Common Criteria

The Value of Common Criteria Evaluations

Stuart Katzke, Ph.D.
Senior Research Scientist
National Institute of Standards & Technology
100 Bureau Drive; Stop 8930
Gaithersburg, MD 20899
(301) 975-4768
skatzke@nist.gov
fax: (301) 975-4964

Common Criteria

Presentation Contents

- The Common Criteria (CC)
  - What is it
  - How is it used
- The significance of the Linux CC evaluation
- The role and importance of product CC evaluations in achieving system assurance

Common Criteria

The International Common Criteria Standard (ISO/IEC 15408)

What the standard is –

- Common structure and language for expressing product/system IT security requirements (Part 1)
- Catalog of standardized IT security requirement components and packages (Parts 2 and 3)

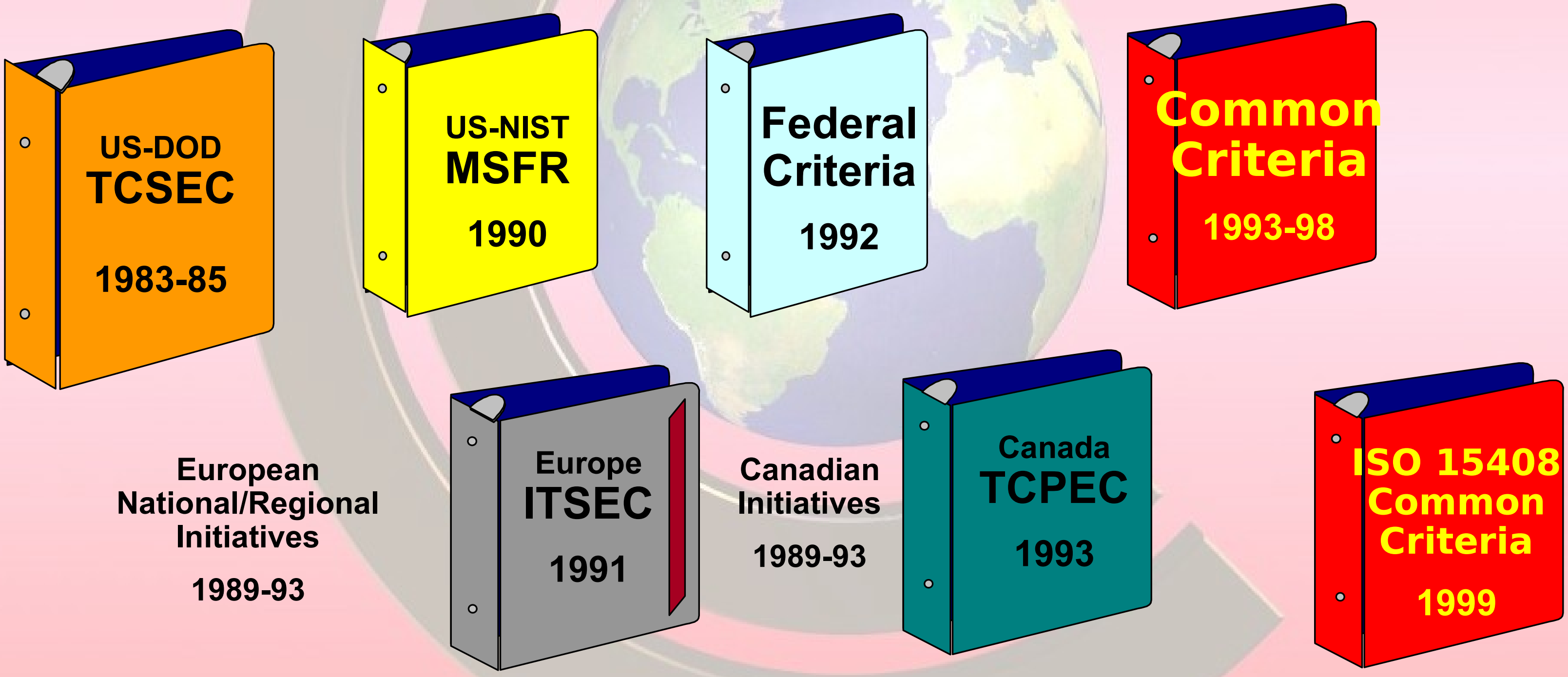
How the standard is used –

- Develop protection profiles and security targets -- specific IT security requirements and specifications for products and systems
- Evaluate products and systems against known and understood IT security requirements

Common Criteria

An Evolutionary Process

Two decades of research and development…



US-DOD TCSEC 1983-85

US-NIST MSFR 1990

Federal Criteria 1992

Common Criteria 1993-98

European National/Regional Initiatives 1989-93

Europe ITSEC 1991

Canadian Initiatives 1989-93

Canada TCPEC 1993

ISO 15408 Common Criteria 1999

IT Security Requirements

The Common Criteria defines two types of IT security requirements--

Functional Requirements

- for defining security behavior of the IT product or system:

• implemented requirements become security functions

Assurance Requirements

- for establishing confidence in security functions:

• correctness of implementation

• effectiveness in satisfying security objectives

Examples:

•*Identification & Authentication*

•*Audit*

•*User Data Protection*

•*Cryptographic Support*

Examples:

•*Development*

•*Configuration Management*

•*Life Cycle Support*

•*Testing*

•*Vulnerability Analysis*

Evaluation Assurance Levels

Common Criteria defines seven hierarchical assurance levels--

	EAL Designation
EAL1	Functionally Tested
EAL2	Structurally Tested
EAL3	Methodically Tested & Checked
EAL4	Methodically Designed, Tested & Reviewed
EAL5	Semiformally Designed & Tested
EAL6	Semiformally Verified Design & Tested
EAL7	Formally Verified Design & Tested

Common Criteria

Protection Profiles (generic) & Security Targets (specific)

Protection Profile contents

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational security policies
- Security Objectives
- Security Requirements
  - Functional requirements
  - Assurance requirements
- Rationale

Security Target contents

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational security policies
- Security Objectives
- Security Requirements
  - Functional requirements
  - Assurance requirements
  - *TOE Summary Specification*
- *PP Claims*
- Rationale

Common Criteria

Profiles and Targets
(Some Examples)

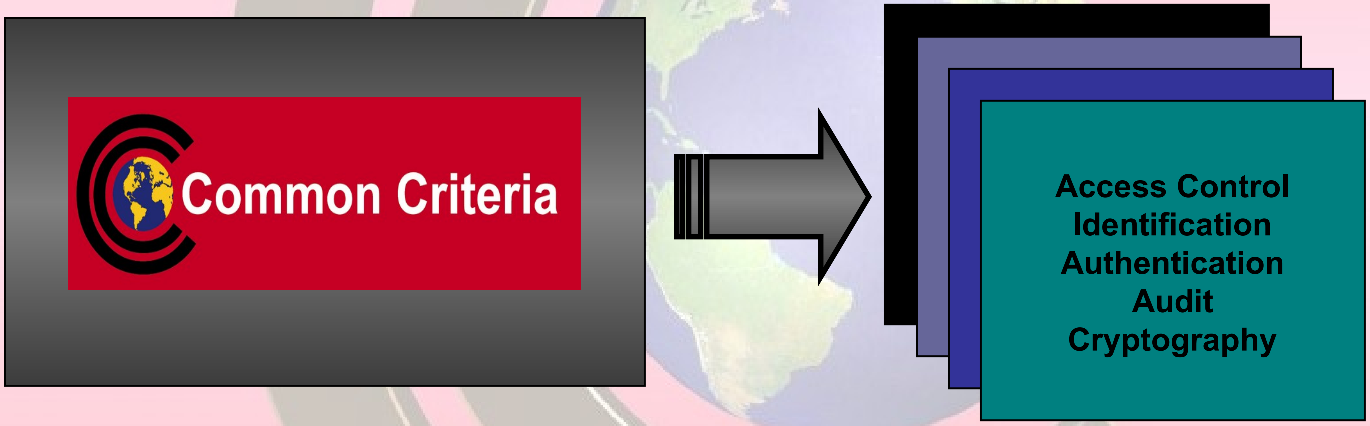
- *Protection Profiles (Product Independent)*
  - Operating Systems (C2, CS2, RBAC)
  - Firewalls (Packet Filter and Application)
  - Smart cards (Stored value and other)
- *Security Targets (Product Specific)*
  - Oracle Database Management System
  - Lucent, Cisco, Checkpoint Firewalls

Common Criteria

Defining Requirements

ISO/IEC Standard 15408

Protection Profiles



Access Control
Identification
Authentication
Audit
Cryptography

- ✓ Operating Systems
- ✓ Database Systems
- ✓ Firewalls
- ✓ Smart Cards
- ✓ Applications
- ✓ Biometrics
- ✓ Routers
- ✓ VPNs

A flexible, robust catalogue of standardized IT security requirements (features and assurances)

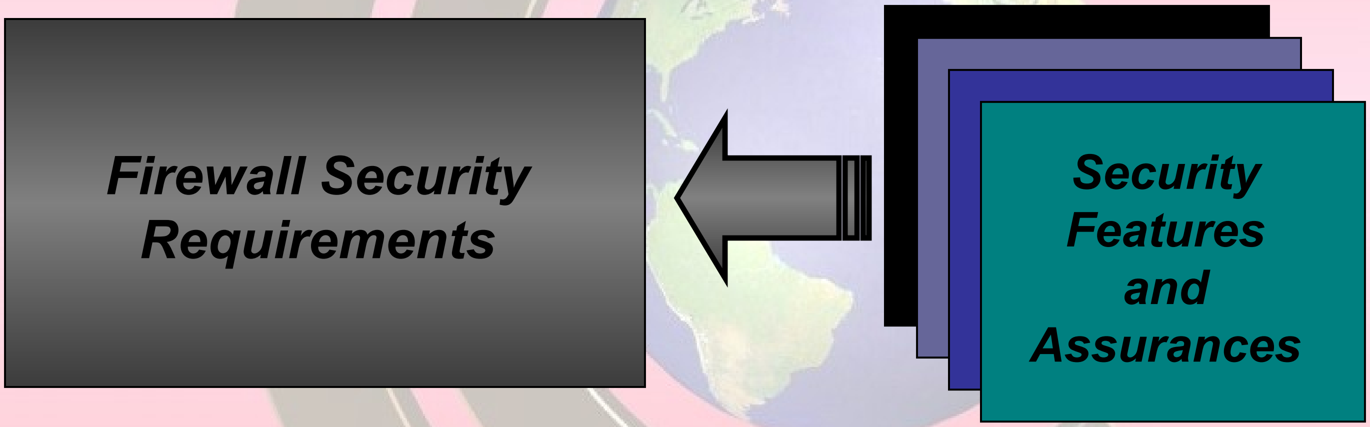
Consumer-driven security requirements in specific information technology areas

Common Criteria

Industry Responds

Protection Profile

Security Targets



Firewall Security Requirements

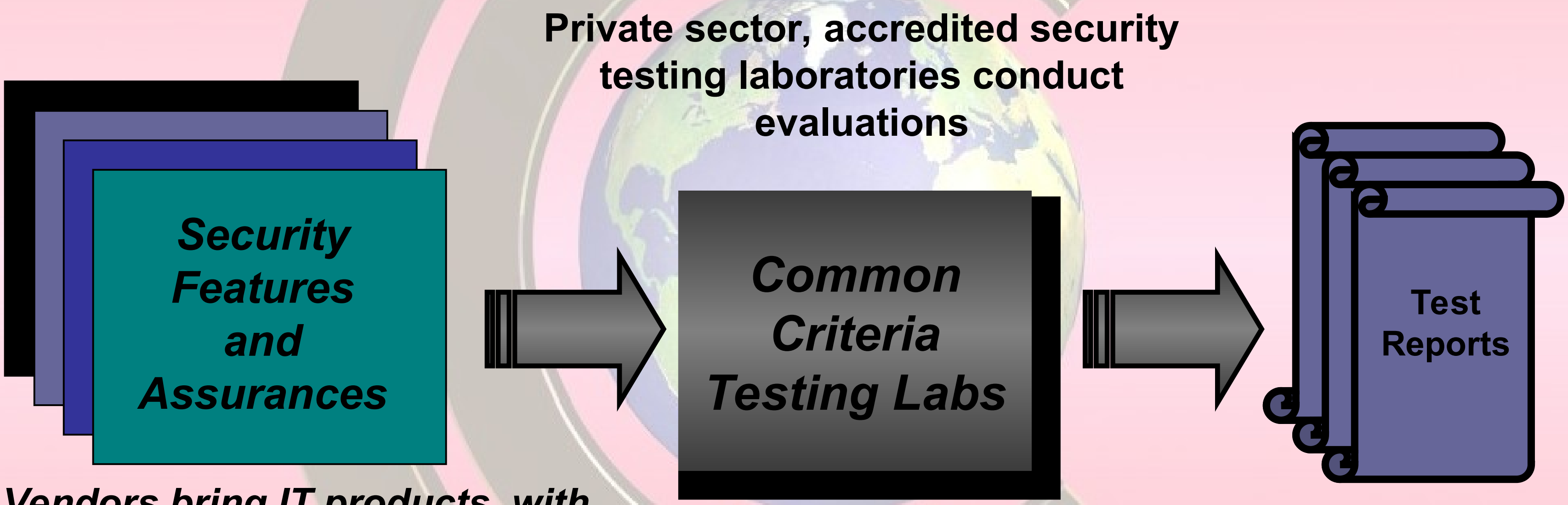
Security Features and Assurances

- ✓ CISCO Firewall
- ✓ Lucent Firewall
- ✓ Checkpoint Firewall
- ✓ Network Assoc. Firewall

Consumer statement of IT security requirements to industry in a specific information technology area

Vendor statements of security claims for their IT products

Demonstrating Conformance



Private sector, accredited security testing laboratories conduct evaluations

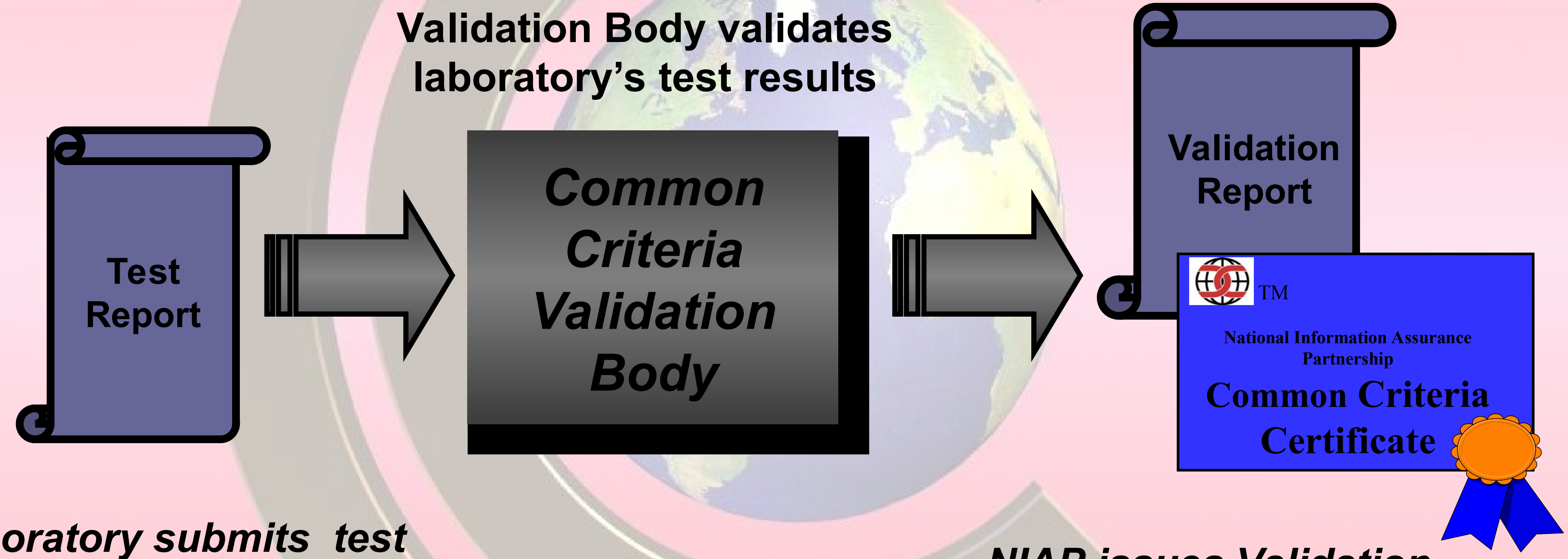
Security Features and Assurances
Common Criteria Testing Labs
Test Reports

Vendors bring IT products, with their security targets, to independent, impartial testing facilities for security evaluation

Test results submitted to NIAP for post-evaluation validation

Common Criteria

Validating Test Results



Validation Body validates laboratory's test results

Test Report

Common Criteria Validation Body

Validation Report

TM

National Information Assurance Partnership

Common Criteria Certificate

Laboratory submits test report to Validation Body

NIAP issues Validation Report and Common Criteria Certificate

Common Criteria

Significance of the Linux Evaluation

- CC was not designed for open source products.
  - Open source not “in vogue” 10 years ago.
- CC assumes a “normal” development process
- Open source does not follow a “normal” development process
- Linux was first attempt at evaluating an open source product
- Linux functionality and development process imposed some limitations on achievable evaluation results
- Demonstrated that an open source product can undergo a successful, traditional CC evaluation –but requires additional developmental activity (as one would expect due to the way open source products are developed).

Assurance in Information Systems (IS)

Building more secure systems requires:

- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

Common Criteria

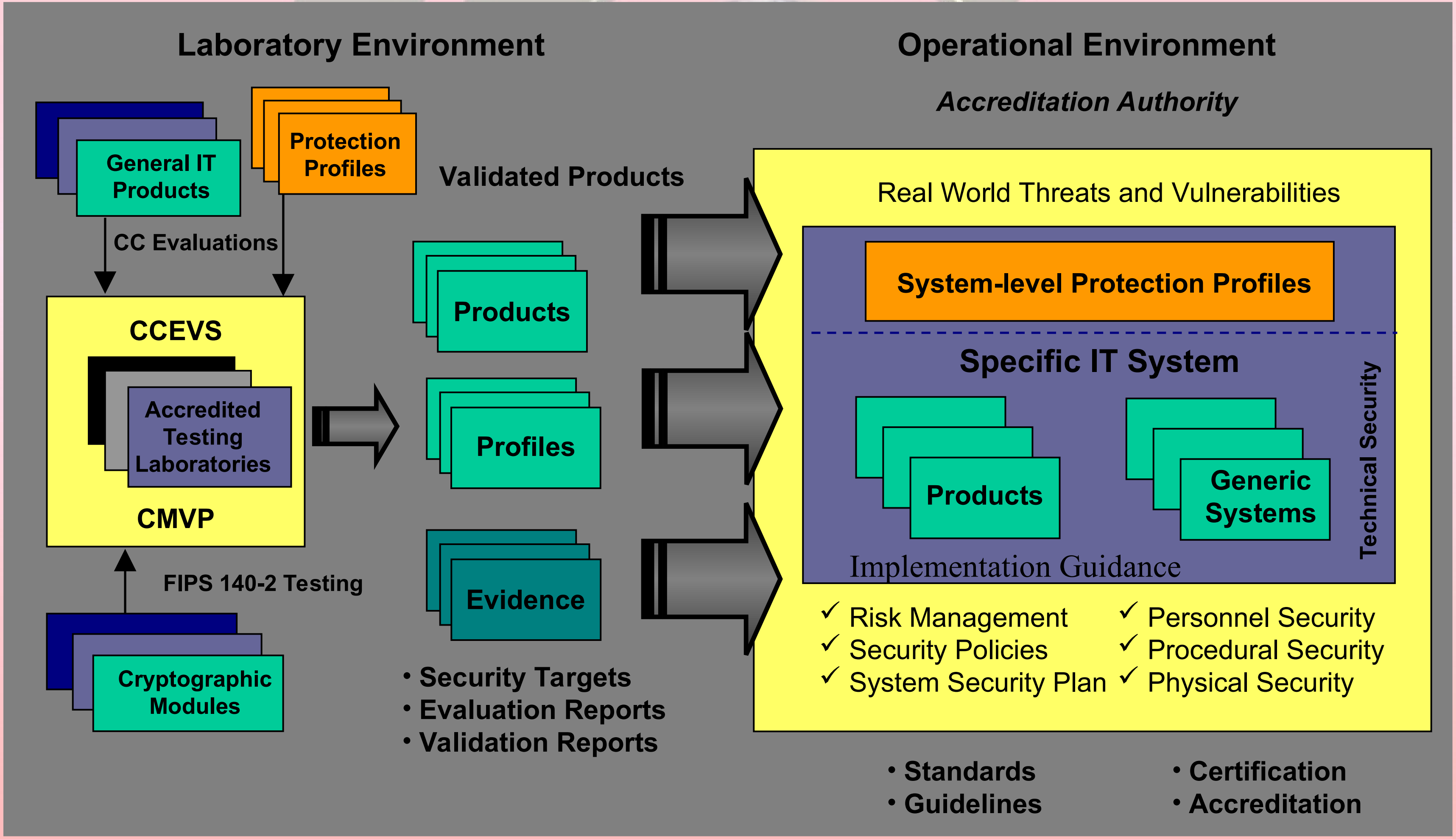
Supporting Tools and Programs

Building more secure systems is enhanced by:

- Standardized Security Requirements and Specifications
  - **U.S. Common Criteria protection profile development project**
  - **Private sector protection profile contributions**
    - ❖ **BITS functional packages**
    - ❖ **Smart Card Security Users Group (SCSUG)**
    - ❖ **Process Control Security Requirements Forum (PCSRF)**
- IT Component-level Product Testing and Evaluation Programs
  - **Common Criteria Evaluation and Validation Schemes (CCRA)**
  - **Cryptographic Module Validation Program (U.S. NIST/Canada CSE)**
- Security Implementation Guidance
  - **Security Technical Implementation Guides**
  - **Security Reference Guides**
- System Certification and Accreditation

Common Criteria

Supporting Tools and Programs



Laboratory Environment

Operational Environment

Accreditation Authority

General IT Products

Protection Profiles

Validated Products

CC Evaluations

CCEVS

Accredited Testing Laboratories

CMVP

FIPS 140-2 Testing

Cryptographic Modules

Products

Profiles

Evidence

- Security Targets
- Evaluation Reports
- Validation Reports

Real World Threats and Vulnerabilities

System-level Protection Profiles

Specific IT System

Products

Generic Systems

Technical Security

Implementation Guidance

✓ Risk Management
✓ Security Policies
✓ System Security Plan

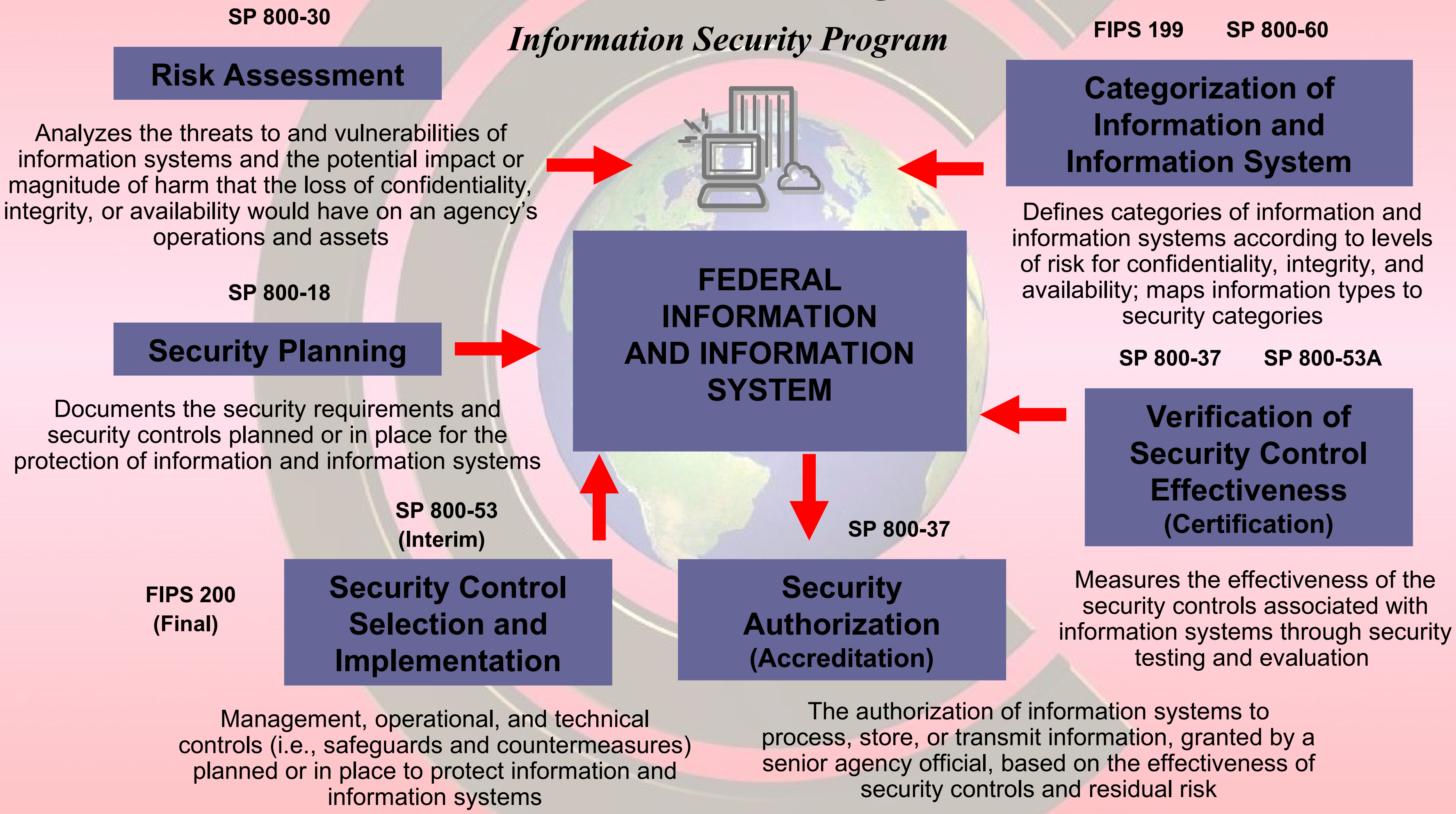
✓ Personnel Security
✓ Procedural Security
✓ Physical Security

- Standards
- Guidelines

- Certification
- Accreditation

Common Criteria

Certification and Accreditation: The Big Picture



Information Security Program

FEDERAL INFORMATION AND INFORMATION SYSTEM

SP 800-30

Risk Assessment

Analyzes the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets

FIPS 199 SP 800-60

Categorization of Information and Information System

Defines categories of information and information systems according to levels of risk for confidentiality, integrity, and availability; maps information types to security categories

SP 800-18

Security Planning

Documents the security requirements and security controls planned or in place for the protection of information and information systems

SP 800-37 SP 800-53A

Verification of Security Control Effectiveness (Certification)

Measures the effectiveness of the security controls associated with information systems through security testing and evaluation

SP 800-53 (Interim)

FIPS 200 (Final)

Security Control Selection and Implementation

Management, operational, and technical controls (i.e., safeguards and countermeasures) planned or in place to protect information and information systems

SP 800-37

Security Authorization (Accreditation)

The authorization of information systems to process, store, or transmit information, granted by a senior agency official, based on the effectiveness of security controls and residual risk