



# Guidelines for Accreditation of PCIs (SP 800-79-1)

---

- Why a New Version
- What are the Changes
- (The New) PCI Accreditation Methodology
  - Overall Process
  - Building Blocks
- Transitioning Issues

# Why a New Version of SP 800-79

---

- The various business models for PCI (in-house, leased, shared etc) had not developed
- Relationship to SP 800-37 Accreditation was fuzzy (timing, scope etc)
- No previous accreditations to incorporate “Lessons Learnt”
- PIV Product Validation Program was just evolving

# What are the Changes in SP 800-79-1

---

- Removal of Attributes as the basis of Assessments  
– because of subjective nature
- Definition of PCI Boundaries & Relationship to SP 800-37 Accreditation
- Introduction of PCI Controls - traceable to FIPS 201-1, OMB 05-24, OMB 06-06, OMB 07-06 and Operations Plan Contents
- A new Accreditation Methodology Consisting of:
  - PCI Accreditation Topics (PAT)
  - Accreditation Focus Areas
  - PCI Controls

# Accreditation Methodology (Overall Landscape)

---

- Players Involved:
  - 6 Mandatory Roles (SAO, PO, OIMO, PCIF Manager, Assessor, DAA)
  - 1 Optional Role (CAR)
- Documents Involved:
  - PCI Operations Plan, PCI Assessment Report, PCI Corrective Actions Plan, SP 800-37 Accreditation Letters, Accreditation Decision Letter

# Accreditation Methodology (Overall Landscape) – Contd ..

---

- Phases:
  - Initiation, Assessment, Accreditation & Monitoring
- Assessment:
  - What is Assessed ? – *Satisfaction of PCI Controls*
  - Methods – *Interview, Review, Observe, Test*
  - Taxonomy of the PCI Controls - *4 PIV*  
*Accreditation Topics, 13 Accreditation Focus Areas and 79 PCI Controls*

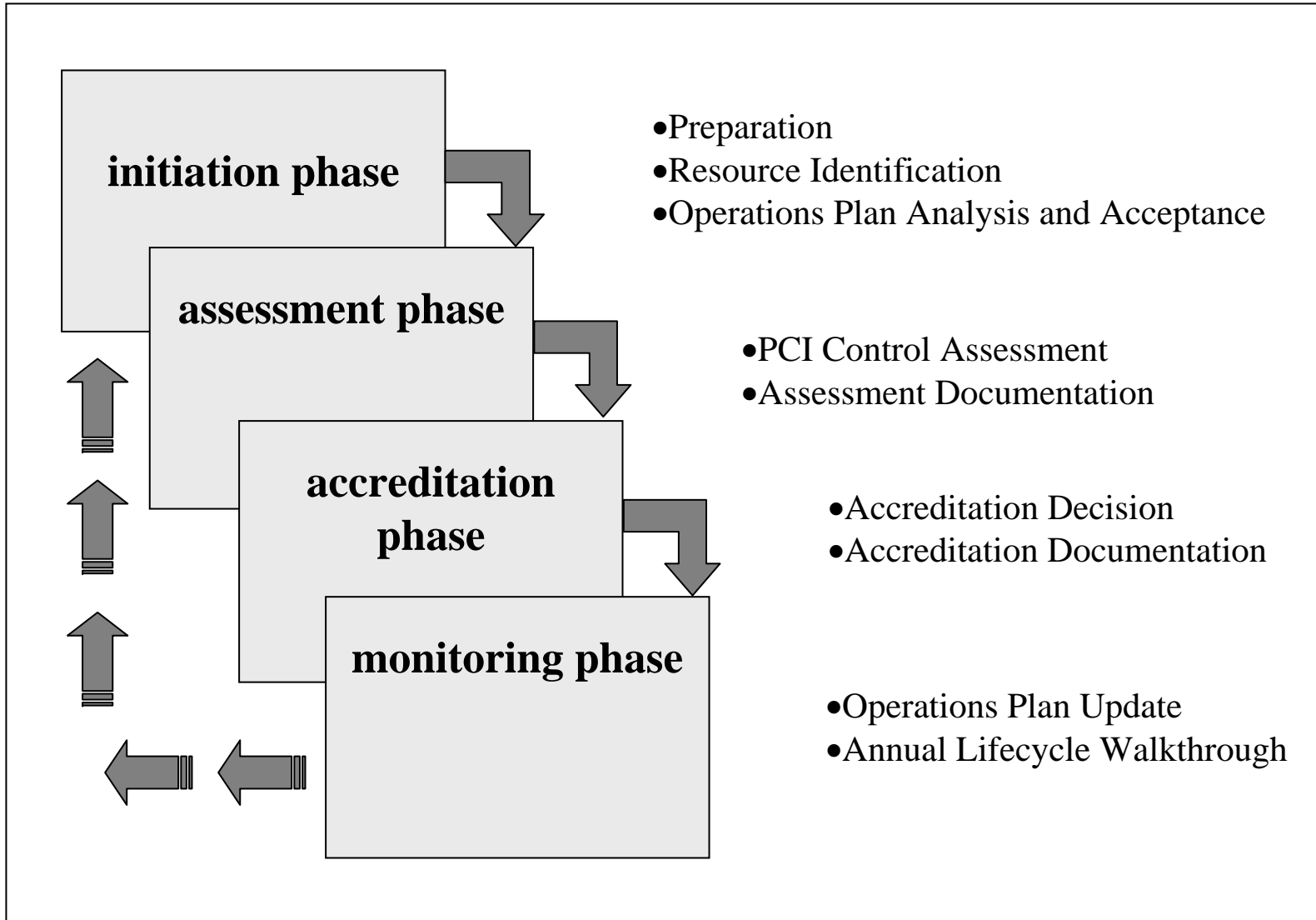
# PCI Accreditation Boundary

---

- Coverage in terms of Functions: should include all operations involved in credential collection, storage, card production, card activation & issuance and card maintenance.
- Coverage in terms of Facilities involved: should specify the facilities involved (some facilities may be excluded because of lack of readiness)

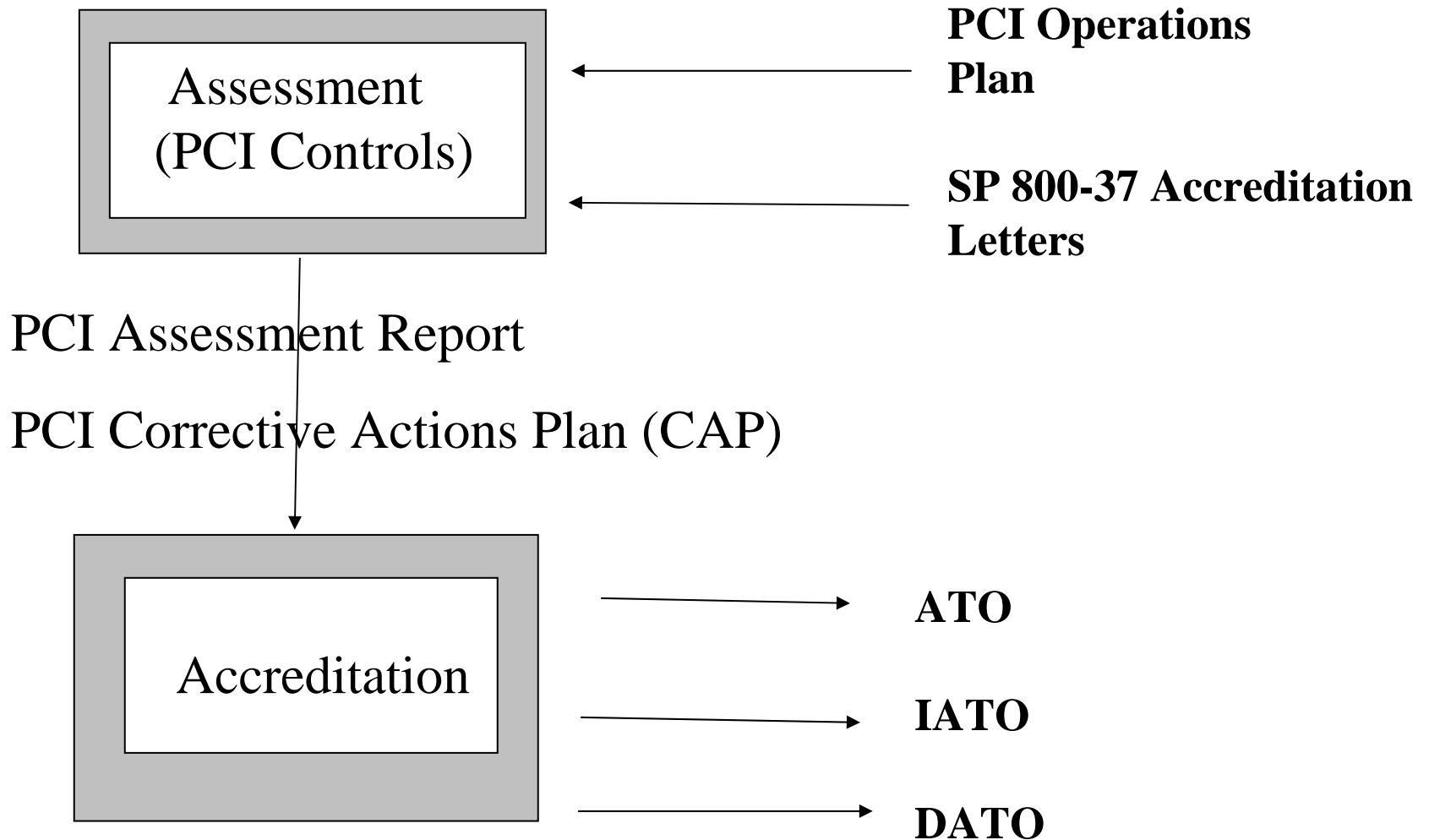
*Target of Accreditation is a PCI and not an individual PCI facility*

# Accreditation Phases



# Inputs and Outputs from Phases

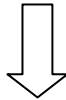
---



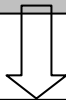
# Organization of PCI Controls

---

PIV Accreditation Topics  
(Major Aspects of PCI Operation)



Accreditation Focus Area  
(Individual Operational Elements)



PCI Controls  
(Derived from FIPS 201-1& related Documents, OMB Memos etc)

# Examples of Accreditation Topics and Focus Areas

---

## **Organizational Preparedness**

Preparation and Maintenance of Documentation (DO)

Assignment of Roles and Responsibilities (RR)

Facility and Personnel Readiness (FP)

## **Security Management & Data Protection**

Protection of Stored and Transmitted Data (ST)

Enforcement of Applicable Privacy Requirements (PR)

## **Infrastructure Elements**

Deployed Products & Information Systems (DP)

Implementation of Credential Infrastructures (CI)

# Examples of Accreditation Topics and Focus Areas – contd ..

---

Processes
Sponsorship Process (SP)
Enrollment/Identity-Proofing Process (EI)
Adjudication Process (AP)
Card Production Process (CP)
Card Activation/Issuance Process (AI)
Maintenance Process (MP)

# An Example of Accreditation Topic, Focus Area & Controls

<b>PAT = Organizational Preparedness</b>			
<b>Accreditation Focus Area</b>	<b>Identifier</b>	<b>PCI Control</b>	<b>Source</b>
Preparation and Maintenance of Documentation (DO)	DO-1	The organization develops and implements a PCI operations plan according to the template in Appendix D. The operations plan references other documents as needed.	SP 800-79-1, Section 2.11 – Accreditation Package and Supporting Documentation
	DO-2	The organization has a written policy and procedures for enrollment/identity proofing that has been approved by the head of the organization.	FIPS 201-1, Section 2.2– PIV Identity Proofing and Registration Requirements

# Relationship to SP 800-37 Accreditation

---

- **Focus**

- SP 800-37 - Security of Information Systems
- SP 800-79-1 – Reliability of a PCI

- **Controls**

- SP 800-37 Security Controls will vary with Operating  
Environments
- SP 800-79-1 – Are fixed as they are derived from

FIPS 201-1 & related documents, OMB Memos etc

***SP 800-37 Accreditation Letters for all Systems involved in Issuance  
and Maintenance of PIV Cards is a Pre-Requisite for SP 800-79-1  
Accreditation***

# Transitioning Issues

---

- When Applicable ?
  - The new guidelines applicable immediately
- Application Targets
  - New PCIs
  - PCIs currently under Accreditation
  - PCIs recently assessed but failed accreditation (both non-operational or operating under IATO)
  - PCIs holding ATO under SP 800-79 must undergo SP 800-79-1 accreditation within one year of the publication date.

# Questions ?

---

- Contact
  - Ramaswamy Chandramouli
  - (301) 975-5013
  - [mouli@nist.gov](mailto:mouli@nist.gov)