4. Risk Due to lack of Broad, Wide Ranging Security Planning

Return to Question 11 | **Provide Feedback**

An important way to make sure the Security Planning is adequate is to design it into the U.S. CBDC from the onset, especially if the U.S. CBDC adopts the use of Distributed Technologies currently in wide use in cryptocurrencies. First, it is important to detail what needs to be secure and why. See Table 1.

For a more detailed discussion, see the OMG DIDO-RA section on Non-Functional requirements for Securability.

Table 1: Main reasons why data needs to be secure.

- Confidentiality
- Data Integrity
- Non-repudiation
- Authenticity
- Accountability

All too often, projects try to “bolt-on” security after products are built. When building something as essential and critical to the U.S. as a new financial mechanism such, ie., the CBDC, it is essential to think about it at every stage of the development, starting at the specification of requirements and at each layer of securability. See Figure 1 and Table 2

Securability is also a layered stack. At each layer, there are different steps that need to be taken to secure the system. For example, **Culture Security** it may just mean having employees hold a security clearance and/or take Drug Tests. For **Physical Security** it may mean having a locked facility to house the computers and network devices. Data Security might be software and cultural procedures such as encrypting all data stored in a disk drive and using software to access the data.

Figure 1: The layers of Security.
Table 2: The layers of Security.

1. Physical Security
2. Data Security
3. Network Security
4. Platform Security
5. Application Security
6. Culture Security

The OMG members recommend a close look at the Reference Architecture (RA) defined by Information Exchange Framework (IEF).

The IEF RA is primarily targeting operational environments that require the ability and capacity to share

information within and beyond organizational boundaries (public and private sectors) and are challenged by rapid, unpredictable changes in operational contexts (e.g., threat, risk, roles & responsibilities, scale, scope, and severity). The IEF RA is targeted towards the following areas:

- Military (coalition and Civilian-Military) operations
- National Security
- Public Safety
- Crisis Management
- Border Security
- Emergency Management
- Peace Keeping
- Humanitarian Assistance

☐ [nick]how to address McL's comment about highlighting the IEF? Think it could have a role to play but is this the place to bring it out? Is there some other place in this document where it could be mentioned? Or is it sufficient to point at the DIDO RA for a citation about the IEF?