FISMA C&A

1. What is FISMA?

- The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.
- The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.
- Reference :
  - https://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act
  - https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

2. What is C&A (Certification and Accreditation)?

- Certification involves the testing and evaluation of the technical and nontechnical security features of an IT system to determine its compliance with a set of specified security requirements (in our case - FISMA).
- Accreditation is a process whereby a authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.
- Reference :
  - https://web.archive.org/web/20110726055231/http://www.fismapedia.org/index.php?title=Certification_and_Accreditation

3. AWS FISMA Compliance

- AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (FISMA).
- This accreditation covers Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC) and the infrastructure upon which they run.
- Reference :
  - https://aws.amazon.com/compliance/fisma/
  - https://aws.amazon.com/about-aws/whats-new/2011/09/15/aws-fisma-moderate/

4. Firebase and Google Cloud FISMA Compliance

- Firebase itself is not FISMA compliant, but it uses Google Cloud App Engine which is FISMA compliant.
- Reference :
  - https://cloud.google.com/security/compliance/nist800-53/
  - https://cloud.googleblog.com/2011/04/the-truth-about-google-apps-and-fisma.html
  - https://cloud.google.com/solutions/mobile/images/overview-firebase-appengine-standard.png

5. Twilio FISMA Compliance

- As of now, Twilio is not FISMA compliant.
- Reference:
    - Section ‘R’ in https://www.twilio.com/legal/amendment-tos

Q: How does an organization determine whether they are FISMA compliant?

- They must categorize their system and identify the controls that need to be implemented. Then they must demonstrate that they’ve implemented the controls identified in NIST 800-53 and developed the associated supporting policies, processes, and procedures to support the secure operation of the system. The assessment of the security controls should be conducted by an independent assessor with a background and experience with the NIST 800-53 controls, the assessment processes, and the ability to document compliance with the controls.
- Based on the outcome of the assessment of the controls, an Authorizing Official (AO) will determine if the risk is acceptable to allow the system to operate in “production,” or to process, store, and transmit “live” government data. An AO is “a senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation” (SP 800-37, Rev 1). The AO determines whether the system sufficiently protects the confidentiality, integrity, and availability of the system and therefore accepts the risk and responsibility for the security of the system. If the risk is sufficiently low, then the AO will grant an ATO which is an Authority to Operate. Receiving an ATO essentially demonstrates FISMA compliance.
- Reference :
    - https://linfordco.com/blog/fisma-compliance/
    - https://nvd.nist.gov/800-53