Deloitte.

Cyber Risk Services

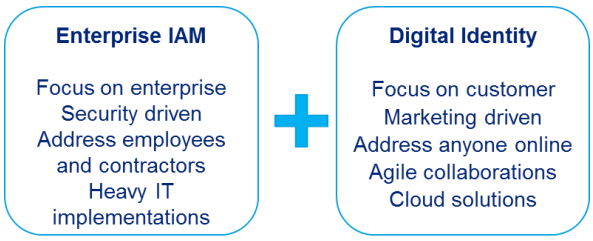
# Identity and Access Management

## The basis for online

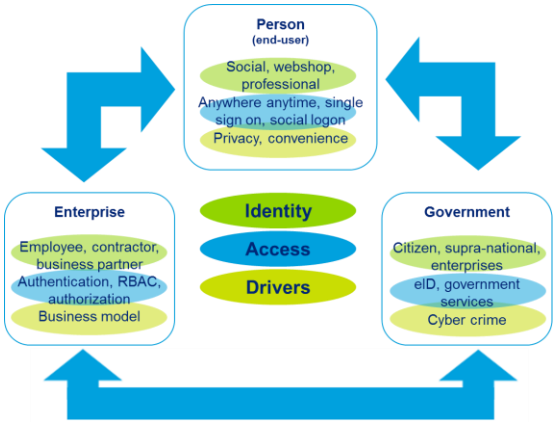
Identifying who is who online becomes the basis for digital business. Both externally, toward customers and partners, as well as internally, toward employees and guests.

**Due to place-independent-commerce it has become a necessity to identify your online customer. Similarly, due to (longstanding) business requirements for providing smooth, timely and correct access to information it is an equal important necessity to identify your employees, contractors and business partners. Identity and Access Management (IAM) provides solutions for both, however in a myriad of different and complex solutions.**

**There is a convergence happening of the traditional drivers of IAM, oriented towards access control (such as risk management, security and compliance) and supporting internal business users, and the current business drivers for IAM that focus much more on customer identification, agility in accepting customers (KYC rules made easy), and working together with business partners in cloud environments (federative solutions).**




**These development leads to the further integration of three main actors in the field of IAM, which are the enterprise, the government, and the person they both interact with.**




### Strategic aspects

The impact of Identity and Access Management (IAM) for the enterprise, the government and the person, and the benefits to be gained from it require a strategic approach. IAM has long since moved past the simple installation of 'IAM software'. How you address IAM can become a deal breaker in the future, or a business accelerator. Especially for identity (service) providers (governments, banks, telcos, to name a few) who are going to define the future or online identity management in the next few years. Enterprises are advised to develop an IAM strategy that address both the internal IAM (business, IT and compliance areas) as well as incorporating external developments that may disrupt their markets. Identity will be one of the most important business drivers for many companies. Identity will be the enabler for several new business models ranging from ISP and big data to customer recognition; moving from a cost centre to profit machine.

### Design and Architecture

Designing an IAM solution properly is a challenging task that needs to be done right. Not just because the world is changing in a rapid pace (and hence some of the business requirements), but also because IAM requires strong ties into different parts of the organization. For example HR and procurement for identities, business departments for entitlements, risk management and security for segregation of duty rules and compliance, IT for the applications, legal

for privacy restrictions, etcetera. The design and architecture needs to be able to absorb internal and external changes and at the same time provide sufficient direction for the organization to define the operating model for IAM, the IAM processes to be followed, the accompanying responsibilities, and the linkage into corporate frameworks through IAM policies and controls. The overarching business architecture for IAM is key to delivering the strategy, and in the end the design results in (multiple) technical architecture(s).

## Tactical Implementations

The implementation is where the rubber hits the road. Within the scope of an enterprises' or governments' mandate an implementation can be directed fairly well. However multiple IAM solutions are available outside the typical IAM mandate borders, meaning that for effective and efficient operations of IAM collaboration is required. This applies to all IAM aspects, including identities, access, entitlements/authorizations, authentication methods, high risk/privilege accounts, cloud solutions and outsourcing. It should not be surprising that one organization ends up with using multiple IAM solutions, maybe even managing multiple IAM solutions in its own domain. Because being able to offer multiple access paths to customers will increase the changes of profitable interactions with customers.

Implementing and managing a single solution is performed under the umbrella of the strategy and design for IAM. This ensures that each implementation is fit for purpose and delivers value, whether it is a two factor authentication device, a single sign on solution, a federative coupling to your business partners' domain, a role based access model or a cloud based identity service. Depending on your environment you may decide to deploy specific solutions for high risk/privilege accounts or integration in existing ticketing processes.

## Input for change

Change seems the only constant, so you better change in the right direction. Getting the right metrics and reports on IAM will support you to adjust in the strategic direction you're aiming for. Besides reporting you should get input from seminars, expert meetings and information sources such as mail/blog subscriptions and analyst firms on what's happening, so you acquire insights on IAM developments and innovations that may impact you.

## Deloitte, your partner in IAM

Deloitte has extensive experience in working with enterprises and governments on the topic of IAM, and we keep a keen eye out for the developments that occur globally and locally that will shape the identity market. We draw from our global network to work on strategies, roadmaps and designs for IAM. Using the proven Deloitte IAM methods methodology we execute on implementations of business operating models, process blueprints and technology solutions.

Deloitte delivers out of IAM experience of over 10 years and we connect IAM to business and security. Also Forrester recognizes Deloitte as leader in their report "The Forrester Wave™: Information Security Consulting Services, Q1 2013. In compiling its ratings, the analyst firm cited Deloitte's "exceptional client feedback and comprehensive, sophisticated, and mature service offerings." The Forrester report also considered Deloitte as one of the leaders demonstrating deep technical expertise and global reach. Deloitte was the top-ranked security and risk consulting provider in the current offering category.

## Contacts

Do you want to further explore IAM? Please contact Deloitte Cyber Risk Services through:


Henk Marsman
+31 (0)6 2078 9905
hmarsman@deloitte.nl

David Sloog
+31 (0)6 1234 4475
dsloog@deloitte.nl