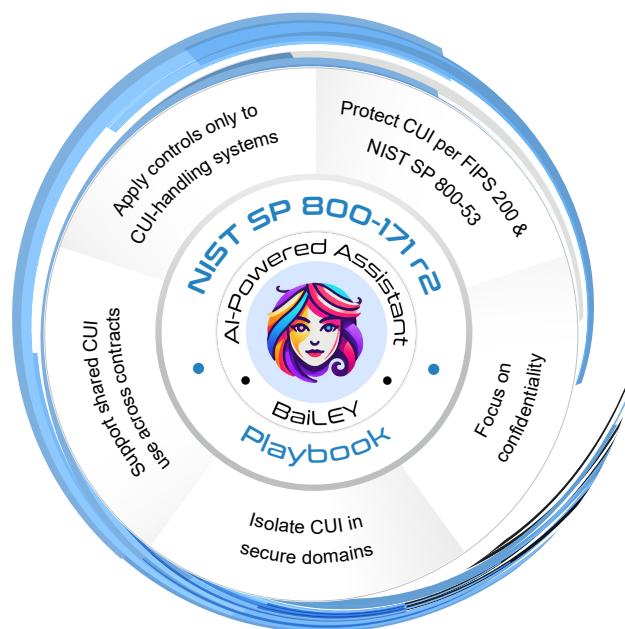


Quick Links

[Home](#)[NIST SP 800-171r2](#)[Source](#)[Control Families](#)[Reference](#)[CMMC Level 2](#)[Source \(Version 2.13\)](#)[Policy Index](#)

Source

[NIST SP 800-171r2](#)[NIST SP 800-171A](#)

Reference

[Brochure](#)[Infographics](#)

Control Families

Control Families

1 ACCESS CONTROL (AC)

[Basic \(2\)](#)[Derived \(20\)](#)

1.1: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Discussion: Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security.

1.2: Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Discussion: Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin.

2 AWARENESS AND TRAINING (AT)

[Basic \(2\)](#)[Derived \(1\)](#)

3 AUDIT AND ACCOUNTABILITY (AU)

[Basic \(2\)](#)[Derived \(7\)](#)

4 CONFIGURATION MANAGEMENT (CM)

[Basic \(2\)](#)[Derived \(7\)](#)Peter.Harvey@ecfirst.comwww.ecfirst.com