Template for Gap Analysis IAP 1.2 - Bronze and Silver

InCommon Bronze and Silver Gap Analysis

Identity Assurance Profile (IAP) Functional Areas from InCommon Identity Assurance Profiles Bronze and Silver 1.2:
4.2.1 Business, Policy, and Operational Criteria
4.2.2 Registration and Identity Proofing
4.2.3 Credential Technology
4.2.4 Credential Issuance and Management
4.2.5 Authentication Process
4.2.6 Identity Information Management
4.2.7 Assertion Content
4.2.8 Technical Environment

Action item (identify section, sub-section, and the gap to close)	B	S	Who (Univ. unit)	Type (documentation, infrastructure, procedure, policy, Identity management system)	Effort (Major, moderate, minor)	Target completion date
4.2.1 Business, Policy, and Operational Criteria						
4.2.1.1 InCommon participant - <Add your gap closure requirement here>	•	•	Department XYZ	<type>	<effort>	mm/dd/yyyy or DONE
4.2.1.2 Notification to InCommon -	•	•				
4.2.1.3 Continuing compliance -	•	•				
4.2.1.4 IdPO risk management -	•	•				
4.2.2 Registration and Identity Proofing						
4.2.2.1 RA Authentication -	n/a	•				
4.2.2.2 Identity verification process -	n/a	•				
4.2.2.3 Registration Records -	n/a	•				
4.2.2.4 Identity Proofing -	n/a	•				
4.2.2.4.1 Existing relationship -	n/a	•				
4.2.2.4.2 In-Person proofing -	n/a	•				
4.2.2.4.3 Remote proofing -	n/a	•				
4.2.2.5 Address of record confirmation -	n/a	•				
4.2.2.6 Protection of personally identifiable information -	•	•				
4.2.3 Credential Technology						
4.2.3.1 Credential unique identifier -	•	•				
4.2.3.2 Basic resistance to guessing authentication secret -	•	n/a				
4.2.3.3 Strong resistance to guessing authentication secret -	n/a	•				
4.2.3.4 Stored authentication secrets --	n/a	•				
4.2.3.5 Basic protection of authentication secrets -	•	n/a				
4.2.3.6 Strong protection of authentication secrets -	n/a	•				
4.2.4 Credential Issuance and Management						
4.2.4.1 Credential issuance -	•	•				
4.2.4.2 Credential revocation or expiration -	•	•				
4.2.4.3 Credential renewal or re-issuance -	•	•				
4.2.4.4 Credential issuance records retention -	n/a	•				
4.2.4.5 Resist token issuance tampering threat -	•	•				
4.2.5 Authentication Process						
4.2.5.1 Resist replay attack -	•	•				
4.2.5.2 Resist eavesdropper attack -	•	•				
4.2.5.3 Secure communication -	•	•				
4.2.5.4 Proof of possession -	•	•				
4.2.5.5 Resist session hijacking threat -	•	•				
4.2.5.6 Mitigate risk of credential compromise -	•	•				
4.2.6 Identity Information Management						
4.2.6.1 Identity record qualification -	•	•				
4.2.7 Assertion Content						
4.2.7.1 Identity attributes -	•	•				
4.2.7.2 Identity assertion qualifier -	•	•				
4.2.7.3 Cryptographic security -	•	•				
4.2.8 Technical Environment						
4.2.8.1 Software maintenance -	n/a	•				
4.2.8.2 Network security -	n/a	•				
4.2.8.3 Physical security -	n/a	•				
4.2.8.4 Reliable operations -	n/a	•				