Integrating Security and Privacy Requirements into Information Systems and Organizations

Information Security and Privacy Advisory Board

October 26, 2011

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The Perfect Storm

- Explosive growth and aggressive use of information technology.
- Proliferation of information systems and networks with virtually unlimited connectivity.
- Increasing sophistication of threat including exponential growth rate in malware (malicious code).

Resulting in an increasing number of penetrations of information systems in the public and private sectors potentially affecting security and privacy…

The Threat Situation

Continuing serious cyber attacks on public and private sector information systems targeting key operations, assets, and individuals…

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with hostile intentions.
- Effective deployment of malware causing significant exfiltration of sensitive information (e.g., intellectual property).
- Potential for disruption of critical systems and services.

Unconventional Threats

Affecting Security and Privacy

Complexity

Connectivity

Culture

Mainstreaming Security and Privacy

- Information security and privacy requirements must be considered *first order requirements* and are critical to mission and business success.
- An effective organization-wide information security and privacy programs help to ensure that security and privacy considerations are specifically addressed in the *enterprise architecture* for the organization and are integrated early into the *system development life cycle*.
- Use *Federal Segment Architecture Methodology* and FEA *Security and Privacy Profile* for implementation.

Mutually Supporting Objectives

- Enterprise Architecture
  - Standardization, consolidation, optimization.
- Information Security
  - Confidentiality, integrity, and availability of information processed, stored, and transmitted by information systems.
- Privacy
  - Confidentiality and integrity of personally identifiable information; collection of information (data minimization); use of information (sharing and disclosure concerns).

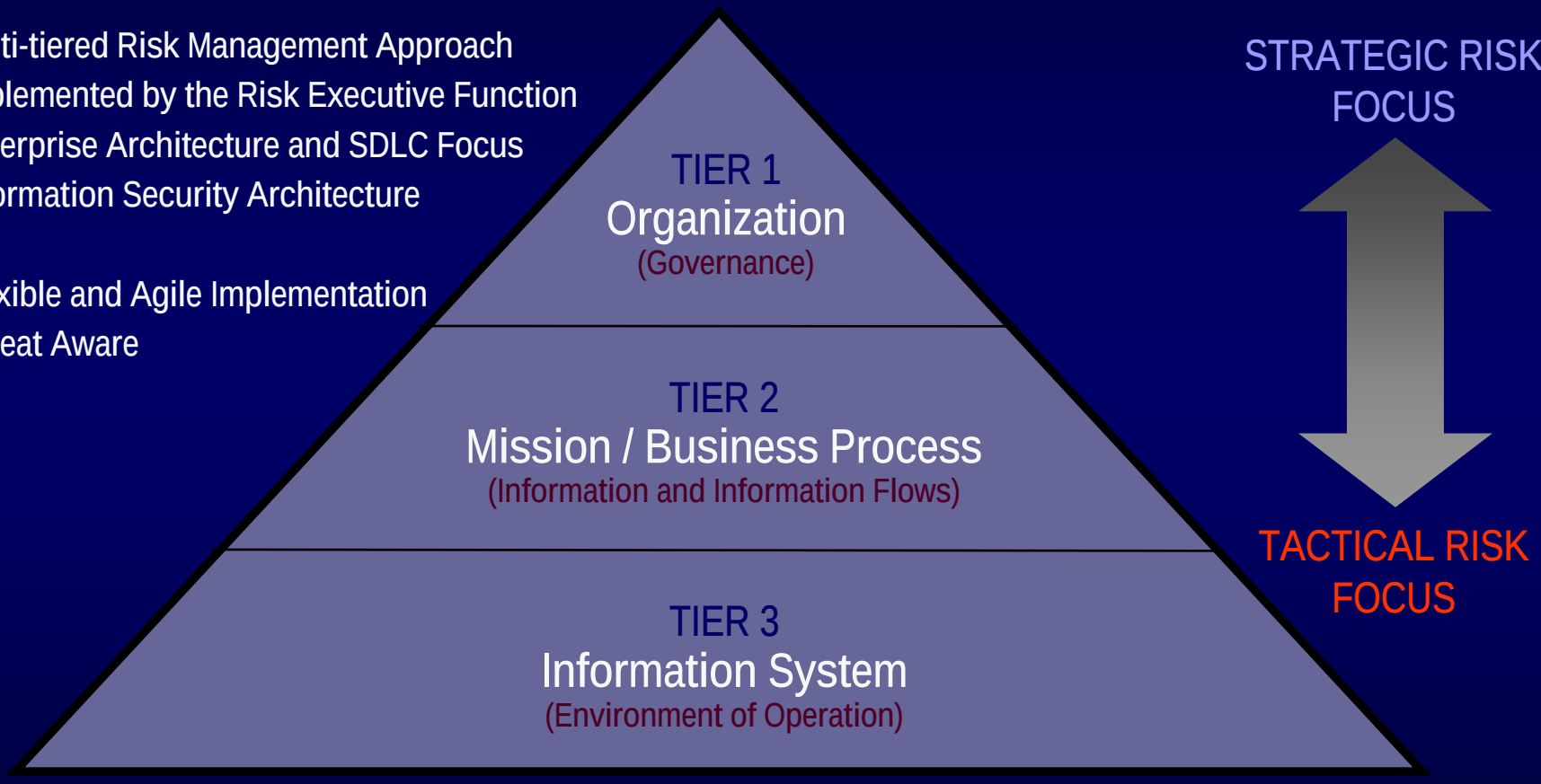
Requires a disciplined, structured process that takes a holistic, organization-wide view…

Information security and privacy, traditional societal values, are at greater risk today due to the ever increasing size of our *digital footprint*…

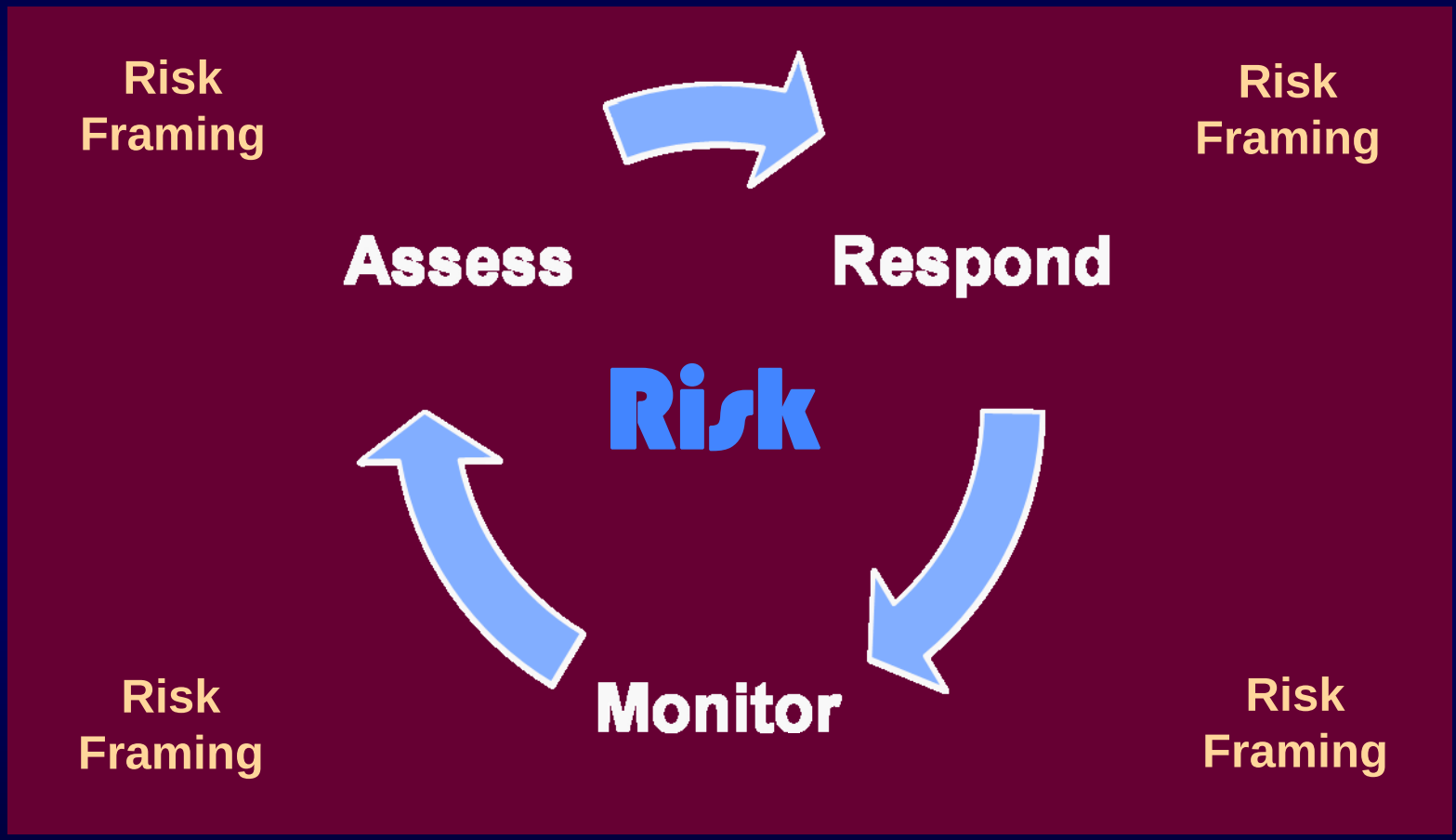
Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Information Security Architecture

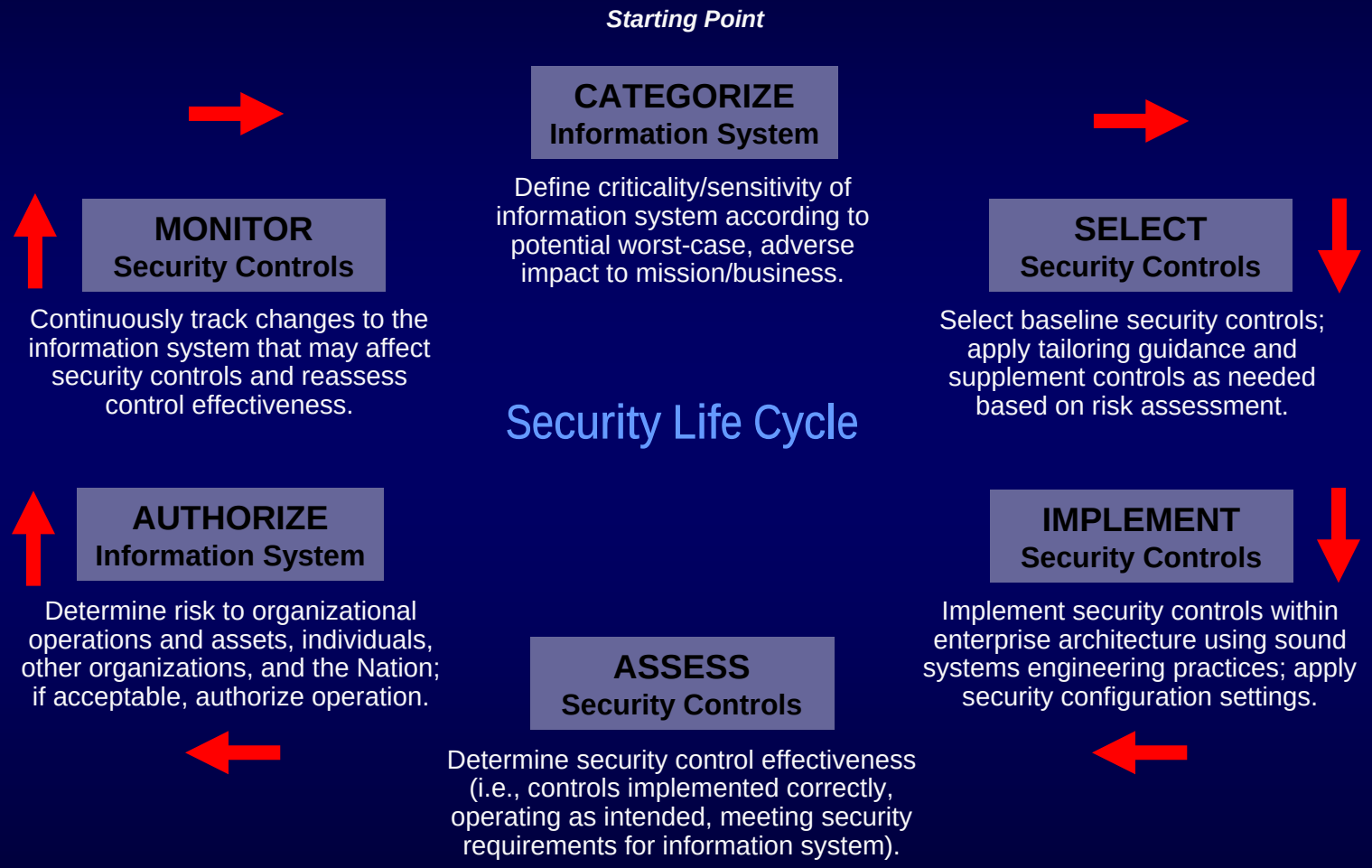
- Flexible and Agile Implementation
- Threat Aware



Risk Management Process



Risk Management Framework



A new initiative to develop privacy controls for federal information systems and organizations…

Privacy Control Families

- Families are based upon the Fair Information Practice Principles (FIPPs)
- Use them to build privacy into new or modified:
  - Programs, research, pilots;
  - Information systems;
  - Technology (surveillance cameras, body imaging devices, data mining); and
  - Any other business-related activity that involves personally identifiable information (PII).

Applying Privacy Control Families
(1 of 2)

- Preliminary steps:
  - Identify the types of PII involved;
  - Identify the legal framework that applies;
    (Statutes, regulations, and policies that must be applied)
  - Map the data flows.
  - Law enforcement and intelligence programs and systems, particularly those that are classified, will require modifications of the FIPPs in light of their legal and operational requirements.

Applying Privacy Control Families
(2of 2)

- Families are interrelated -- action taken in one family likely will affect the implementation of another.
- Families are not in any particular order and should be considered individually and as a whole.
- Families are iterative and must be revisited to determine the impact of changes to any particular family.
- Families must be analyzed and applied to each agency's distinct mission, operation, and legal authorities and obligations.

Fair Information Practice Principles

- Transparency
- Individual Participation and Redress
- Purpose Specification
- Data Minimization and Retention
- Use Specification
- Data Quality and Integrity
- Security
- Accountability and Auditing

What do we achieve?

Benefits

- Well defined privacy controls that help demonstrate compliance to federal legislation and policies.
- Measurable and enforceable privacy requirements.
- Closer linkage to enterprise cyber security programs to provide a solid foundation for privacy.
- Enterprise-wide defense-in-depth for security and privacy.
- Security and privacy requirements traceability.

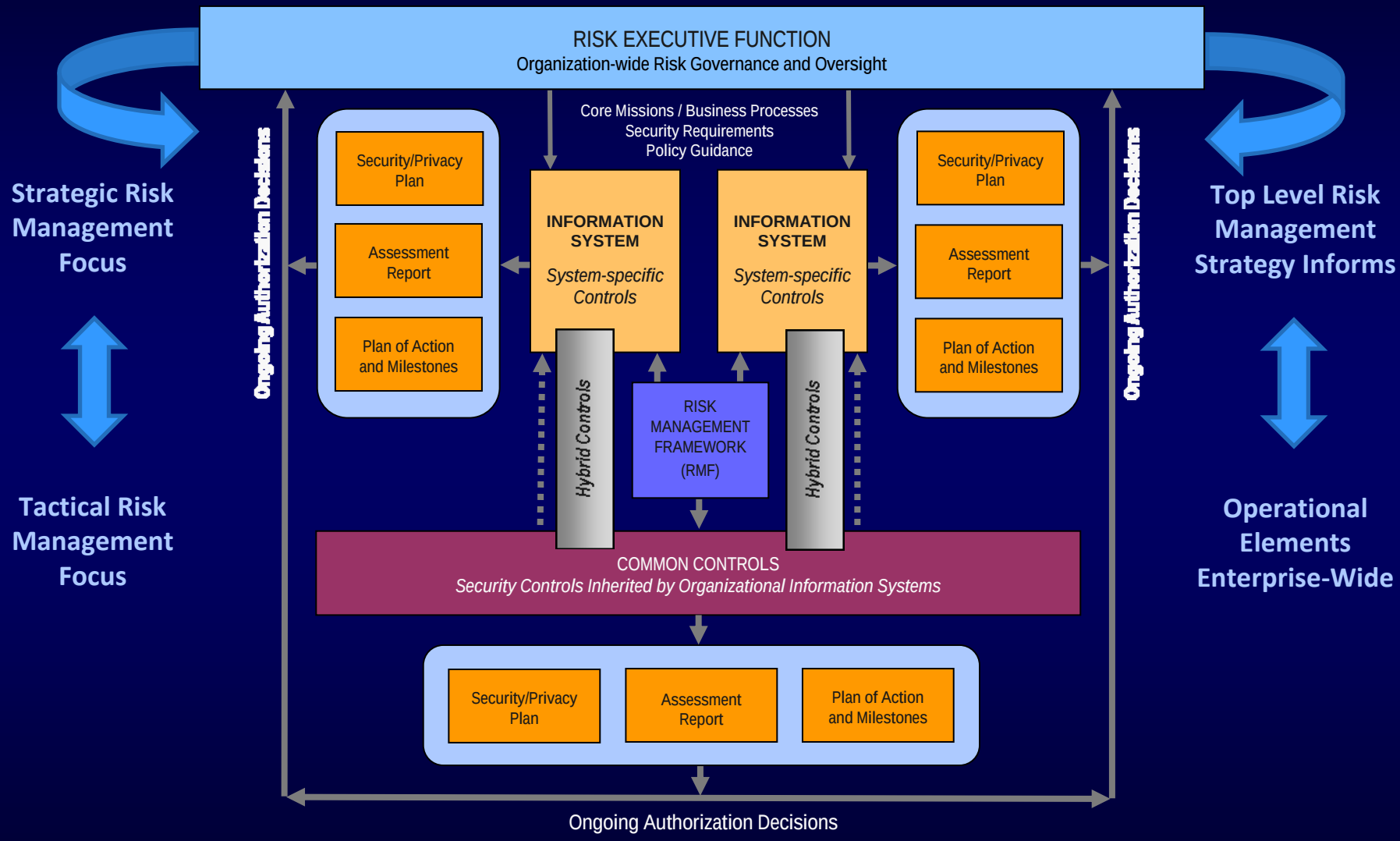
Defense-in-Depth

Links in the Security and Privacy Chain: Security and Privacy Controls

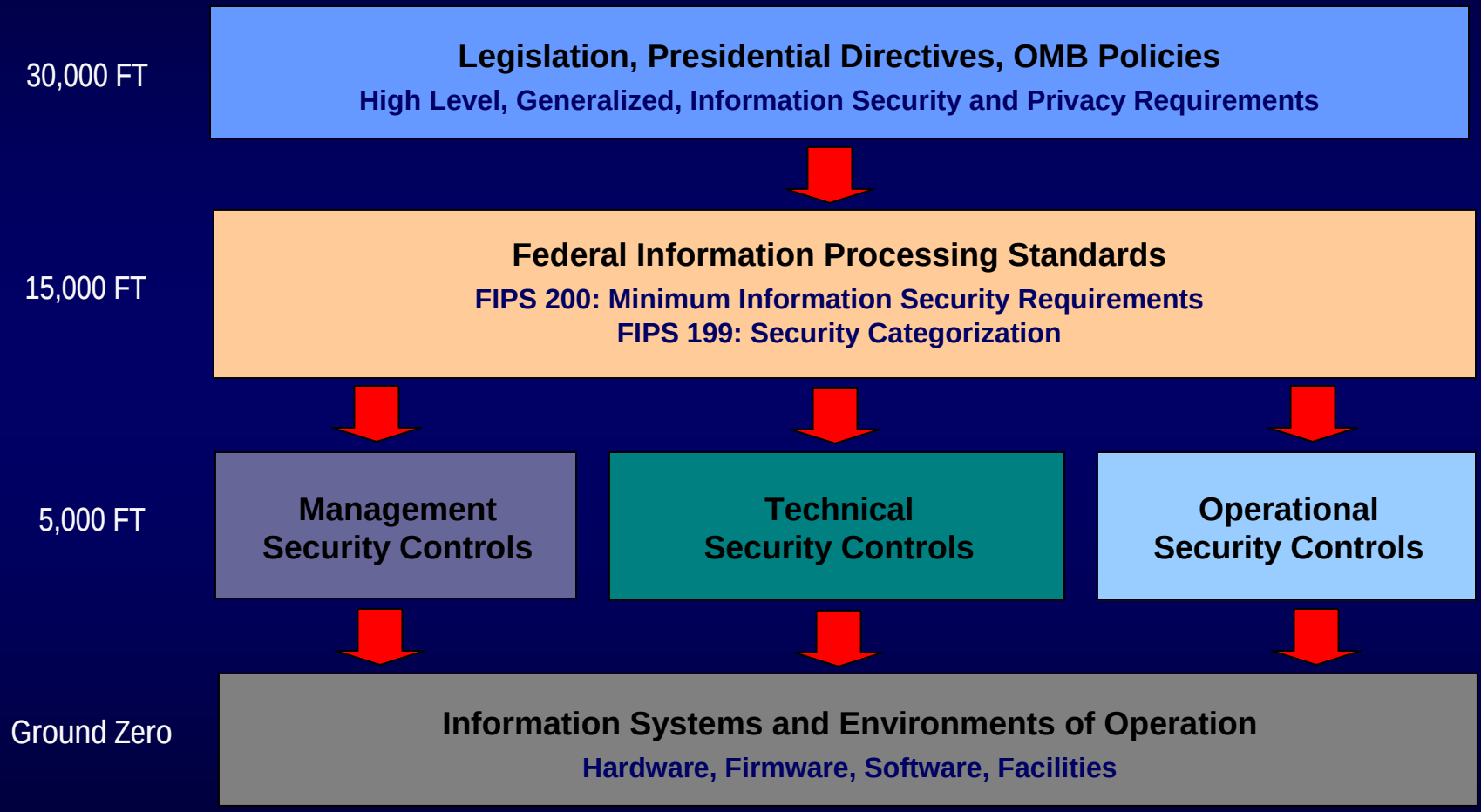
- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical and personnel security
- ✓ Security assessments and authorization
- ✓ Continuous monitoring
- ✓ Privacy protection
- ✓ 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?

Defense-in-Breadth



Requirements Traceability



Joint Task Force Transformation Initiative

Core Risk Management Publications

- NIST Special Publication 800-53, Revision 3

  Recommended Security Controls for Federal Information Systems and Organizations

  SP 800-53, Revision 4 – Appendix J: Privacy Control Catalog

Completed

- NIST Special Publication 800-53A, Revision 1

  Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

  SP 800-53A, Revision 2 – Privacy Assessment Procedures

Completed

Milestone Schedule

- SP 800-53 Appendix J – Initial Public Draft (Extract)
  - *August 2011*
- SP 800-53, Rev 4, Appendix J – Initial Public Draft
  - *December 2011 (Projected)*
- SP 800-53, Rev 4, Appendix J – Final
  - *March 2012 (Projected)*

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