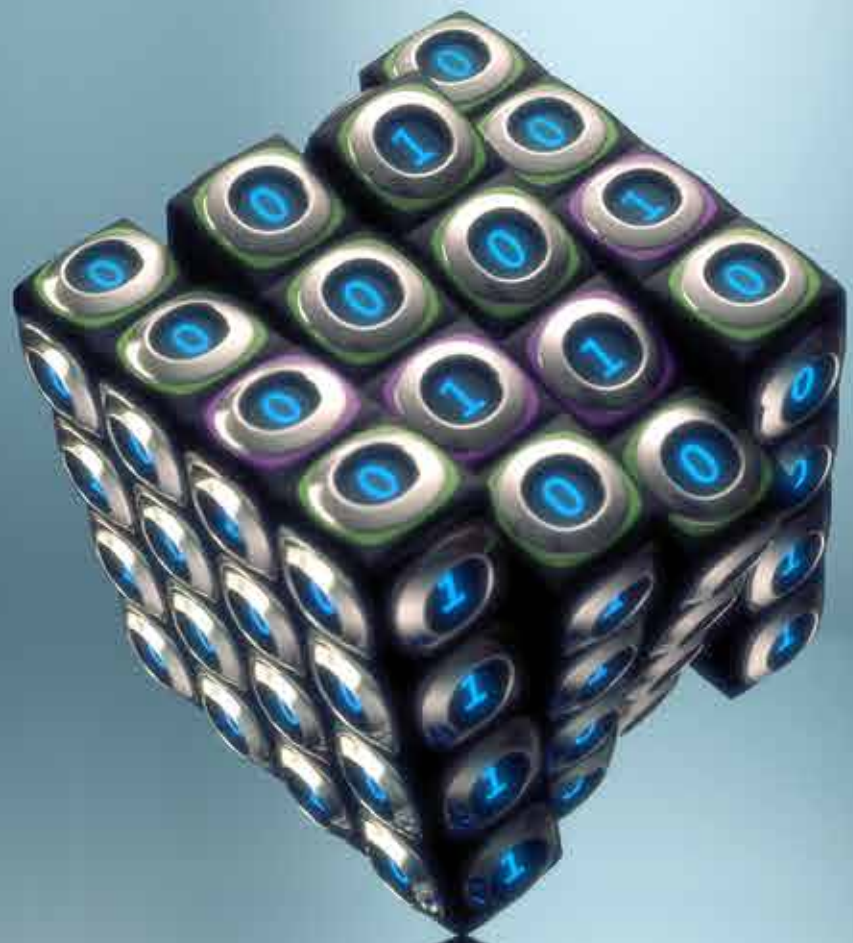
THE FIVE
Cs FOR DATA SECURITY

Prepared for 2016 B20 China Taskforces - Paris, May 2016



SINCE INFORMATION IS THE CURRENCY OF THE FUTURE, IT MUST BE SECURELY EXCHANGED.

Even at the technical level we must ensure a non-monopolistic balance by selecting the most qualified technology firms under an equal opportunity process from the world's 4 regions, represented by at least 3 companies within each region. It is essential that the technology board be diverse so that all regions of the globe have a seat at the table in terms of responsibility, accountability and decision-making to ensure that data is secure and continuously available for all.

C.4) Controlled Segregated Technology Development

While all the above is necessary, privacy and security at the data hosting and coding levels are a must. This requires multiple layers of security and segregation of duties. At the data hosting level, multiple data centers with state of the art firewalls and physical access constraints, as well as multiple companies and employees from diverse countries, are required to minimize any monopolistic and geopolitical concerns. Further, all software coding should be segregated into a minimum of 5 separate departments. Each will work on isolated modules that will then be integrated by a separate, independent integrator who would not be involved in the coding. This will ensure the highest level of security for the data centers and minimize any backdoor entry to the data.

C.5) Continuous and Comprehensive Audits

To ensure the utmost transparency, there must be additional checks and balances through a hierarchy of audits. First, continuous audits at every level of the operations will flag exceptions and weaknesses in internal controls thanks to a layered management structure. Second, periodic external audits should be performed by world class auditors who will provide reports related to security compliance.

Third, on-demand audits can be requested by interested parties in order to address specific concerns and verify compliance with data privacy requirements. In summary, this multi-layered audit mechanism will ensure the organization does what they say and says what they do.

The custodians of the global economy agree that trade is the engine to drive economic prosperity around the world. In today's 21st century technology era the digitization of trade has become a policy imperative of the B20/G20 but its power can only be unleashed when accompanied by a truly Global Data Security Standard

Global bodies such as the UN, WTO, APEC, OECD and the World Bank have attempted to address data security, where each have released principles or guidelines to cover these concerns. However, these guidelines are generally unenforceable as they are restricted by country jurisdictions.

What is needed is a new Global Data Security Standard (GDSS) that must safeguard the privacy of individuals and the data security of both public and private organizations. However, it is neither the mission nor focus of governments to provide security solutions directly to the market place.

It is also not acceptable for the private sector, which has earned the world's trust through its proven capabilities and skills, to monopolize security solutions. Understanding that data must be shared across borders, one must address nations' interdependent security needs and respect their sovereignties, which can only be realized through true Public-Private Partnerships (PPP).

Based on 15 years of R&D a PPP involving over 150 countries through their Pan regional organizations, 26 NGOs/IGOs and the world's most prominent private firms proposes a new Global Data Security Standard based on the following "Axioms of the 5Cs":

C.1) Consortium Of Globally Balanced Ownership

It is necessary to ensure a globally balanced ownership of any organization entrusted to manage the storage and dissemination of information in order to offset monopolistic concerns. Furthermore, such ownership must involve semi-government organizations whose mission is to serve the public good.

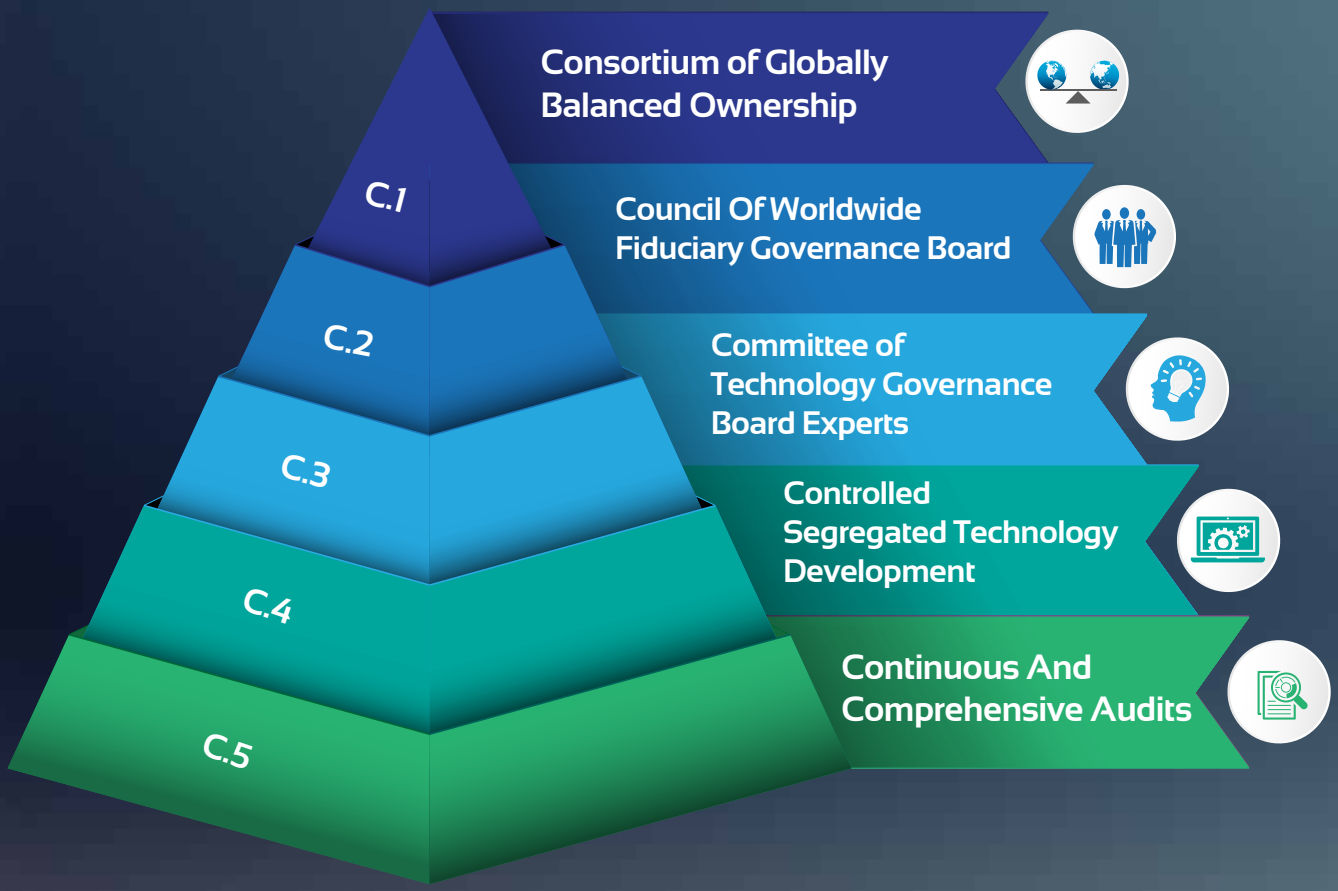
C.2) Council Of Worldwide Fiduciary Governance Board

To oversee any system of data management it is fundamental that the governance is geo-politically neutral and non-monopolistic so that no one country or company has undue influence. To ensure an equitable balance, the governance board requires representation from the 4 regions of the world - Europe, Middle East and Africa, Asia and the Americas.

Each region should be represented by semi-government organizations from the 6 major economies in that area with a representative from another country to act as the Chair. In this way 28 countries across the world will represent the governing body.

C.3) Committee Of Technology Governance Board Experts

It is not enough that the ownership and governance is geo-politically balanced. There also needs to be a balance at the technical level through a technology board that brings together the best minds of the world to ensure the quality and security of the data.



Global Data Security Standard (GDSS) - Axioms of the 5 Cs

It is clear that data security requires a comprehensive and global solution, one that serves the needs of developed, emerging and developing countries alike. It should allow the public and private sector to contribute to the development and the implementation of the standard in a geo-politically diverse and non-monopolistic manner, thereby garnering acceptance by all the regions of the world. It must also involve multiple layers of governance within a true Public-Private Partnership.

Only then will information be truly protected and become the currency of our future that can be safely exchanged throughout the world with confidence, securing our economic prosperity, now and for generations to come.