InCommon Identity Assurance and HEISC Information Security Guide Cross Reference

InCommon IAP and Information Security Guide – a Cross Reference updated for IAP v1.2 and ISO 27002:2013

Link to InCommon Identity Assurance Profiles Bronze and Silver v1.2
Link to HEISC Information Security Guide

4.2 Specification of Identity Assurance Requirements	Applicable Topics in the Information Security Guide
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.	ISO 6 Organization of Information Security
.1 InCommon Participant.	ISO 18 Compliance
.2 Notification to InCommon	ISO 18 Compliance
.3 Continuing Compliance	ISO 18 Compliance
4.2.2 Registration and Identity Proofing	ISO 7 Human resources Security. Including pre-employment screening procedures in the Guide could help InCommon participants. Alternatively, the Guide might point to the IAP for identity proofing procedures for onboarding employees. ISO 9 Access control Page 59 of AACRAO Vol. 87 No. 3: Establishing Remote Student Identity would be a useful reference for the Guide. See definitions from the AACRAO article at InCommon Assurance Remote Proofing Definitions and Concepts
.1 RA authentication	ISO 9.2 User access management ISO 10 Cryptography
.2 Identity verification process	ISO 9.2 User access management
.3 Registration records	ISO 9.1 Business Requirements for Access Control ISO 9.2 User access management
.4 Identity proofing	ISO 7.1 Prior to employment
.4.1 Existing relationship	ISO 7.1 Prior to employment
.4.2 In-person proofing	ISO 7.1 Prior to employment
.4.3 Remote proofing	ISO 7.1 Prior to employment
.5. Address of Record confirmation	ISO 7.1 Prior to employment
4.2.3 Credential Technology	ISO 9 Access control ISO 10 Cryptography
Criteria	
.1 Credential unique identifier	ISO 9.2 User access management
.2 Resistance to guessing Authentication Secret	ISO 9.4 System and application access control ISO 10 Cryptography
.3 Strong resistance to guessing Authentication Secret	ISO 9.4 System and application access control ISO 10 Cryptography
.4 Stored Authentication Secrets	ISO 10 Cryptography
.5 Protected Authentication Secrets	ISO 10 Cryptography
4.2.4 Credential Issuance and Management	ISO 9 Access control
.1 Credential issuance process	ISO 9.2 User access management
.2 Credential revocation or expiration	ISO 9.2 User access management
.3 Credential renewal or re-issuance	ISO 9.2 User access management
.4 Retention of Credential issuance records	
4.2.5 Authentication Process	ISO 9 Access Control ISO 12 Operations security ISO 14 System acquisition, development, and maintenance
Criteria	

.1 Resist replay attack	ISO 14.1 Security requirements of information systems
.2 Resist eavesdropper attack	ISO 12.2 Protection from malware
.3 Secure communication	ISO 14.1 Security requirements of information systems
.4 Proof of Possession	ISO 14.1 Security requirements of information systems
.5 Resist session hijacking threat	ISO 14.1 Security requirements of information systems ISO 14.2 Security in development and support processes
.6 Mitigate credential compromise	ISO 5 Security Policies ISO 9.3 User Responsibilities
4.2.6 Identity Information Management	
Criteria	
.1 Identity record qualification	
4.2.7 Assertion Content	
Criteria	
.1 Identity Attributes	
.2 Identity Assertion Qualifier	
.3 Cryptographic security	ISO 10 Cryptography
4.2.8 Technical Environment	ISO 11 Physical and Environmental Security ISO 12 Operational Security ISO 13 Communications Security ISO 16 Information security incident management
Criteria	
.1 Software maintenance	ISO 12.6 Technical vulnerability management
.2 Network security	ISO 13.1 Network security management
.3 Physical security	ISO 11 Physical and Environmental Security
.4 Reliable operations	ISO 12.1 Operational procedures and responsibilities ISO 12.4 Logging and monitoring ISO 13.1 Network security management ISO 16.1 Management of information security incidents and improvements