Wiki Template for Management Assertions, IAP 1.2

Link to InCommon Identity Assurance Profiles Bronze and Silver

4.2 Specification of Identity Assurance Requirements	This section contains all of the normative language for the Bronze and Silver IAPs.
4.2.1 Business, Policy and Operational Criteria	IdP Operators must have the organizational structures and processes to come into and remain in compliance with the provisions of this IAP.
Criteria	**Management Assertion** <Institution> is a legal entity that is an InCommon Participant in good standing, and has the organizational structures and processes to comply with the provisions of this IAP.
.1 InCommon Participant.	
.2 Notification to InCommon	
.3 Continuing Compliance	
.4 IdPO Risk Management	
4.2.2 Registration and Identity Proofing	Identity proofing in this IAP uses verified information to create a record for the Subject in the IdPO's IdMS.
Criteria	**Management Assertion** <Institution> asserts that identity proofing in this IAP is based on a government-issued ID and that information verified at the time of employment is used to create a record for the Subject in <Institution's> Identity Management System.
.1 RA authentication	
.2 Identity verification process	
.3 Registration records	
.4 Identity proofing	
.4.1 Existing relationship	
.4.2 In-person proofing	
.4.3 Remote proofing	
.5. Address of Record confirmation	
4.2.3 Credential Technology	These InCommon IAPs are based on use of "shared Authentication Secret" forms of identity Credentials. If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements.
Criteria	**Management Assertion** <Institution> uses a shared authentication secret that meets the requirements of this IAP. or <Institution> uses a multi factor authentication credential. <Institution> asserts that this multi-factor credential meets or exceeds the requirements of the IAP. Additional guidance is provided in NIST 800-63.
.1 Credential unique identifier	
.2 Basic resistance to guessing Authentication Secret	
.3 Strong resistance to guessing Authentication Secret	
.4 Stored Authentication Secrets	
.5 Basic Protection of Authentication Secrets	
.6 Strong Protection of Authentication Secrets	
4.2.4 Credential Issuance and Management	The authentication Credential must be bound to the physical Subject and to the IdMS record pertaining to that Subject.
Criteria	**Management Assertion** The authentication Credential is bound to the physical Subject and to the IdMS record pertaining to the Subject.
.1 Credential issuance process	
.2 Credential revocation or expiration	
.3 Credential renewal or re-issuance	
.4 Retention of Credential issuance records	
4.2.5 Authentication Process	The Subject interacts with the IdP to prove that he or she is the holder of a Credential, enabling the subsequent issuance of Assertions.
Criteria	**Management Assertion** <Institution's> IdP authentication implementation allows the Subject to interact with the IdP in a manner that proves he or she is the holder of a Credential, thus enabling the subsequent issuance of Assertions.
.1 Resist replay attack	
.2 Resist eavesdropper attack	
.3 Secure communication	
.4 Proof of Possession	
.5 Session authentication	
.6 Mitigate risk of Credential compromise	

4.2.6 Identity Information Management	Subject records in the IdPO's IdMS must be managed appropriately so that Assertions issued by the IdPO's IdP are valid.
Criteria	**Management Assertion** Subject Records are managed appropriately so that Assertions issued by the IdP are valid. IdPO management practices are described below and documented at <Insert link to documentation.>
.1 Identity record qualification	
4.2.7 Assertion Content	The IdPO must have processes in place to ensure that information about a Subject's identity conveyed in an Assertion of identity to an SP is from an authoritative source.
Criteria	**Management Assertion** Processes are in place at <Institution> to ensure that information about a Subject's identity conveyed in an Assertion of identity to an SP is from an authoritative source.
.1 Identity Attributes	
.2 Identity Assertion Qualifier	
.3 Cryptographic security	
4.2.8 Technical Environment	IdMS Operations must be managed to resist various potential threats such as unauthorized intrusions and service disruptions that might result in false Assertions of Identity or other erroneous communications.
Criteria	**Management Assertion** <Institution's> IdMS Operations are managed to resist various potential threats such as unauthorized intrusions and service disruptions that might result in false Assertions of Identity or other erroneous communications.
.1 Software maintenance	
.2 Network security	
.3 Physical security	
.4 Reliable operations	