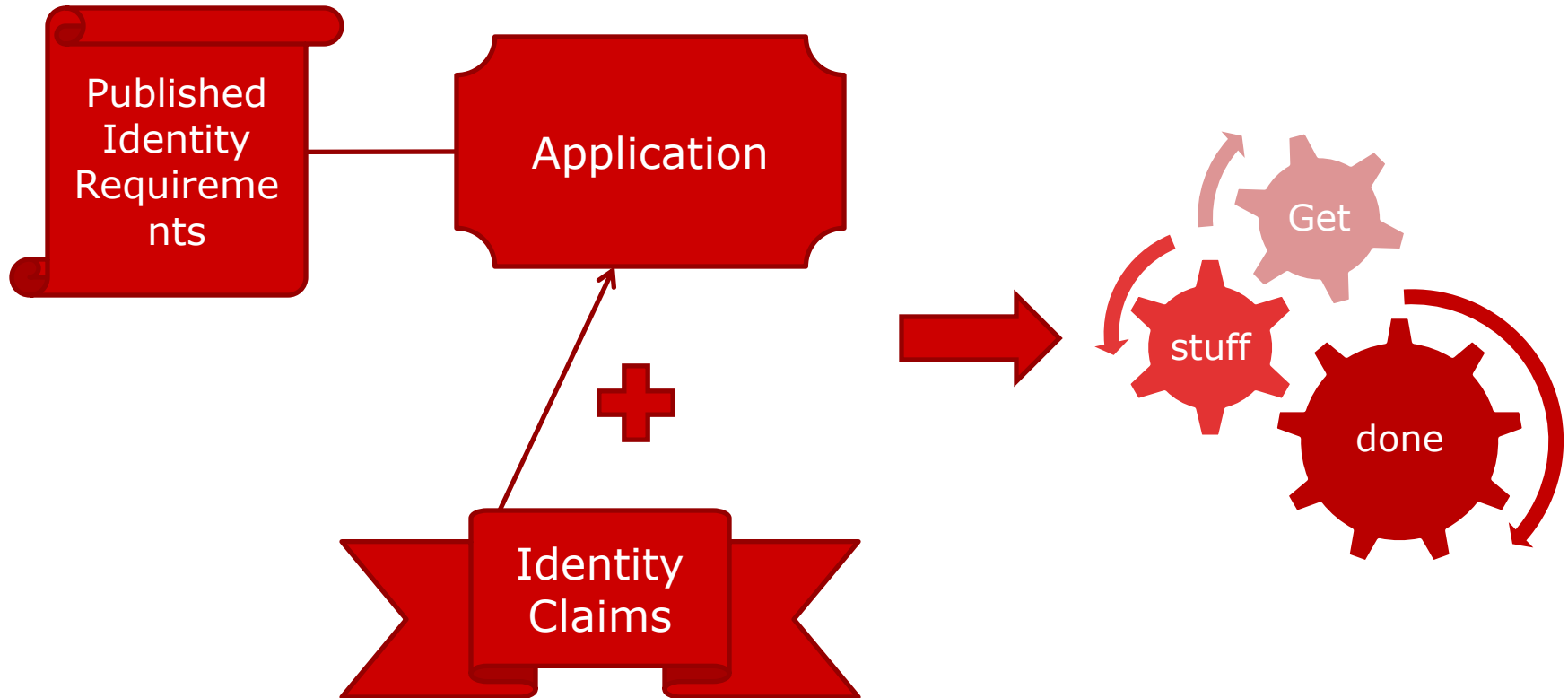
Enterprise:

- Decouple identity from applications
- Extend identity to enable collaboration

Users:

- Give control over identity back to users
- Create a safe identity environment for users

Just-in-time Identity



Missing end-to-end security

End-to-End Security

- Acting in the context of an user across all services
- Might be roles, groups, constraints etc. derived from an user

Risks of missing end-to-end security

- „coded“ security
- Limited accountability
- Security risks
- Management issues with technical accounts

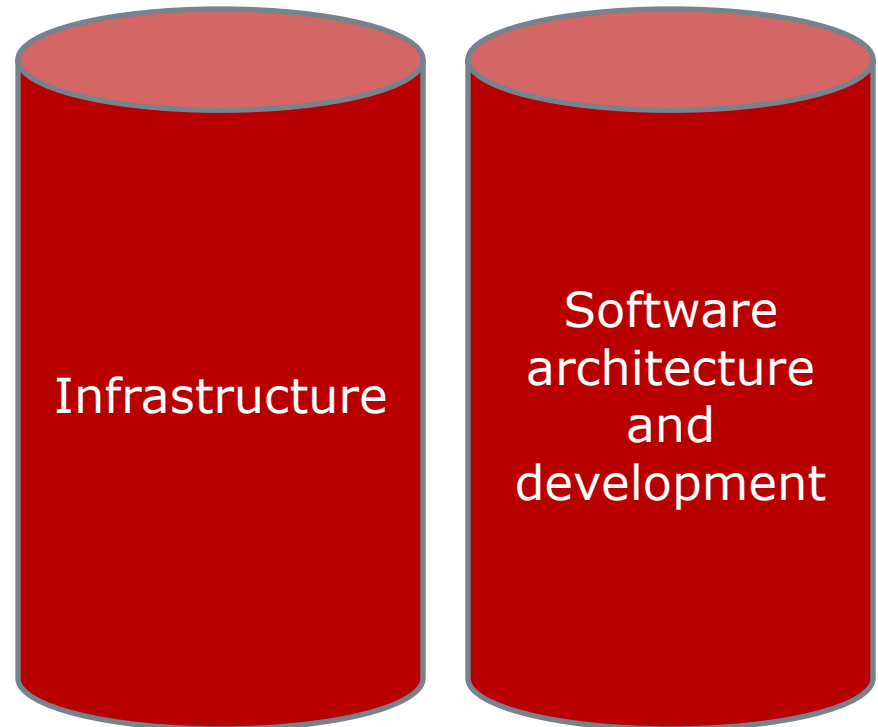
The main reason why: Siloed IT organizations

Two silos:

- Infrastructure
- Software development

Do they talk with
each other?

Do they work with
each other?



Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

Risk-based authentication

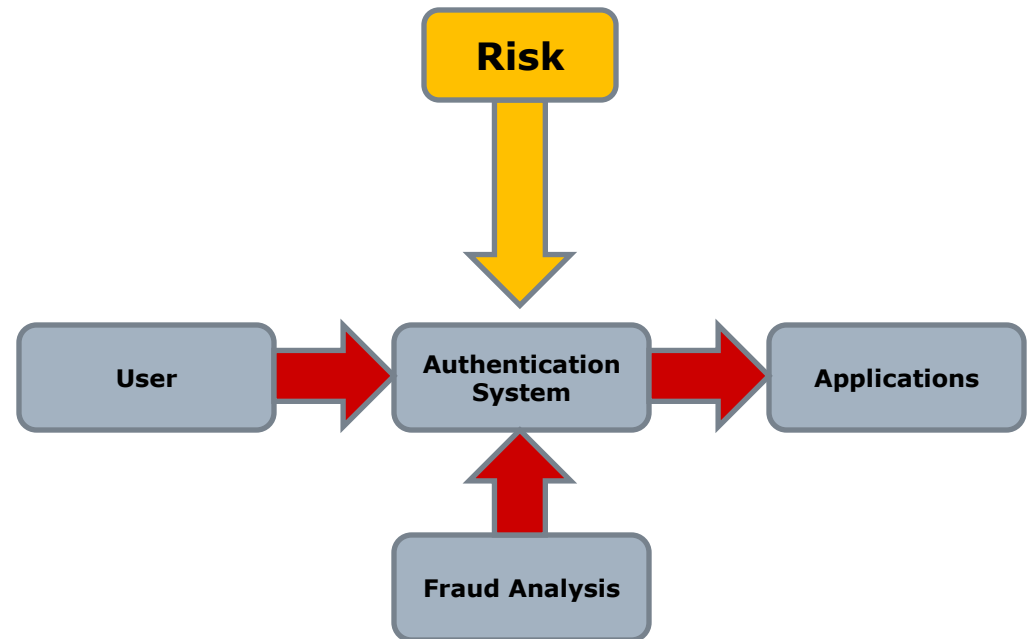
Using risks as element within an authentication decision

Risk typically := assumed Fraud attempt

Risk scores define action

No authentication, additional means, restricted access

Origin: eBanking



Risk-based authorization

Using risks as element within an authentication and **authorization** decision

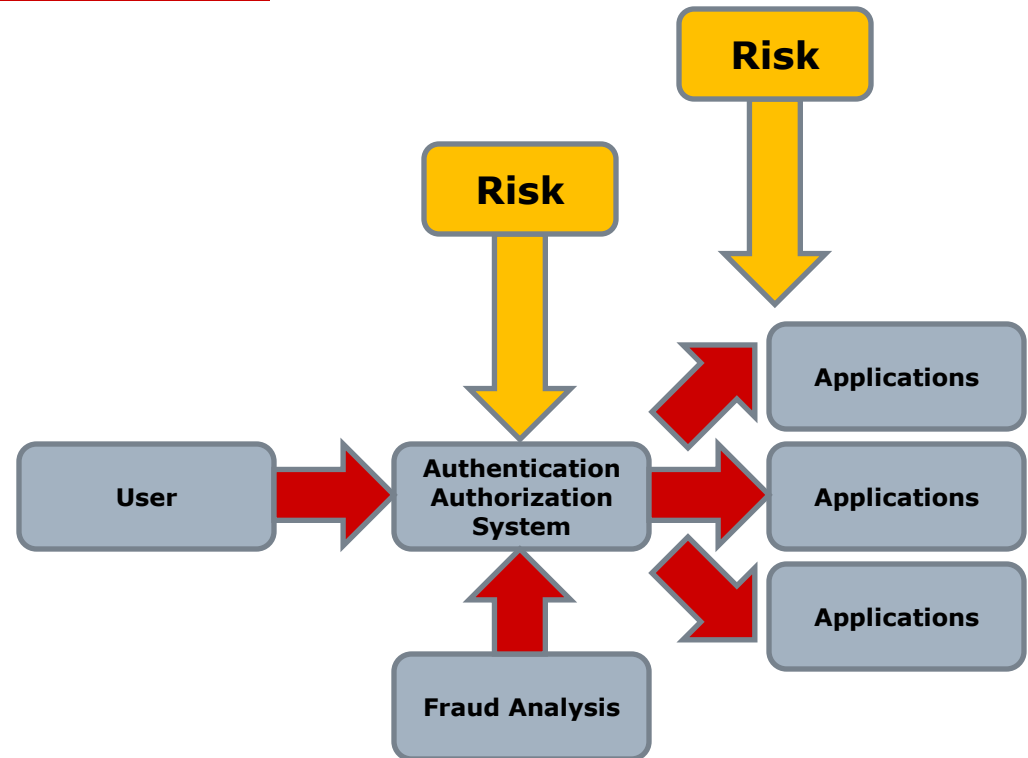
Risk typically := still assumed Fraud attempt

Risk scores define action

No authentication, additional means, restricted access

Authorization granted, authorization restricted to specific features, authorization denied

Origin: eBanking



Moving from risks to context

Using **context** as element within an authentication and authorization decision

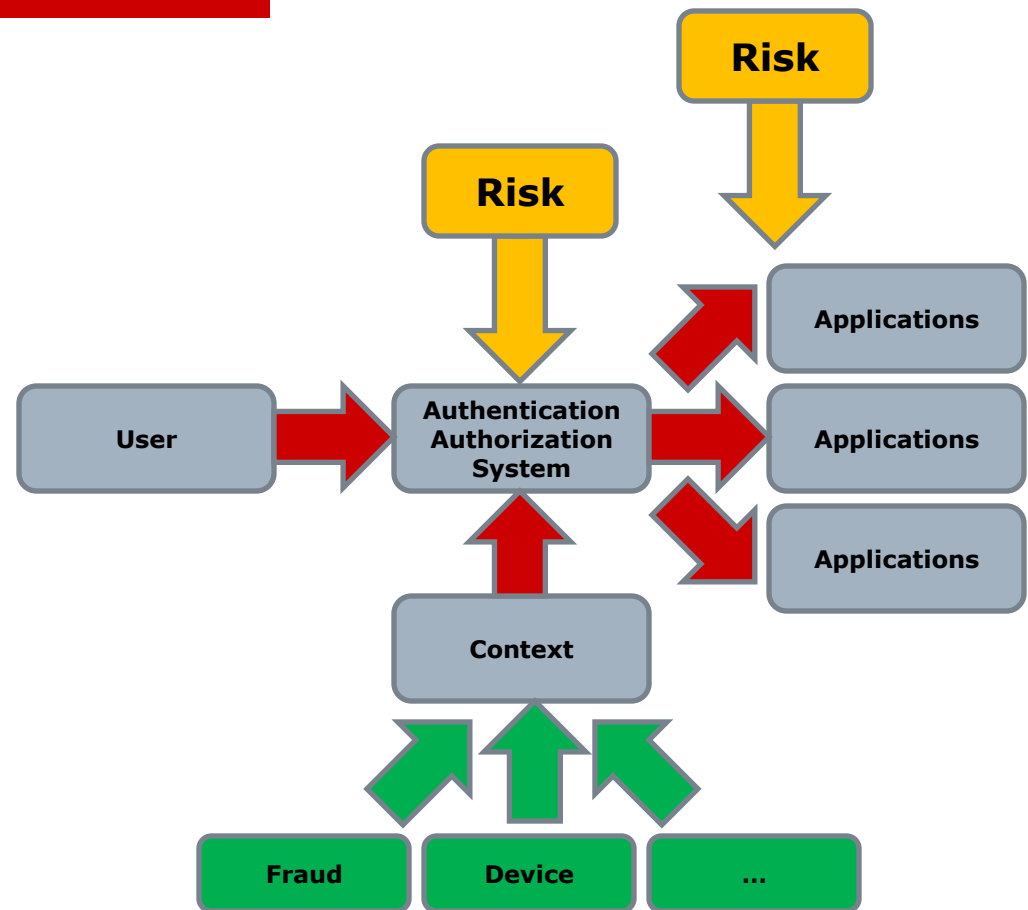
Context: Fraud, Location, Device, Device status,...

Risk scores define action

No authentication, additional means, restricted access

Authorization granted, authorization restricted to specific features, authorization denied

Target: Any sensitive application



Adding multi-factor authentication: Versatility

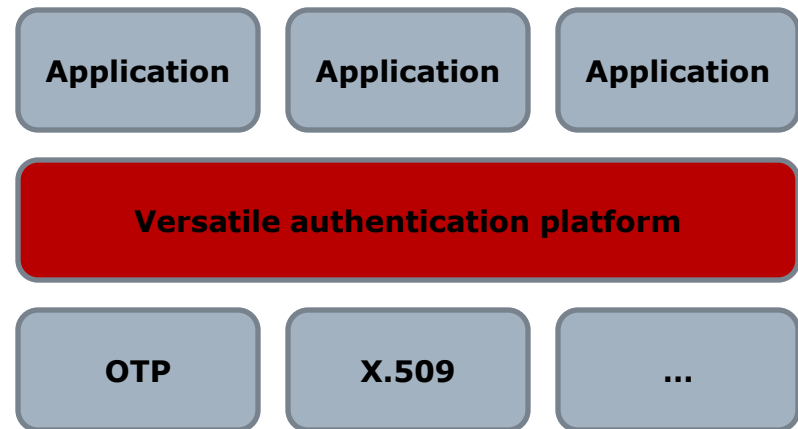
Versatile authentication describes approaches which allow different authentication technologies to be used with one platform

Supporting different users needs – internal users, mobile users, externals,...

Supporting different security requirements as well

Versatile authentication approaches are a clear trend – supporting strong authentication beyond a single technical solution like OTP or Smartcards with Certificates

Soft-Tokens as a typical option



The enterprise: Beyond eBanking and eCommerce

eBanking: Pioneers in securing their transactions

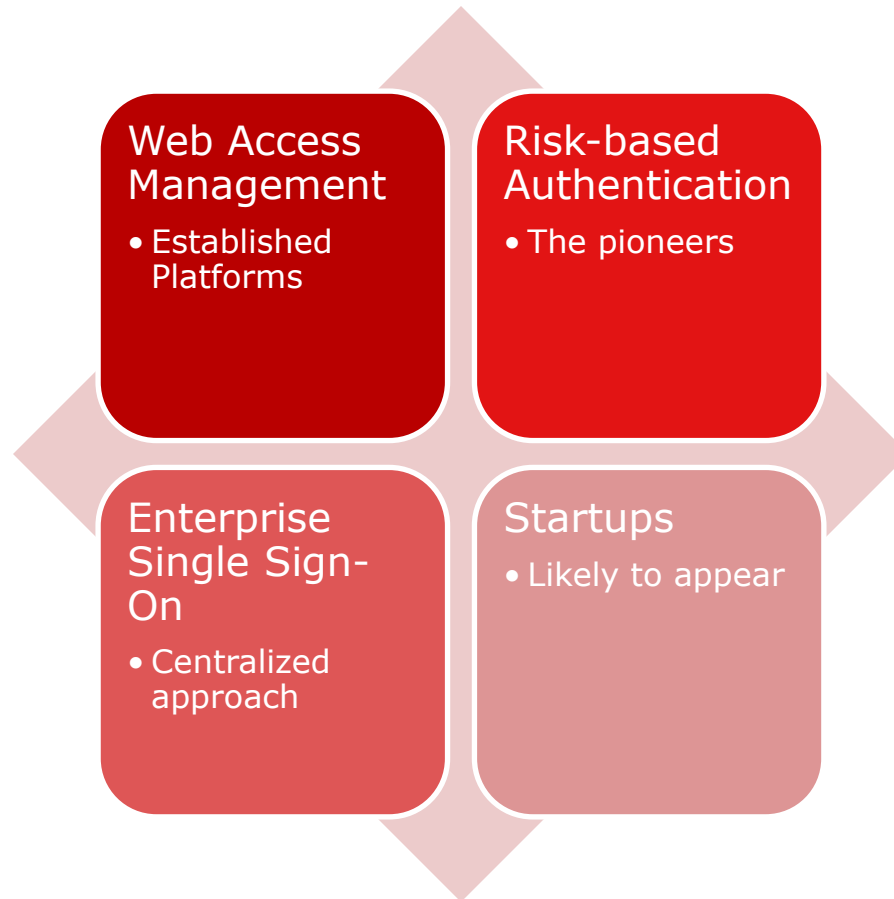
Enterprises: The future mass market for differentiated instead of binary authentication and authorization decisions

eCommerce: Sometimes close follower

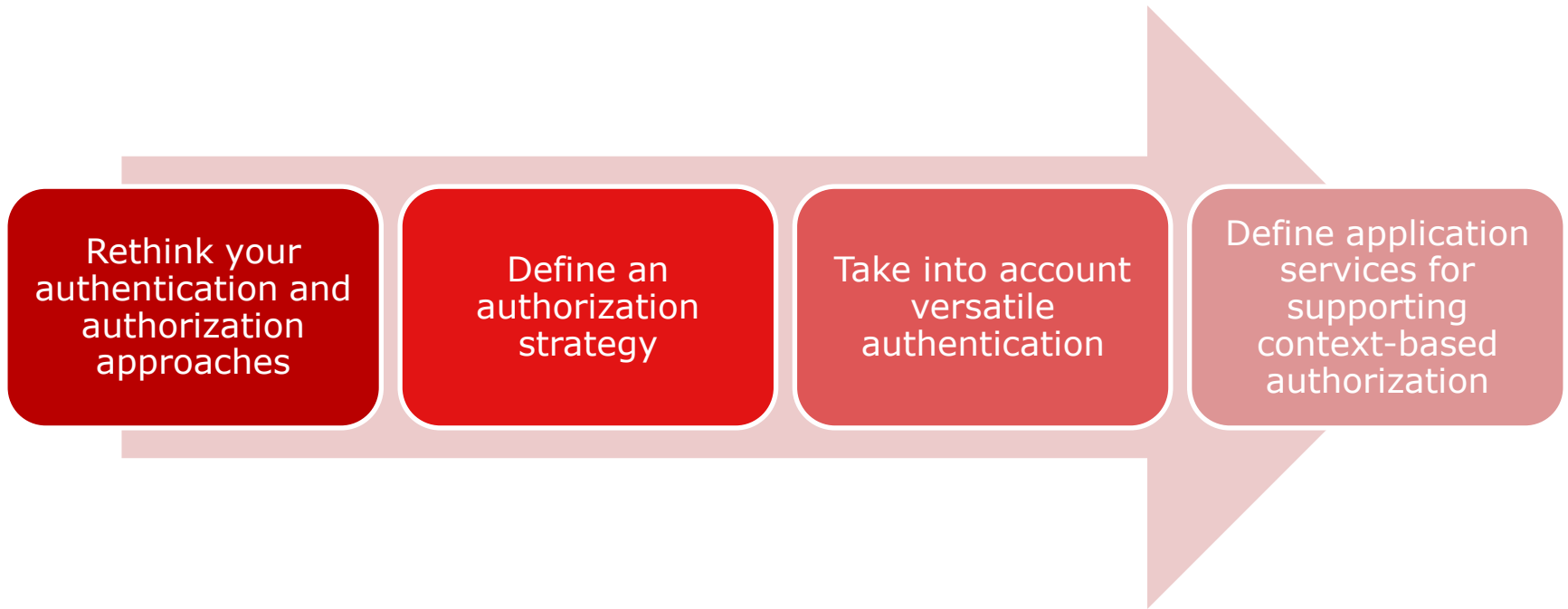
Impacts to context and multi-factor



The approaches: Web Access Management and others



Recommendations



Reduce your IT risks by intelligent, differentiated authentication and authorization decisions

Beyond enterprise authentication

Some trends in authentication

- Managed Identity Providers
- Claims-based approaches
- Electronic Passports (EAC 2.0, Extended Access Control for Public/Private)
- Soft-Tokens

There will be more options for strong authentication of end users

- With physical tokens
- Without tokens

Strategy for versatile and context-based authentication

- Platforms should support these approaches (in the near future)
- Some approaches will be used in E2E and B2B situations

Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

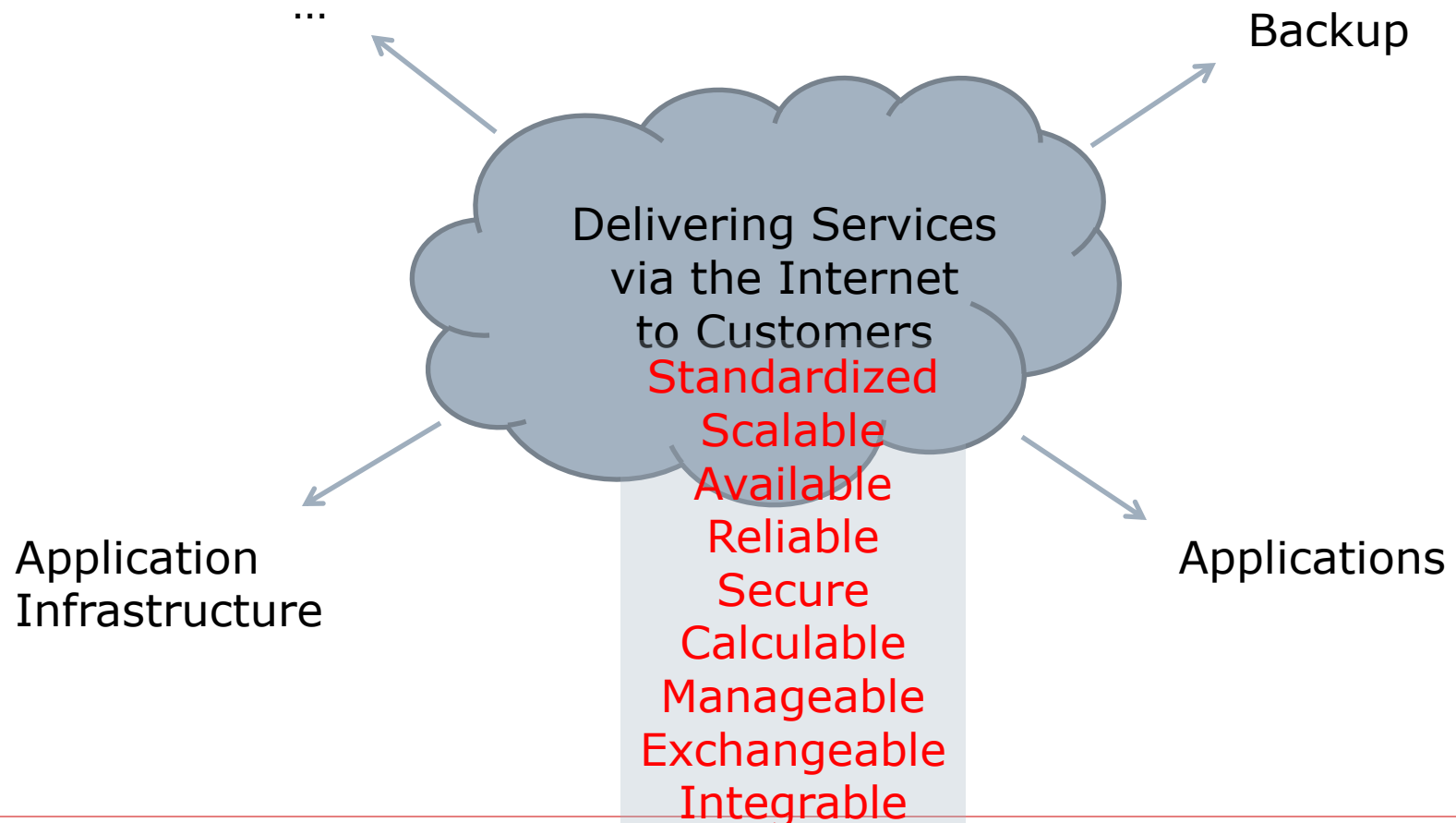
The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

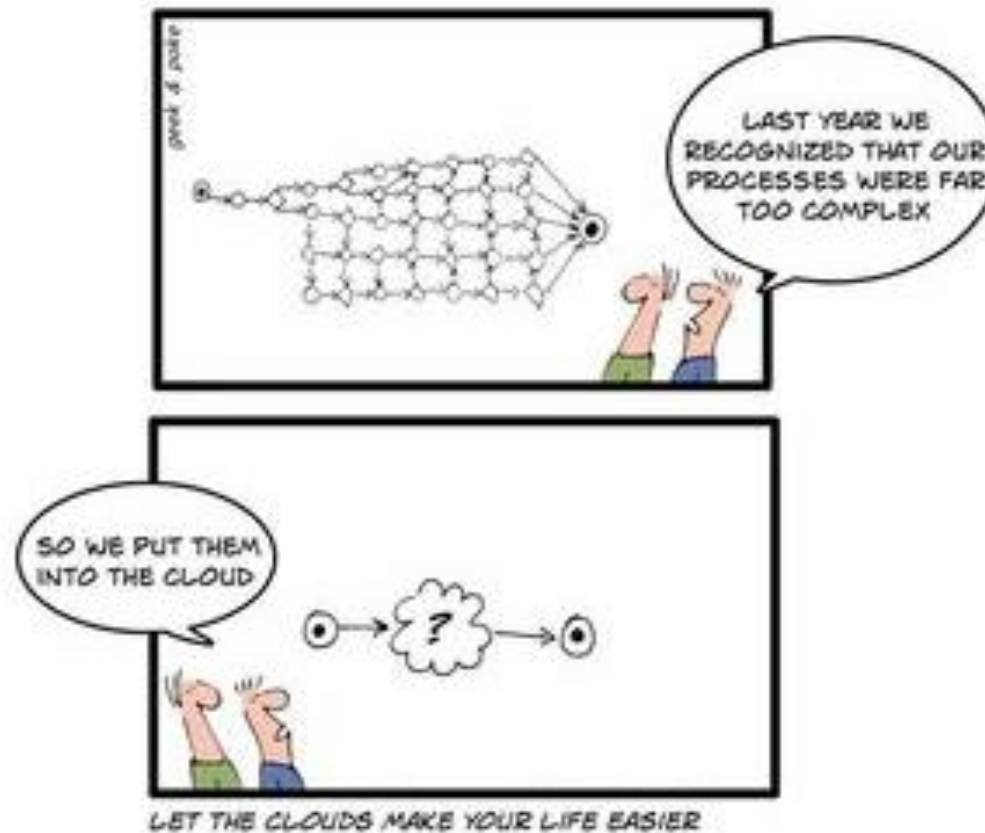
IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

The „cloud“



The reality about the cloud...



Quelle: www.ende-der-vernunft.org

Levels of Cloud Services I

Application Cloud

Platform Cloud

Infrastructure Cloud

Levels of Cloud Services II

Applications

Office, Communication, Collaboration

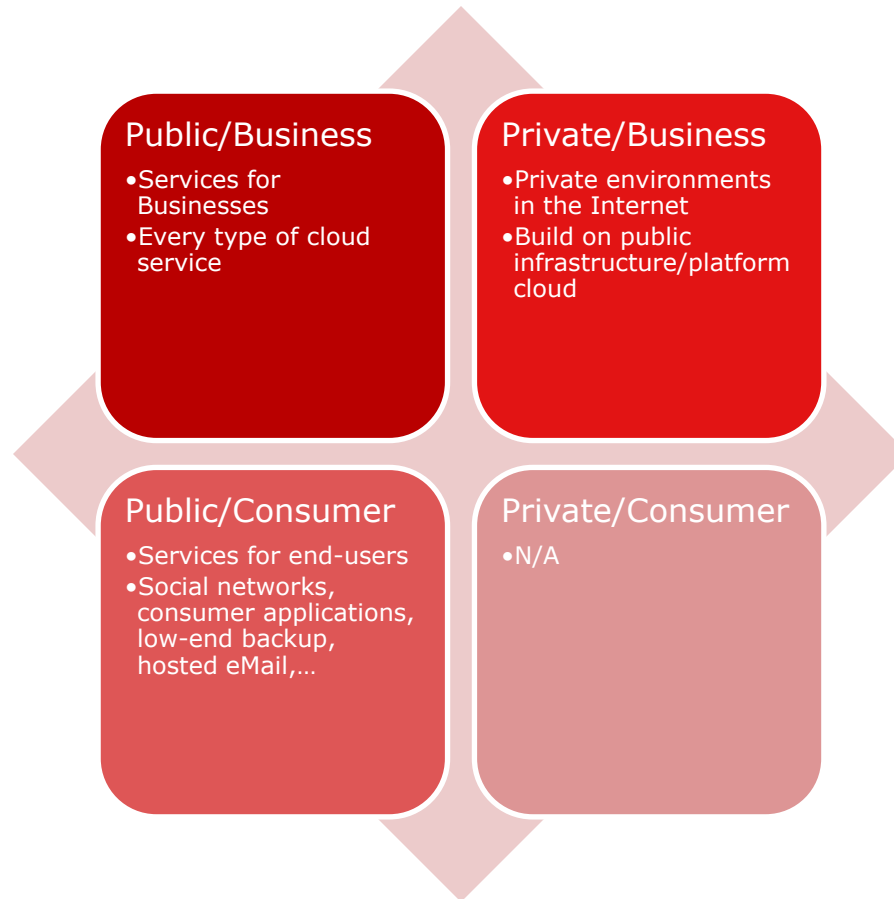
Application Infrastructure and Web Services

Infrastructure Services

Operating Environments

Hardware

Public, Private – Business, Consumer



Cloud Services: Promises and Opportunities

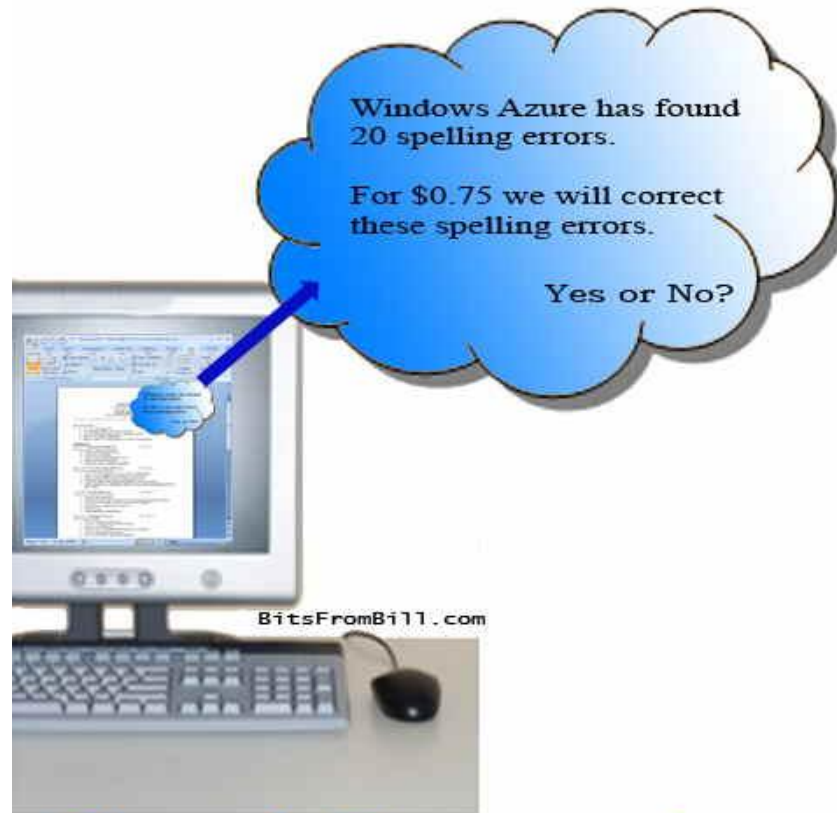
Promise

- Less internal IT resources
- Lower capital costs
- More flexibility in resource usage
- Lower overall costs
- Improving business processes
- Improved IT services

Opportunity

- Optimized resource allocation
- Continuous fees
- Using resources „on-demand“
- Better service quality
- New, affordable services
- Defined service levels

Calculable costs?



Cloud Computing

Quelle: <http://www.bitsfrombill.com>

12 Threats for Cloud Computing

Standardization	<ul style="list-style-type: none">•Lack of standards in many areas (Application packaging, Security, Identity, GRC, Management,...)
Scalability	<ul style="list-style-type: none">•Not every provider ensures the required scalability – and it is not always as easy to scale as imagined, especially at the application level
Availability	<ul style="list-style-type: none">•If services are moved to the cloud, the dependency of the business increases
Reliability	<ul style="list-style-type: none">•There are no standards – and there is a lack of SLAs (and many SLAs are not sufficient)
Security	<ul style="list-style-type: none">•Not every provider will ensure the required level of security – and IaaS is frequently missing
Calculability	<ul style="list-style-type: none">•Price models might appear promising – but are they really that cheap?
Manageability	<ul style="list-style-type: none">•Managing cloud services currently is a pain – no centralized management
Exchangeability	<ul style="list-style-type: none">•Moving from one provider to another might become a threat – a might be quite expensive
Integratability	<ul style="list-style-type: none">•It is pretty hard to integrate cloud services with either other cloud services or existing applications – at least above the web service level
Legitimacy	<ul style="list-style-type: none">•Not every service might be hosted everywhere – keep the laws in mind
Maturity	<ul style="list-style-type: none">•Not every cloud service is mature (most aspects of virtualization,...)
Completeness	<ul style="list-style-type: none">•Some required cloud services are still missing (some aspects of virtualization, GRC,...)

Cloud Governance

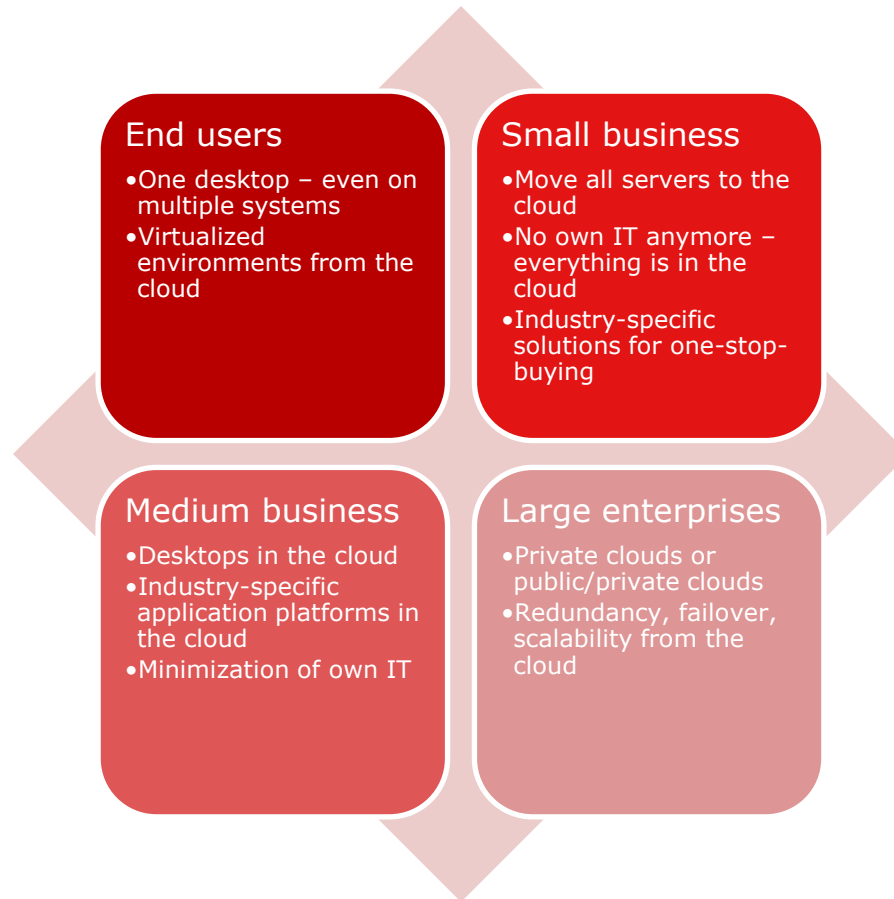
Governance:

- Ensuring that the right things are done correctly

Cloud Governance:

- Governance for the cloud
- Enhancing GRC to the cloud (notably: not only IAM-GRC)

Cloud Visions



Agenda

10 Top Trends 2009

Observations 2008 – Expectations 2009

Outlook up to 2019

How GRC will affect IAM – and how GRC will change

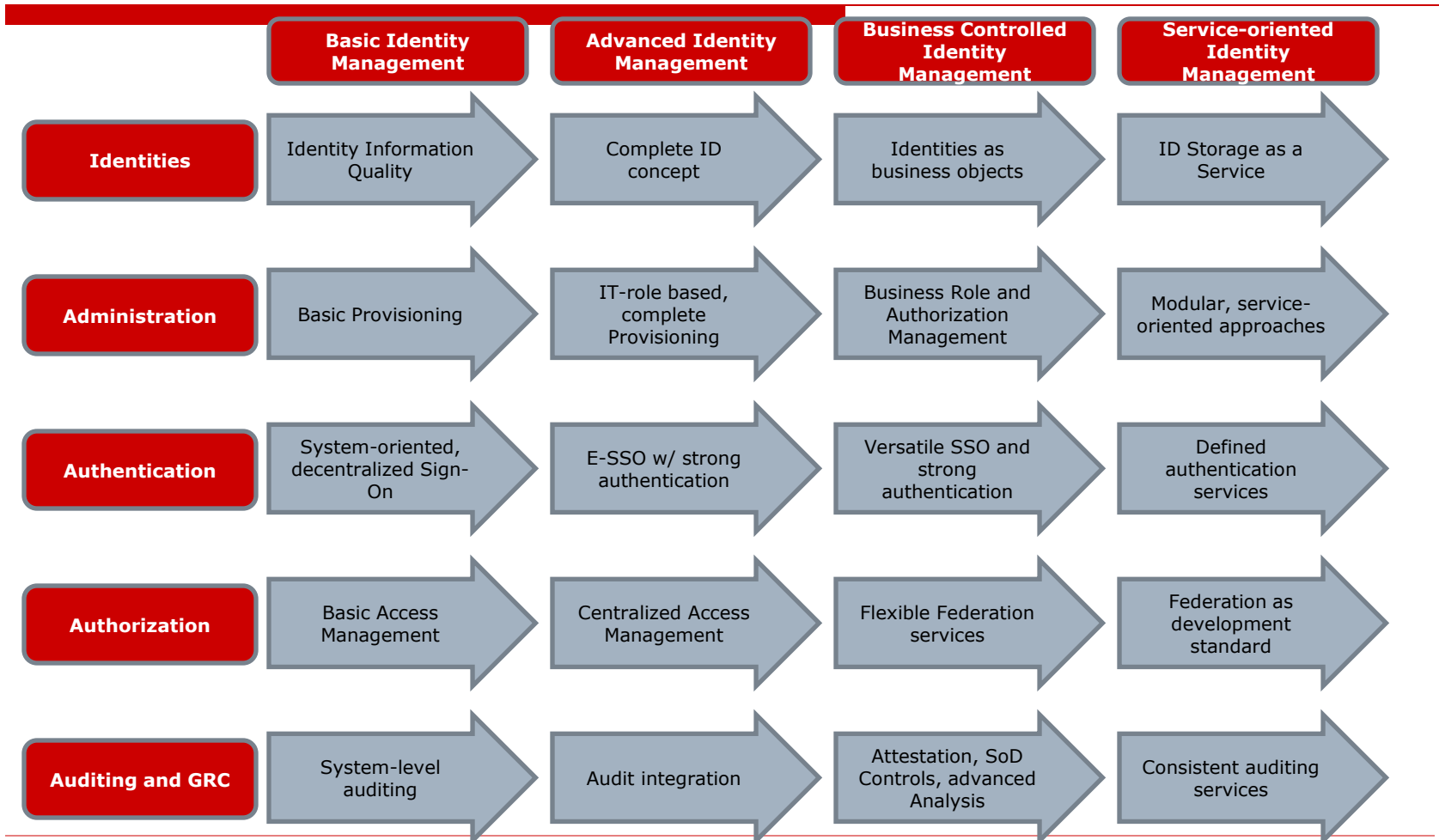
The impact of Identity 2.0 for business and service-orientation

Multipurpose cards, versatility, and context

IAM, GRC, and the cloud

Kuppinger Cole IAM Roadmap

Roadmap Overview



Dimension 1:

Areas of Identity Management

Identities:

- The definition and storage of identities and accounts.

Administration:

- The management of identity and authorization lifecycles. That includes aspects of provisioning, role management, and authorization/entitlement management.

Authentication:

- The identification of users. This includes areas like Single Sign-On and strong authentication technologies. The authentication part of Federation is covered here.

Authorization:

- The access management part. This includes Web Access Management, Federation, and user-centric Identity Management (as specific form of Federation).

Auditing and GRC:

- The area of auditability and control. Beyond classical auditing, this covers GRC approaches and policy-based management.

Dimension 2: Maturity Levels

Basic Identity Management:

- The entry level to IdM. At that level, IdM provides basic functionality, mainly with focus on administrative support.

Advanced Identity Management:

- Most aspects here are still more administration-focused. That level describes comprehensive IdM implementations on the maturity level which is realistic to achieve today and found in several existing implementations.

Business-controlled Identity Management:

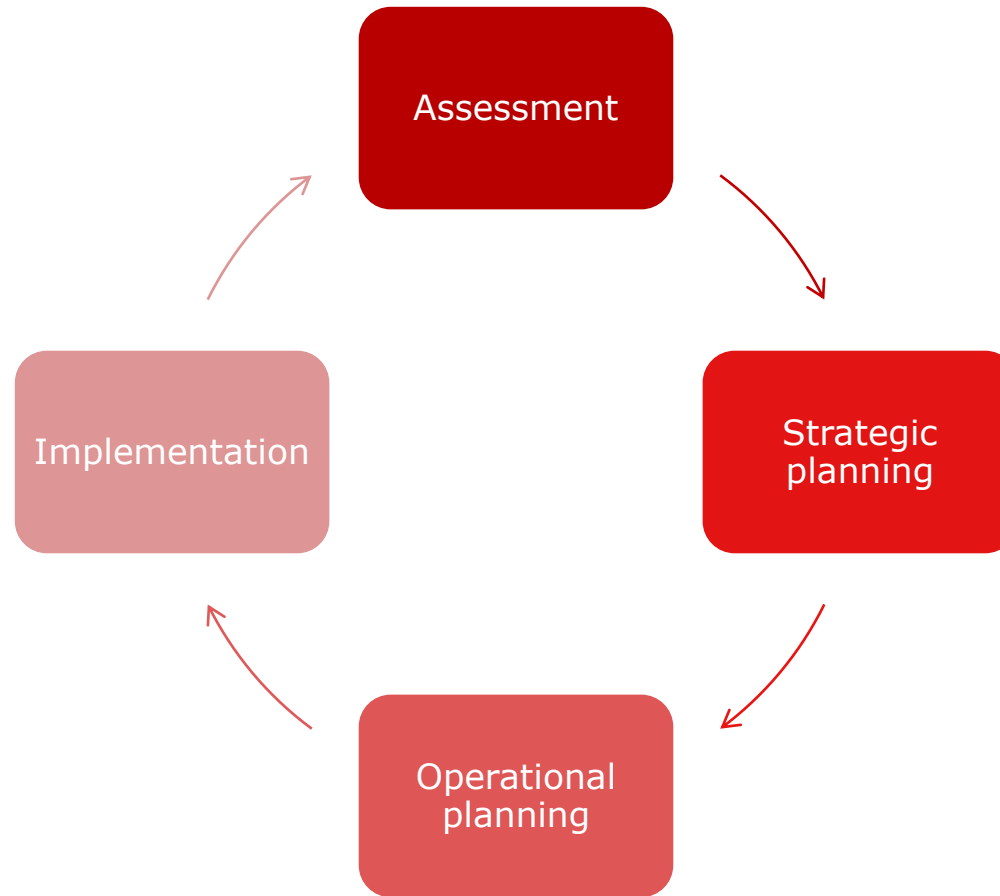
- At that level, some of the features are pretty new or still missing. It describes the next evolutionary step of IdM towards a stronger business alignment, with control through business roles and rules. It can be achieved at least partially and should be the guideline which affects the IdM strategy.

Service-oriented Identity Management:

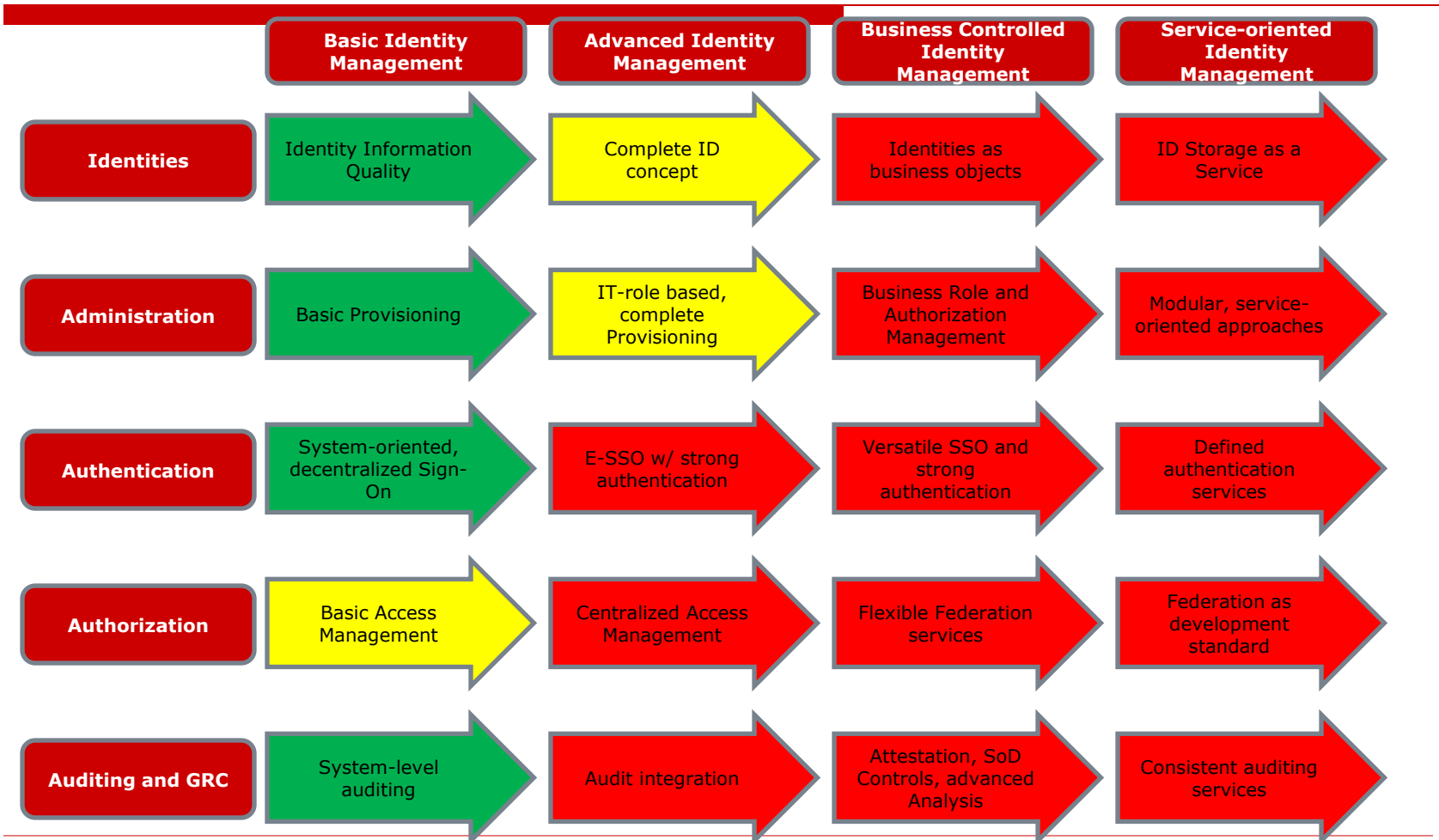
- That level, which is somewhat parallel to Business-controlled Identity Management, describes the integration of IdM with applications. Many of the targets at that level can be achieved today. The current situation with siloed IT organizations and few communication between IdM and Application Architecture/Development and the high pressure in the area of Business-controlled Identity Management anyway will lead to a situation in which most organizations will achieve that level after implementing at least significant parts of Business-controlled Identity Management.

Using the roadmap

Roadmap cycle



Using the roadmap Assessment



Using the roadmap Assessment

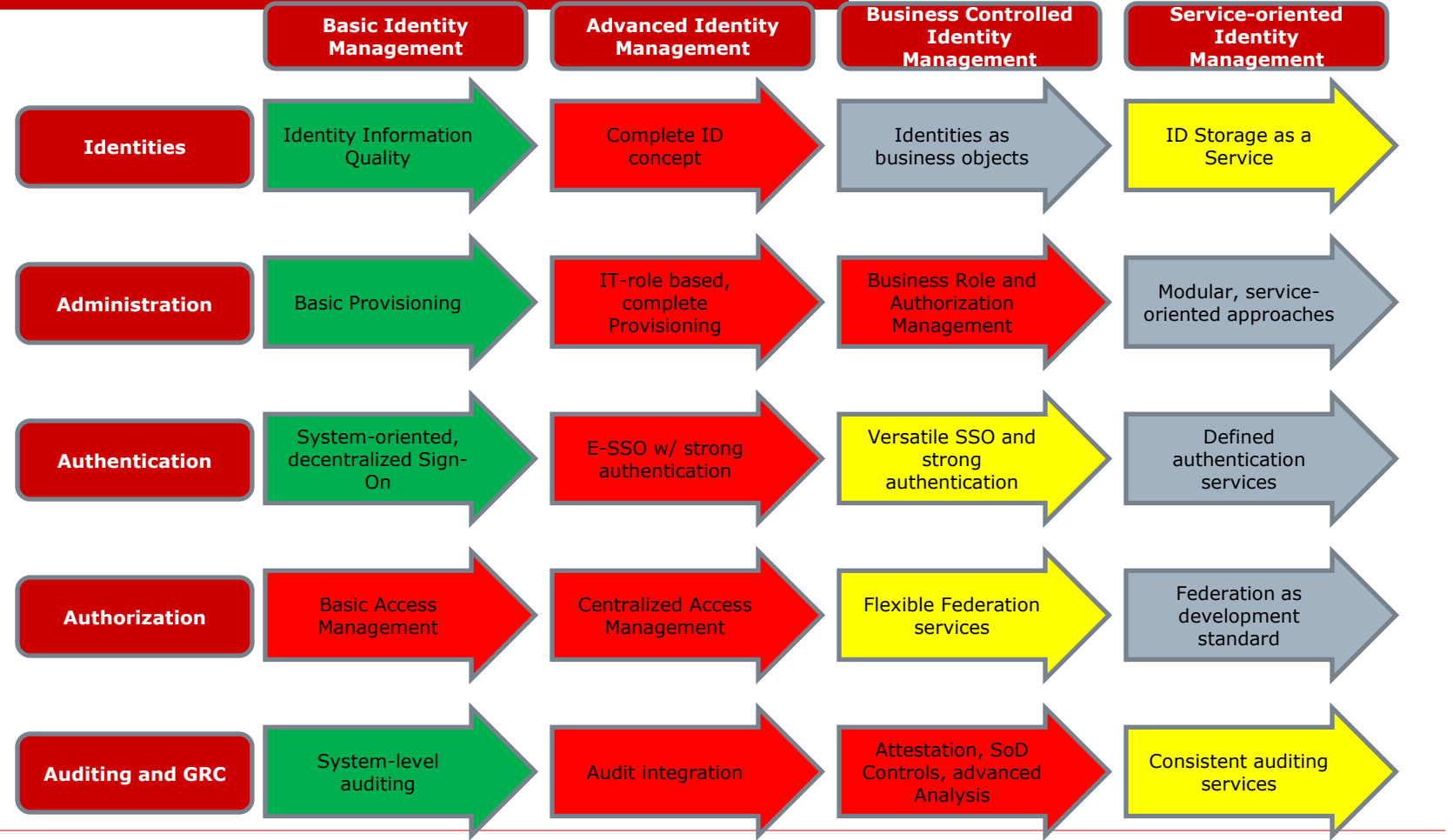
Measure your status using the defined maturity levels

Indicators:

- Green: Fully implemented
- Yellow: Partially implemented
- Red: Not implemented yet

Don't overestimate what you have done until now!

Using the roadmap Planning



Using the roadmap Planning

Define your requirements

Where should you invest?

- Green: Solved – no need for investments
- Red: Prioritized steps
- Yellow: Should be done – but with lower priority
- Grey: Not relevant yet

There might be larger steps, spreading more than one maturity level

Roadmap Fast Track

Identity Information Quality

Complete ID concept

IT-role based, complete Provisioning

First steps towards Business Role-based approaches

E-SSO w/strong authentication, some support for versatile authentication

Centralized access management, some federation support

Attestation, SoD Controls, advanced Analysis (either as part of provisioning or with separate GRC solutions)