 Objective 1: Explain the basic elements of an identity solution
   1.1 Explain identity system components
   1.2 Determine appropriate architectural patterns for identity
   1.3 Differentiate the identity requirements of customer, workforce, and partner audiences
   1.4 Identify the difference between the management of non-human and human identities
   1.5 Explain the implications of privacy, ethics, and bias in relation to identity solutions

 Objective 2: Describe identifiers, identity lifecycle, and identity proofing
   2.1 Demonstrate an understanding of the role of identifiers in the identity lifecycle
   2.2 Describe the characteristics of a digital identity lifecycle
   2.3 Identity proofing and identity binding

 Objective 3: Know the core concepts of security for identity
   3.1 Demonstrate and apply an understanding of fundamental authentication core concepts
   3.2 Demonstrate an understanding of fundamental authorization core concepts
   3.3 Demonstrate an understanding of fundamental access management core concepts
   3.4 Explain the cryptographic essentials of identity systems
   3.5 Describe common security exploitations, vulnerabilities, and best practices
   3.6 Demonstrate an ability to do high-level threat modeling on common identity architectures

 Objective 4: Describe the rules and standards that relate to identity
   4.1 Demonstrate an understanding of the different levels of legal rules that apply to identity systems
   4.2 Explain various approaches to compliance for identity systems
   4.3 Enumerate and describe core IAM standards and standards bodies

 Objective 5: Explain identity operational considerations
5.1 Describe the customer service considerations of identity solutions
5.2 Explain the operational requirements of privilege management in identity
5.3 Explain strategies for identifying and responding to identity operational event
5.4 Demonstrate an understanding of the impact of privacy on identity operations
5.5 Explain specific implications of operating of identity systems