NATIONAL E-SECURITY STANDARD

Overview and highlights about the US FISMA

NATIONAL E-SECURITY STANDARD

AGENDA

The two guards

Exploring how others did their national security standard

What is us fisma ?

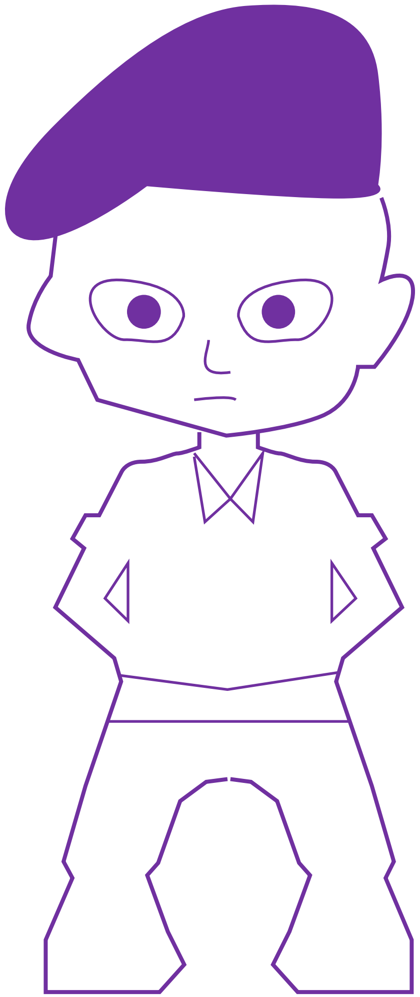
What FISMA leads to

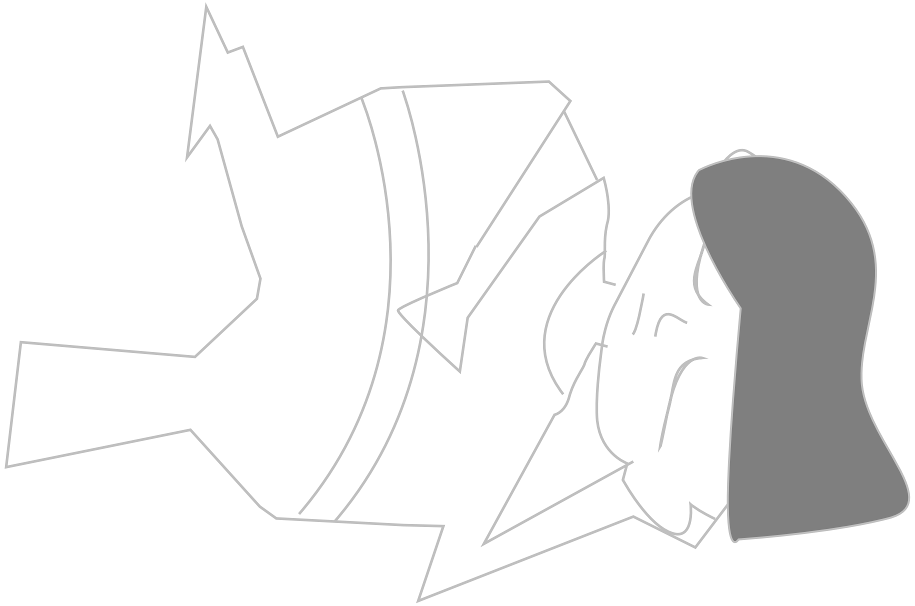
Managing enterprise risk

Minimum security requirements

Conclusion

TWO GUARDS





OBJECTIVE: NATIONAL WIDE SECURITY STANDARD

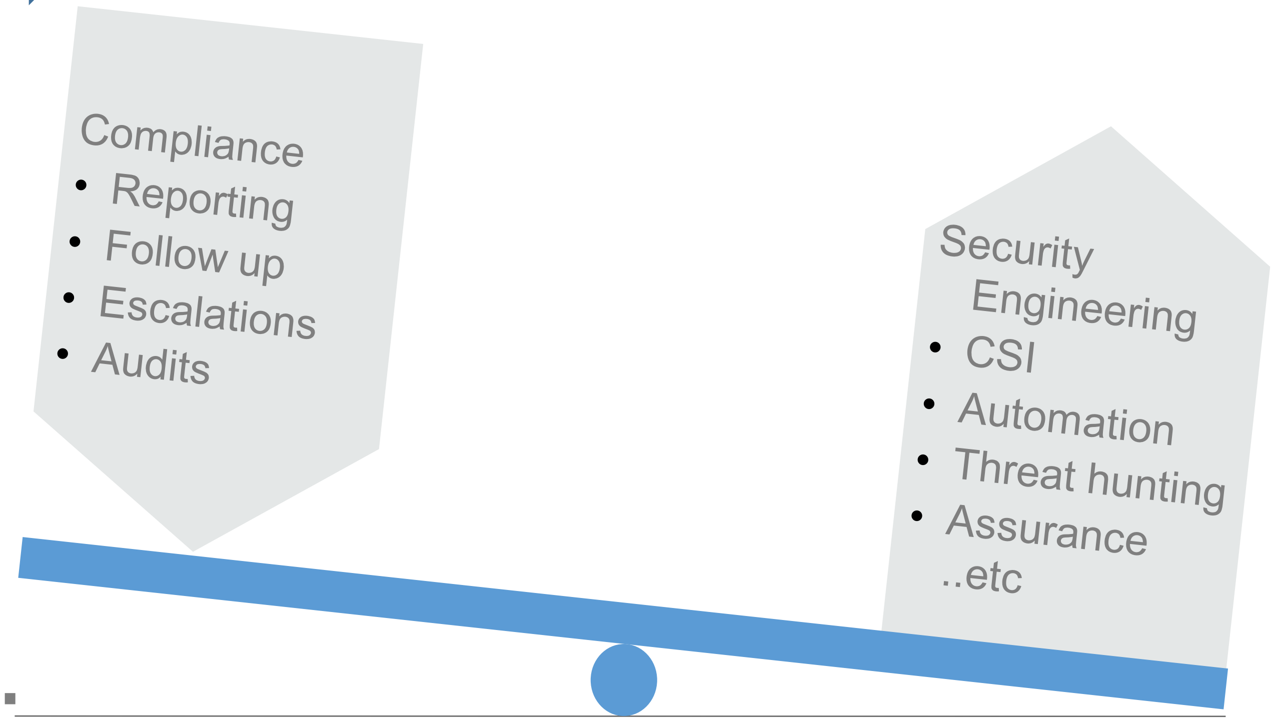
How did the others do their national security standard?

- Government enforced
- Business-driven
- Well structured
- Risk-focused and Prioritized
- Scalable
- Demonstrates compliance
- Auditable

At the end We need..

✓ **Spend less time in security compliance..**

✓ **More time in security engineering..**



They implemented FISMA…

WHAT IS FISMA

FISMA : Federal information management act , Signed into law in December 2002 and it got updated after

Brought information security best practices, more focused structured standards to the US federal operations, they empowered NIST to define and maintain the standards

VISION:

Ensure the entities are having an adequate security controls to prevent against *disclosure*, *disruption*, *modification*, or *destruction* of information(CIA). promote the development of key security standards and guidelines to support the implementation of and compliance with the standard.

KEY FOCUS AREA

Standards for **categorizing** information and systems by mission impact

Guidance for **selecting** appropriate security controls for systems

Standards for **implementing** security requirements for information and systems

Guidance for the security **authorization** of systems

Guidance for **assessing** security controls in systems and determining security control effectiveness

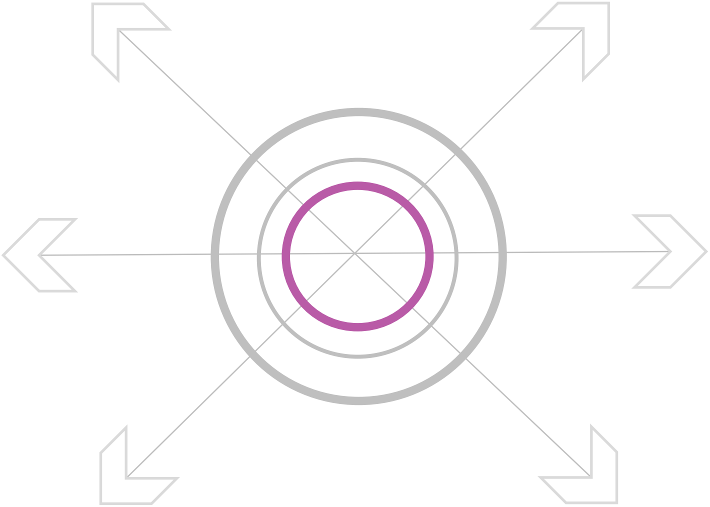
Guidance for **monitoring** the security controls

VISION LEADS TO

The implementation of **cost-effective, risk-based Information security programs**

The establishment of a level of **security due diligence for all the related entities**

More consistent and **cost-effective Implementation of security controls** across the related entities’ technology infrastructure



More consistent and proper security **control assessments**

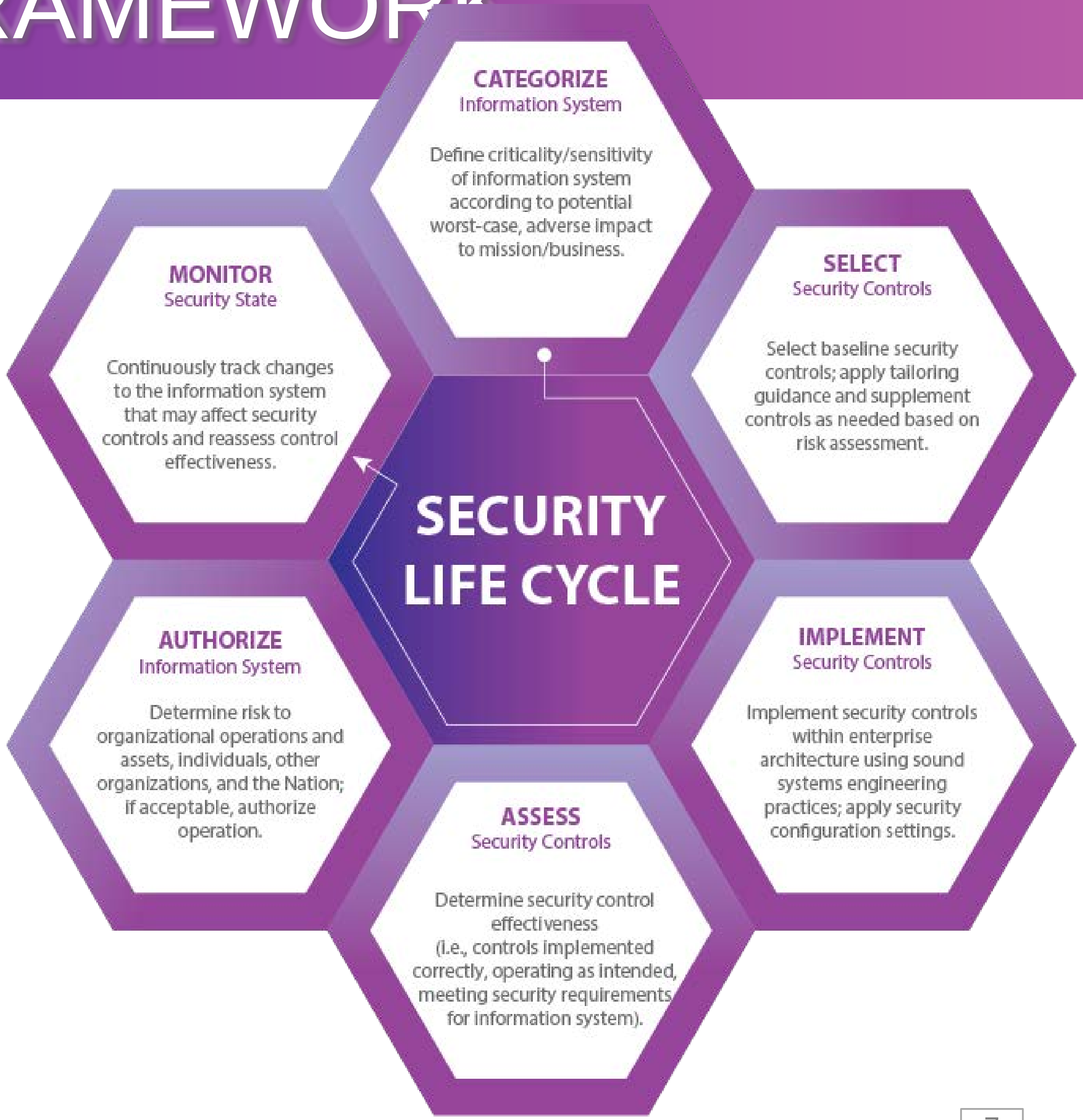
A better understanding of **enterprise-wide mission risks** resulting from the operation of information systems

Guidance for **monitoring the security controls** and the security authorization of systems

RISK MANAGEMENT FRAMEWORK

Key activities in managing enterprise-level risk—risk resulting from the operation of an information system:

- Categorize the information systems
- Select set of minimum (baseline) security controls
- Implement the security controls in the information system
- Assess the security controls
- Authorize information system operation
- Monitor security controls on a continuous basis



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.

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).

AUTHORIZE
Information System

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

MONITOR
Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

SECURITY LIFE CYCLE

RISK MANAGEMENT FRAMEWORK STEPS

Security Categorization	Categorize the information system and document the results of the security categorization in the security plan.
Result	To influence the selection of appropriate security controls

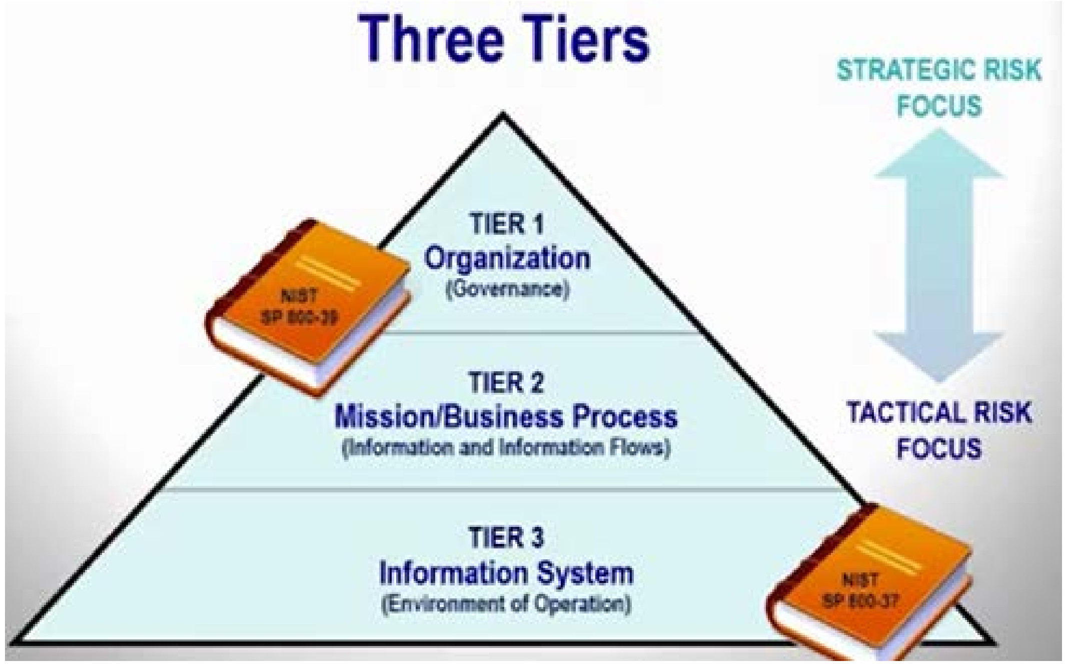
Describe The Information System	Describe the information system and document the description in the security plan
Result	Support the risk management

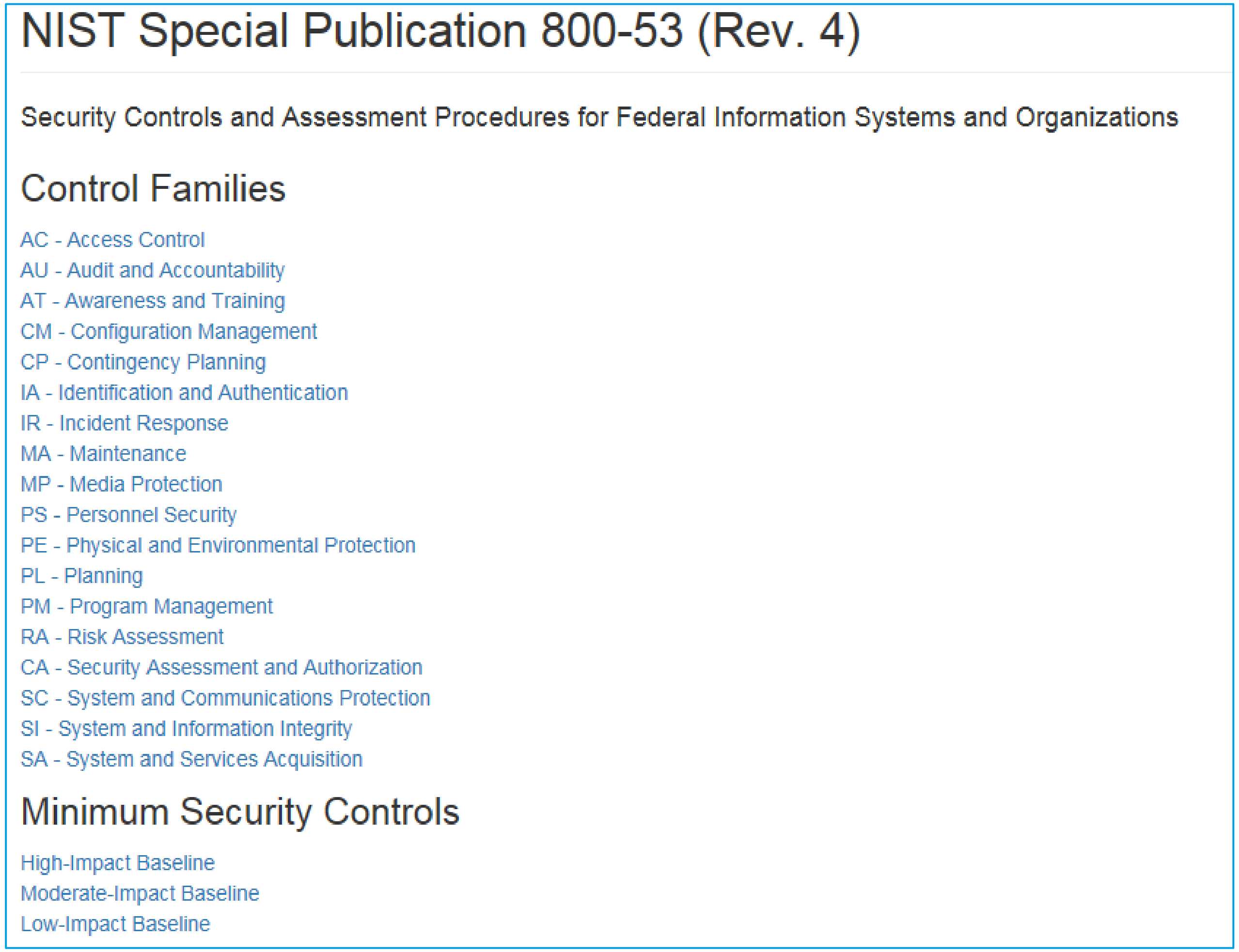
Information System Registration	Register the information system with appropriate asset management tool
Result	Effective tracking of information systems

CONTROLS SELECTIONS = A HEAD OF ADVERSARIES

Document 800.53 provides a comprehensive set of security controls, three security control baselines (low, moderate, and high impact)

The **management, operational,** and **technical controls** protect the confidentiality, integrity, and availability of the system and its information





NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Control Families

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

Minimum Security Controls

- High-Impact Baseline
- Moderate-Impact Baseline
- Low-Impact Baseline

BEING SPONTANEOUS DOES NOT HELP

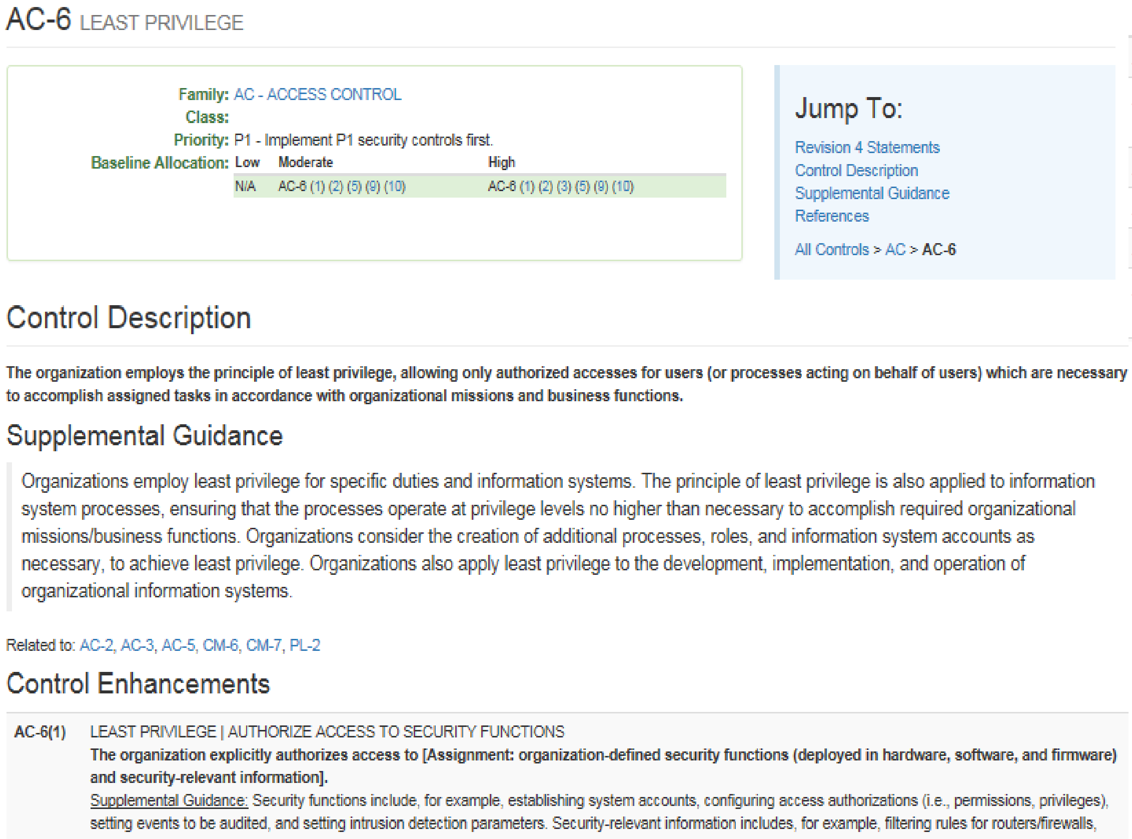
NIST controls

- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Planning
- Personnel security
- Risk assessment
- Systems and services acquisition
- System and communications protection
- System and information integrity

SECURITY CONTROLS

For each control you will se:

- ✓ Description
- ✓ Supplemental guidance
- ✓ Control enhancement



AC-6 LEAST PRIVILEGE

Family:	AC - ACCESS CONTROL		
Class:			
Priority:	P1 - Implement P1 security controls first.		
Baseline Allocation:	Low	Moderate	High
	N/A	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)

Jump To:

Revision 4 Statements
Control Description
Supplemental Guidance
References

All Controls > AC > **AC-6**

Control Description

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance

> Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

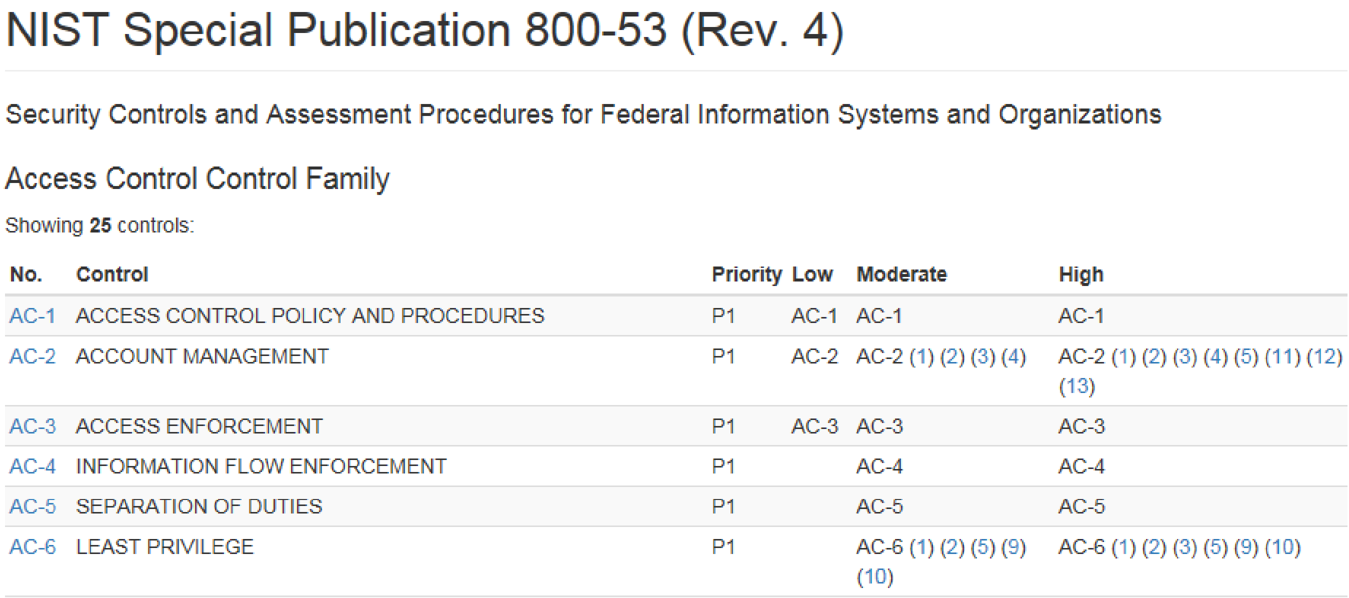
Related to: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2

Control Enhancements

AC-6(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls,



NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Access Control Control Family

Showing **25** controls:

No.	Control	Priority	Low	Moderate	High
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	ACCESS ENFORCEMENT	P1	AC-3	AC-3	AC-3
AC-4	INFORMATION FLOW ENFORCEMENT	P1		AC-4	AC-4
AC-5	SEPARATION OF DUTIES	P1		AC-5	AC-5
AC-6	LEAST PRIVILEGE	P1		AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)

ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME
AC-1	**Access Control Policy and Procedures**
AC-2	**Account Management**
AC-3	**Access Enforcement**
AC-4	**Information Flow Enforcement**
AC-5	**Separation of Duties**
AC-6	**Least Privilege**
AC-7	**Unsuccessful Login Attempts**
AC-8	**System Use Notification**
AC-9	**Previous Logon (Access) Notification**
AC-10	**Concurrent Session Control**
AC-11	**Session Lock**
AC-12	**Session Termination**
AC-13	**Supervision and Review—Access Control**
AC-14	**Permitted Actions without Identification or Authentication**
AC-15	**Automated Marking**
AC-16	**Security Attributes**
AC-17	**Remote Access**
AC-18	**Wireless Access**
AC-19	**Access Control for Mobile Devices**
AC-20	**Use of External Information Systems**
AC-21	**User-Based Collaboration And Information Sharing**
AC-22	**Publicly Accessible Content**

CENTER OF INTERNET SECURITY BEANCHMARK- CIS

WHAT IS CIS BENCHNCHMARK ?

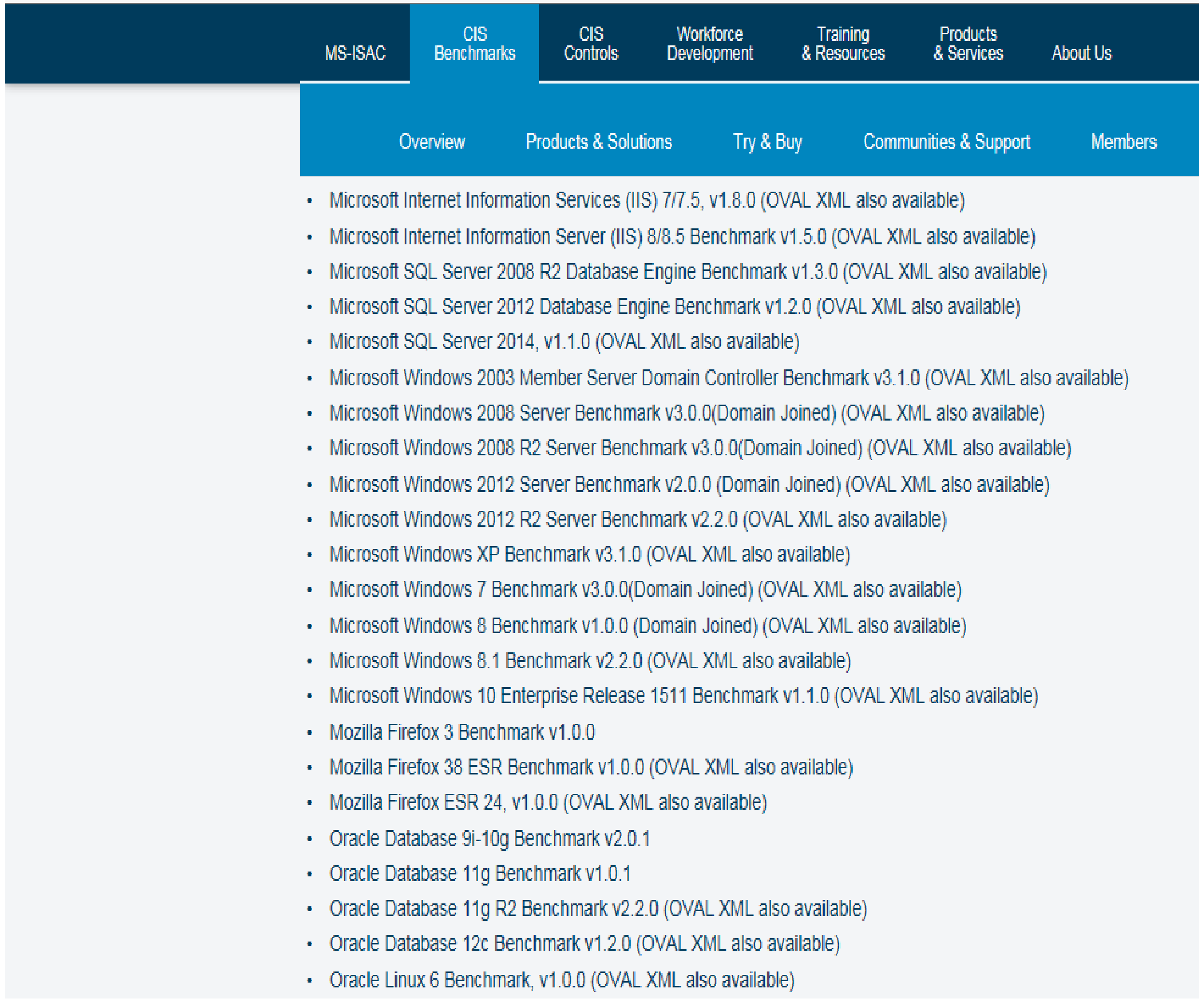
Recommended technical settings for operating systems, middleware and software applications, and network devices

PURPOSE

The CIS Controls were crafted to answer the frequent question: “**Where should I start when I want to improve my cyber defenses**?”

Practical Guidance for Implementing the Critical Security Controls

Compliance requirements for FISMA



- Microsoft Internet Information Services (IIS) 7/7.5, v1.8.0 (OVAL XML also available)
- Microsoft Internet Information Server (IIS) 8/8.5 Benchmark v1.5.0 (OVAL XML also available)
- Microsoft SQL Server 2008 R2 Database Engine Benchmark v1.3.0 (OVAL XML also available)
- Microsoft SQL Server 2012 Database Engine Benchmark v1.2.0 (OVAL XML also available)
- Microsoft SQL Server 2014, v1.1.0 (OVAL XML also available)
- Microsoft Windows 2003 Member Server Domain Controller Benchmark v3.1.0 (OVAL XML also available)
- Microsoft Windows 2008 Server Benchmark v3.0.0(Domain Joined) (OVAL XML also available)
- Microsoft Windows 2008 R2 Server Benchmark v3.0.0(Domain Joined) (OVAL XML also available)
- Microsoft Windows 2012 Server Benchmark v2.0.0 (Domain Joined) (OVAL XML also available)
- Microsoft Windows 2012 R2 Server Benchmark v2.2.0 (OVAL XML also available)
- Microsoft Windows XP Benchmark v3.1.0 (OVAL XML also available)
- Microsoft Windows 7 Benchmark v3.0.0(Domain Joined) (OVAL XML also available)
- Microsoft Windows 8 Benchmark v1.0.0 (Domain Joined) (OVAL XML also available)
- Microsoft Windows 8.1 Benchmark v2.2.0 (OVAL XML also available)
- Microsoft Windows 10 Enterprise Release 1511 Benchmark v1.1.0 (OVAL XML also available)
- Mozilla Firefox 3 Benchmark v1.0.0
- Mozilla Firefox 38 ESR Benchmark v1.0.0 (OVAL XML also available)
- Mozilla Firefox ESR 24, v1.0.0 (OVAL XML also available)
- Oracle Database 9i-10g Benchmark v2.0.1
- Oracle Database 11g Benchmark v1.0.1
- Oracle Database 11g R2 Benchmark v2.2.0 (OVAL XML also available)
- Oracle Database 12c Benchmark v1.2.0 (OVAL XML also available)
- Oracle Linux 6 Benchmark, v1.0.0 (OVAL XML also available)

THE JOURNEY …

Practical considerations we should make to succeed in this journey:

NATIONAL WIDE:

- ❑ Having a Formal Act: Having a national wide E-Security standard that is supported and enforced by the government
- ❑ Entities program manager: Senior management should be on boarded for support and accountability

ORGANIZATIONAL WIDE:

- ❑ Gap analysis: Start with a gap analysis assessment and audit the current organization’s status against the standard **requirements** and have matrix and dashboards to always assess the security posture and set **action plan**
- ❑ Long term sustainability: Impliment long-term sustainability to maintain the security of the information systems
- ❑ Education and awareness: Train workforce members towards adopting the standard

THANK YOU