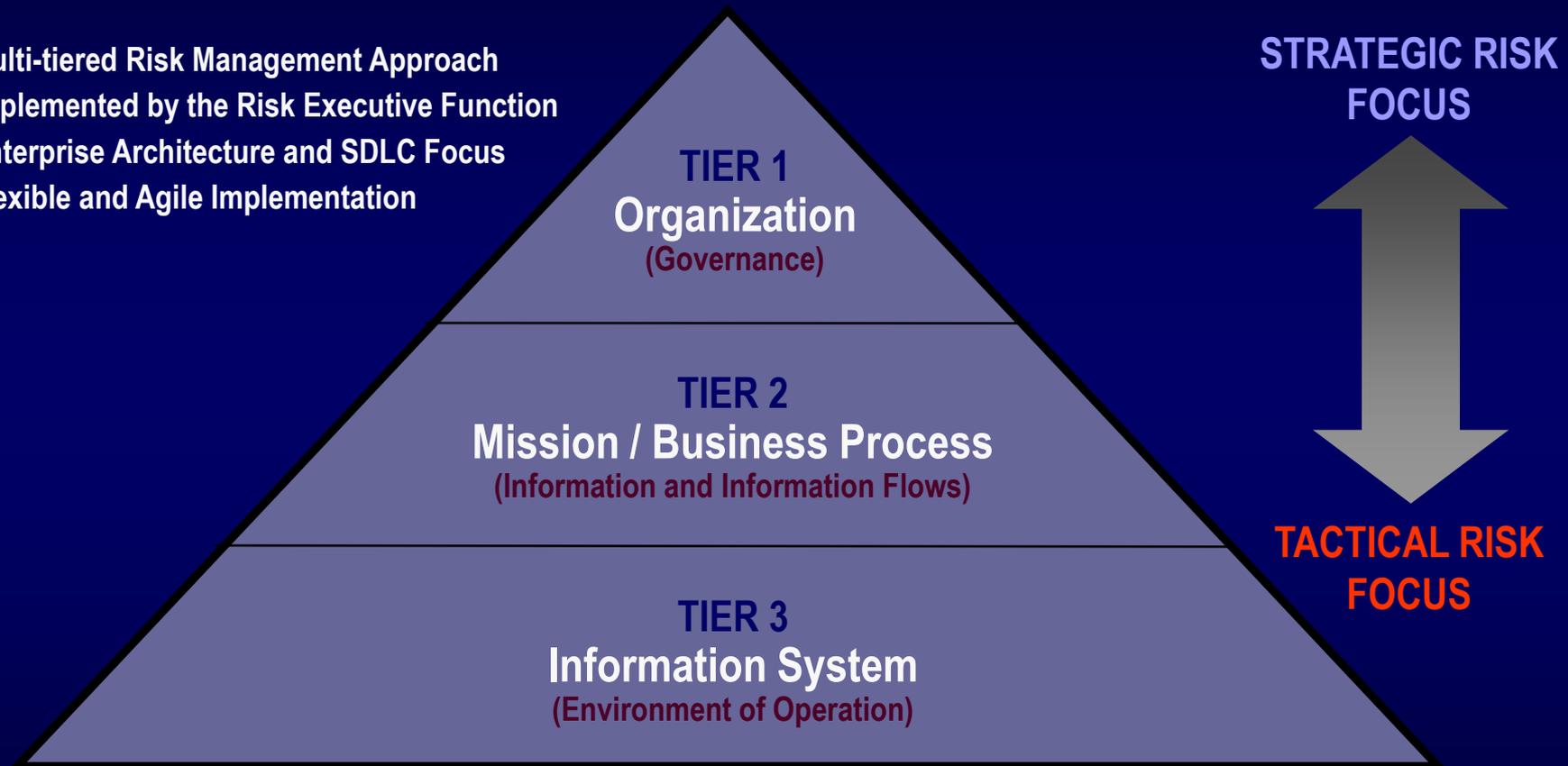
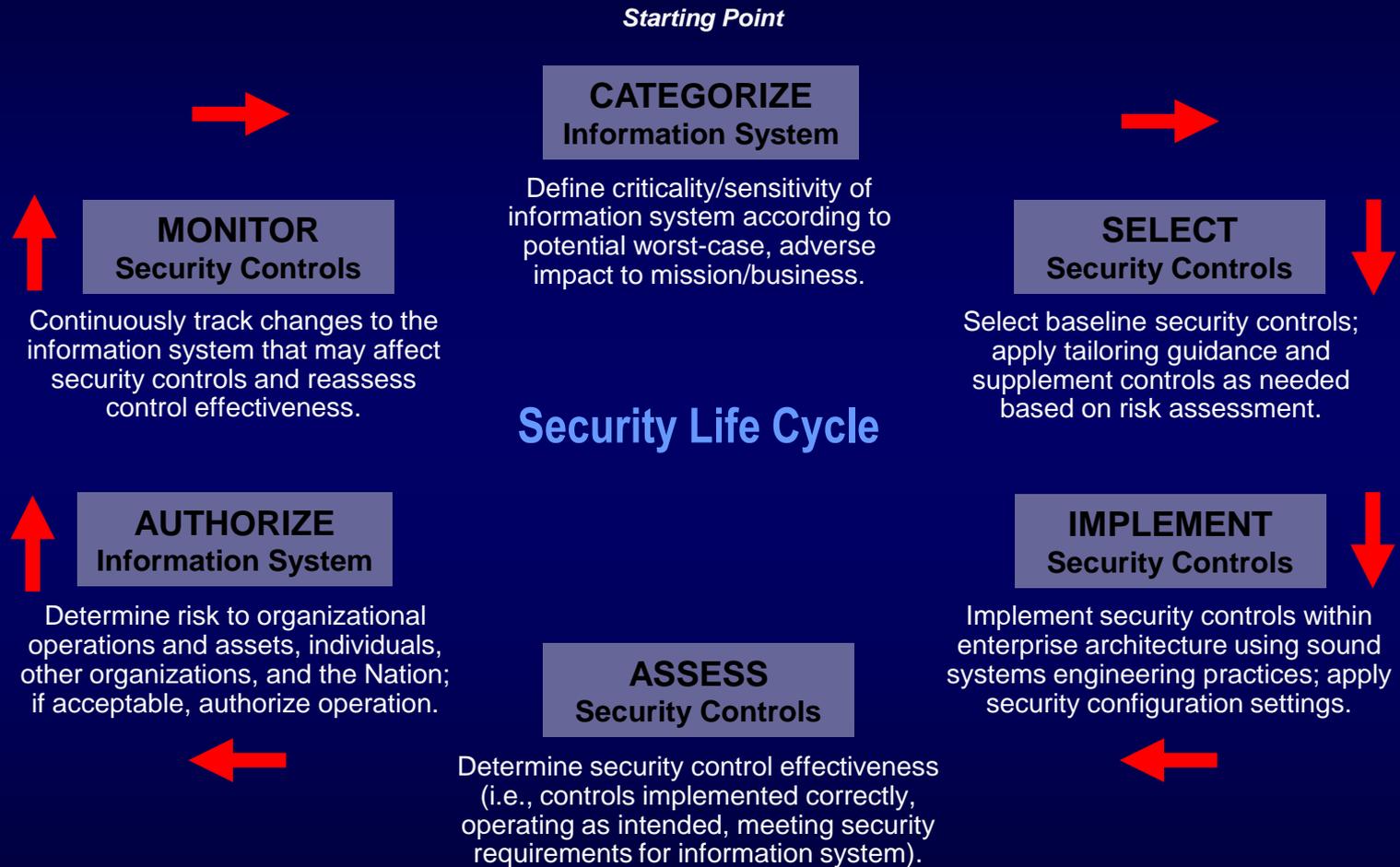


# Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



# Risk Management Framework



# Defense-in-Depth Security Controls

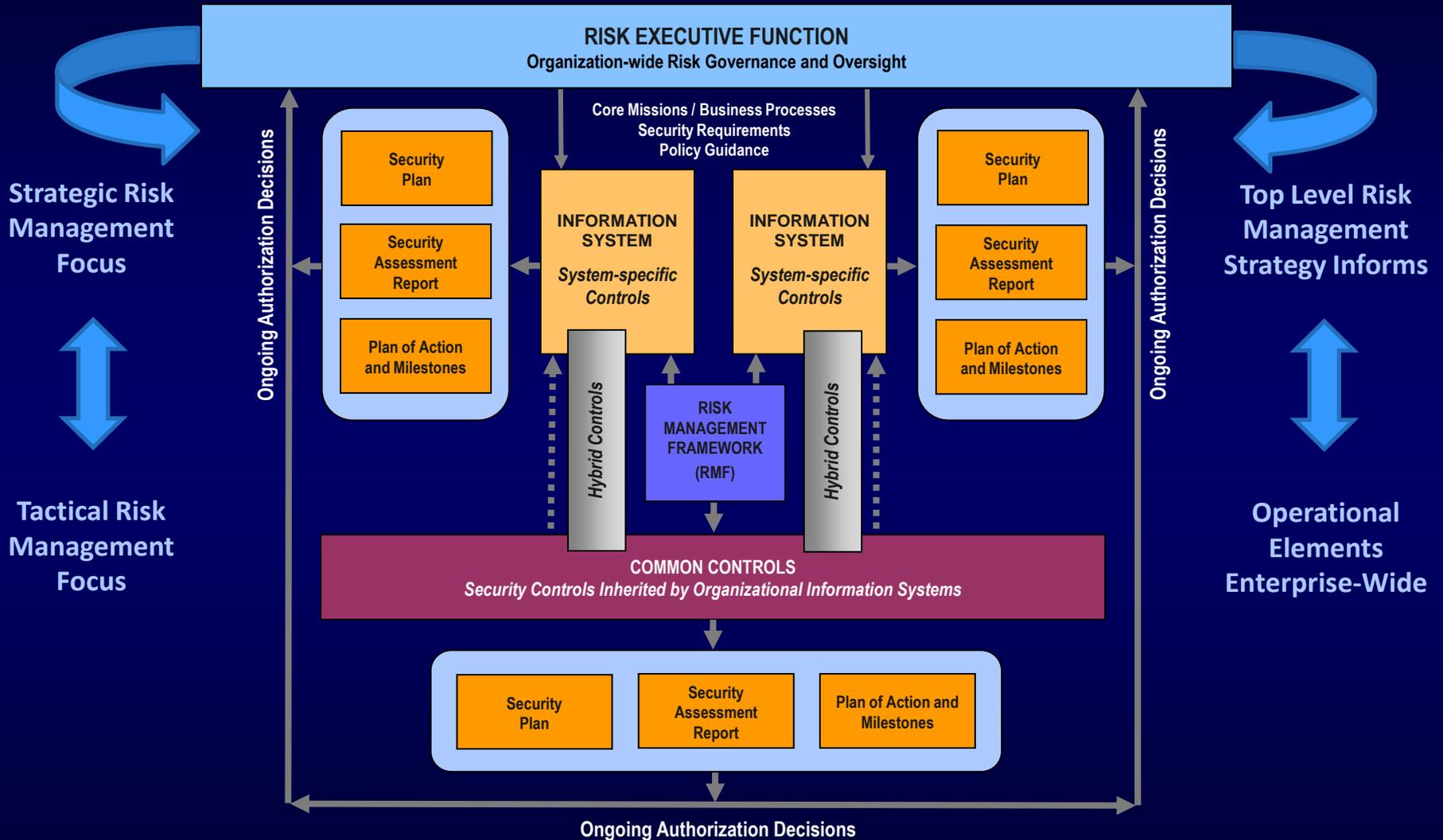
*NIST Special Publication 800-53*

## Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments and authorization
- ✓ Continuous monitoring
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

Adversaries attack the weakest link...where is yours?

# Security Control Allocation



# Contact Information

100 Bureau Drive Mailstop 8930  
Gaithersburg, MD USA 20899-8930

## *Project Leader*

Dr. Ron Ross  
(301) 975-5390  
[ron.ross@nist.gov](mailto:ron.ross@nist.gov)

## *Administrative Support*

Peggy Himes  
(301) 975-2489  
[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## *Senior Information Security Researchers and Technical Support*

Marianne Swanson  
(301) 975-3293  
[marianne.swanson@nist.gov](mailto:marianne.swanson@nist.gov)

Kelley Dempsey  
(301) 975-2827  
[kelley.dempsey@nist.gov](mailto:kelley.dempsey@nist.gov)

Pat Toth  
(301) 975-5140  
[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

Arnold Johnson  
(301) 975-3247  
[arnold.johnson@nist.gov](mailto:arnold.johnson@nist.gov)

Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)

Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)