

# Identity and Access Management

John Austin, September 2011

This document presents a brief point of view on the relevance and issues relating to Identity and Access Management (IAM). Its purpose is to provide a basis for further discussion on the breadth and complexity of issues relating to IAM.

## Key trends impacting Information Security to 2020

1	Infrastructure revolution	<ul style="list-style-type: none"> <li>Increase in penetration of high speed broadband and wireless networks</li> <li>Centralisation of computing resources and widespread adoption of cloud computing</li> <li>Proliferation of IP (internet protocol) connected devices and growth in functionality</li> <li>Improved global ICT (Information and Communications Technology) infrastructure enabling greater outsourcing</li> <li>Device convergence and increasing modularisation of software components</li> <li>Blurring work/personal life divide and 'Bring Your Own' approach to enterprise IT</li> <li>Evolution in user interfaces and emergence of potentially disruptive technologies</li> </ul>
2	Data explosion	<ul style="list-style-type: none"> <li>Greater sharing of sensitive data between organisations and individuals</li> <li>A significant increase in visual data</li> <li>More people connected globally</li> <li>Greater automated traffic from devices</li> <li>A multiplication of devices and applications generating traffic</li> <li>A greater need for the classification of data</li> </ul>
3	An always-on, always-connected world	<ul style="list-style-type: none"> <li>Greater connectivity between people driven by social networking and other platforms</li> <li>Increasingly seamless connectivity between devices</li> <li>Increasing information connectivity and data mining</li> <li>Increased Critical National Infrastructure and public services connectivity</li> </ul>
4	Future finance	<ul style="list-style-type: none"> <li>Rising levels of electronic and mobile commerce and banking</li> <li>Development of new banking models</li> <li>Growth in new payment models</li> <li>Emergence of digital cash</li> </ul>
5	Tougher regulation and standards	<ul style="list-style-type: none"> <li>Increasing regulation relating to privacy</li> <li>Increasing standards on Information Security</li> <li>Globalisation and net neutrality as opposing forces to regulation and standardisation</li> </ul>
6	Multiple internets	<ul style="list-style-type: none"> <li>Greater censorship</li> <li>Political motivations driving new state/regional internets</li> <li>New and more secure internets</li> <li>Closed social networks</li> <li>Growth in paid content</li> </ul>
7	New Identity and trust models	<ul style="list-style-type: none"> <li>The effectiveness of current identity concepts continues to decline</li> <li>Identity becomes increasingly important in the move from perimeter to information based security</li> <li>New models of trust develop for people, infrastructure, including devices, and data</li> </ul>

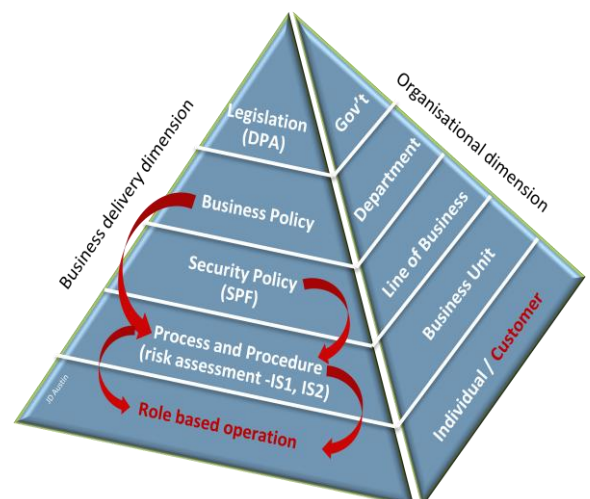
Key initiatives across both public and private sectors is the use of shared and cloud services. A shared service is considered to be where there is collaboration within a closed and trusted community. This can be for sharing information or a common process.

Cloud services are considered to be where a service is provided by a 3<sup>rd</sup> party and accessed by a wider, more open community. In both cases the need for confidentiality, integrity and availability of the information processed is, in most cases, a critical factor.

Revolution or Evolution? Information Security 2020, Technology Strategy Board / PwC, May 2010

The Technology Strategy Board view of key trends for Information Security through to 2020, highlights the infrastructure changes that will be as a result of the move to Shared and Cloud Services. Crucially, key trend 7 focuses on the aspects of identity and trust models that will be implemented to provide access management.

A government department is engaged in a pilot study on a "Hub" G-Cloud based service for HM Government that, through multiple factors of authentication, will provide Customer and Partner agency access to core online services. Currently access to these systems is controlled for internal staff and a limited number of external parties through secure connections. The use of role based access models, based on evolving security policies [TSB report trend 5] will be directly linked to mechanisms for authentication. The relationship between policy and the implementation of process and procedure has been researched by the author and is a key element of any IAM implementation.



Based on "Security Awareness in Large Public Sector Organisations, John D Austin, RHUL, March 2011

Identity and Access Management as a service is required to address multiple aspects of information security that have to meet the business needs. These include:

**Authentication:** Users of all shared systems are required to authenticate to gain access. Where a higher level of security access is required then two, or more, factors of authentication are required. Two factor authentication using something you know and something you have most commonly uses a User Id and password (something you know) and a One Time Password (OTP) that is often a number. The OTP as a synchronised 6 or 8 digit number obtained via a software token passed to a smart phone is growing in use as the footprint of Blackberry, iPhone and Android devices expands. Whilst RSA and VeriSign are the best known solutions in this space, an alternative example of use of the OTP for the mass market is GridSure.

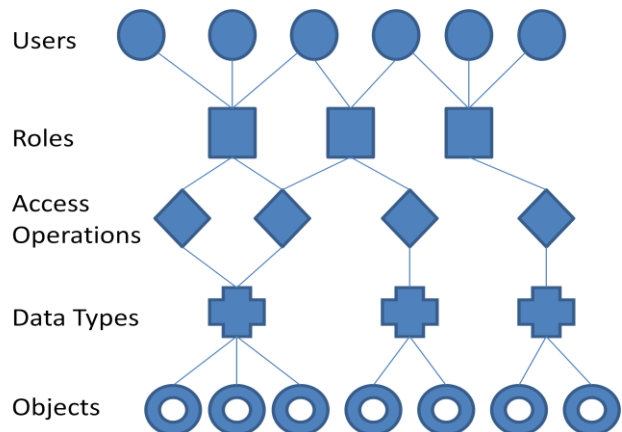
**Session Connection:** Users of secure cloud services may be required to further authenticate the device and session to securely manage the connection time to the application for limited period to enable a specific process to be performed. A common mechanism for this Session connection is the Kerberos ticketing system and is used on both Unix and Windows operating systems. The connection between end point device and host service front end will need to be secure and often adopt an SSL / TLS public key infrastructure encrypted “tunnel” at the transport layer.

**End point protection and management:** Implementing multiple security measures at the gateway and communication channel does not protect the User or Organisation if the end point has been compromised. Consideration should be given to methods of verifying the security status of the end point and if required pushing and executing protective software to the end point before access is allowed. Technology development for secure virtual sessions at the end point, continue to evolve.

**Access Control Models:**

Access to information is often based upon the level of access right and responsibility to perform specific operations. The standard models are:

- Bell LaPadula: no read up, no write down;
- Clark – Wilson: role based access as shown in the adjacent diagram;
- Chinese Wall: conflict of interest access;
- SWORD / SeaView: Dual User authorised operations.



**Oracle access control:** Controls within the SQL instruction set for DBMS’s can override designed access models. Applications developed with Oracle as the under lying database are common and yet Oracle has many commands that can easily undermine an access management policy.

**Single Sign-On:** Users don’t have just one set of credentials to access a wide variety of applications and the management of users access rights can be an onerous task. Single Sign-On (SSO) technology greatly improves the User experience by managing multiple login credentials whilst the User only has to login once. SSO also offers significant access rights management benefits from an IT operations perspective.

**Content monitoring and filtering:** A growing consideration for many organisations is the management of information flowing outside. Data losses can affect an organisation’s credibility and / or financial standing. Users with appropriate access rights can be the weakest link in the implementation of a security policy and, in spite of security awareness training, are the cause of many headline breaches. Content monitoring and filtering technology can assist or mitigate this risk.