- Security
  - Managed identities for Azure resources
    - registers app in Azure Active Directory
  - Responsibility
    - Customer
      - Data
      - Endpoints
      - Accounts
      - Access Management
  - Inputs and Outputs
    - Inputs
      - SQL Injection
      - Validate input always
      - Use parameterized queries
    - Output
      - Always encode
      - Cross-Site Scripting (XSS).
  - Encryption
    - Types
      - Semmetric
        - Uses the same key to encrypt and decrypt the data
      - Asymmetric
        - Uses a public key and private key pair
        - Either key can encrypt
        - Single key can't decrypt its own encrypted data
    - Approaches
      - Encryption at rest
      - Encryption in transit
    - Azure Services
      - Storage Services
        - Automatic encryption before persisting
        - Automatic decyption on retrieval
      - Disk Encryption
        - BitLocker
          - Windows
        - dm-crypt
          - Linux
        - Integrated with KeyVault
      - Transparent Data Encryption
        - Real time encryption
        - Enabled for Azure SQL
          - Unique key per logical server intance
        - Can use a custom key
    - Certificates
      - x.509 V3
        - signed by a trusted certificate authority
        - self-signed
      - Types
        - Service
          - attached to cloud services
        - Management
          - authenticate with the classic deployment model.
          - not related to cloud services
  - Implement OAuth2 authentication
    - Authentication
      - OpenID Connect
        - built on top of OAuth 2.0
      - proving you are who you say you are
    - Authorization
      - OAuth 2.0
      - act of granting an authenticated party permission to do something
    - Security tokens
      - Types
        - ID tokens
          - ID tokens are sent to the client application as part of an OpenID Connect flow. They can be sent along side or instead of an access token, and are used by the client to authenticate the user
        - access token
          - security token that is issued by an authorization server as part of an OAuth 2.0 flow
          - JWT
          - Claims
            - Header
              - Provides information about how to validate the token
            - Payload
              - data about the user or app
            - Signature
              - raw material used to validate the token
        - refresh token
          - client application can then exchange this refresh token for a new access token when needed
          - Token timeouts
            - token lifetime configuration, the lifetime of refresh tokens can be altered
          - Revocation
            - Refresh tokens can be revoked by the server due to a change in credentials, or due to use or admin action
      - Validation
        - Signing
          - token is signed by the Security Token Server (STS) with a private key
          - STS publishes the corresponding public key
        - signature segment can be used to validate the authenticity of the token