

Recommendations - Voting

Please select one of the 4 categories for each of the 8 recommendations:

A Is absolutely urgent to address to prevent an almost inevitable major loss of competitiveness and/or a major loss due to security failures.

B Is urgent to address to prevent a likely major loss of competitiveness and/or a major loss due to security failures.

C Is for sure to address but less important.

X Not urgent

Controlling Instant On Demand Business in CFI: Authentication, Identity Management, Resilience and Denial of Service

1. Classification of identity attributes for on-line and mobile users of financial services should be defined and well understood by providers of these services and their customers.
2. Trust indicators need to be developed, which allow for the various gradients of trust any entity might achieve when using specific financial services.
3. Support platforms are needed for the management of multiple identities to allow consumers to authenticate themselves with various professional and private identity attributes.

Entitlement Management and Securing Content in the Perimeterless Financial Environment: Identity, Policy, Privacy and Audit

4. Digital identities are required that are highly standardised across the financial services sector, with the introduction of mandatory IDs for all financial institutions, cross border interoperability and a single/global identity issuing authority.
5. Data Security measures are required, such that a digital identity links directly with a security policy to a data object, that data is secured as encapsulated entities, and with flexible security policies that are based on individual access rights plus Digital Rights Management (DRM) for enterprise content to allow for flexible security policies and geographic boundary control.
6. New Computing Paradigms need to be analysed, which allow for de-perimeterization of the organisation, e.g. Cloud Computing, supported by any new security focus. Predictive models need to be created to understand security risks. Cross border legal issues need to be resolved.

Business Continuity and Control in an Interconnected and Interdependent Service Landscape: Cross Border and Cross Organisations

7. Design and implementation of secure platforms and applications, which should include an alternative and secure communication system/infrastructure, to be overseen by adequate coordination response team(s) at a national and international level.
8. Testing, design and implementation of such secure platforms, applications and infrastructures through trustworthy exercises between CIP-sectors and governments. Models for business continuity need to be extended to (1) sharing risks and (2) end-to-end communication between trade participants, as well as to (3) the volume and the complexity of specific financial markets. These models should be "crash" tested, regularly evaluated and updated.

1. 2. 3. 4. 5. 6. 7. 8.