#SHAREorg

SHARE
Technology · Connections · Results

Big Brother is Watching Your Big Data: z/OS Actions Buried in the FISMA Security Regulation

Bill Valyo
CA Technologies

February 7, 2013
Session #12765

SHARE in San Francisco 2013

Quick Abstract:
About this Presentation

- This presentation is part FISMA primer…
- …and part best practice guide for z/OS.
- In short, it's intended to give you an idea as to how to address FISMA in the z/OS environment. Including:
  - Compliance perspective
  - Technology perspective

Some Disclaimers

- I work for CA Technologies.
  - CA has vested interest in some of the security software mentioned.
  - But I am going to be very generic here.
- I am not an attorney or an auditor.
  - Suggestions herein focus on potential *technical* solutions for FISMA requirements.
  - Please review with legal and auditing professionals.

Legal

Certain information in this presentation may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available (i) for sale to new licensees of such product; and (ii) in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of such product who are current subscribers to CA maintenance and support on a when and if-available basis.

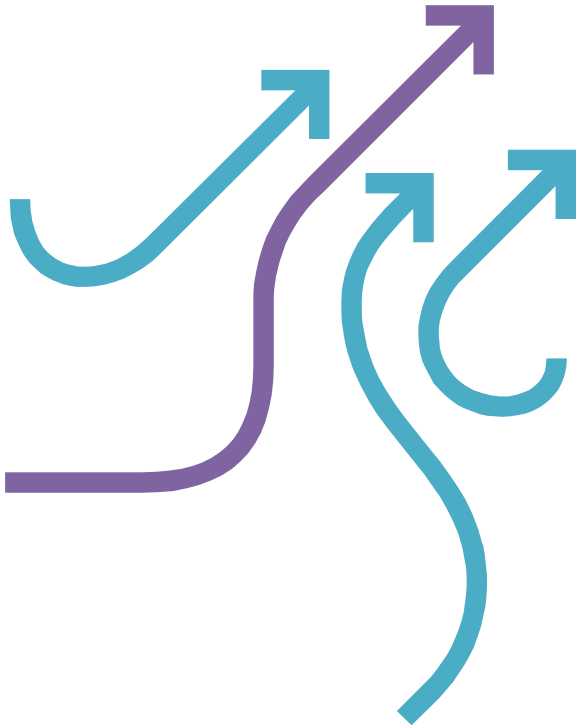
THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised of the possibility of such damages.

Agenda

- *Brief* Level Set: Who Should Follow FISMA
  - Some Surprises Here!
- FISMA Basis
  - Chain of Legal Documents
- FISMA Technical Requirements Overview
  - Best Practice/Project Approach – 10 steps!
- FISMA and z/OS Technology
  - Walk Through Control Families
- The *Present* Future

Brief Level Set

Getting on the Same Page:
What is FISMA?



- FISMA: Federal Information Security Management Act of 2002
- US Federal Law
- Targeted Toward Securing US Federal Data
- Spawning Useful Standards and Infrastructure (even outside of US borders)

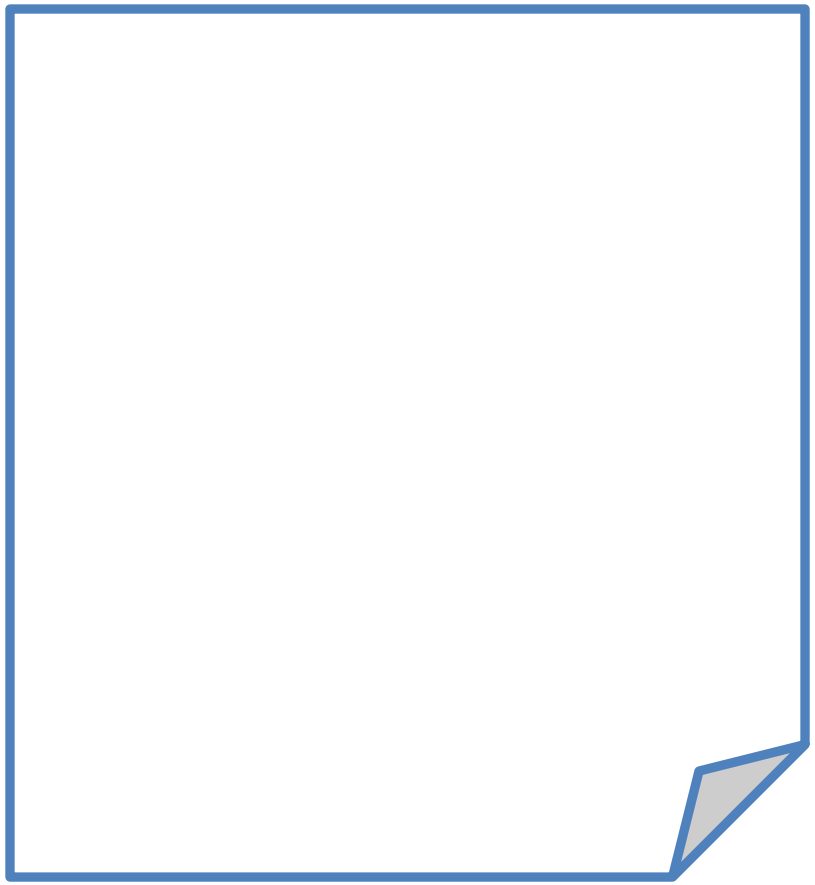
Getting on the Same Page:
What is FISMA?

§ 3541. Purposes
The purposes of this subchapter are to—
(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

- FISMA

- Targeted Toward Securing US Federal Data

Who *Should* Follow FISMA?



- Any Organization
  - Useful standard
  - Very useful evolving infrastructure

Who *Should* Follow FISMA?

§ 3544. Federal agency responsibilities
(a) IN GENERAL.—The head of each agency shall—
(1) be responsible for—
(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

- Any Organization
  - Useful standard
  - Very useful evolving infrastructure
- US Federal Agencies
  - Partially Excluding:
    - National Security Systems
    - DoD and CIA

Who *Should* Follow FISMA?

§ 3544. Federal agency responsibilities
(a) IN GENERAL.—The head of each agency shall—
(1) be responsible for—
(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

- Any Organization
  - Useful standard
  - Very useful evolving infrastructure
- US Federal Agencies
  - Partially Excluding:
    - National Security Systems
    - DoD and CIA
  - Including:
    - Data Center Outsourcers?

Who *Should* Follow FISMA?

§ 3544. Federal agency responsibilities
(a) IN GENERAL.—The head of each agency shall—
(1) be responsible for—
(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

- Any Organization
  - Useful standard
  - Very useful evolving infrastructure
- US Federal Agencies
  - Partially Excluding:
    - National Security Systems
    - DoD and CIA
  - Including:
    - Data Center Outsourcers?

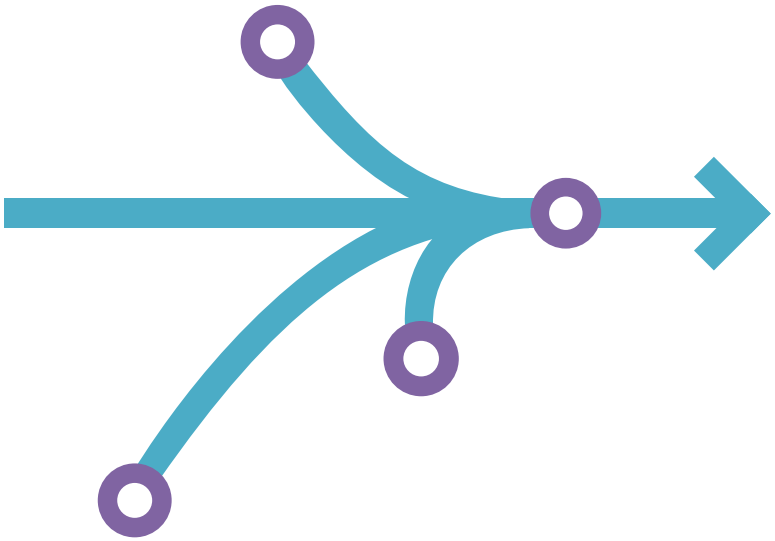
Who *Should* Follow FISMA?

§ 3544. Federal agency responsibilities
(a) IN GENERAL.—The head of each agency shall—
(1) be responsible for—
(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

- Any Organization
  - Useful standard
  - Very useful evolving infrastructure
- US Federal Agencies
  - Partially Excluding:
    - National Security Systems
    - DoD and CIA
  - Including:
    - Data Center Outsourcers?
- Any Organization that Provides Data to US Federal Agencies?

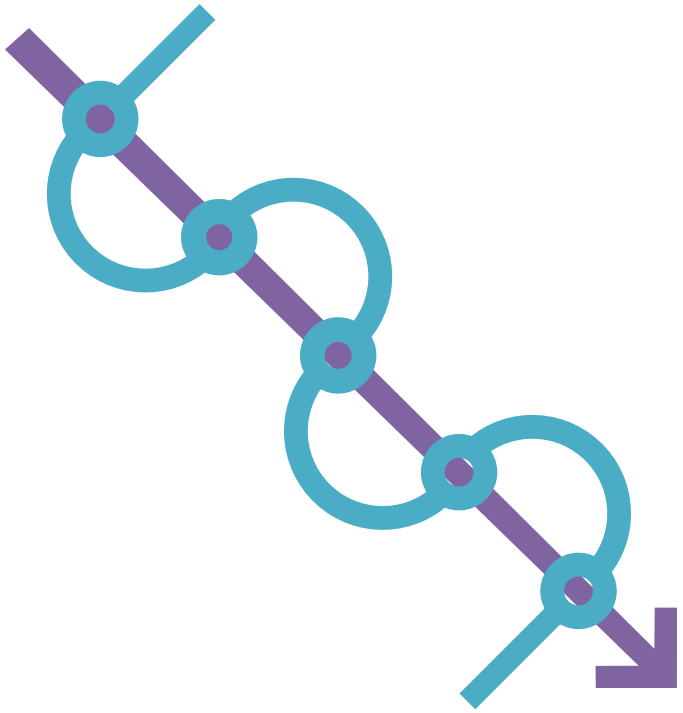
Do You Provide Data to Federal Agencies?
Examples Only

- State Governments:
  - Tax (IRS) and Social Security (SSA) Data
  - Medicaid Data
- Health Insurance Companies and Healthcare Providers
  - Medicare/Medicaid Transactions (CMS)
- Banks/FCUs/Brokerages
  - Transactions over $10,000
- Federal Contractors
  - Medicare Processing
  - Student Loan Processing
  - Etc.



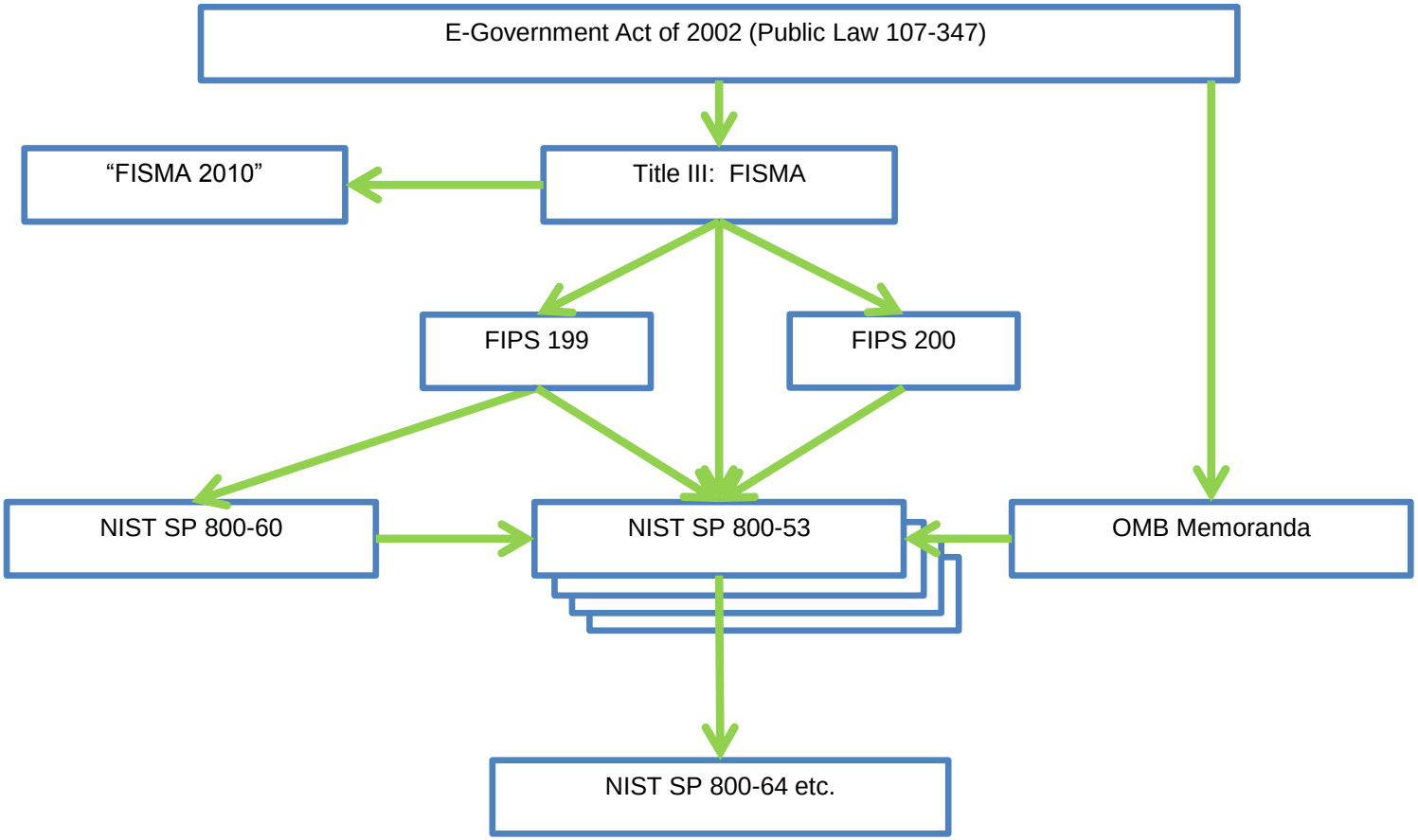
FISMA Basis

Federal Laws Tend to Spawn Other Documents



- Initial Law
- Agency that Qualifies Standard
- Additional Agency Variations
- Jurisdictional Mandates/Modifications
- Potential Modifying Laws

The FISMA Paper Trail



FISMA Requirements: Project Approach

Best Practice: Initial Steps

Best Practice: Initial Steps

1. Obtain SP 800-53 from NIST.

NIST SP 800-53


NIST Special Publication 800-53
Revision 3

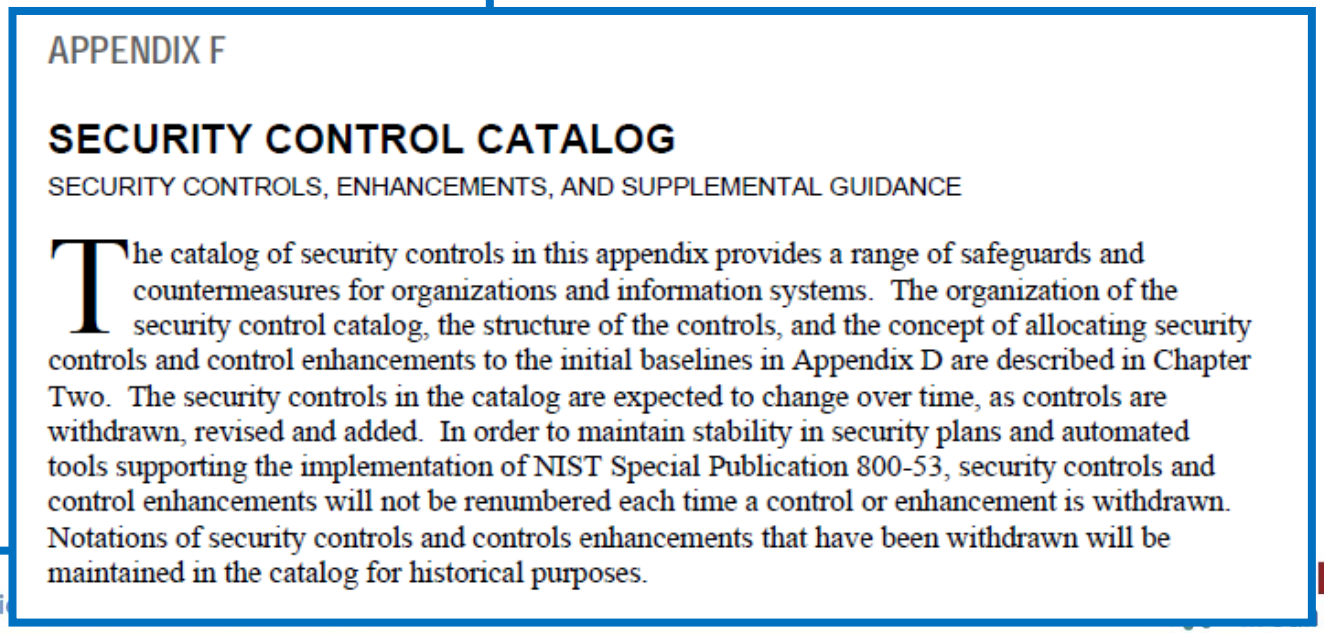
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Recommended Security Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

INFORMATION SECURITY

- Current Revision
  - Revision 3
- Draft Revision
  - Revision 4 (final comment draft released this week)
  - Anticipated in April 2013
- Go right to Appendix F!


APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems. The organization of the security control catalog, the structure of the controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog are expected to change over time, as controls are withdrawn, revised and added. In order to maintain stability in security plans and automated tools supporting the implementation of NIST Special Publication 800-53, security controls and control enhancements will not be renumbered each time a control or enhancement is withdrawn. Notations of security controls and controls enhancements that have been withdrawn will be maintained in the catalog for historical purposes.

Best Practice: Initial Steps

1. Obtain SP 800-53 from NIST.
2. Obtain *specific* controls from federal department/agency.

Example Control

Control

Specifics

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** AC-11	**HIGH** AC-11

Best Practice: Initial Steps

1. Obtain SP 800-53 from NIST.
2. Obtain *specific* controls from federal department/agency.
3. Determine security/impact level per *affected* LPAR.

Example Control

Control → **AC-11 SESSION LOCK**

Control: The information system:

Specifics →

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

Level →

P3	LOW Not Selected	MOD AC-11	HIGH AC-11

Security and Impact Level

Background:

- Ranked:
  - High
  - Moderate
  - Low
- Based Upon (“CIA”)
  - C – Confidentiality
  - I – Integrity
  - A – Availability
- Use “high water mark”
  - (Highest of CIA).

Process:

- Federal department may have already determined level.
- Use FIPS 199, generally (my rules):
  - High: People will die.
  - Moderate: People will be seriously impacted.
  - Low: People will be inconvenienced.
- See SP 800-60
  - Examples of federal systems by “industry”.

Best Practice: Initial Steps

1. Obtain SP 800-53 from NIST.
2. Obtain *specific* controls from federal department/agency.
3. Determine security/impact level per *affected* LPAR.
   - Usually the production machine with the federal data
   - Common to maintain similar controls on all machines
     - Avoids the possibility that auditor will determine that development is part of the production infrastructure.

Best Practice: Initial Steps

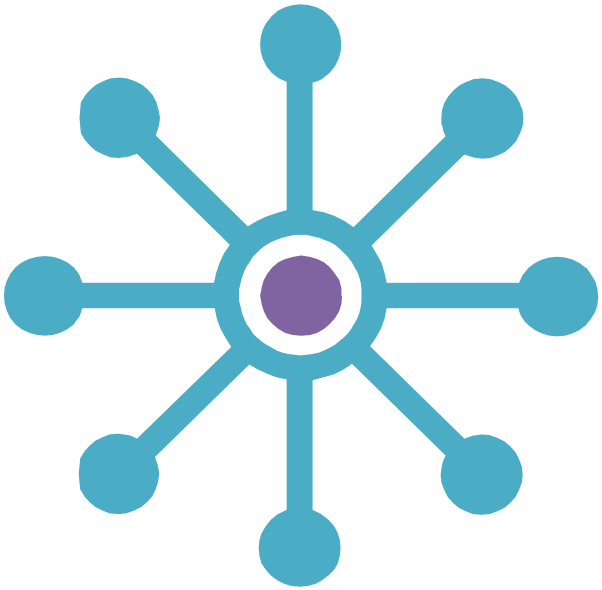
1. Obtain SP 800-53 from NIST.
2. Obtain *specific* controls from federal department/agency.
3. Determine security/impact level per *affected* LPAR.
   - Usually the production machine with the federal data
   - Common to maintain similar controls on all machines
     - Avoids the possibility that auditor will determine that development is part of the production infrastructure.
4. Outline a document!

Control Families

- Doc is made up of control families.
- The first control is always a chapter.
- But… change the order.

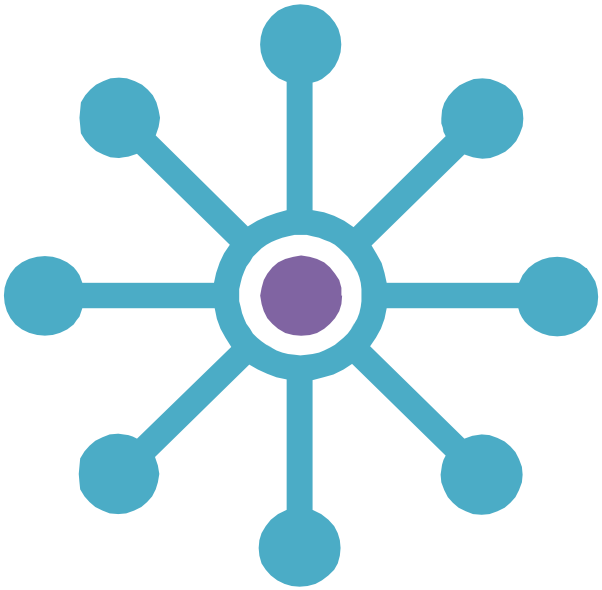
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	Information System Connections	P1	CA-3	CA-3	CA-3
CA-4	Security Certification (Withdrawn)	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P3	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P3	CA-7	CA-7	CA-7
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (4)	CM-2 (1) (2) (3) (5) (6)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	P1	CM-6	CM-6 (3)	CM-6 (1) (2) (3)
CM-7	Least Functionality	P1	CM-7	CM-7 (1)	CM-7 (1) (2)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1

Control Family:
Planning (PL)



- Good first place to start.
- Sets up the process.

Control Family:
Planning (PL) *and* Risk Assessment (RA)



- Good second chapter.
- The creation of the document itself parallels the risk assessment.
- See SP 800-160 (draft)

Best Practice: Initial Steps

1. Obtain SP 800-53 from NIST.
2. Obtain *specific* controls from federal department/agency.
3. Determine security/impact level per *affected* LPAR.
   - Usually the production machine with the federal data
   - Common to maintain similar controls on all machines
     - Avoids the possibility that auditor will determine that development is part of the production infrastructure.
4. Outline a document.
   - Each control family is a chapter.
   - Do planning and risk assessment first.
   - Others arrange in a logical order
     - (i.e.: Identification and Authentication before Access Control)

Best Practice: Initial Steps

5. Divide controls into solution approach:
   - Policy Document (first control of each family)
   - Policy Detail (documented procedures in that family)
   - Technical Control (may imply software or software settings)

Example Control

Control

Solution

Specifics

Level

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** AC-11	**HIGH** AC-11

Determining Solution Type

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

- Policy Document (or Chapter)

Determining Solution Type

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

- Policy Document (or Chapter)

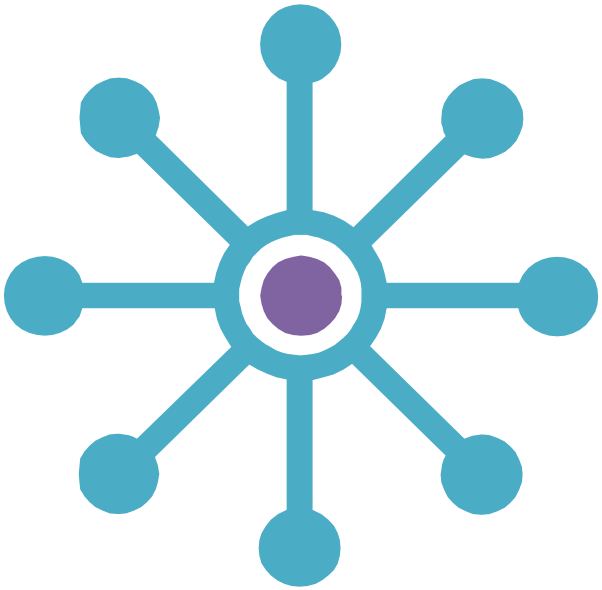
AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including:

a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);

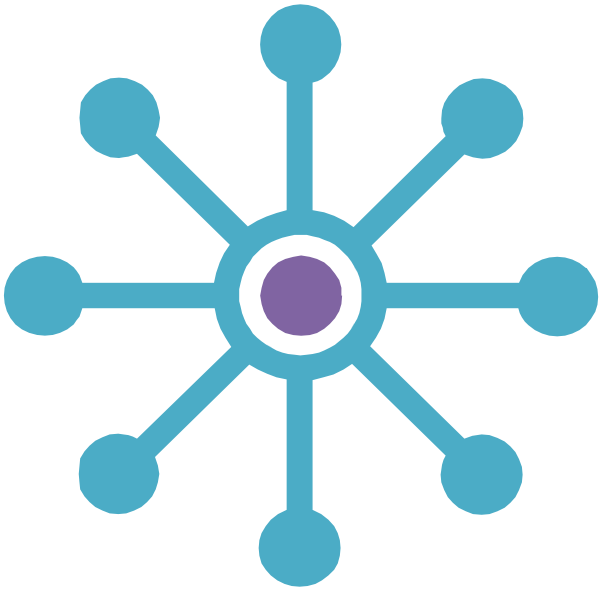
- Policy Detail

Control Family:
Contingency Planning (CP)



- Primarily Disaster Recovery Plans
- Backup and Recovery Tools

Control Family:
Software Acquisition (SA)

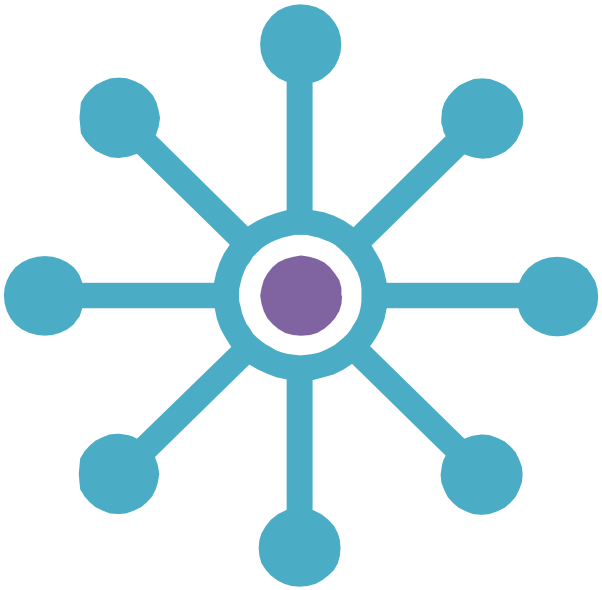


- Software Acquisition is:
  - Purchase/Lease (Supply Chain)
  - User Software
  - Development
- Mainframe Development Procedures and Promotion Software
  - See SP 800-64

Best Practice: Initial Steps

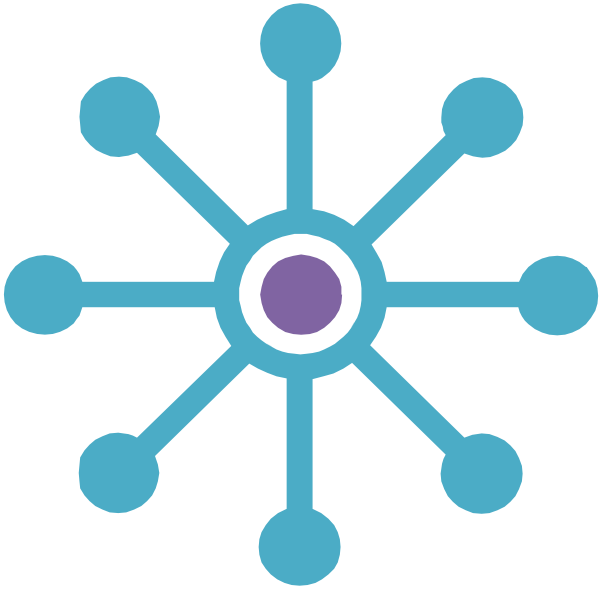
5. Divide controls into solution approach:
   - Policy Document (first control of each family)
   - Policy Detail (documented procedures in that family)
   - Technical Control (may imply software or software settings)
6. Create chapter subsections that correspond to controls.
7. Retrofit existing documents.
8. Assign entire families that have not been documented.

Control Family:
System Maintenance Policy and Procedures (SM)



- Mostly procedural.
- Primarily hardware maintenance.

Control Family:
Physical and Environmental (PE)



- Physical security (i.e. door locks)
- Environmental (electricity, fire protection, etc.)
- No mainframe software

Best Practice: Initial Steps

5. Divide controls into solution approach:
   - Policy Document (first control of each family)
   - Policy Detail (documented procedures in that family)
   - Technical Control (may imply software or software settings)
6. Create chapter subsections that correspond to controls.
7. Retrofit existing documents.
8. Assign entire families that have not been documented.
9. Evaluate technical controls:
   - Determine what fields or options relate to control.
   - Determine where software is missing or unused.

Determining Solution Type

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and

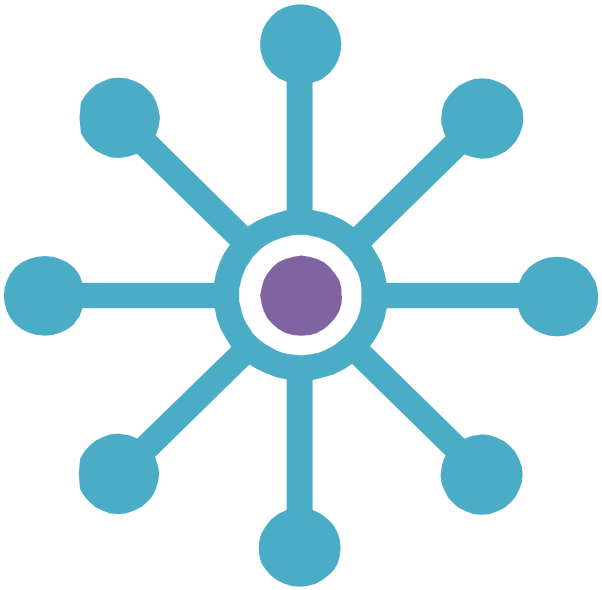
b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

- Technical Control

Best Practice: Initial Steps

5. Divide controls into solution approach:
   - Policy Document (first control of each family)
   - Policy Detail (documented procedures in that family)
   - Technical Control (may imply software or software settings)
6. Create chapter subsections that correspond to controls.
7. Retrofit existing documents.
8. Assign entire families that have not been documented.
9. Evaluate technical controls:
   - Determine what fields or options relate to control.
   - Determine where software is missing or unused.
   - Eliminate non-mainframe technologies. (wifi, virus, etc.)

Control Family:
System and Information Integrity (SI)



- Example: Virus Protection
- System change review.
- System change monitoring:
  - Compliance Manager for z/OS (CA)
    - Chorus: Security and Compliance Role
  - Potentially others.

#SHAREorg

SHARE
Technology · Connections · Results

Technical Controls: FISMA and z/OS Technology

SHARE in San Francisco 2013

Example Control

Control

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

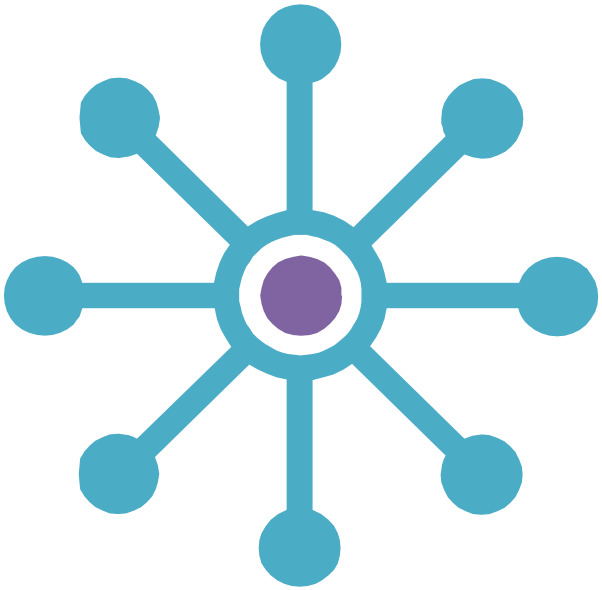
(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

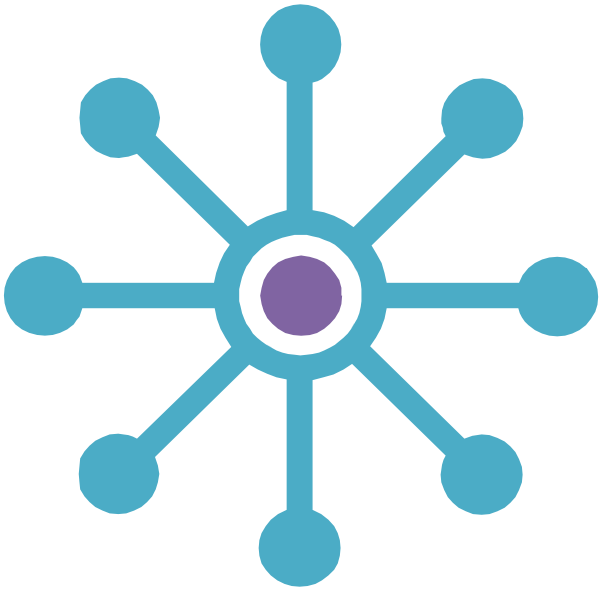
P3	**LOW** Not Selected	**MOD** AC-11	**HIGH** AC-11

Control Family:
Personnel Security (PS)



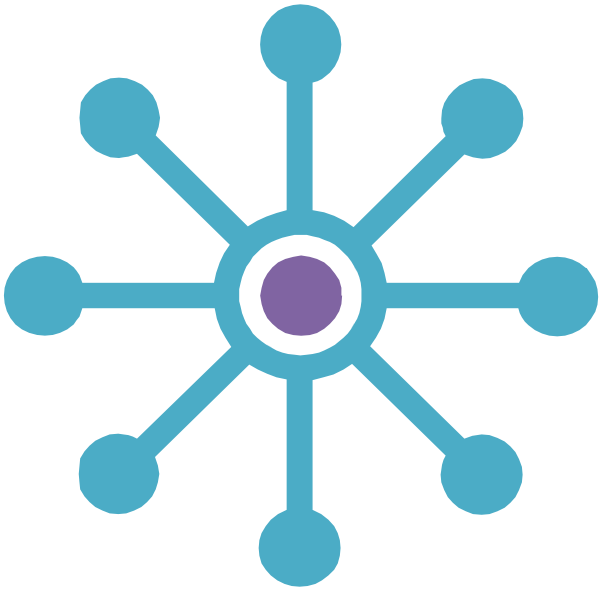
- Defines roles of individuals.
- No mainframe software.
- But is a precursor to understanding roles.
- Example: PS-2: Position Categorization – identifies risky roles.

Control Family:
Identification and Authentication (IA)



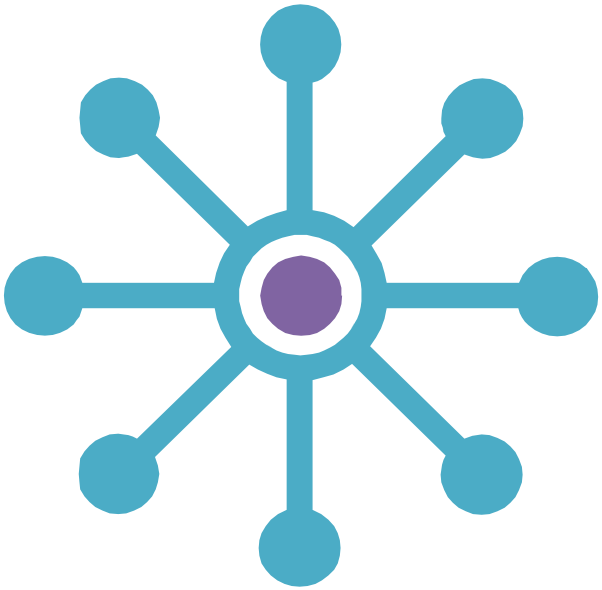
- Access Control Products (for password and digital certificates):
  - ACF2 (CA)
  - RACF (IBM)
  - Top Secret (CA)

Control Family:
Access Control (AC)



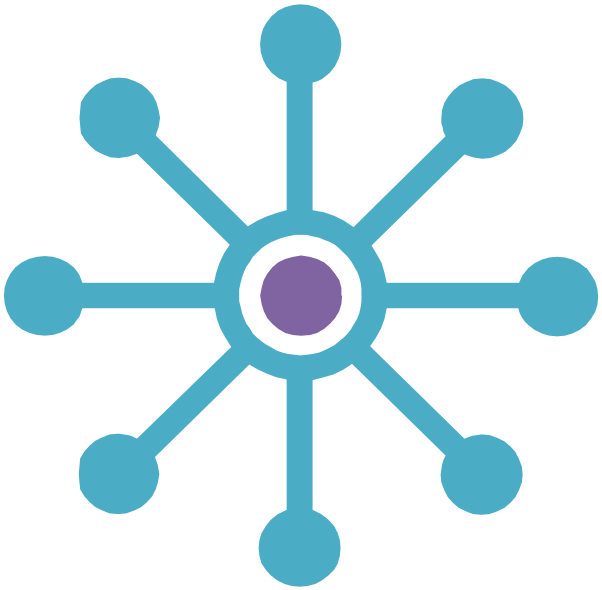
- Access Control Products:
  - ACF2 (CA)
  - RACF (IBM)
    - Policy Manager (Vanguard)
    - inCompliance (Vanguard)
  - Top Secret (CA)
- Online Systems (for session control)
  - TSO (IBM)
  - CICS (IBM)
  - IMS (IBM)
- Provisioning Products (for account management aspects):
  - IdentityMinder (CA)
  - Numerous others.

Control Family:
Audit and Accountability (AU)



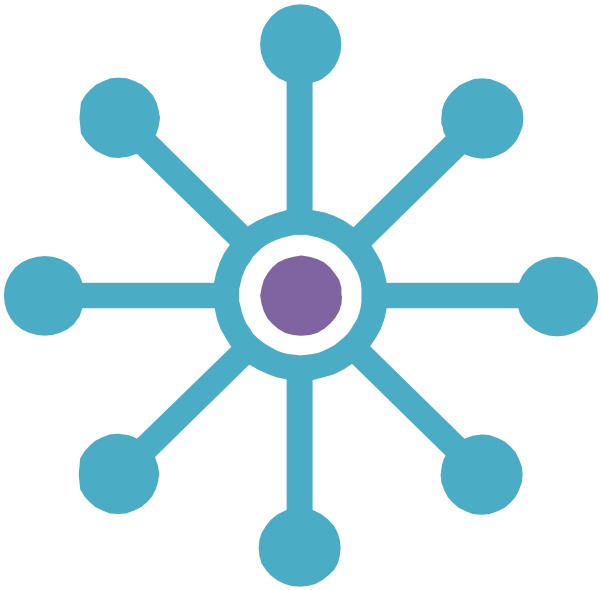
- z/OS Audit Trail
  - SMF (IBM)
- Access Control Products:
  - ACF2 (CA)
  - RACF (IBM)
  - Top Secret (CA)
- Event Management Software
  - Compliance Manager for z/OS (CA)
    - Chorus: Security and Compliance Role
  - Vanguard
  - IBM
  - Potentially others.

Control Family:
Security Assessment and Authorization (CA)



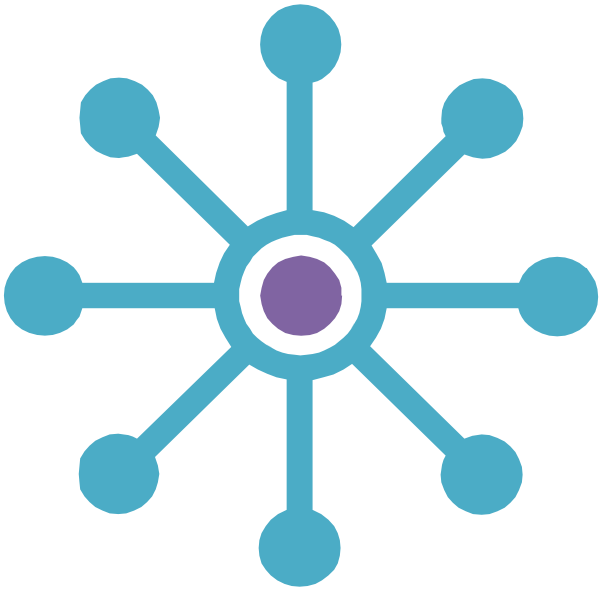
- Continuous Monitoring (CA-7)
  - Compliance Manager for z/OS (CA)
    - Chorus: Security and Compliance Role
  - Vanguard Tools
  - IBM Tools
  - Potentially Others
- (Everything else is policy.)

Control Family:
Incident Response (IR)



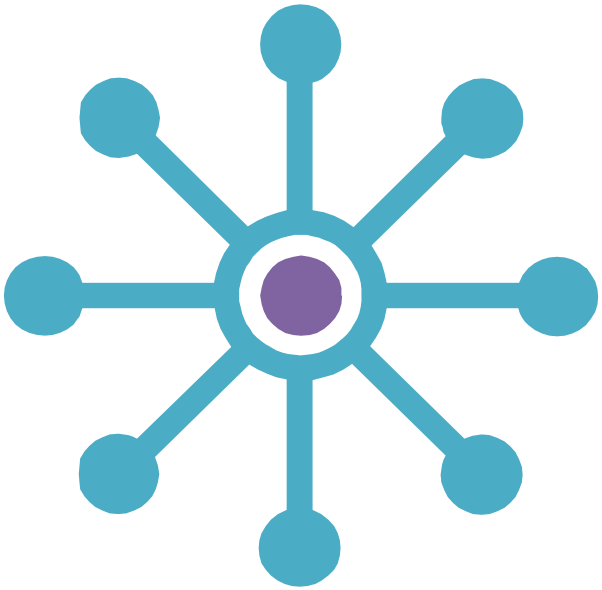
- Mostly procedural.
- Helpdesk software is implied
  - Numerous vendors including CA.
- Monitoring (same as auditing):
  - z/OS Audit Trail
    - SMF (IBM)
  - Access Control Products:
    - ACF2 (CA)
    - RACF (IBM)
    - Top Secret (CA)
  - Event Management Software
    - Compliance Manager for z/OS (CA)
      - *Chorus: Security and Compliance Role*

Control Family:
Configuration Management (CM)



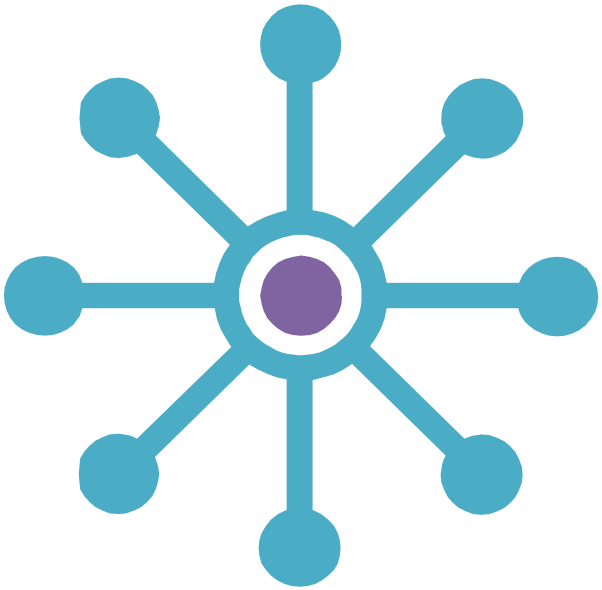
- Baseline
  - Auditor (CA)
  - Vanguard Tools
  - IBM Tools
  - Potentially Others
- System Change Control
- Configuration Change Monitoring
  - Compliance Manager for z/OS (CA)
    - Chorus: Security and Compliance Role
  - Vanguard Tools
  - IBM Tools
  - Potentially Others

Control Family:
Media Protection (MP)



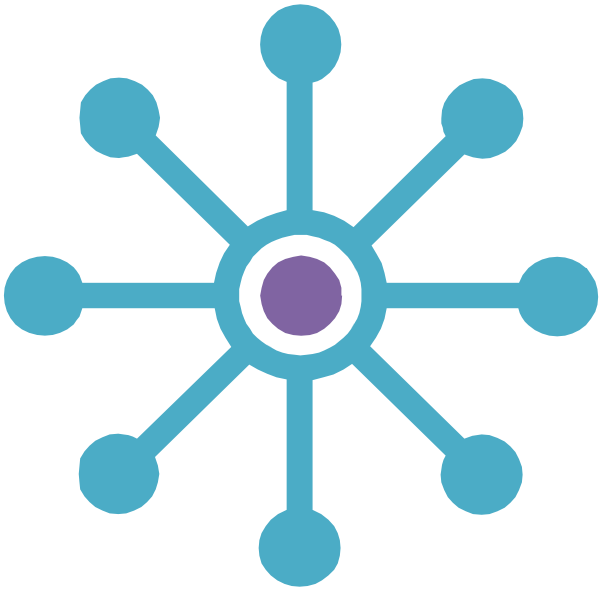
- Mostly procedural.
- Tape Management:
  - CA-1 (CA)
  - RMM (IBM)
  - TLMS (CA)
  - Others
- Overwrite of Disk Data:
  - ACF2 (CA)
  - RACF (IBM)
  - Top Secret (CA)

Control Family:
System and Communication Protection (SC)



- Data transmission (integrity, encryption)
  - Network based encryption (usually outside of mainframe boundary)
  - File transfer (includes mainframe)
- Key management
  - May include:
    - ACF2 (CA)
    - RACF (IBM)
    - Top Secret (CA)
- Mainframe network monitoring (to a degree)
- Most other provisions are outside mainframe.

Control Family:
Awareness and Training (AT)



- Example: AT-5: Contacts with Security Groups and Associations
  - “To stay up to date”
  - “To share security-related information including threats, vulnerabilities…”
- PTF notification for Access Control Products:
  - ACF2 (CA)
  - RACF (IBM)
  - Top Secret (CA)

Best Practice: Technical Steps

10. Prioritize.
    - Relative Priorities, 1 through 3.

Example Control

Control

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: OMB Memorandum 06-16.

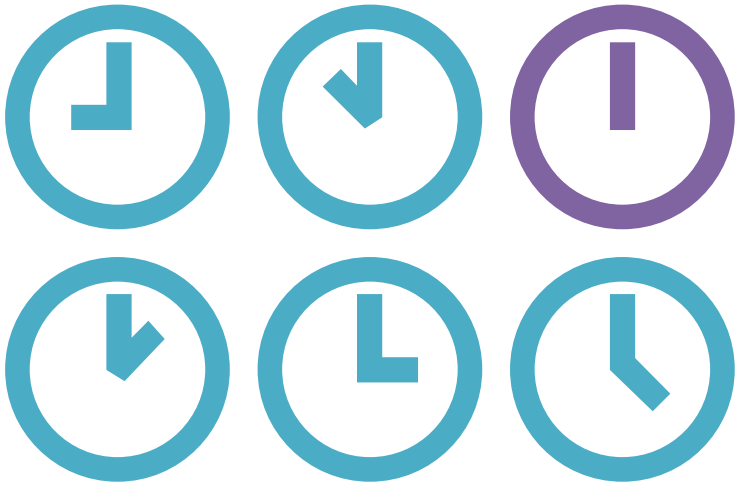
Priority and Baseline Allocation:

Priority

P3	**LOW** Not Selected	**MOD** AC-11	**HIGH** AC-11

The *Present* Future

Evolving Practices
The Future is Now



- NIST SP 800-53 Revision 4
  - Due out in April
- Cyberscope and Continuous Monitoring
  - DHS
- NIST SCAP Infrastructure
  - Security Content Automation Protocol

#SHAREorg

SHARE
Technology · Connections · Results

Thanks!

Bill Valyo William.Valyo@CA.com

Session #12765

SHARE in San Francisco 2013