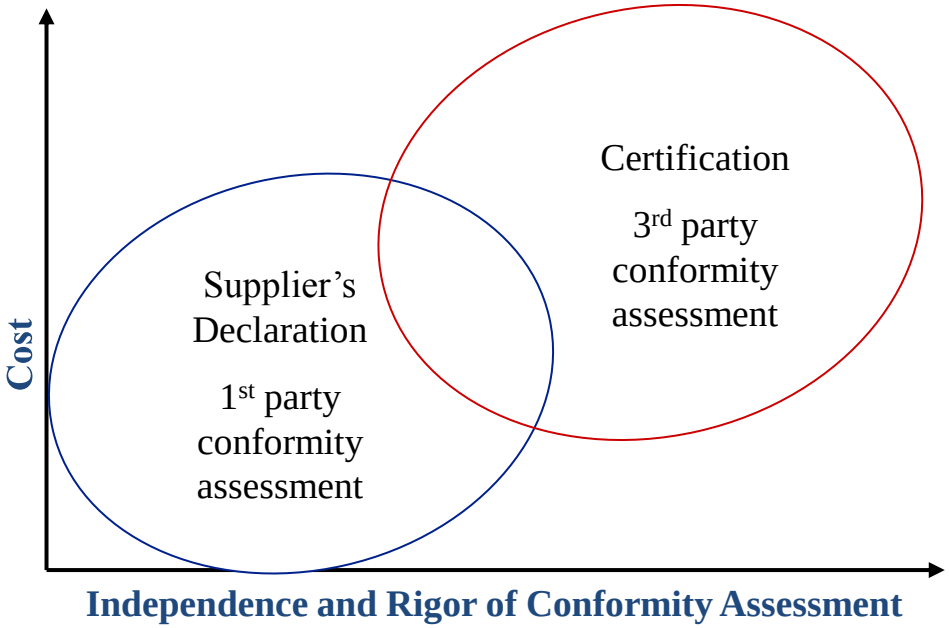
Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP 3PAOs: Management Requirements

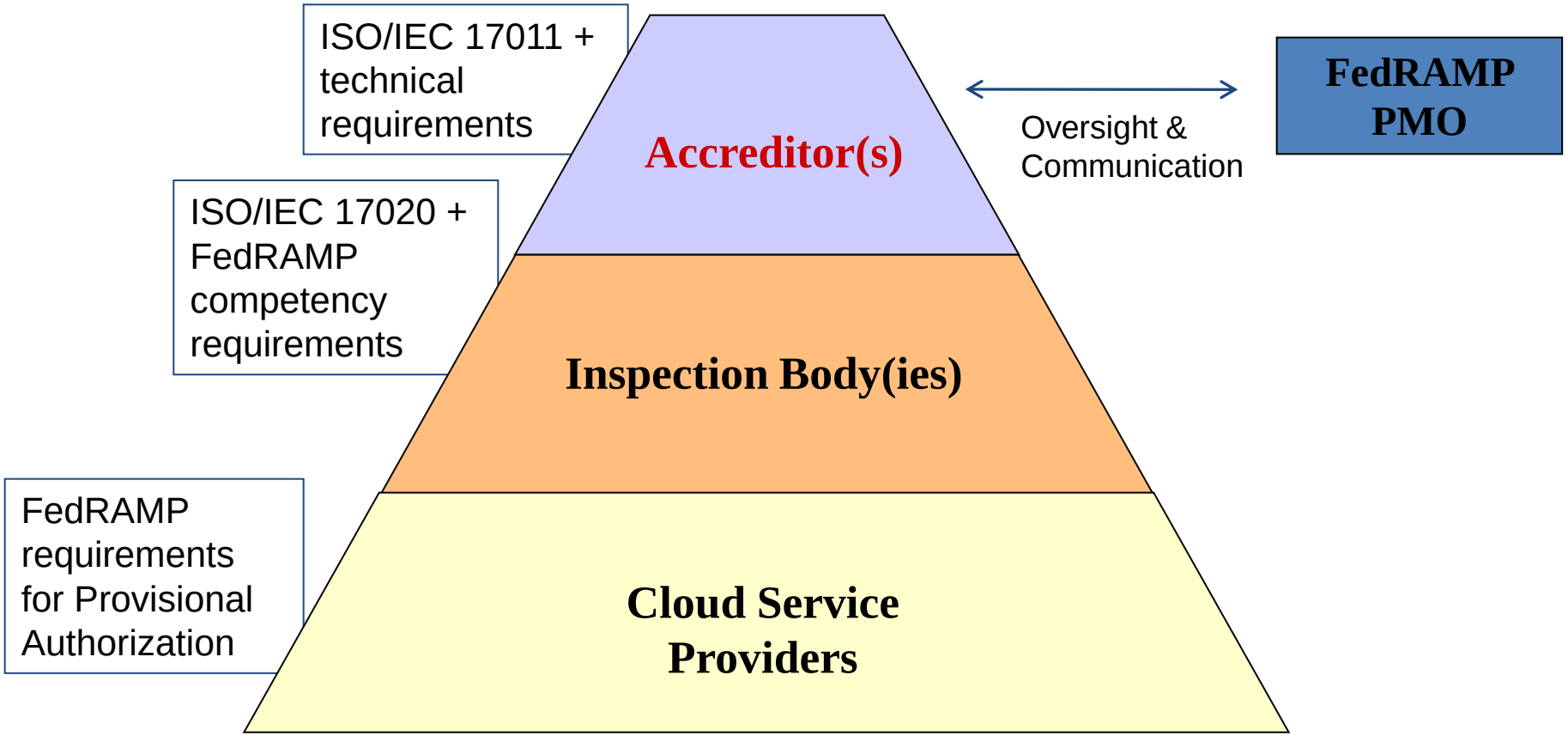
Gordon Gillerman
Manager – NIST Standards Services
National Institute of Standards & Technology

Federal Programs using Conformity Assessment Approaches

- Examples: Health IT, FCC, CPSC (toys), WaterSense, CMVP
  - Balance confidence to impact of non-conformance
  - Maximize confidence and minimize market burden and cost
  - Maximize private sector business to minimize Fed resource

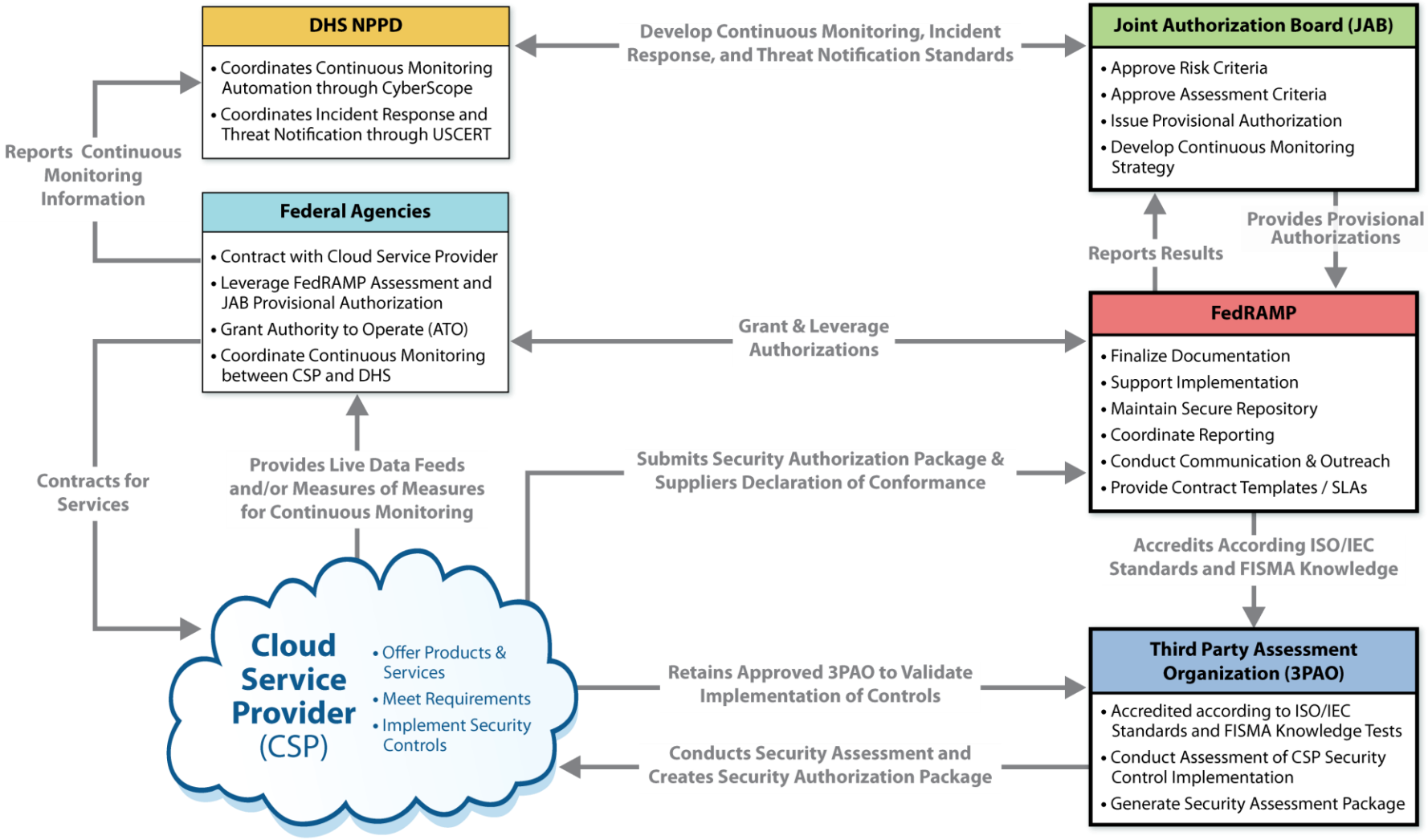


Notional Conformity Assessment Hierarchy for Inspection



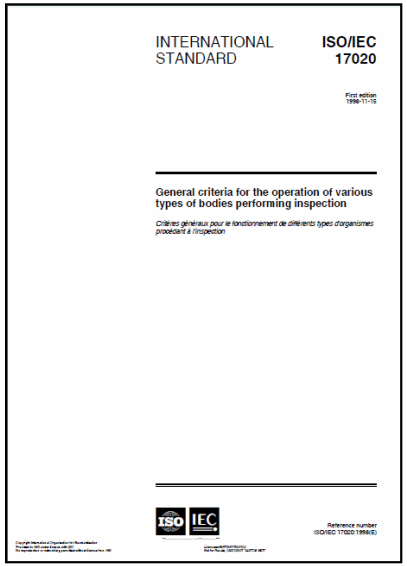
ISO/IEC 17011; Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17020; General criteria for the operation of various types of bodies performing inspection

FedRAMP Stakeholder Roles and Interaction



Inspection Body
Roles & Responsibilities

- Accredited Inspection Body assesses cloud service provider based on FedRamp security requirements
- Participates in ongoing FedRamp activities to continuously improve FedRamp program



INTERNATIONAL STANDARD

ISO/IEC 17020

First edition
1998-11-15

General criteria for the operation of various types of bodies performing inspection

Critères généraux pour le fonctionnement de différents types d'organismes procédant à l'inspection

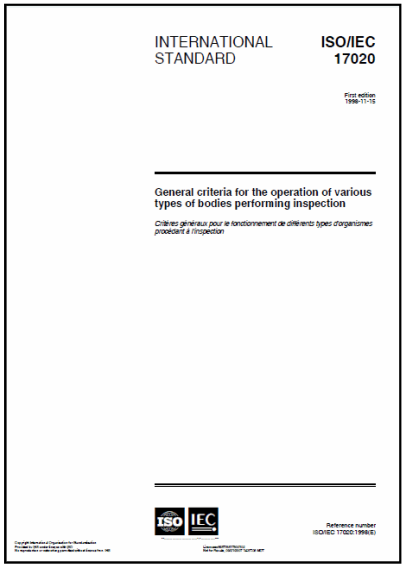
Reference number
ISO/IEC 17020:1998(E)

Additional FedRamp Admin/Tech Requirements

- Shall meet FedRAMP technical competency requirements
- Shall use security assessment method required by FedRAMP
- Shall produce security assessment reports required by FedRAMP
- …

ISO/IEC 17020:1998

Applicants attest to conforming to the requirements and commit to meet them on an ongoing basis.


INTERNATIONAL STANDARD

ISO/IEC 17020

First edition
1998-11-15

General criteria for the operation of various types of bodies performing inspection

Critères généraux pour le fonctionnement de différents types d'organismes procédant à l'inspection

Reference number
ISO/IEC 17020:1998(E)

- **ISO/IEC 17020:1998 (Significant Sections)**
- Organization identity, inspection services & other services
- Independence, impartiality & integrity
- Confidentiality
- Roles & responsibilities
- Quality management system
- Personnel
- Inspection methods & procedures
- Records
- Subcontracting
- Complaints & Appeals
- Cooperation

Useful Resources

- http://www.fedramp.gov
- ISO/IEC 17020:1998

  http://www.iso.org/iso/catalogue_detail?csnumber=29342
- Guidelines for Implementation of ISO/IEC 17020:1998 (Google '17020 guidelines')
  - ILAC: *http://www.ilac.org/documents/IAF-ILAC-A4_2004_guidance_on_the_application_of_ISO-IEC_17020.pdf*
  - *IAS: http://www.iasonline.org/Inspection_Agencies/iamr.pdf*

* Guideline documents listed here does not imply endorsement of organizations by GSA or NIST