Requirement Number	Objective Number	Objective Description
3.1.1	3.1.1[a]	Determine if authorized users are identified
3.1.1	3.1.1[b]	Determine if processes acting on behalf of users are identified
3.1.1	3.1.1[c]	Determine if devices (and other systems) authorized to connect to the system are identified
3.1.1	3.1.1[d]	Determine if system access is limited to authorized users
3.1.1	3.1.1[e]	Determine if system access is limited to processes acting on behalf of authorized users
3.1.1	3.1.1[f]	Determine if system access is limited to authorized devices (including other systems)
3.1.10	3.1.10[a]	Determine if the period of inactivity after which the system inititaes a sesson lock is defined
3.1.10	3.1.10[b]	Deternine if access to the system and viewing of data is prevented by initiating a session lock aft
3.1.10	3.1.10[c]	Determine if previoulsy visible information is concealed via a pattern-hiding display after the de
3.1.11	3.1.11[a]	Determine if a condition(s) requiring a user session terminate are defined
3.1.11	3.1.11[b]	Determine if a user session is automatically terminated after any of the defined conditions
3.1.12	3.1.12[a]	Determine if remote access sessions are permitted
3.1.12	3.1.12[b]	Determine if the types of permitted remote access are identified
3.1.12	3.1.12[c]	Determine if remote access sessions are controlled
3.1.12	3.1.12[d]	Determine if remote access sessions are monitored
3.1.13	3.1.13[a]	Determine if cryptographic mechamisms to protect the confidentiality of remote access sessior
3.1.13	3.1.13[b]	Determine if cryptographic mechamisms to protect the confidentiality of remote access sessior
3.1.14	3.1.14.[a]	Determine if managed access control points are identified and implemented
3.1.14	3.1.14[b]	Determine if remote access is routed through managed network access control points
3.1.15	3.1.15[a]	Determine if privileged commands authorized for remote execution are identified
3.1.15	3.1.15[b]	Determine if security-relevant information authorized to be accessed remotely is identified
3.1.15	3.1.15[c]	Determine if the execution of the identified privileged commands via remote access is authorize
3.1.15	3.1.15[d]	Determine if access to the identified security-relevant information via remote access is authori
3.1.16	3.1.16[a]	Determine if wireless access points are identiified
3.1.16	3.1.16[b]	Determine if wireless access is authorized prior to allowing such connections
3.1.17	3.1.17[a]	Detemine if wireless access to the system is protected using authentication
3.1.17	3.1.17[b]	Determine if wireless access to the system is protected using encryption
3.1.18	3.1.18[a]	Determine if mobile devices that process, store, or transmit CUI are identified
3.1.18	3.1.18[b]	Determine if mobile devices are authorized
3.1.18	3.1.18[c]	Determine if mobile devices are monitored and logged

3.1.19	3.1.19[a]	Determine if mobile devices and mobile computing platforms that process, store, or transmit CU
3.1.19	3.1.19[b]	Determine if encryption is employed to protect CUI on identified mobile devices and mobile con
3.1.20	3.1.20[a]	Determine if connections to external systems are identified
3.1.20	3.1.20[b]	Determine if the use of external systems is identified
3.1.20	3.1.20[c]	Determine if connections to external systems are verified
3.1.20	3.1.20[d]	Determine if the use of external systems is verified
3.1.20	3.1.20[e]	Determine if connections to external systems are controlled / limited
3.1.20	3.1.20[f]	Determine if the use of external systems is controlled / limited
3.1.2	3.1.2[a]	Determine if types of transactions and functions that authorized users are permitted to execute
3.1.2	3.1.2[b]	Determine if system access is limited to the defined types of transactions and functions for auth
3.1.21	3.1.21[a]	Determine if the use of portable storage devices containing CUI on external systems is identified
3.1.21	3.1.21[b]	Determine if limits on the use of portable devices containing CUI on external systems are define
3.1.21	3.1.21[c]	Determine if the use of portable storage devices containinfg CUI on external systems is limited a
3.1.22	3.1.22[a]	Determine if individuals authorized to post or process information or publicly accessible system
3.1.22	3.1.22[b]	Determine if procedures ensure CUI is not posted or processed on pubicly accessible systems a
3.1.22	3.1.22[c]	Determine if a review process is in place prior to posting of any content to publicly accessible sy
3.1.22	3.1.22[d]	Determine if content on pubicly accessible systems is reviewed to ensure that it does not includ
3.1.22	3.1.22[e]	Determine if mechanisms are in place to remove and address improper posting of CUI
3.1.3	3.1.3[a]	Determine if Information Flow control policies are defined
3.1.3	3.1.3b]	Determine if methods and enforcement mechanisms for controlling the flow of CUI are defined
3.1.3	3.1.3[c]	Determine if designated sources and destinations (e.g., networks, individuals and devices) for C
3.1.3	3.1.3[d]	Determine if authorizations for controlling the flow of CUI are defined
3.1.3	3.1.3[e]	Determine if authorizations for controlling the flow of CUI are enforced
3.1.4	3.1.4[a]	Determine if the duties of individuals requiring separation are defined.
3.1.4	3.1.4[b]	Detemine if the responsibilities for duties that require separation are assigned to separate indiv
3.1.4	3.1.4[c]	Detemine if access privileges that enable individuals to exercise the duties that require separat
3.1.5	3.1.5[a]	Determine if privileged accounts are identified
3.1.5	3.1.5[b]	Determine if access to privileged accounts is authorized in accordance with the principle of lea
3.1.5	3.1.5[c]	Determine if security functions are identified
3.1.5	3.1.5[d]	Determine if access to security functions is authorized with the principle of least privilege
3.1.6	3.1.6[a]	Determine if non-privileged account functions are defined

3.1.6	3.1.6[b]	Determine if users are required to use non-privileged accounts when accessing nonsecurity fun
3.1.7	3.1.7[a]	Determine if privileged functions are defined
3.1.7	3.1.7[b]	Determine if non-privileged users are identified
3.1.7	3.1.7.[c]	Determine if non-privileged users are prevented from executing privileged functions
3.1.7	3.1.7.[d]	Determine if the execution of privileged functions is captured in audit logs
3.1.8	3.1.8[a]	Determine if the means of limiting unsuccessful login attempts is defined
3.1.8	3.1.8[b]	Determine if the means of limiting unsuccessful login attempts is implemented
3.1.9	3.1.9[a]	Determine if privacy and security notices required by CUI-specified rules are identified, consist
3.1.9	3.1.9[b]	Determine If privacy and security notices are displayed