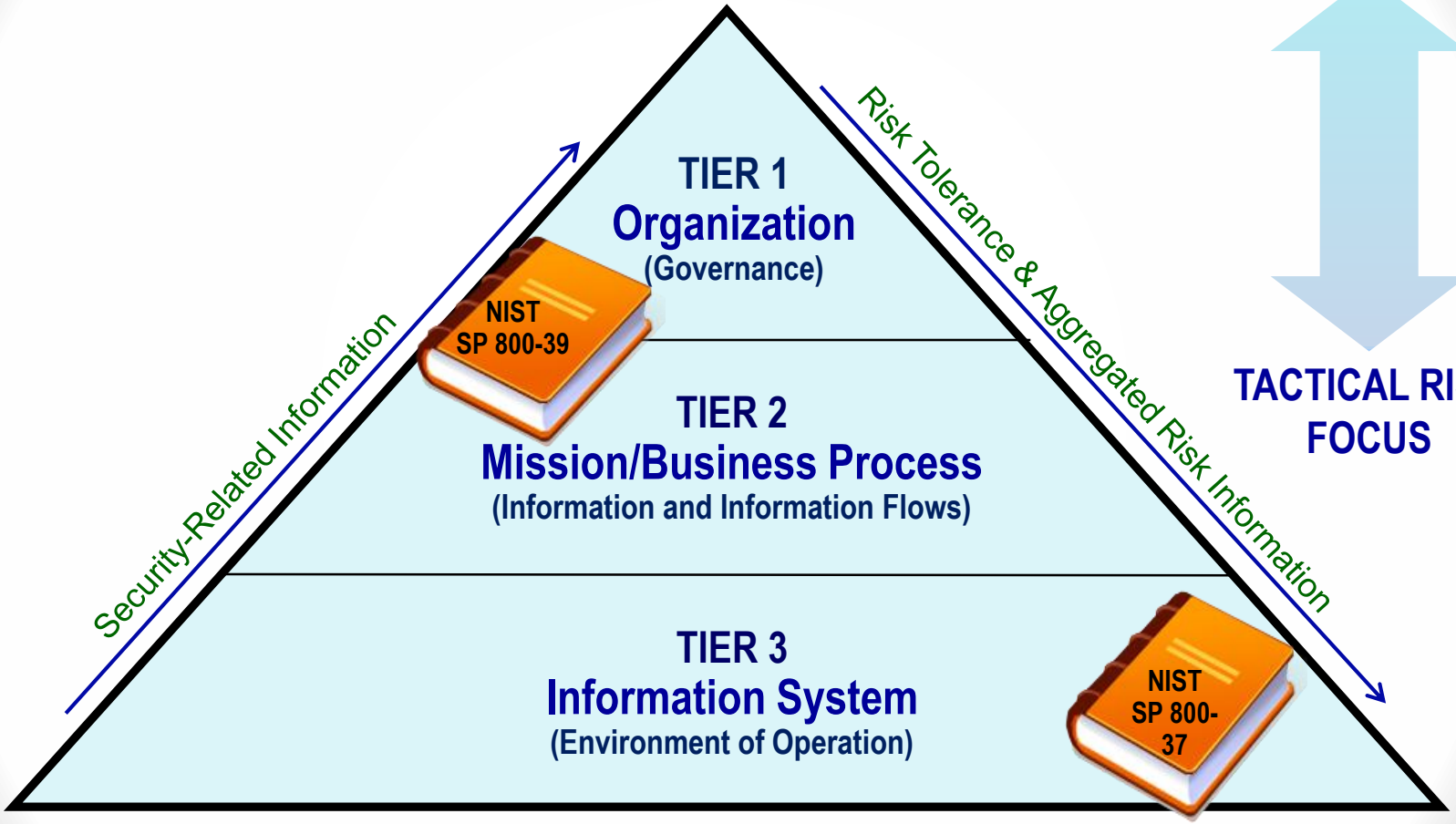
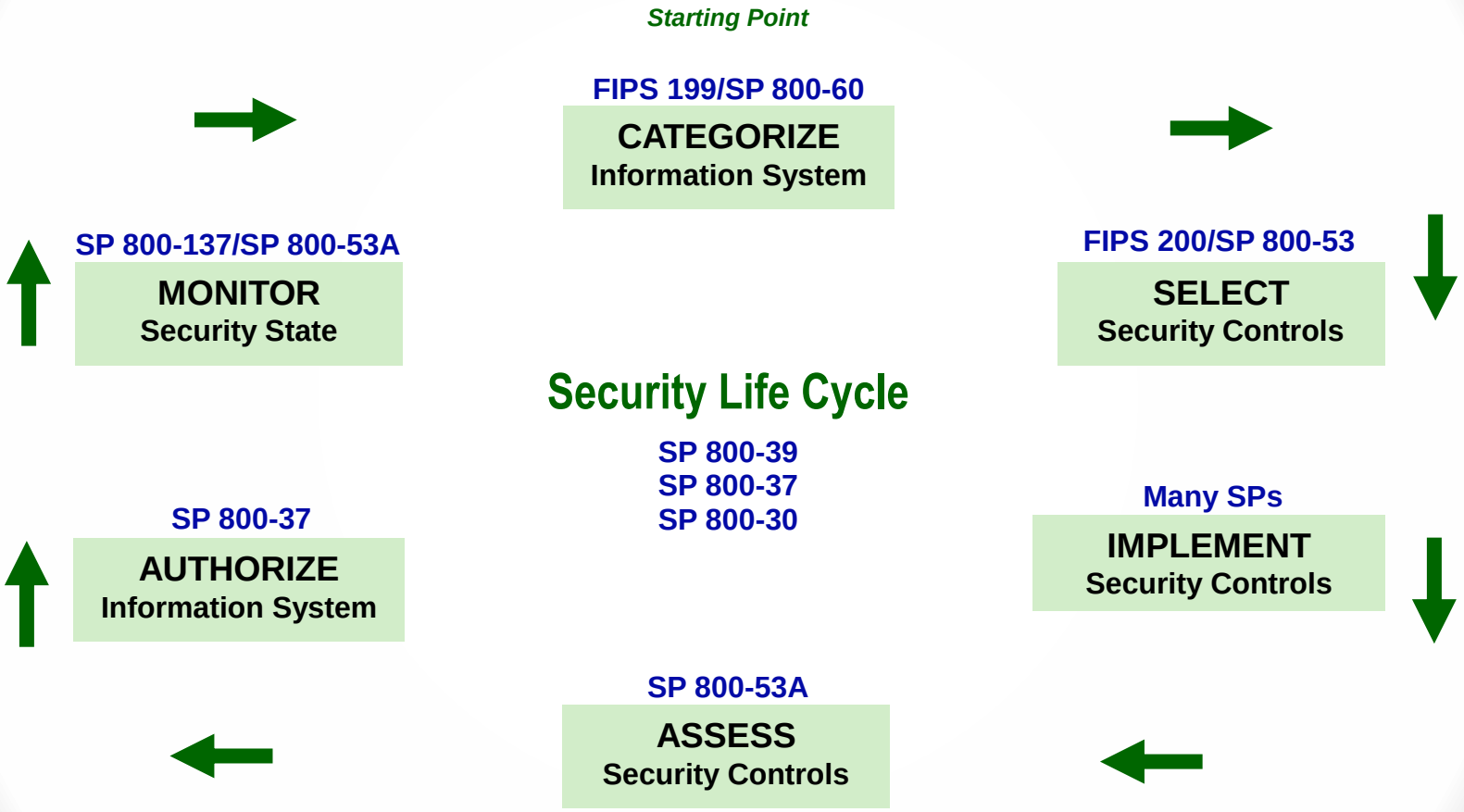
Standards/Guidelines for FISMA & RM

- **FIPS -** Federal Information Processing Standards
  - FIPS 199 – Standards for Security Categorization
  - FIPS 200 – Minimum Security Requirements
- **SPs** – Special Publications
  - SP 800-18 – Guide for System Security Plan development
  - **SP 800-30 – Guide for Conducting Risk Assessments**
  - SP 800-34 – Guide for Contingency Plan development
  - **SP 800-37 – Guide for Applying the Risk Management Framework**
  - **SP 800-39 – Managing Information Security Risk**
  - **SP 800-53/53A – Security controls catalog/assessment procedures**
  - SP 800-60 – Mapping Information Types to Security Categories
  - SP 800-128 – Security-focused Configuration Management
  - SP 800-137 – Information Security Continuous Monitoring
  - Many others for operational and technical implementations

Three Tiers


STRATEGIC RISK FOCUS
TACTICAL RISK FOCUS
Security-Related Information
Risk Tolerance & Aggregated Risk Information
TIER 1
Organization
(Governance)
NIST SP 800-39
TIER 2
Mission/Business Process
(Information and Information Flows)
TIER 3
Information System
(Environment of Operation)
NIST SP 800-37

Risk Management Framework



CSF/RMF Synergy Training Roles (by Tier)

- Organization (Governance) Tier
  - Risk Executive Function – RE(F)
  - CIO
  - Senior Information Security Officer - SISO
- Mission/Business Process Tier
  - Information Security Architect
  - Common Control Provider
  - Information Owner (may also be at the Information System Tier)
- Information System Tier
  - Authorizing Official – AO
  - Information System Owner
  - Information System Security Officer - ISSO
  - Security Control Assessor