

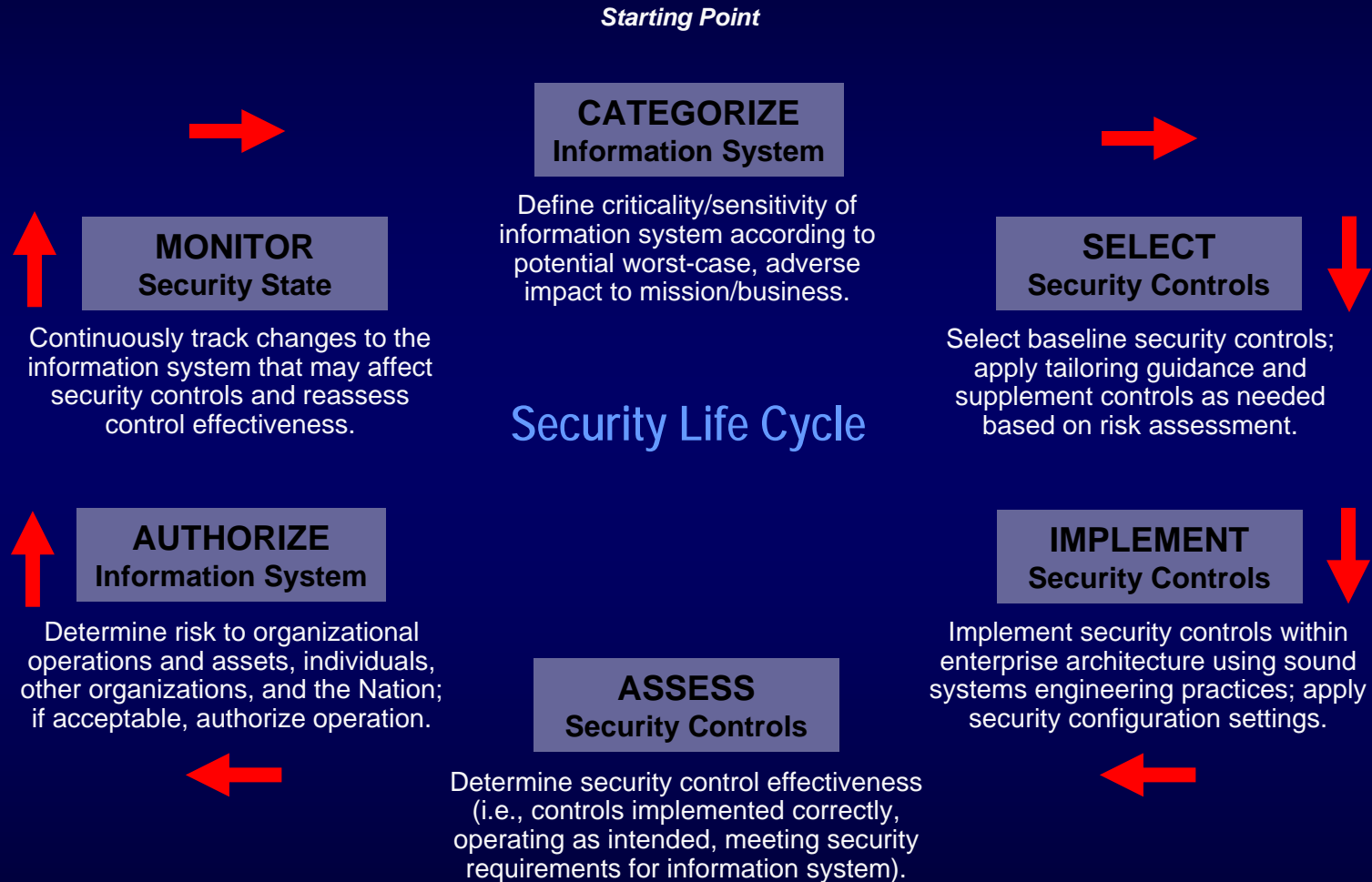
Risk Management Framework

Computer Security Division
Information Technology Laboratory

Managing Enterprise Risk

- Key activities in managing **enterprise-level risk**—risk resulting from the operation of an information system:
 - ✓ **Categorize** the information system
 - ✓ **Select** set of minimum (baseline) security controls
 - ✓ **Refine** the security control set based on risk assessment
 - ✓ **Document** security controls in system security plan
 - ✓ **Implement** the security controls in the information system
 - ✓ **Assess** the security controls
 - ✓ **Determine** agency-level risk and risk acceptability
 - ✓ **Authorize** information system operation
 - ✓ **Monitor** security controls on a continuous basis

Risk Management Framework



Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Controls)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-37 (System Risk Management Framework)
- NIST Special Publication 800-39 (Enterprise-Wide Risk Management)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation...

Information Security Program

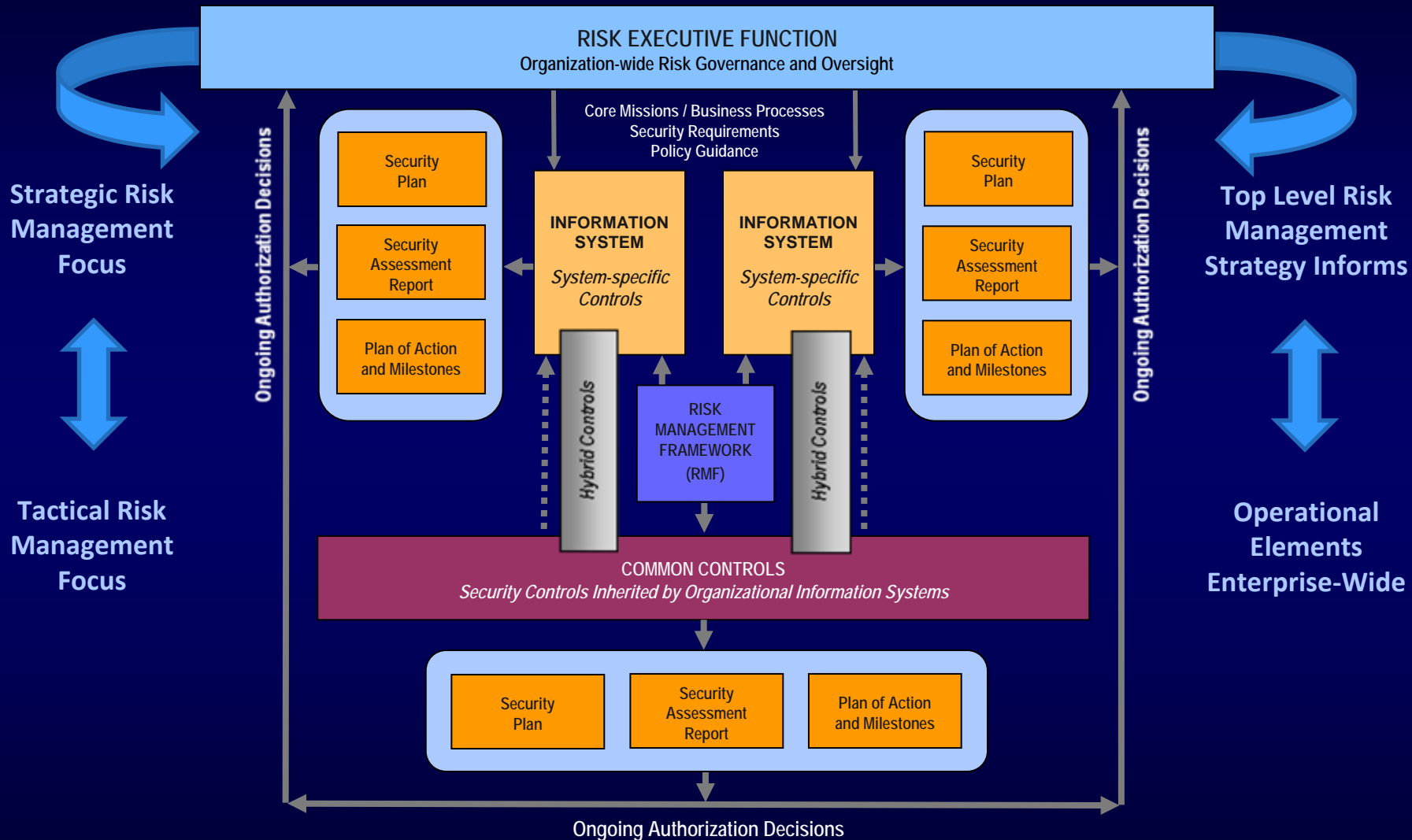


Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Physical security
- ✓ Personnel security
- ✓ Certification, accreditation, and security assessments
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Security configuration settings
- ✓ Anti-viral software
- ✓ Smart cards

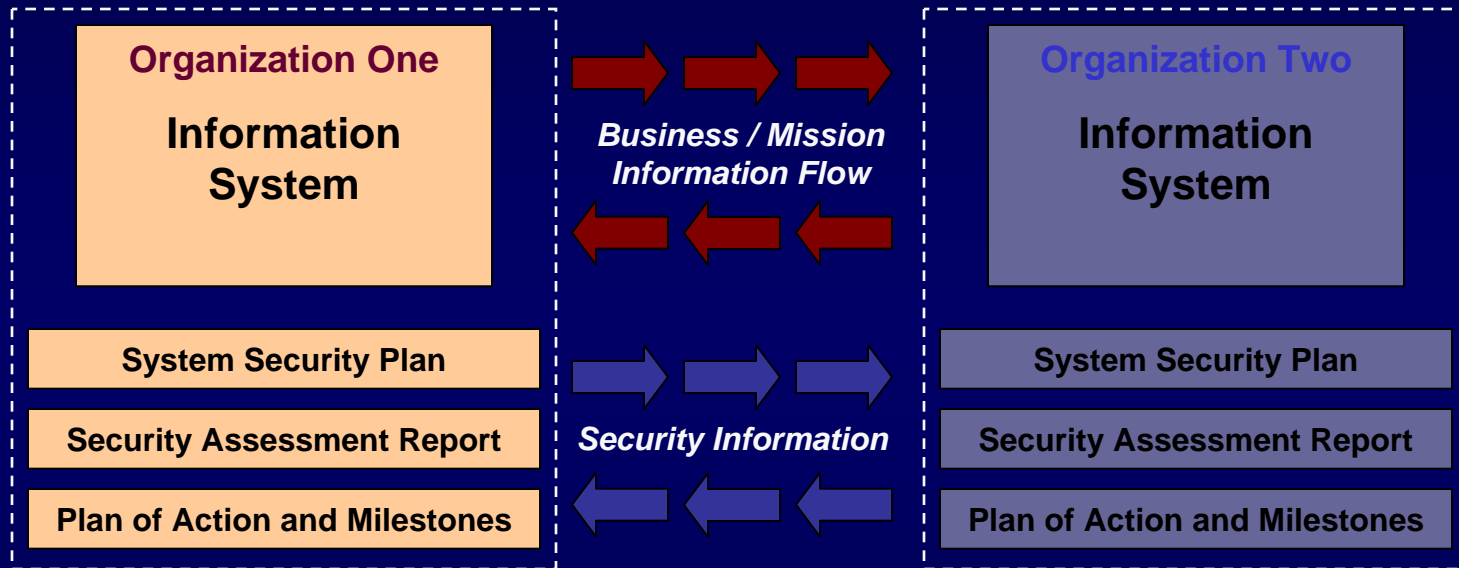
Adversaries attack the weakest link...where is yours?

Security Control Accountability



The Desired End State

Security Visibility Among Business/Mission Partners



Determining the risk to the first organization's operations and assets and the acceptability of such risk

Determining the risk to the second organization's operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs **BEFORE** critical/sensitive communications begin...establishing levels of security due diligence.

Contact Information

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

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov