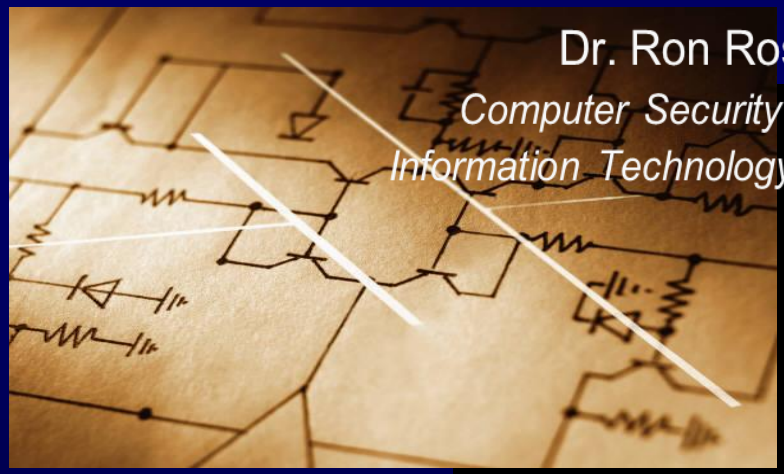
Object Management Group Technical Meeting

Managing Security Risk

In a World of Complex Systems and IT Infrastructures

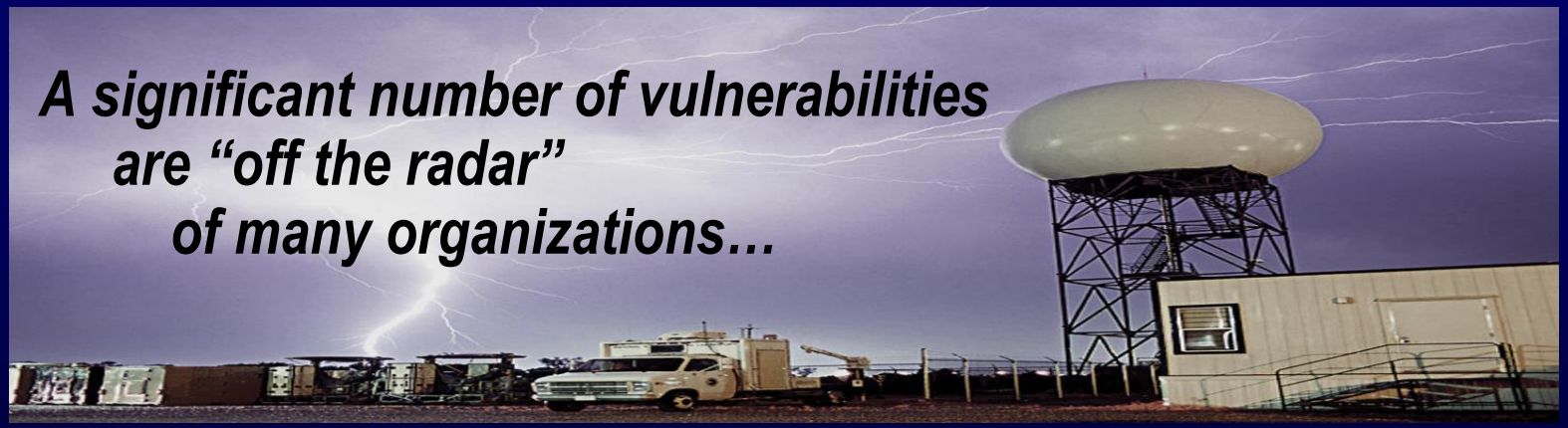


Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

Classes of Vulnerabilities

A 2013 Defense Science Board Report described—

- Tier 1: Known vulnerabilities.
- Tier 2: Unknown vulnerabilities (zero-day exploits).
- Tier 3: Adversary-created vulnerabilities (APT).



Good cyber hygiene is necessary…
But not sufficient.

You can't count, configure, or patch your way out of this problem space.

Difficult decisions ahead.

The hard cybersecurity problems are buried below the water line…

In the hardware, software, and firmware.

The argument for building stronger, more resilient information systems…

Software assurance.

Systems security engineering.

Supply chain risk management.

Getting the attention of the C-Suite.

If you are not solving the right problems, you cannot effectively manage security risk.

TACIT Security

- **T**hreat
- **A**ssets
- **C**omplexity
- **I**ntegration
- **T**rustworthiness

Threat

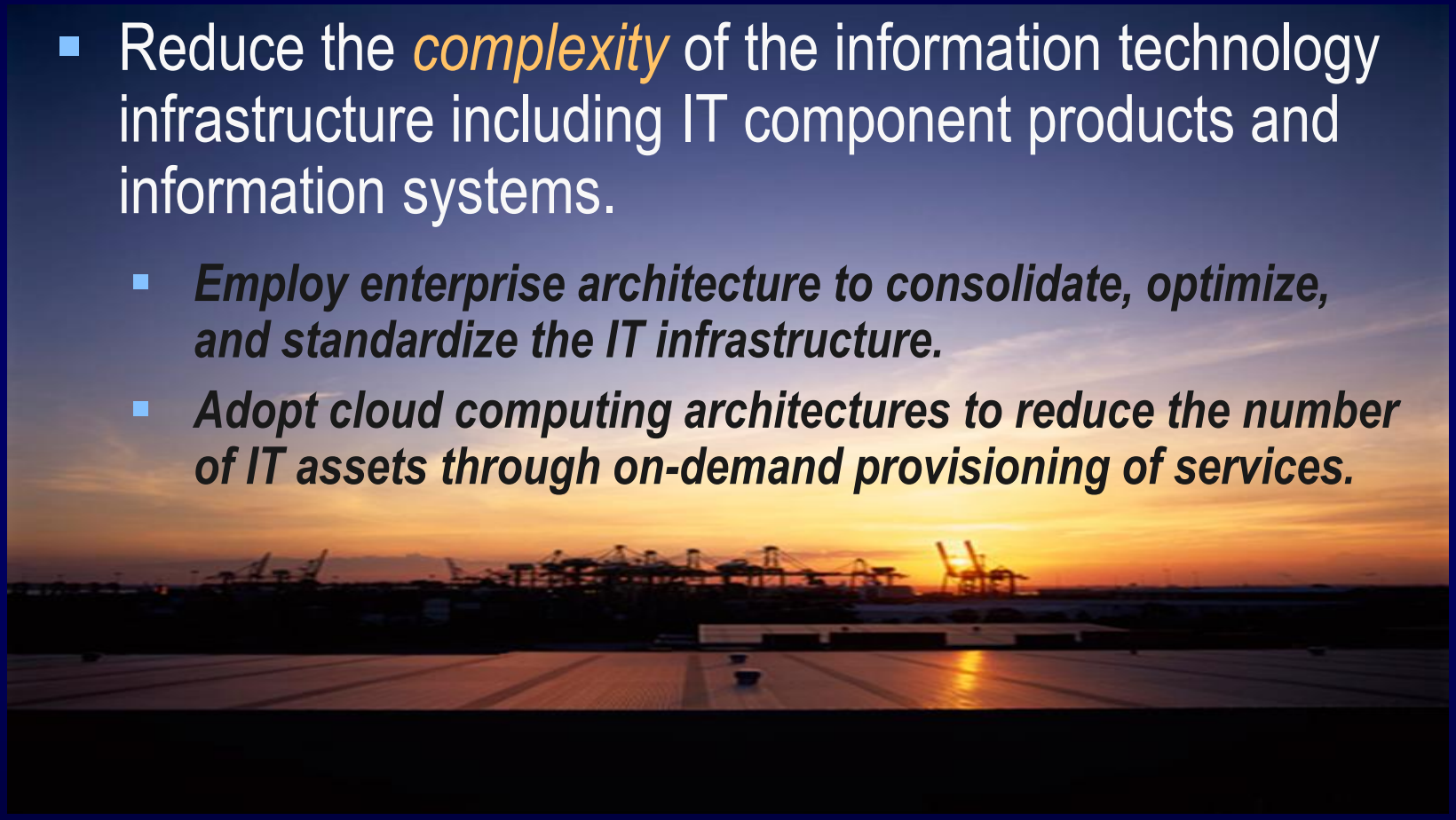
- Develop a better understanding of the *modern threat space*, including the capability of adversaries to launch sophisticated, targeted cyber-attacks that exploit specific organizational vulnerabilities.
  - ***Obtain threat data from as many sources as possible.***
  - ***Include external and insider threat analysis.***

Assets

- Conduct a comprehensive criticality analysis of *organizational assets* including information and information systems.
  - ***Focus on mission/business impact.***
  - ***Use triage concept to segregate assets by criticality.***

Complexity

- Reduce the *complexity* of the information technology infrastructure including IT component products and information systems.
  - ***Employ enterprise architecture to consolidate, optimize, and standardize the IT infrastructure.***
  - ***Adopt cloud computing architectures to reduce the number of IT assets through on-demand provisioning of services.***



Integration

- Integrate information security requirements and the security expertise of individuals into organizational *development* and *management processes*.
  - ***Embed security personnel into enterprise architecture, systems engineering, SDLC, and acquisition processes.***
  - ***Coordinate security requirements with mission/business owners; become key stakeholders.***

Trustworthiness

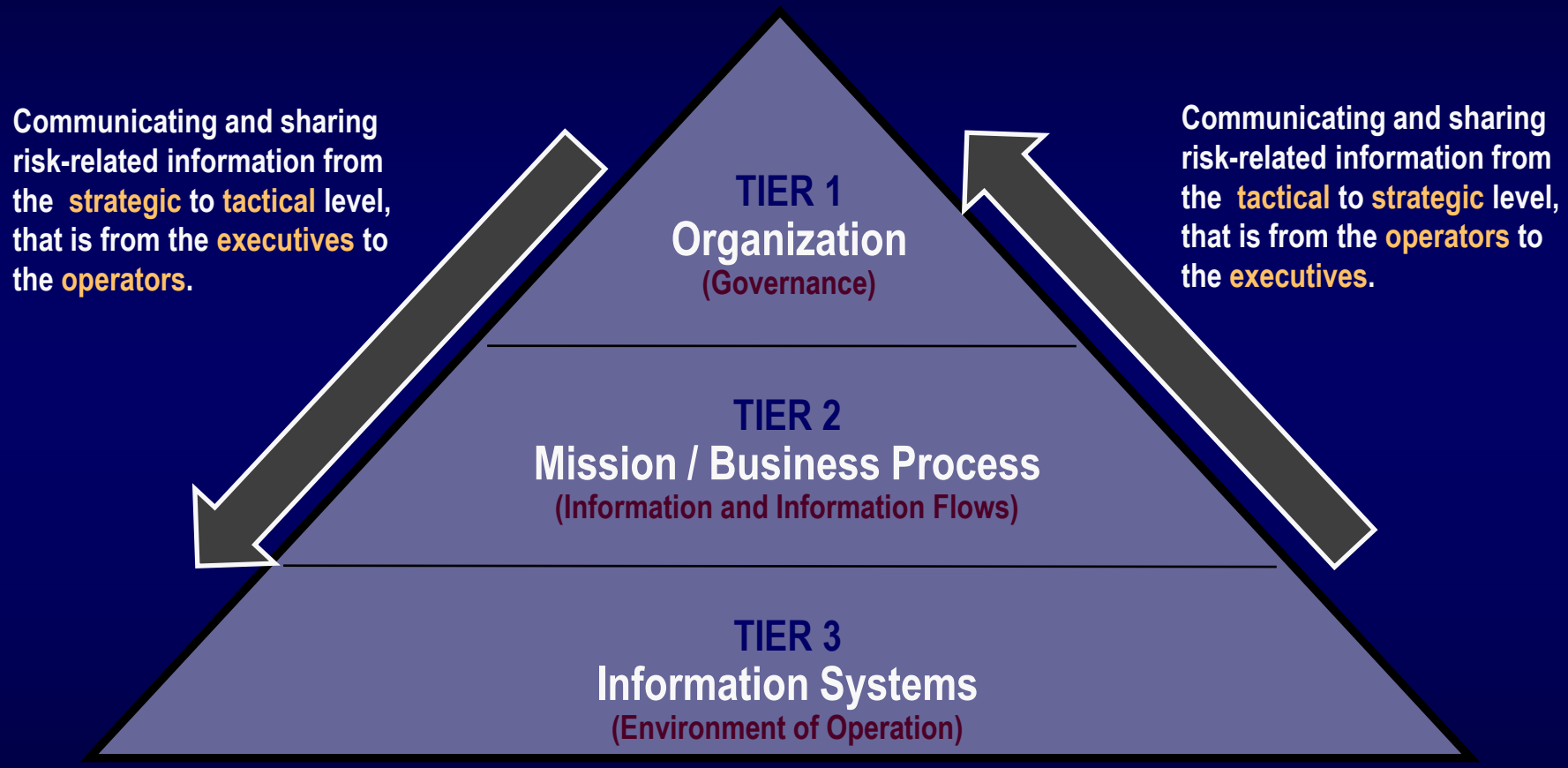
- Invest in more *trustworthy* and *resilient* information systems supporting organizational missions and business functions.
  - ***Isolate critical assets into separate enclaves.***
  - ***Implement solutions using modular design, layered defenses, component isolation.***

Summary – TACIT Security

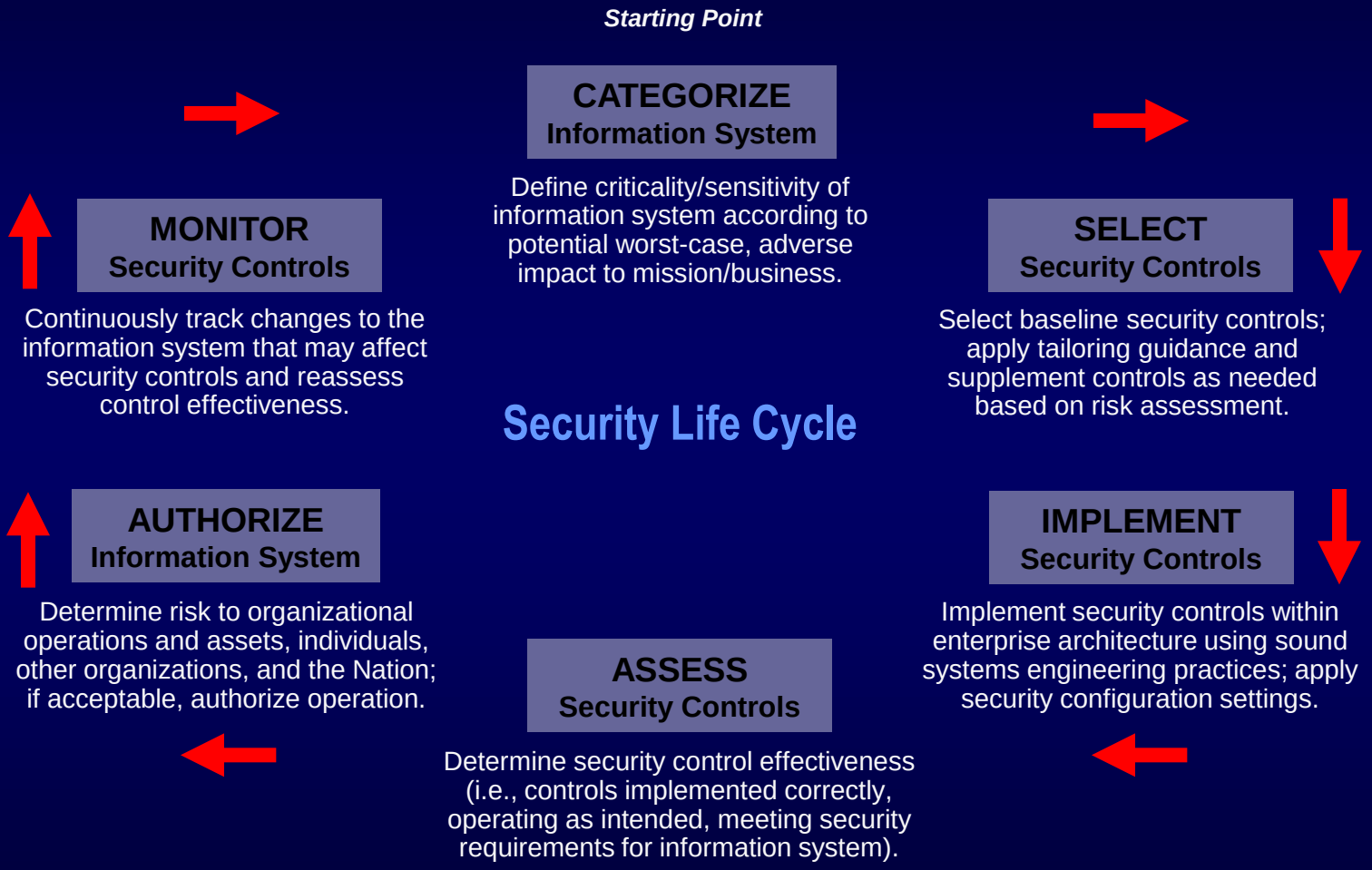
- Understand the cyber threat space.
- Conduct a thorough criticality analysis of organizational assets.
- Reduce complexity of IT infrastructure.
- Integrate security requirements into organizational processes.
- Invest in trustworthiness and resilience of IT components and systems.

Risk Management Approach

Frame – Assess – Respond – Monitor



Risk Management Framework



Joint Task Force

Risk Management Toolset

- **NIST Special Publication 800-39**
  Managing Information Security Risk: Organization, Mission, and Information System View
- **NIST Special Publication 800-30**
  Guide for Conducting Risk Assessments
- **NIST Special Publication 800-37**
  Applying the Risk Management Framework to Federal Information Systems
- **NIST Special Publication 800-53**
  Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST Special Publication 800-53A**
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations

On the Horizon…

NIST Special Publication 800-160

Systems Security Engineering

An Integrated Approach to Building Trustworthy Resilient Systems

Building on International Standards

Integrating the RMF and security concepts, principles, and best practices into IEEE/ISO/IEC 15288

Systems and software engineering — System life cycle processes

- Stakeholder requirements definition.
  - Requirements analysis.
    - Architectural design.
      - Implementation.
        - Integration.
          - Verification.
        - Transition.
      - Validation.
    - Operation.
  - Maintenance.
- Disposal.

Security must be a by-product of good design and development practices.

Government

Academia

Cybersecurity is a team sport.

Industry

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

LinkedIn
http://www.linkedin.com/in/ronrossnist

Senior Information Security Researchers and Technical Support

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

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

Web: csrc.nist.gov

Comments: sec-cert@nist.gov