Impact Levels and Security Controls
Understanding FIPS 199, FIPS 200 and SP 800-53

NIST Cryptographic Key Management Workshop

March 5, 2014

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory
Communicating and sharing risk-related information from the strategic to tactical level, that is from the executives to the operators.

Communicating and sharing risk-related information from the tactical to strategic level, that is from the operators to the executives.

TIER 1
Organization
(Governance)

TIER 2
Mission / Business Process
(Information and Information Flows)

TIER 3
Information System
(Environment of Operation)

STRATEGIC (EXECUTIVE) RISK FOCUS

TACTICAL (OPERATIONAL) RISK FOCUS
Risk Management Framework

Starting Point

CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT
Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

AUTHORIZE
Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

IMPLEMENT
Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

MONITOR
Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
FIPS 199 Security Objectives

- **CONFIDENTIALITY**
  - “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…”
  - A loss of confidentiality is the unauthorized disclosure of information

- **INTEGRITY**
  - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…”
  - A loss of integrity is the unauthorized modification or destruction of information

- **AVAILABILITY**
  - “Ensuring timely and reliable access to and use of information…”
  - A loss of availability is the disruption of access to or use of information or an information system
## Security Categorization

<table>
<thead>
<tr>
<th>FIPS 199</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>The loss of confidentiality could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The loss of confidentiality could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The loss of confidentiality could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>The loss of integrity could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The loss of integrity could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The loss of integrity could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>The loss of availability could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The loss of availability could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The loss of availability could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>

**Baseline Security Controls for High Impact Systems**

**Guidance for Mapping Types of Information and Information Systems to FIPS 199 Security Categories**

**SP 800-60**
Security Controls

The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Controls
Provide functionality and assurance.

FUNCTIONALITY

ASSURANCE

What is observable in front of the wall.

What is observable behind the wall.
Assurance and Trustworthiness

TRUSTWORTHINESS
(Systems and Components)

Facilitates risk response to a variety of threats, including hostile cyber attacks, natural disasters, structural failures, and human errors, both intentional and unintentional.

Enables

Security Requirements

Satisfies

Security Capability
Mutually Reinforcing Security Controls
(Technical, Physical, Procedural Means)

Provides Confidence In

Security Assurance
Developmental/Operational Actions
(Assurance-Related Controls)

Promotes Traceability from Requirements to Capability to Functionality with Degree of Assurance

Produces

Security Functionality
Features, Functions, Services, Mechanisms, Processes, Procedures
(Functionality-Related Controls)

Generates

Security Evidence
Development Artifacts, Flaw Reports, Assessment Results, Scan Results, Integrity Checks, Configuration Settings

Provides

Confidence In

Security Assurance Developmental/Operational Actions
(Assurance-Related Controls)
# NIST SP 800-53 Security Control Families

<table>
<thead>
<tr>
<th>ID</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
</tr>
<tr>
<td>CA</td>
<td>Security Assessment and Authorization</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>PL</td>
<td>Planning</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>SA</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>SC</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>PM</td>
<td>Program Management</td>
</tr>
</tbody>
</table>
Control Naming Convention

AC-9  PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: The information system notifies the user, upon successful interactive logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance: This control is intended to cover both traditional logons to information systems and accesses to systems that occur in other types of architectural configurations (e.g., service oriented architectures). Related controls: AC-7, PL-4.

Control Enhancements:

(1) PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS
The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) PREVIOUS LOGON NOTIFICATION | SUCCESSFUL/UNSUCCESSFUL LOGONS
The information system notifies the user of the number of [Selection: successful logons/accesses; unsuccessful logon/access attempts; both] during [Assignment: organization-defined time period].
Security Control Baselines

- Starting point for the security control selection process.
- Chosen based on the security category and associated impact level of the information system determined in accordance with FIPS 199 and FIPS 200, respectively.
- Three sets of baseline controls have been identified corresponding to low-impact, moderate-impact, and high-impact information system levels.
- Appendix D provides a listing of baseline security controls.
Security Control Baselines

Baselines are determined by:
- Information and system categorization (L, M, H)
- Organizational risk assessment and risk tolerance
- System level risk assessment

Baselines can be tailored:
- Instantiate parameters in controls
- Implement scoping considerations and compensating controls
- Supplement by with additional controls/enhancements.
Clarification of Term *Baseline*

The use of the term *baseline* is intentional. The security controls and control enhancements listed in the initial baselines are *not* a minimum—but rather a proposed starting point from which controls and controls enhancements may be removed or added based on the tailoring guidance in Section 3.2.

*Specialization of security plans is the objective...*
Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls

Baseline Security Controls
Low Impact Information Systems

Baseline Security Controls
Moderate Impact Information Systems

Baseline Security Controls
High Impact Information Systems

Low Baseline

Moderate Baseline

High Baseline

Tailored Baseline

Tailored Baseline

Tailored Baseline

A cost effective, risk-based approach to achieving adequate information security…
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

<table>
<thead>
<tr>
<th>INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)</th>
<th>TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before Tailoring</td>
<td>After Tailoring</td>
</tr>
</tbody>
</table>

**Assessment of Organizational Risk**

**Tailoring Guidance**
- Identifying and Designating Common Controls
- Applying Scoping Considerations
- Selecting Compensating Controls
- Assigning Security Control Parameter Values
- Supplementing Baseline Security Controls
- Providing Additional Specification Information for Implementation

**DOCUMENT SECURITY CONTROL DECISIONS**
Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

**Document risk management decisions made during the tailoring process to provide information necessary for authorizing officials to make risk-based authorization decisions.**
# Tables in SP 800-53 Appendix D

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>WITHDRAWN</th>
<th>ASSURANCE</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>CONTROL NAME</strong></td>
<td></td>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td></td>
<td><em>Control Enhancement Name</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL-1</td>
<td>Security Planning Policy and Procedures</td>
<td>A</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PL-2</td>
<td>System Security Plan</td>
<td>A</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PL-2 (1)</td>
<td>SYSTEM SECURITY PLAN</td>
<td>CONCEPT OF OPERATIONS</td>
<td>W</td>
<td>Incorporated into PL-7.</td>
</tr>
<tr>
<td>PL-2 (2)</td>
<td>SYSTEM SECURITY PLAN</td>
<td>FUNCTIONAL ARCHITECTURE</td>
<td>W</td>
<td>Incorporated into PL-8.</td>
</tr>
<tr>
<td>PL-2 (3)</td>
<td>SYSTEM SECURITY PLAN</td>
<td>PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</td>
<td>A</td>
<td>x</td>
</tr>
<tr>
<td>PL-4</td>
<td>Rules of Behavior</td>
<td>A</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PL-4 (1)</td>
<td>RULES OF BEHAVIOR</td>
<td>SOCIAL MEDIA AND NETWORKING RESTRICTIONS</td>
<td>A</td>
<td>x</td>
</tr>
<tr>
<td>PL-7</td>
<td>Security Concept of Operations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL-8</td>
<td>Security Architecture</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**
Kelley Dempsey  
(301) 975-2827  
kelley.dempsey@nist.gov

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

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

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