opengear
A DIGI COMPANY

Demystifying FIPS 140-2: Terminology, Implementation Challenges, and Lessons Learned

Khosrow Ramezani

Agenda

- FIPS overview
- Motivation to adopt FIPS
- FIPS terminology
- Validation process
- Compliance process
- Lessons learned and Implementation notes

FIPS Overview

- U.S. Federal Information Processing Standards.
- Collection of standards for information security.
- Mandated for federal agencies like NSA, CSI, NIST.
- Often adopted by U.S. states and non-governmental agencies.
- Embraced by other countries and Common Criteria.
- Focuses on cryptographic security for sensitive data.
- Applies to computer, telecom, and voice systems.
- Mandatory for designing modules in federal departments.
- Bars use of unvalidated cryptography in federal systems

FIPS 140 Overview

FIPS 140-2

Published in 2001

Change notes were incorporated in 2002

Recently, FIPS 140-2 underwent a review

Sunset in 2026

FIPS 140-3

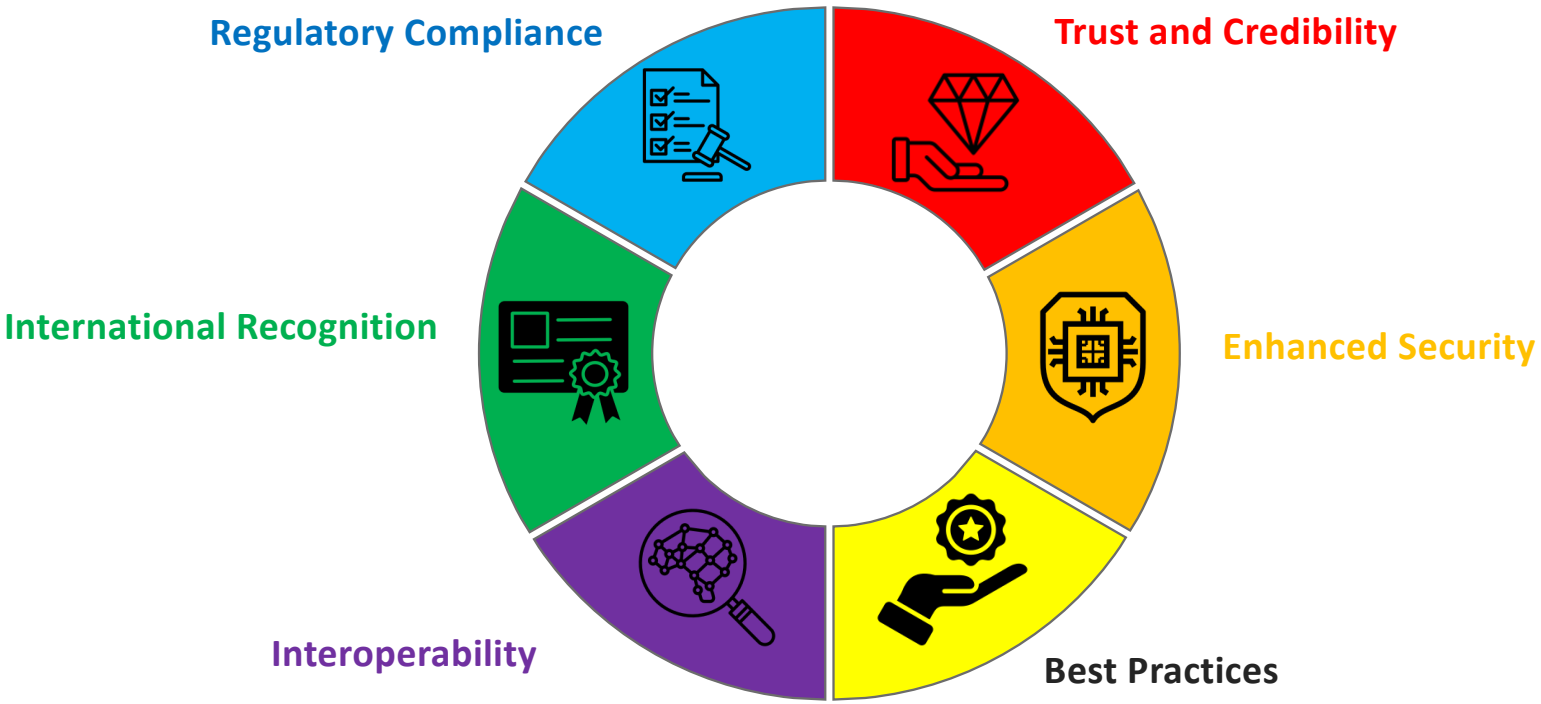
Supersedes FIPS 140-2

Published in March 2019

ISO/IEC 19790:2012

ISO/IEC 24759:2014

Motivation to adopt FIPS



FIPS functional areas

1. **Cryptographic Module Specification**
   Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation.

2. **Cryptographic Module Ports and Interfaces**
   Required and optional interfaces ,logically or physically separation of ports

3. **Roles, Services, and Authentication**
   Logical separation of roles , Role-based or identity-based, Identity-based authentication

4. **Finite State Model**
   Specification of finite state model and diagrams

5. **Physical Security**
   Production grade equipment, Locks or tamper evidence, Tamper detection and response for covers and doors. Tamper detection and response envelope. EFP or EFT.

FIPS functional areas

6 **Operational Environment**
Single operator, PPs evaluated at EAL2 to EAL4

7 **Cryptographic Key Management**
Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization

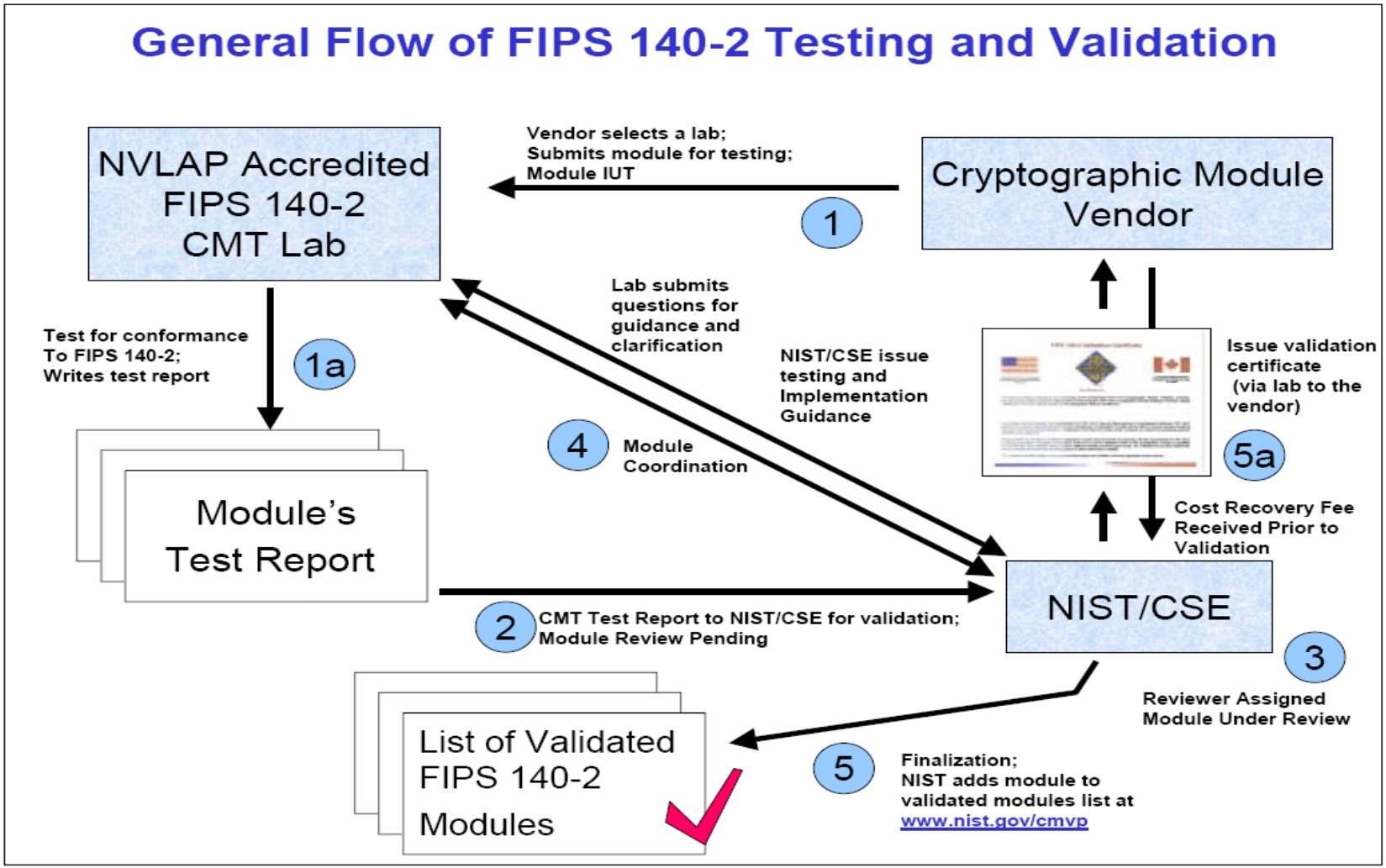
8 **EMI/EMC**
47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio)

9 **Self-Tests**
Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests

10 **Design Assurance**
Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents

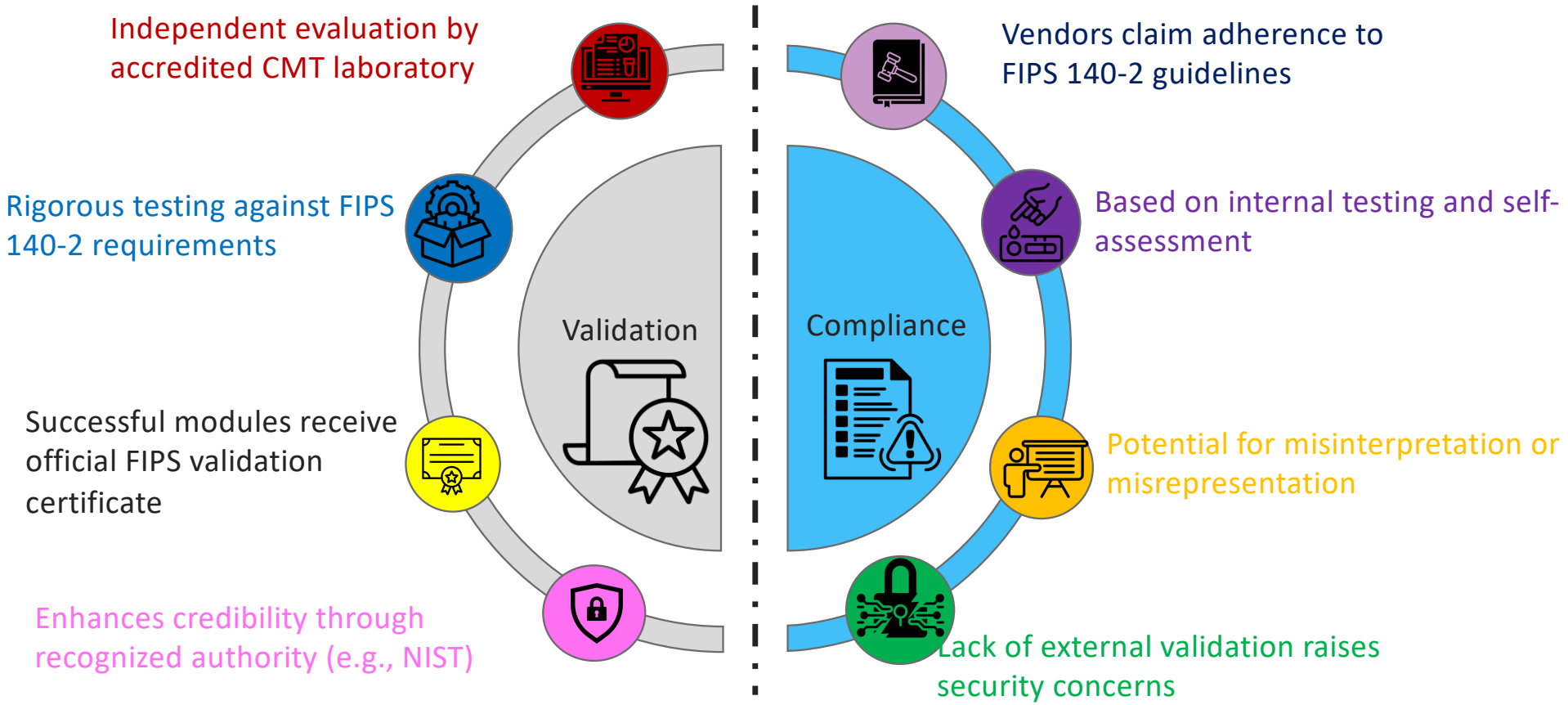
11 **Mitigation of Other Attacks**
Specification of mitigation of attacks for which no testable requirements are currently available

Validation Process



https://csrc.nist.rip/groups/STM/cmvp/documents/fips140-2/140-2flow.pdf

Compliance vs Validation



Compliance vs Validation

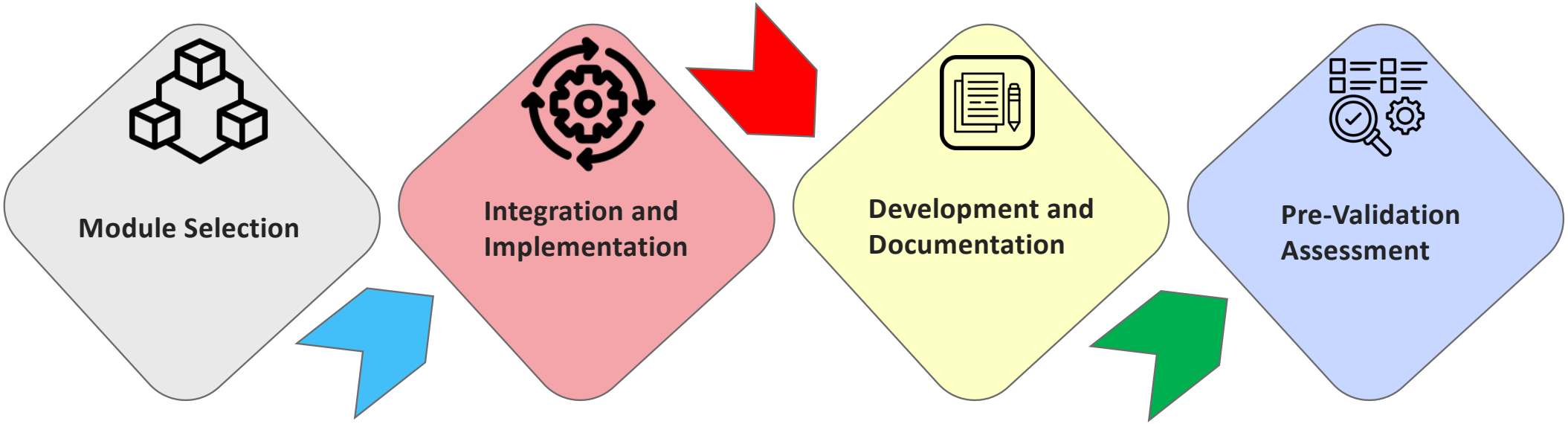
- The dilemma with FIPS validation lies in the
  - complexity
  - cost
  - time

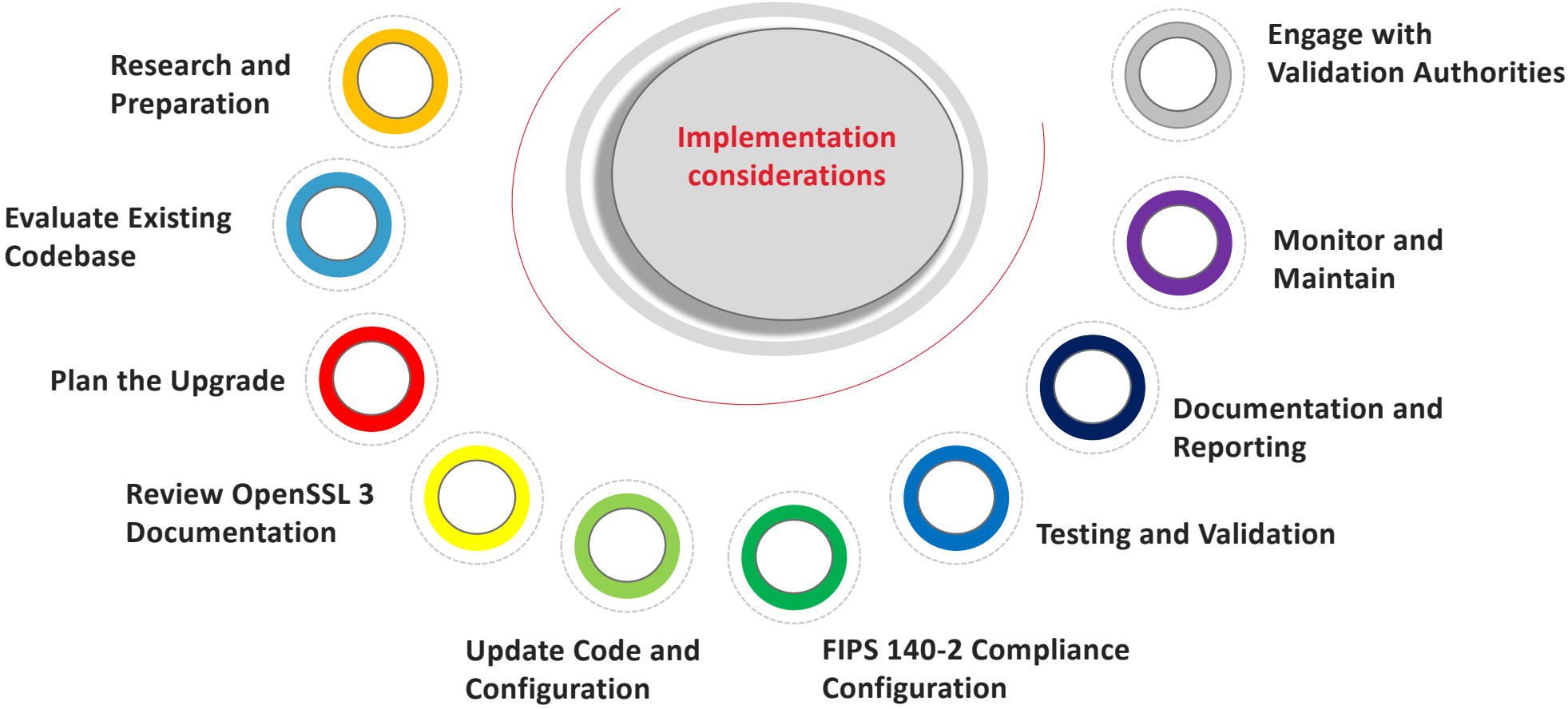
- Validation requires significant effort and resources which is challenging for smaller companies or open-source projects.

- As a result, some products may be technically compliant with FIPS 140-2 but have not undergone the official validation process, leading to potential trust and credibility issues.

- Ultimately, users and organizations need to consider the context and sensitivity of their applications when choosing between FIPS-compliant and FIPS-validated cryptographic modules.

FIPS level 1 Compliance process




Implementation considerations
Research and Preparation
Evaluate Existing Codebase
Plan the Upgrade
Review OpenSSL 3 Documentation
Update Code and Configuration
FIPS 140-2 Compliance Configuration
Testing and Validation
Documentation and Reporting
Monitor and Maintain
Engage with Validation Authorities

Lessons learned

1. Complexity and Stringency
2. Resource Intensive
3. Scope Management
4. Compatibility
5. Vendor Lock-In
6. Performance Impact
7. User Experience
8. Ongoing Maintenance
9. Misinterpretation of Requirements
10. Lack of Flexibility

Certification and frameworks that rely on FIPS 140-2

- **Common Criteria (CC):** International standard evaluating IT product security.
- **Payment Card Industry Data Security Standard (PCI DSS):** Protects credit card transactions; may require FIPS 140-2 for cryptographic modules.
- **Health Insurance Portability and Accountability Act (HIPAA):** Protects patient data; FIPS 140-2 for ePHI encryption.
- **Defense Federal Acquisition Regulation Supplement (DFARS):** Cybersecurity standards for DoD contractors; FIPS 140-2 for defense systems.
- **National Institute of Standards and Technology (NIST) Guidelines:** NIST references FIPS 140-2 for cryptographic module requirements.
- **Federal Risk and Authorization Management Program (FedRAMP):** Standardized cloud provider assessment; FIPS 140-2 for cryptographic services."

Thank You!

Khosrow Ramezani
PhD,CISSP,CCSP
Khosrow.Ramezani@digi.com

www.opengear.com