NIST RMF Overview

IT 727-A & OL – Managing Cybersecurity Risk
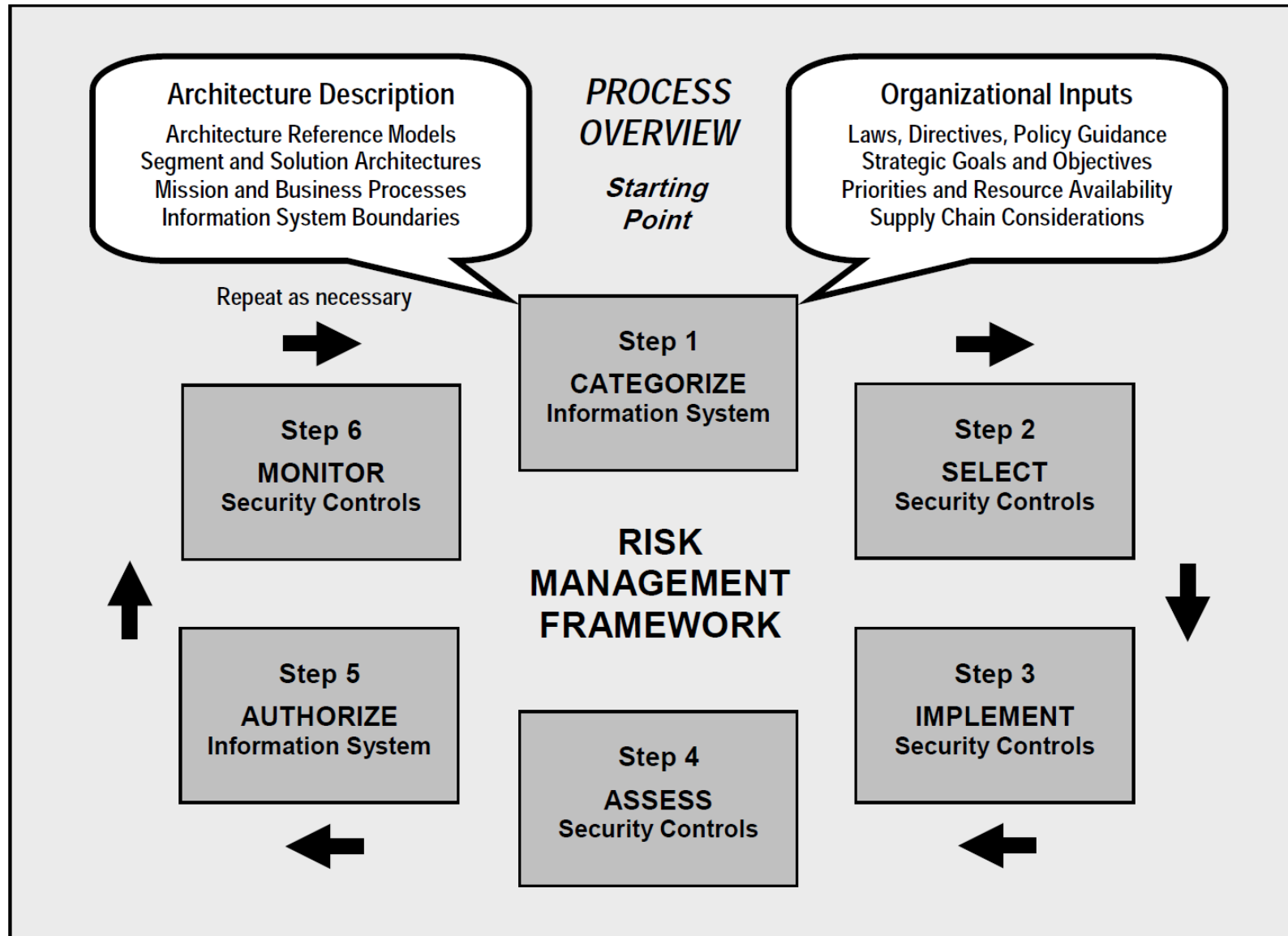
Dr. Ibrahim Waziri Jr.

FISMA/NIST/FIPS

```
┌─────────────────────────┐
│   FISMA – Law           │
│  (Congress/White House) │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│  RMF 800-37 – Policy    │
│      (NIST)             │
└─────────────────────────┘
             │
   ┌─────┬───┴───┬─────┐
   ▼     ▼       ▼     ▼
```

| Standards | Baselines | Guidelines | Procedures |
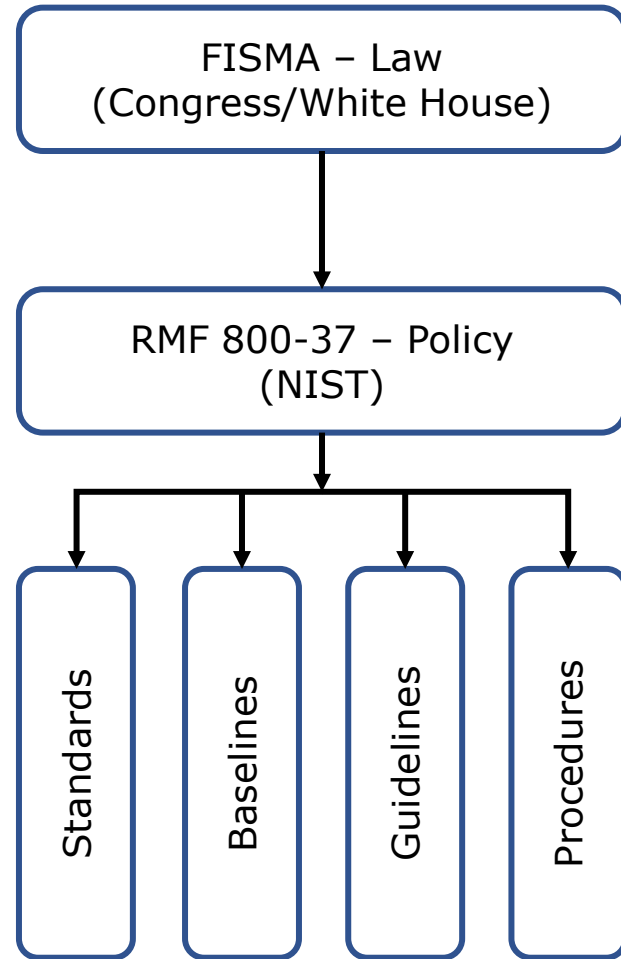
NIST 800 Series
FIPS Documents

NIST RMF 800-37

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information System

Step 6
MONITOR
Security Controls

Step 2
SELECT
Security Controls

RISK MANAGEMENT FRAMEWORK

Step 5
AUTHORIZE
Information System

Step 4
ASSESS
Security Controls

Step 3
IMPLEMENT
Security Controls

Prepare – Step 0/1

- Architecture & Diagrams
- Project Scope & Lifecycle
- Security Boundaries
- Templates & Checklist
- Agreements
- User Roles
- Oversight, Ownership,
- ATO Process
- SAP etc.

ISACA

- Identification
- Assessment
- Response & Mitigation
- Monitoring & Reporting