Evolving Cybersecurity Strategies
NIST Special Publication 800-53, Revision 4

ISSA National Capital Chapter

April 17, 2012

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Advanced Persistent Threat

An adversary that —

- Possesses significant levels of expertise / resources.
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, deception).
- Establishes footholds within IT infrastructure of targeted organizations:
  - **To exfiltrate information.**
  - **Undermine / impede critical aspects of a mission, program, or organization.**
  - **Position itself to carry out these objectives in the future.**

Unconventional Threats to Security

Complexity

Connectivity

Culture

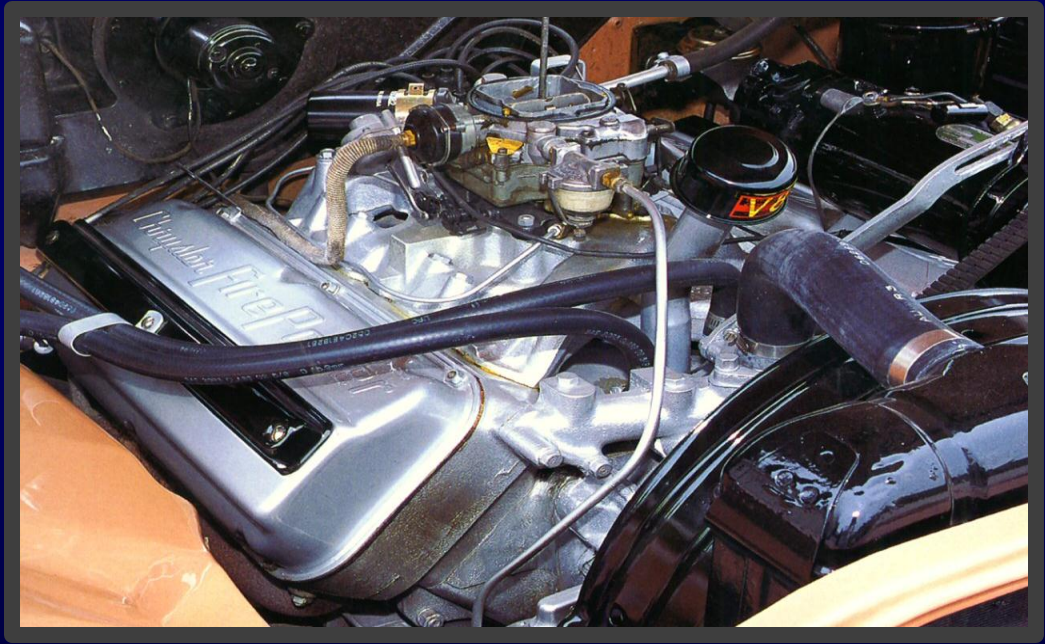
NIST SP 800-53, Revision 4 Supports

A New Cyber Defense Vision

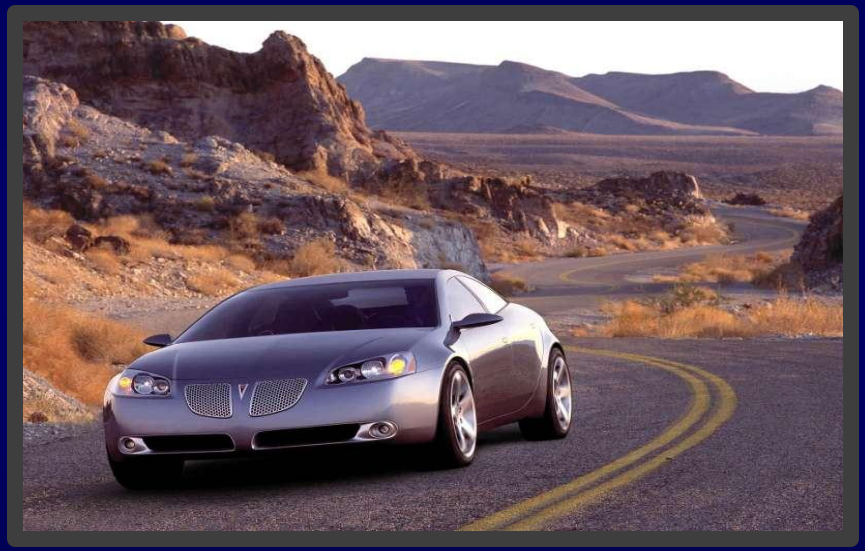
Build it right – Continuously monitor

The Present

We have our heads under the hood looking at every last detail in the engine compartment—that is, pursuing an endless number of *information system* vulnerabilities…



Instead of trying to figure out what type of car we need—that is, what level of information system *resiliency* is necessary to effectively support our core missions and business functions…



Active Cyber Defense – The Future

- Develop *risk-aware* mission and business processes.
- Develop and implement *enterprise architectures* with embedded information security architectures that support organizational mission/business processes.
- Use information technology *wisely* considering current threat landscape (capabilities, intent, and targeting).
- Develop and implement robust *continuous monitoring* programs.

Cyber Defense Vision

Core Principles

- Strong, resilient, penetration-resistant information systems supporting core missions / mission processes.
- Ongoing monitoring of the security state of information systems and environments of operation.
- Continuous improvement in security controls.
- Flexibility and agility in cyber security and risk management activities.

Fundamental Concepts

Developing IT Products and Systems

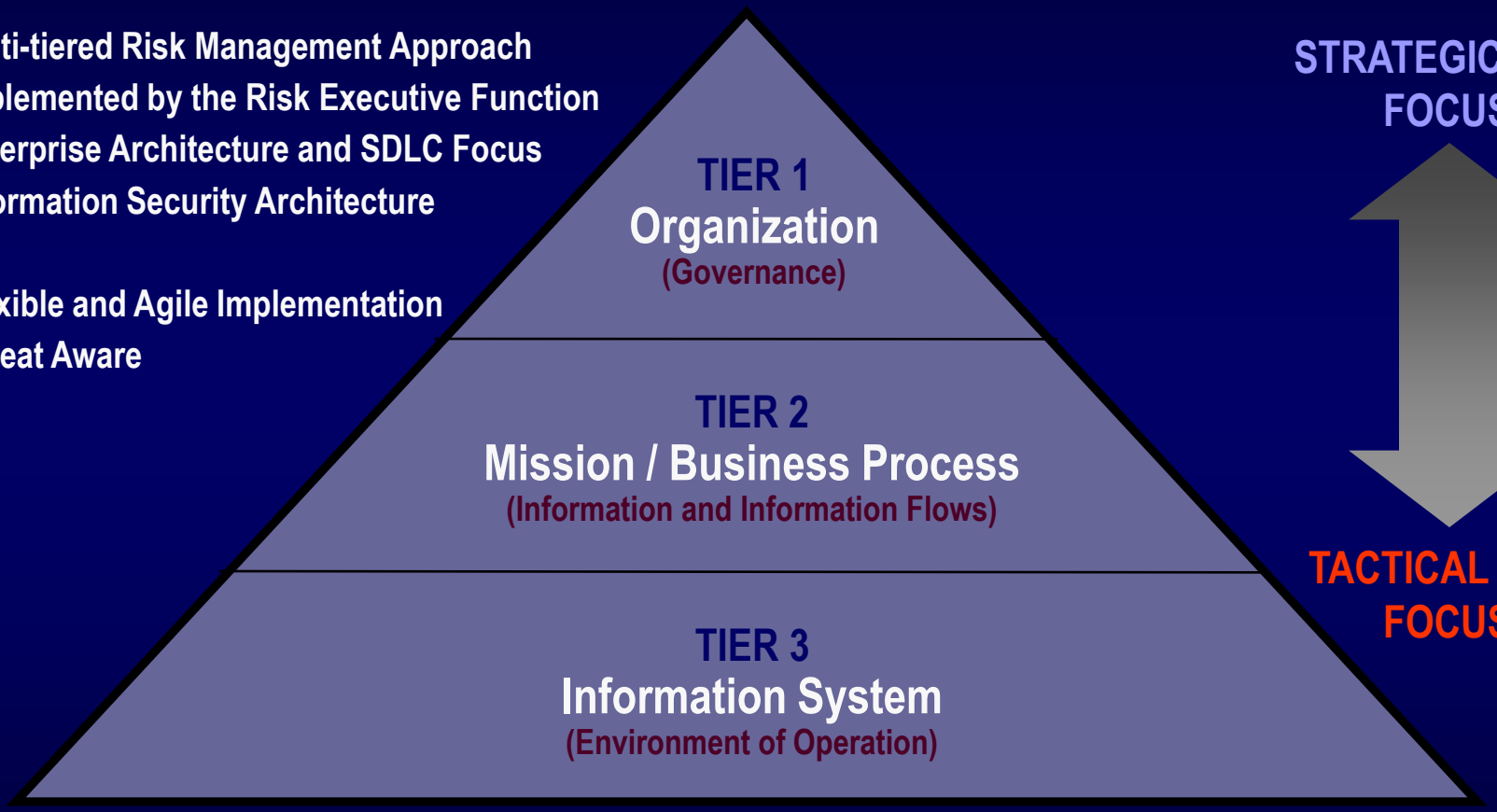
- Modularity.
- Layering.
- Monitoring.

To achieve defense-in-depth and defense-in-breadth.

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



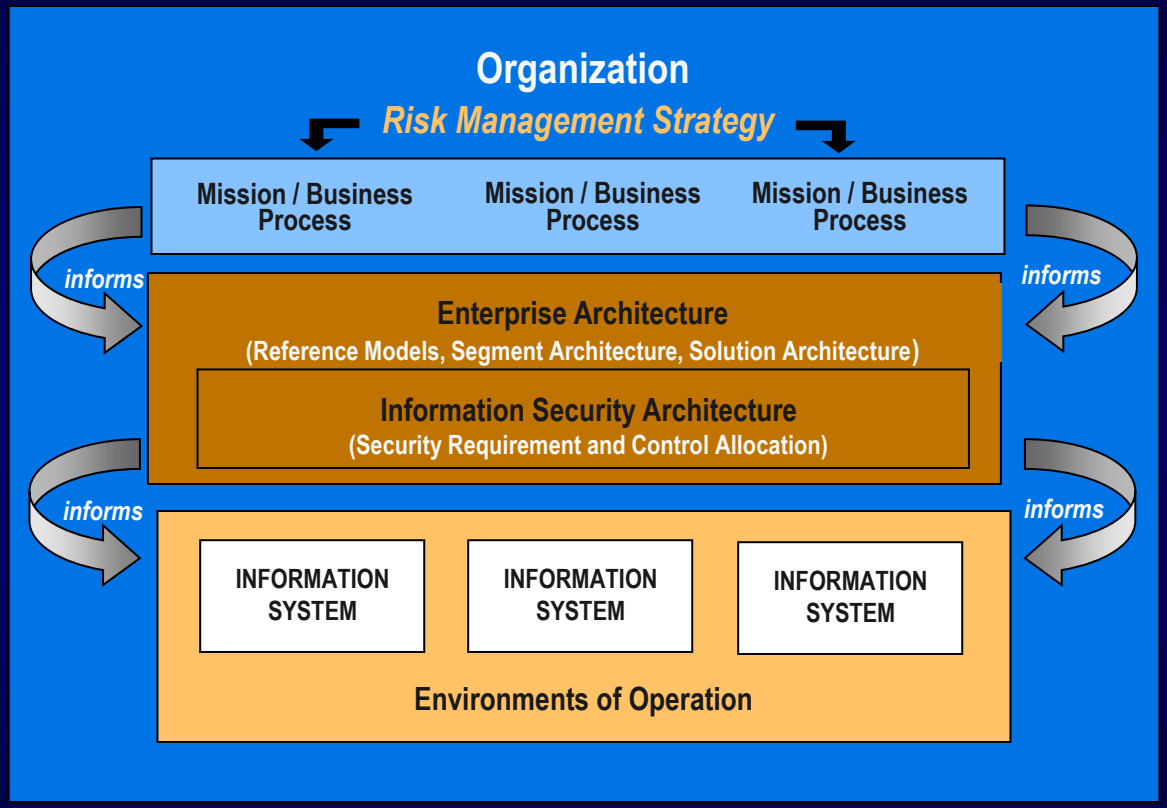
Enterprise Architecture

- Consolidation.
- Optimization.
- Standardization.

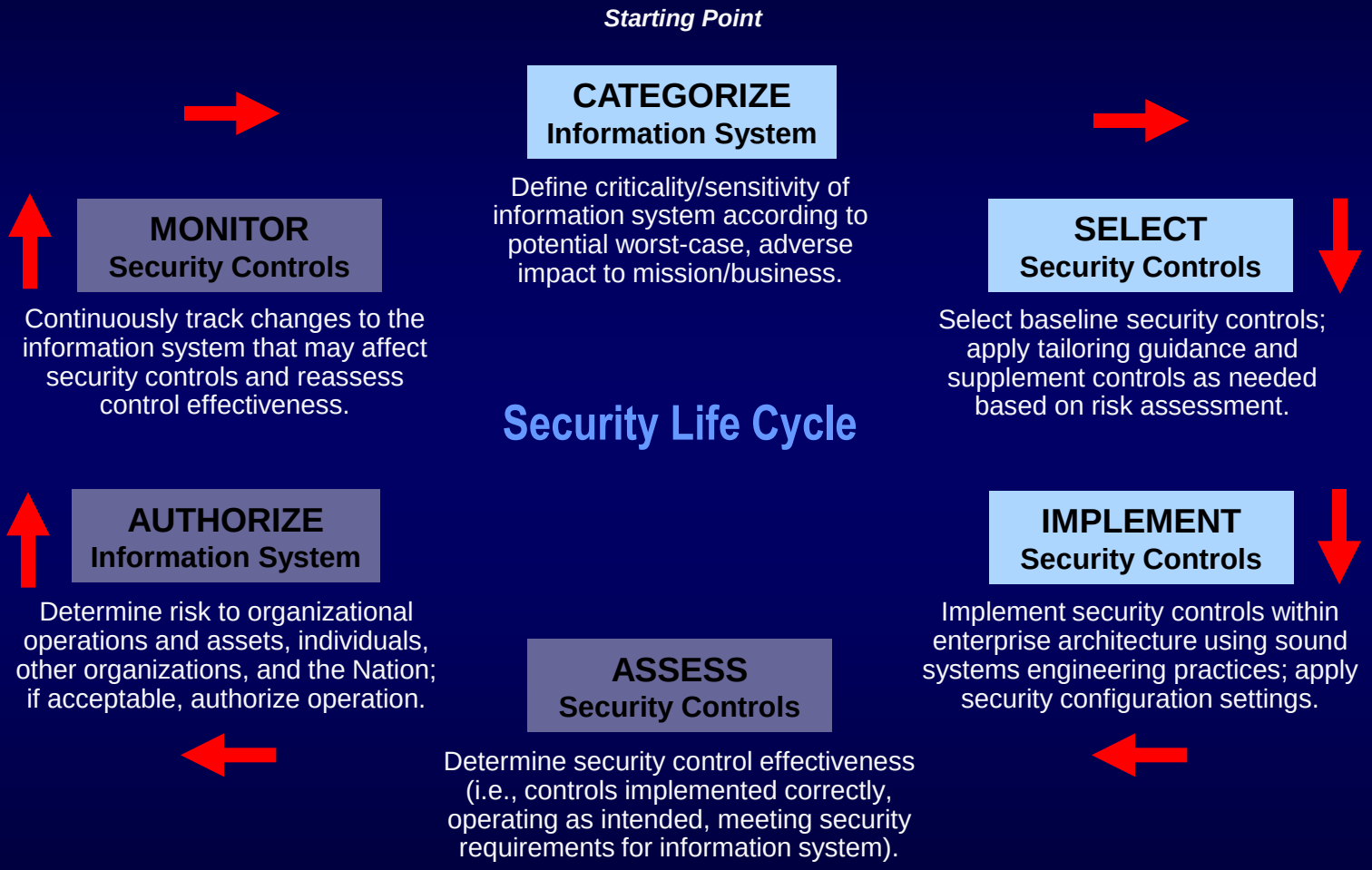
And the integration of information security architecture…

- **Reduces the size and complexity of IT infrastructures, promotes good cyber security and privacy, and can potentially lower costs (significantly) for organizations.**

Architectural and Engineering Approach



Build It Right – RMF Steps 1, 2, 3



Highlights of SP 800-53 Update

Major Drivers for Update

- Current threat landscape.
- Empirical data obtained from cyber attacks.
- Gaps in coverage in current security control catalog.
- Insufficient attention to security assurance and trustworthiness.
- Need for additional tailoring guidance for specific missions, technologies, and environments of operation.

Gap Areas Addressed

- Insider threat.
- Application security.
- Supply chain risk.
- Security assurance and trustworthy systems.
- Mobile and cloud computing technologies.
- Advanced persistent threat.
- Tailoring guidance and overlays.
- Privacy.

Control Family Labels

Eliminated management, operational, and technical labels on security control families—

ID	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	
CA	Security Assessment and Authorization	
CM	Configuration Management	
CP	Contingency Planning	
IA	Identification and Authentication	
IR	Incident Response	
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	
PL	Planning	
PS	Personnel Security	
RA	Risk Assessment	
SA	System and Services Acquisition	
SC	System and Communications Protection	
SI	System and Information Integrity	Operational
PM	Program Management	Management

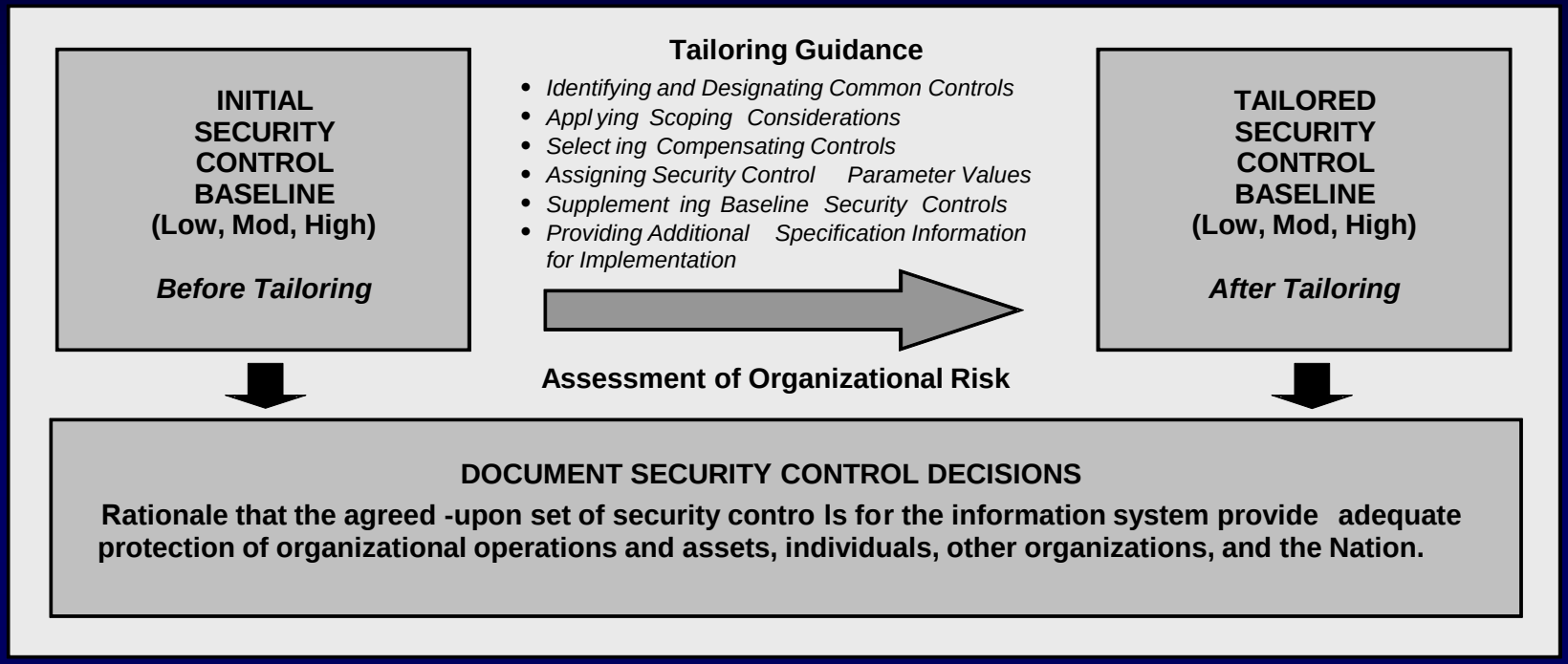
Expanded Tailoring Guidance
(1 of 2)

- Identifying and designating common controls in initial security control baselines.
- Applying scoping considerations to the remaining baseline security controls.
- Selecting compensating security controls, if needed.
- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements.

Expanded Tailoring Guidance
(2 of 2)

- Supplementing baselines with additional security controls and control enhancements, if needed.
- Providing additional specification information for control implementation.

Tailoring the Baseline



Document risk management decisions made during the tailoring process to provide information necessary for authorizing officials to make risk-based authorization decisions.

Overlays

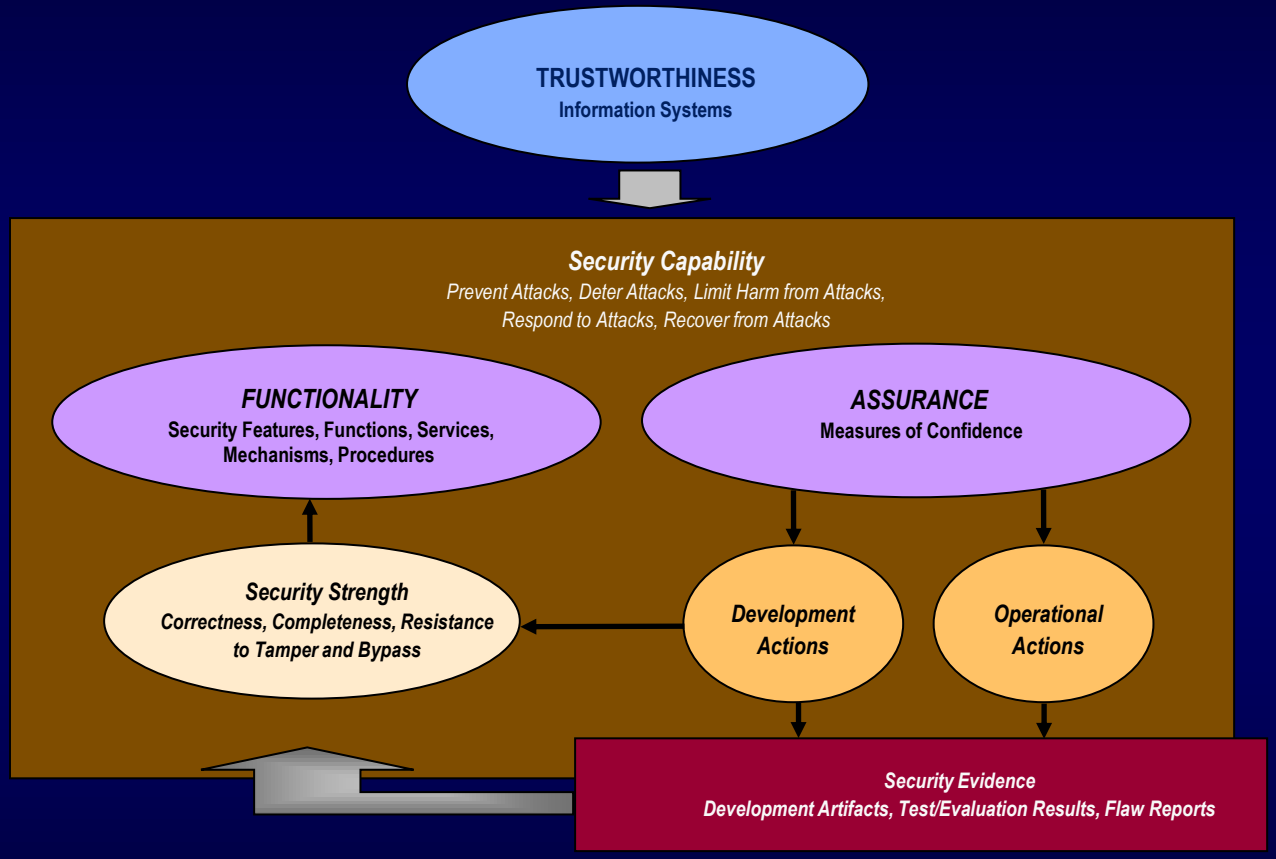
Overlays complement initial security control baselines—

- Provide the opportunity to add or eliminate controls.
- Provide security control applicability and interpretations.
- Establish community-wide parameter values for assignment and/or selection statements in security controls and control enhancements.
- Extend the supplemental guidance for security controls, where necessary.

Types of Overlays

- Communities of interest (e.g., healthcare, intelligence, financial, law enforcement).
- Information technologies/computing paradigms (e.g., cloud/mobile, PKI, Smart Grid).
- Industry sectors (e.g., nuclear power, transportation).
- Environments of operation (e.g., space, tactical).
- Types of information systems (e.g., industrial/process control systems, weapons systems).
- Types of missions/operations (e.g., counter terrorism, first responders, R&D, test, and evaluation).

Assurance and Trustworthiness



Enables Understanding of Security Capability

Minimum Assurance – Appendix E

- Appendix E has been completely revised and reworked.
- The *minimum* required assurance is provided by implementation of the appropriate baseline set of controls.
- The *assurance-related* controls for each baseline are provided in tables E-1, E-2, and E-3.
- Additional assurance-related controls are provided in table E-4, i.e., assurance-related controls not in any baseline.

Table E-1 - Minimum Assurance for Low Impact Baseline

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-5, SA-9
IA	IA-1	SC	SC-1, SC-41
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

Privacy Control Families

- Authority and Purpose **(AP)**
- Accountability, Audit, and Risk Management **(AR)**
- Data Quality and Integrity **(DI)**
- Data Minimization and Retention **(DM)**
- Individual Participation and Redress **(IP)**
- Security **(SE)**
- Transparency **(TR)**
- Use Limitation **(UL)**

Policy Changes

OMB 2011 FISMA Reporting Guidance, *Memorandum-11-33*

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf ***Question #28***

- "28. Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?

  No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate reauthorization process is not necessary……."

- Follow guidance consistent with NIST Special Publication 800-37, Revision 1.

Bottom Line: Rather than enforcing a static, every-three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs.

Continuous Monitoring

- Determine effectiveness of risk mitigation measures.
- Identify changes to information systems and environments of operation.
- Verify compliance.

Bottom Line: Increase situational awareness to help determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

Focus Areas — 2012 and Beyond

- NIST Special Publication 800-30, Revision 1
  Guide for Conducting Risk Assessments
- NIST Special Publication 800-160
  Security Engineering Guideline
- Update to NIST Special Publication 800-53, Revision 4
  Security and Privacy Controls for Federal Information Systems and Organizations
- Update to NIST Special Publication 800-53A, Revision 2
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations

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