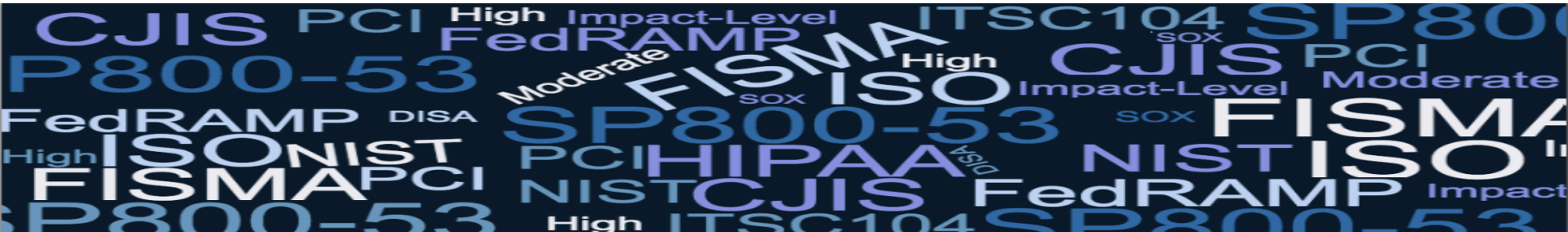
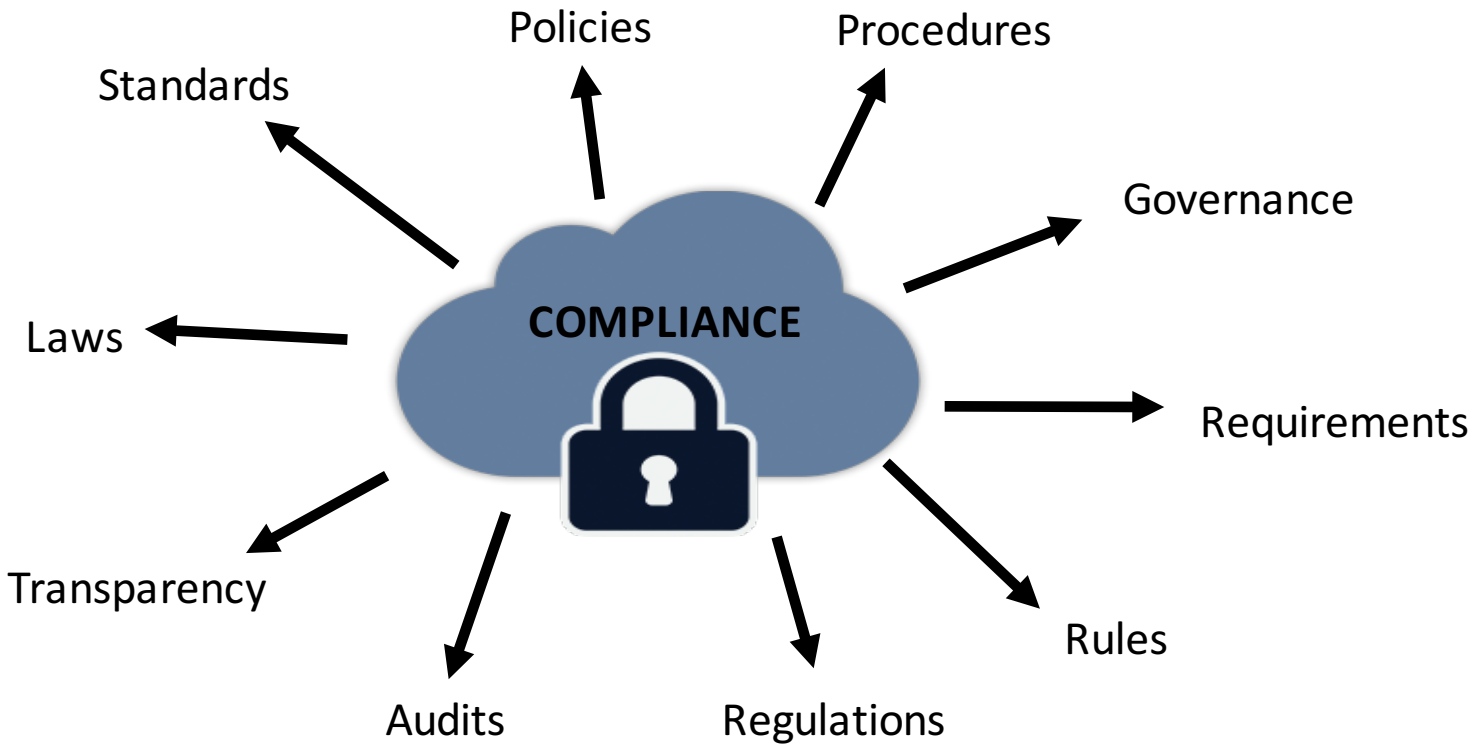
Regulatory Compliance in the Cloud

David L. Jenkins
IBM Executive Architect
david.jenkins@us.ibm.com



Is my data secure in the cloud?

- Access Controls
  - How many times can I try to login?
  - How many authentication factors are required?
  - What are the password requirements?
- Security Boundaries
  - Is the industrial controls network (think HVAC, lighting, etc) on the same network as the Applications?
  - Is every boundary interface managed, controlled, monitored?
  - Do firewalls fail to a secure state?
- Encryption
  - Is my data encrypted? As it travels across the network and when its stored
  - What encryption algorithm is used?
- Physical Access
  - Who has access to the data center where my application/data resides?
  - Are logs correlated, reviewed, monitored? (physical access & system audit)
  - What happens to old computer hardware when it is cycled out and replaced with new?

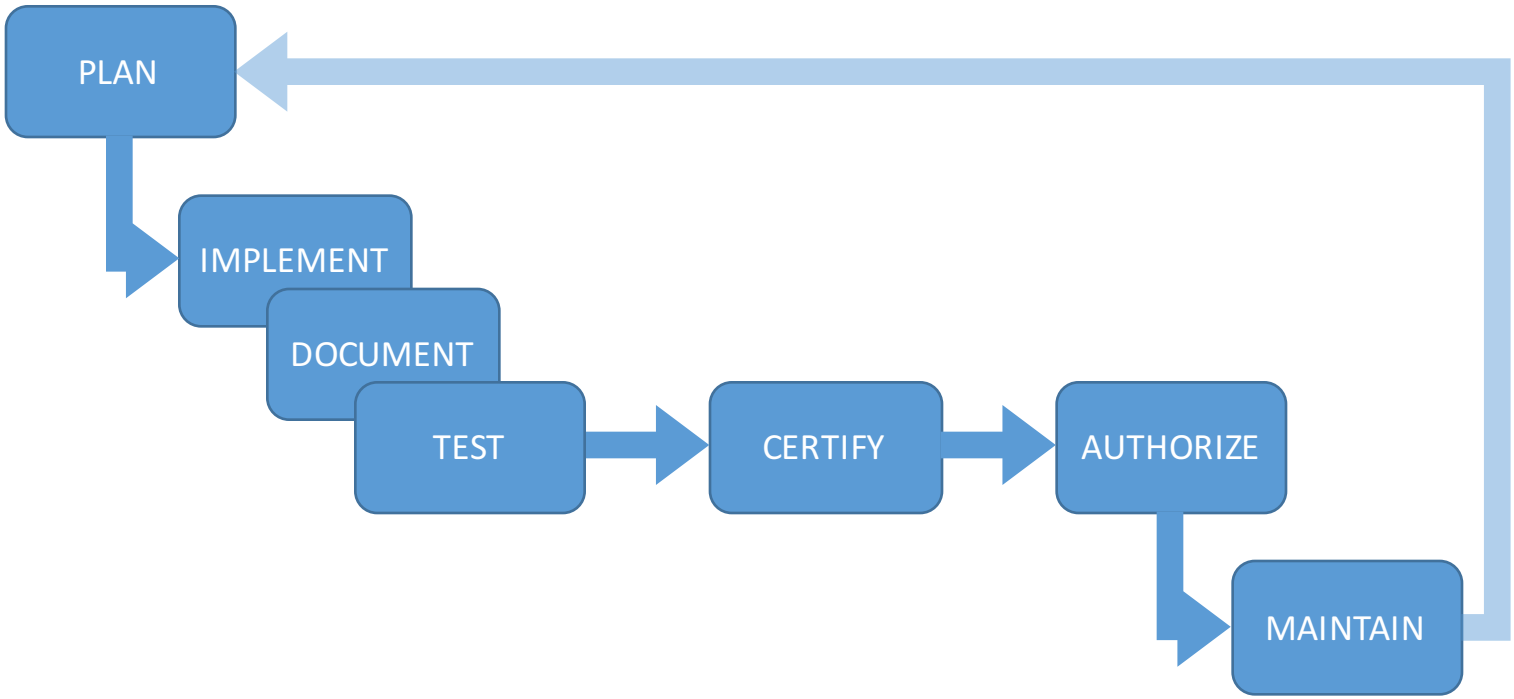

Policies
Procedures
Standards
Governance
COMPLIANCE
Laws
Requirements
Transparency
Rules
Audits
Regulations

Regulatory Types

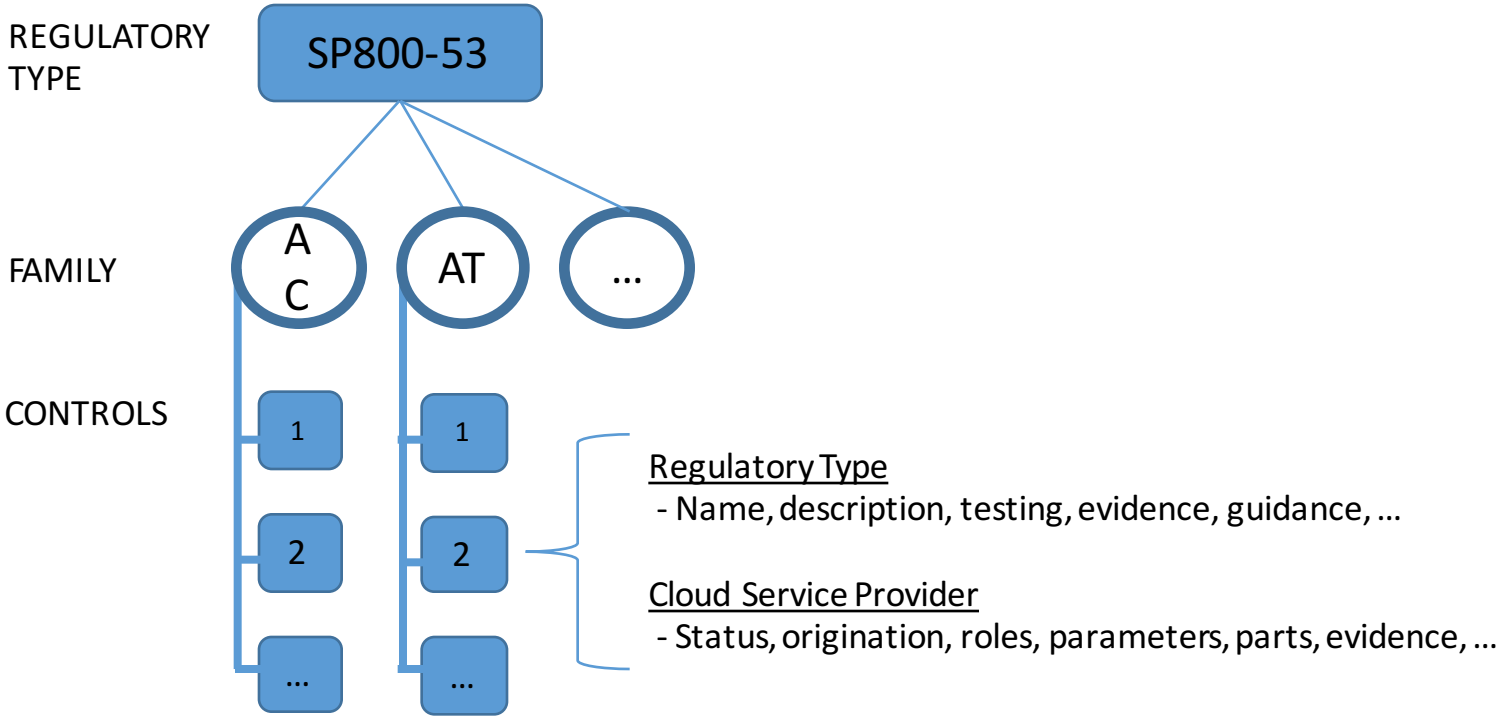
Exist to enable controlled sharing of information, while protecting the privacy and security

- ✓ PCE DSS
- ✓ HIPAA
- ✓ CJIS
- ✓ FISMA
- ✓ DISA
- ✓ FedRAMP
- ✓ CSA
- ✓ SOX
- ✓ Safe Harbor
- ✓ ISO27017/18
- ✓ FFIEC
- ✓ ISO27001
- ✓ ITIL
- ✓ FIPS
- ✓ ITAR
- ✓ NIST
- ✓ SP800-53
- ✓ CobiT
- ✓ ISO27002
- ✓ …

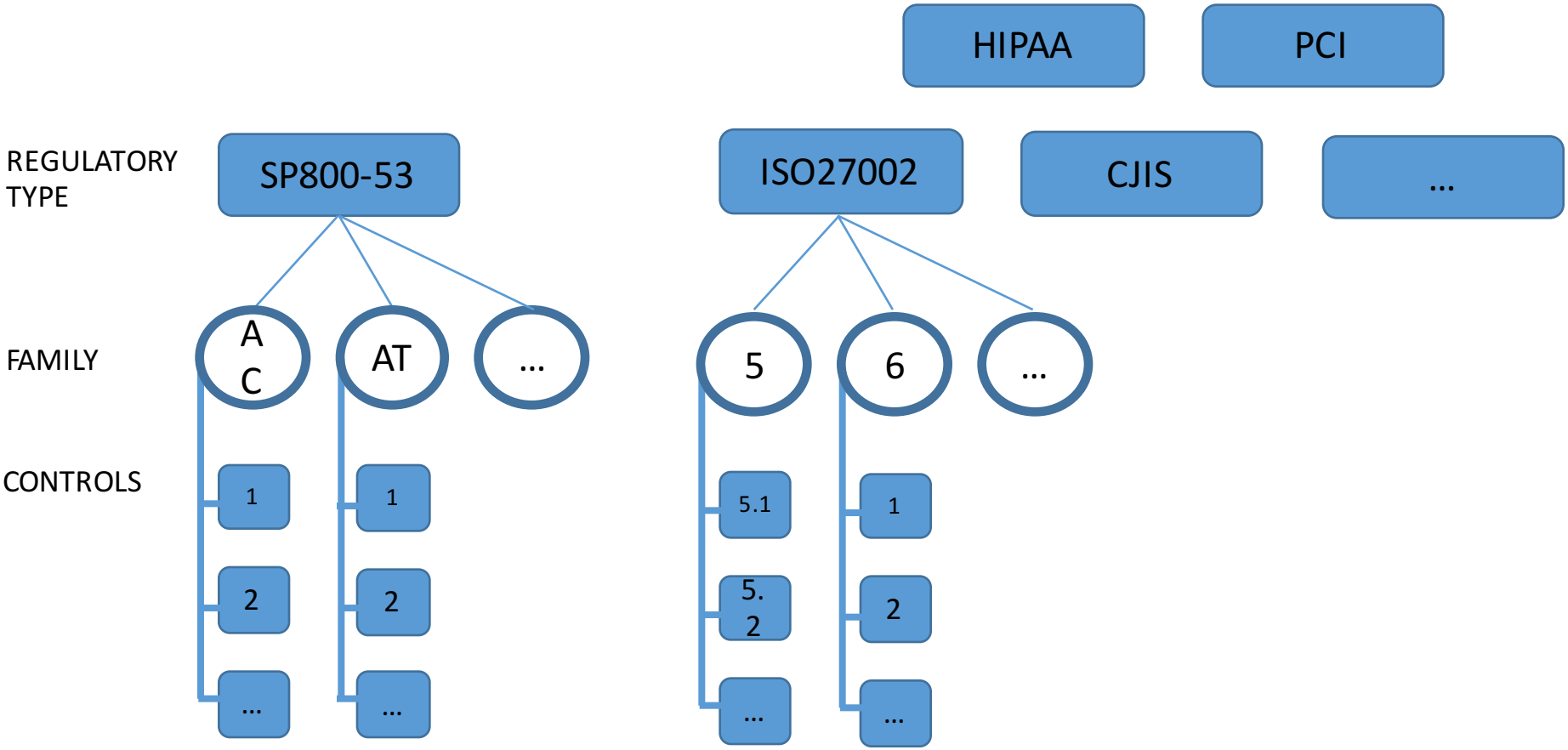
Accreditations, Evaluations and Assessments



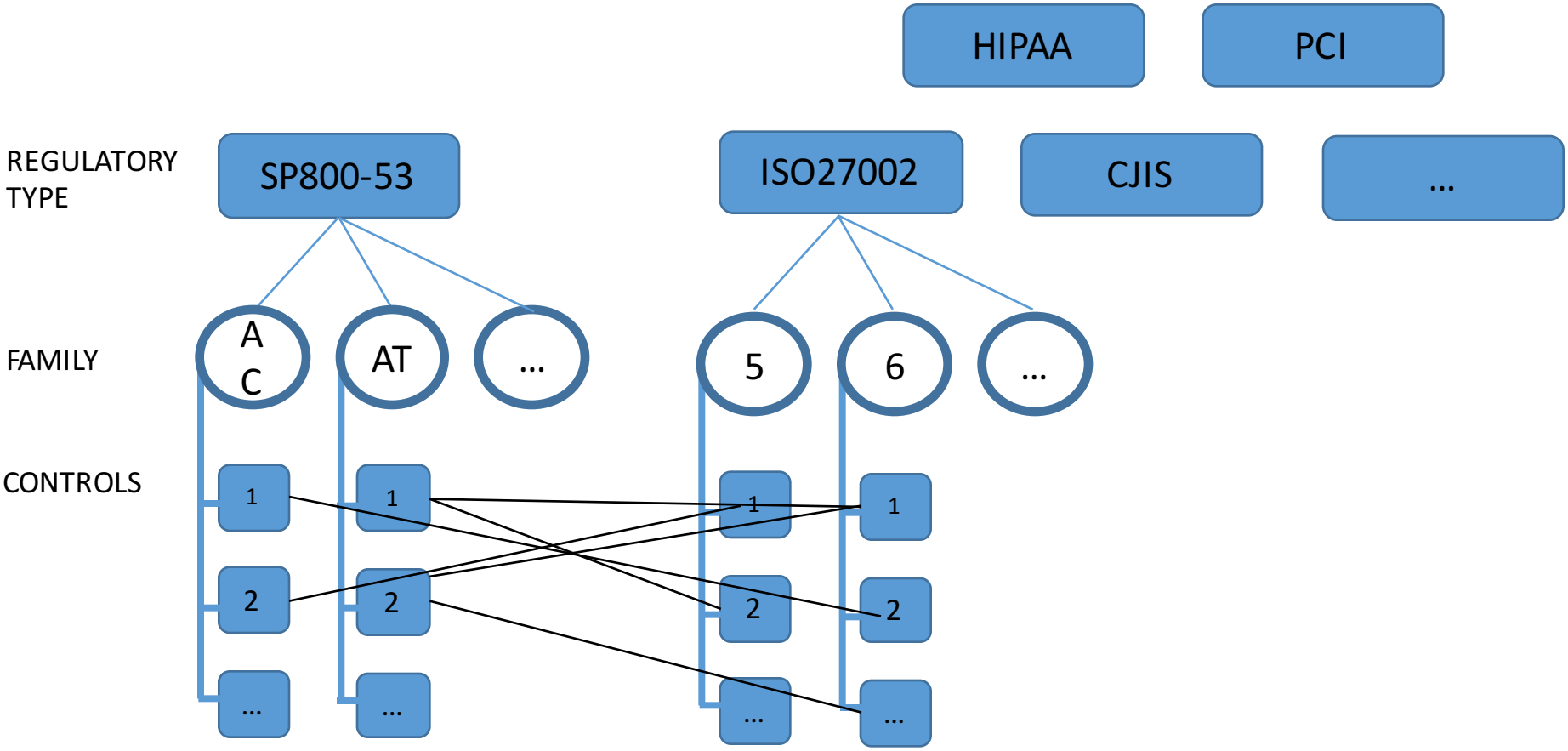
Security Controls - Structure



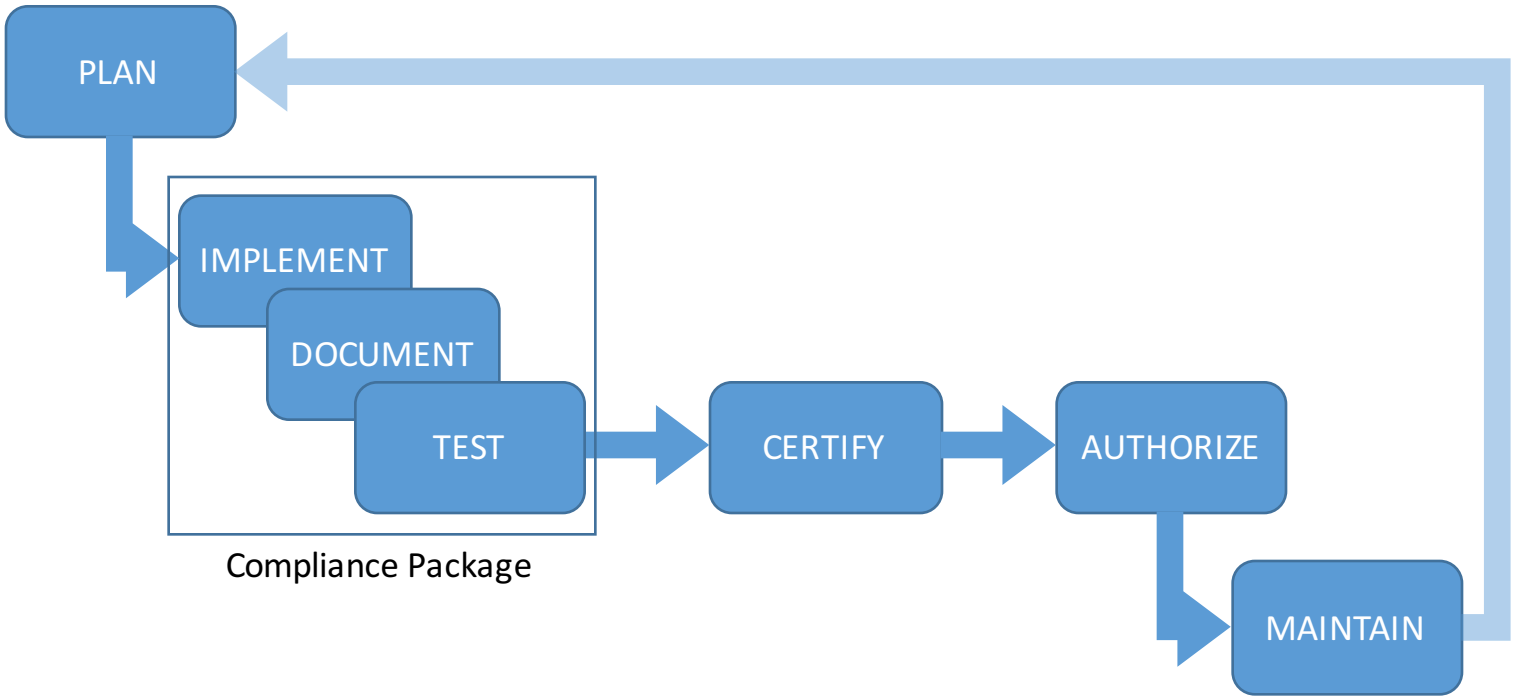
Security Controls – Regulatory Types



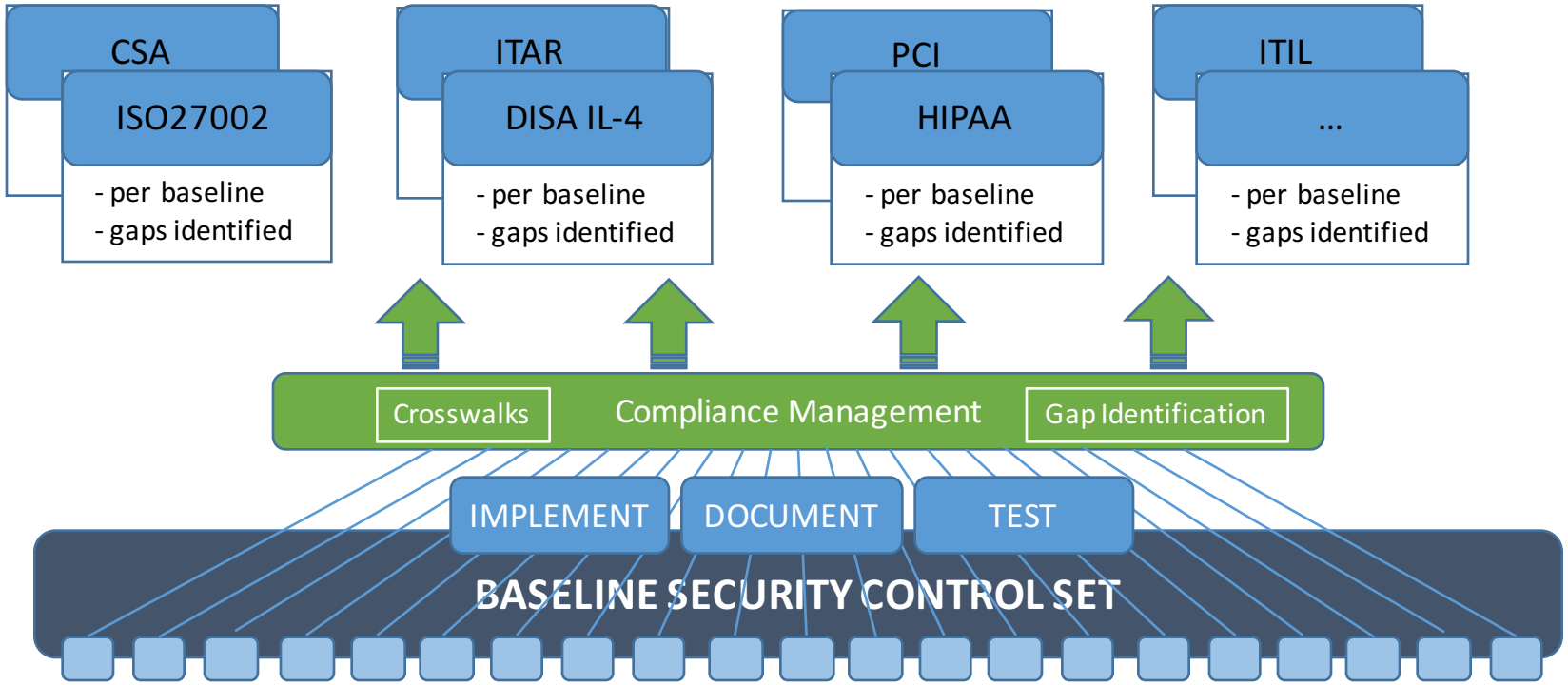
Functionally Equivalent Controls - Crosswalks



Accreditations, Evaluations and Assessments



Baseline Security Compliance



Selecting a baseline

Criteria

- Standards-based
- Comprehensive
- Detailed
- Industry Supported

Options

1. NIST SP800-53
2. ISO27002


COMPLIANCE


FedRAMP
DISA
SP800-53
SOX
FISMA
High
ISO
NIST
PCI
HIPAA
NIST
ISO