b) Cyber Resiliency

Return to Question 13-1 | **Provide Feedback**

Overview

Return to Top

Cyber Resiliency is tied to the Securability of the system. Securability is not a single “thing” that can be added to a system. To be truly secure, the entire End-to-End Solution (E2ES) needs to be secure and needs to be considered during the entire System Lifecycle.. As shown in Figure 1, a layered approach is used to help isolate the security needs. Each layer represents a portion of the Information Technology (IT) stack, including the people who use and have access to the IT stack.

Figure 1: The layers of security.

In many ways, **Cyber Resiliency** is the Security non-functional requirement in Operational Resiliency .

The **Security non-Functional Requirement** includes the following sub-requirements.

Table 1: The sub-requirements of the Security non-Functional Requirement.

Confidentiality	Confidentiality is usually covered by using a Confidentiality Agreement or Non-Disclosure Agreement (NDA), which defines a set of rules or a promise limiting access or places restrictions on certain types of information. Areas that have legal agreements covering confidentiality are: 1. Legal Confidentiality 2. Medical Confidentiality 3. Clinical and Counseling Psychology 4. Commercial Confidentiality 5. Banking Confidentiality 6. Public Policy Concerns 7. Religious Confidentiality As a rule of thumb, it is best to treat all Personal Identifiable Information (PII) as confidential and to secure it (i.e., require authentication both to access the data and log access to the data).
Data Integrity	Data Integrity is the completeness, accuracy and consistency of data throughout the entire data lifecycle of the data as well as when the Data is at Rest, Data-in-Motion and Data-in-Use.[1)]
Non-Repudiation	Non-Repudiation, (Computer Security Resource Center (CSRC) Accessed 14 August 2020, Non-Repudiation) means that it is not possible to repudiate (i.e., deny) that an action has been taken. For example, the signed contract witnessed by two people could not be repudiated. In other words, the contract now has Non-Repudiation. Non-Repudiation is about providing assurance using evidence that an action has been done. For example, a data sender is provided evidence (i.e., proof) of delivery while the receiver is provided evidence (i.e., proof) of the sender's identity. As a consequence, neither the sender nor the receiver can deny having processed the data.

Authenticity	Authenticity is a property indicating the source and origin of the information[2]. The process of authenticating a source starts when an entity (i.e., user, remote process, intelligent agent, etc.) attempts to access resources on a Computer Platform. The entity proves its identity in order to gain access rights. For example, traditionally when logging into a computer, users use Single-Factor Authentication (SFA) , providing a `username` and `password` to confirm their identity and allow authentication for future access to resources. However, the `username` and `password` login combination is no longer considered secure enough, especially if the Security Culture is poor. As a consequence, many systems have added Two-Factor Authentication (2FA) that require Biometrics (i.e., facial recognition, fingerprints, etc.) or One-Time PIN (OTP) . These 2FA methods generally require the user to be physically present to successfully log in.
Accountability	Accountability is the principle of holding an individual entrusted to safeguard and control key components of a system or program (i.e., equipment, keying material, and information) answerable to proper authority for the loss or misuse of that component. [3] Accountability is a security goal outlined in ISO/IEC 24010[4] requiring the actions of an entity to be traced uniquely to that entity. Accountability directly supports Non-Repudiation. It also provides deterrence, helps with fault isolation, and is useful in intrusion detection and prevention. In many cases, it is a key source of the evidence used in an After Action Review (AAR) and can ultimately, if needed, support legal actions.

The first step in designing for Cyber Resiliency is to begin with a Systems Engineering approach and to survey CBDC Stakeholders in order to refine the definitions and expectations of Cyber Resiliency. See CBDC Stakeholders for a more detailed discussion.

Guidelines for Developing Cyber-Resilient Systems

Return to Top

An important first step is to follow the NIST Special Publication SP 800-16 volume 2 guidelines for developing cyber-resilient systems. [5]. Skipping this step and going right to design and implementation often ends with the problem space (i.e., CBDC) being defined by the product(s) it chooses to use rather than by stakeholder requirements. A product-based solution can work, but it often misses many key requirements important to the stakeholders. For example, the design must be Quantum Computing "safe" or resistant.

SP 800-16 provides a framework for conducting cyber resiliency engineering. It starts with defining and setting the goals, objectives, techniques, implementation approaches, and design principles. Table 2 summarizes the definition and purpose of each construct, and how each construct is applied at the system level. **Note:** The framework is applicable to levels beyond the system level (e.g., mission or business function level, organizational level, or sector level).

Table 2: Cyber Resiliency Constructs[6]

Construct	Definition, Purpose, and Application at the System Level
Goal	A high-level statement supporting (or focusing on) one aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyber resiliency. **Purpose:** Align the definition of cyber resiliency with definitions of other types of resilience. **Application:** Can be used to express high-level stakeholder concerns, goals, or priorities.
Objective	A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security. The objectives are more specific than goals and more relatable to threats. **Purpose:** Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate the definition of metrics or Measures of Effectiveness (MoEs). **Application:** Used in scoring methods or summaries of analyses (e.g., cyber resiliency posture assessments).
Sub-Objective	A statement, subsidiary to a cyber resiliency objective, that emphasizes different aspects of that objective or identifies methods to achieve that objective. **Purpose:** Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. **Application:** Used in scoring methods or analyses; may be reflected in system functional requirements.
Activity or Capability	A statement of a capability or action that supports the achievement of a sub-objective and, hence, an objective. **Purpose:** Facilitate the definition of metrics or MoE. While a representative set of activities or capabilities have been identified in [Bodeau18b], these are intended solely as a starting point for selection, tailoring, and prioritization. **Application:** Used in scoring methods or analyses; reflected in system functional requirements.
Strategic Design Principle	A high-level statement that reflects an aspect of the risk management strategy, which informs systems security engineering practices for an organization, mission, or system. **Purpose:** Guide and inform engineering analyses and risk analyses throughout the system life cycle. Highlight different structural design principles, cyber resiliency techniques, and implementation approaches. **Application:** Included, cited, or restated in system non-functional requirements (e.g., requirements in a Statement of Work [SOW] for analyses or documentation).

Once the Systems Engineering is completed, a design can be achieved to foster cyber resiliency.

1)

What is Data Integrity, Accessed 8 July 2020, https://www.talend.com/resources/what-is-data-integrity/

2)

Authenticity, Computer Security Resource Center (CSRC) Accessed 14 August 2020, Authenticity

3)

Accountability, Computer Security Resource Center (CSRC) Accessed 14 August 2020, https://csrc.nist.gov/glossary/term/accountability

4)

Accessed 15 August 2020, https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&start=6

5) 6)

Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie McQuaid, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, National Institute for Standards and Technology (NIST), NIST Special Publication 800-160, Volume 2, Revision 1, December 2021, Accessed: 11 April 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf