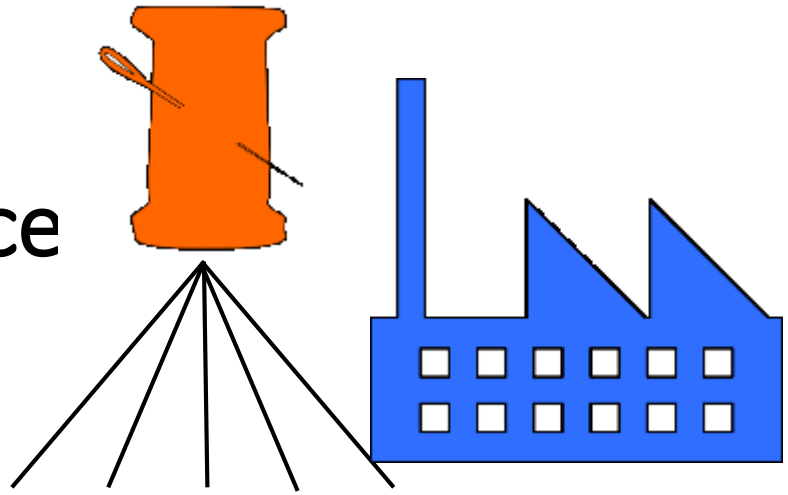
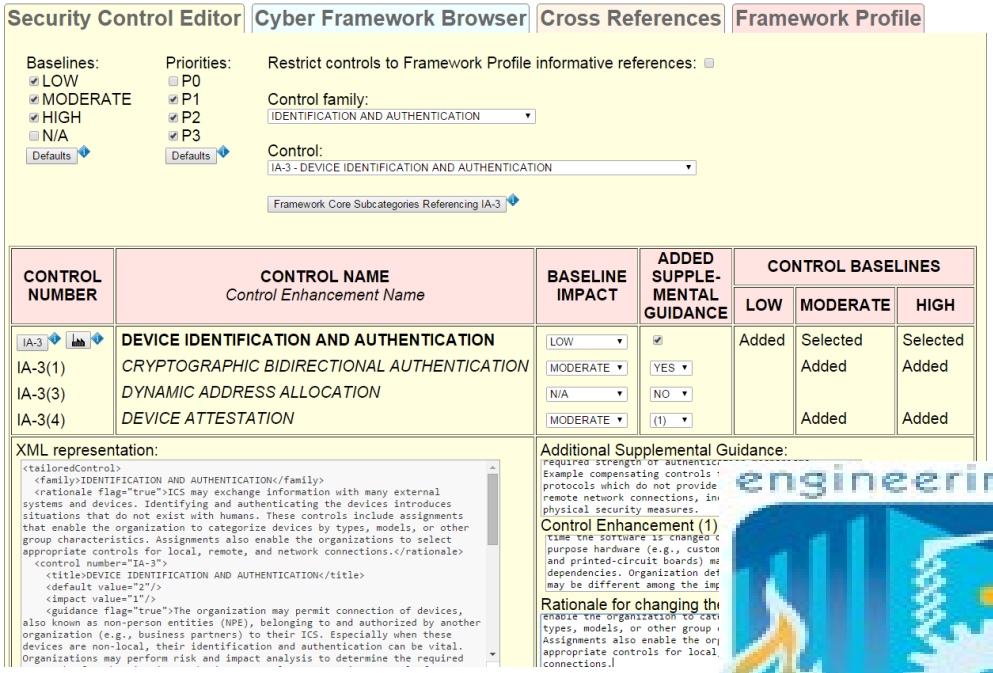
Integrating Top-down and Bottom-up Cybersecurity Guidance Using XML

Joshua Lubell

Balisage Markup Conference

August 2016





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

engineering laboratory

Disclaimer

Certain third-party products are identified to help explain the research. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Acronyms

FISMA	Federal Information Security Management Act
HTTP	Hyper Text Transfer Protocol
ICS	Industrial Control System
NIST	National Institute of Standards and Technology
SP	Special Publication
UI	User Interface
XHTML	Extensible Hyper Text Markup Language
XML	Extensible Markup Language
XSLT	Extensible Style Language Transformation

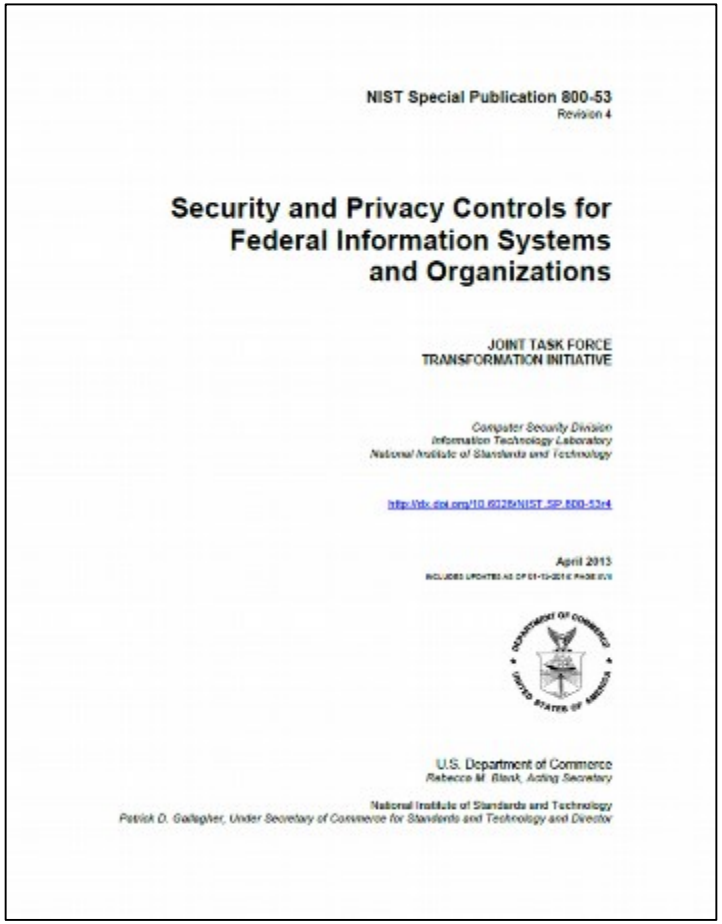
Outline

- NIST SP 800-53, the Cybersecurity Framework, and my integration problem
- A general XML-centric approach
- Application to my integration problem
- Demo
- Discussion

NIST SP 800-53, Revision 4

- Foundation of FISMA (Federal Information Security Management Act of 2002)
- Used in public and private sectors

Provides comprehensive catalog of customizable, ***technology-neutral*** *security controls for organizations to manage cyber-risk*


NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

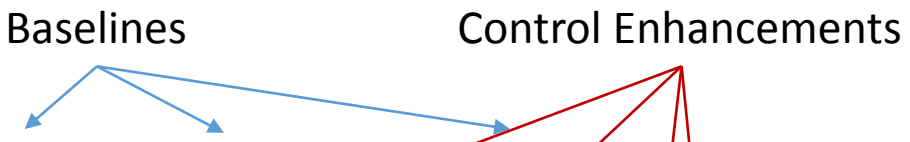
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

April 2013

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

First six controls in the Access Control (AC) family



ID	NAME	LOW	MODERATE	HIGH
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)

AC-2 (Account Management)

Control Description

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of information system accounts;

h. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

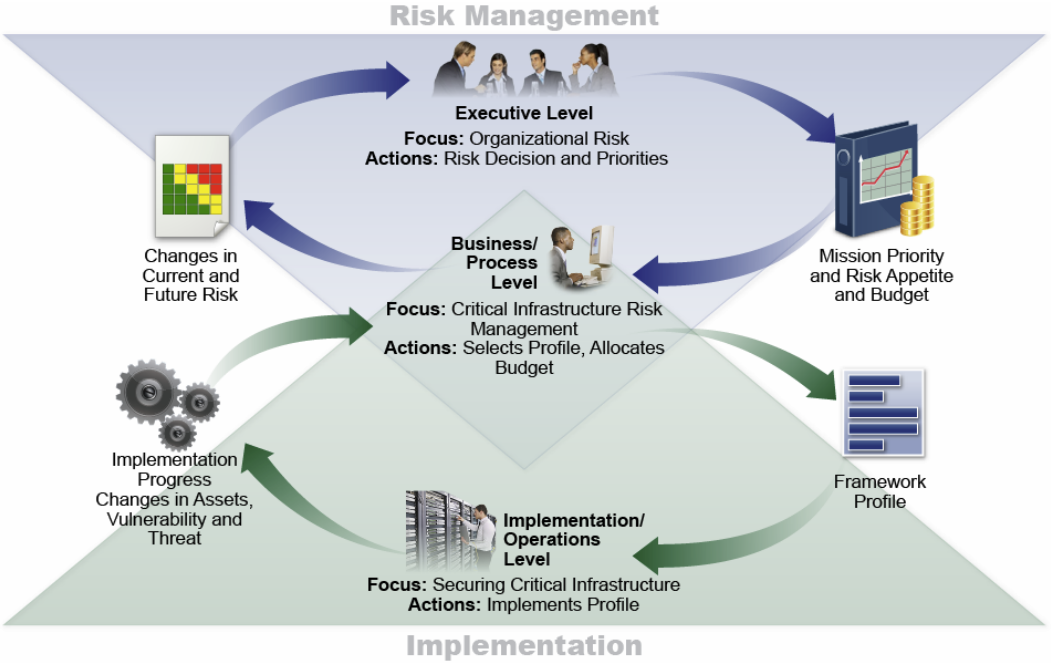
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

United States Cybersecurity Framework

"Framework for Improving Critical Infrastructure Cybersecurity"
Version 1.0 (February 2014)

Can specify ***Profile*** describing current cybersecurity posture and target state

- Identify opportunities for improvement
- Assess progress
- Communicate with stakeholders



Framework Core

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
PR.AC-1: Identities and credentials are managed for authorized devices and users	IA family, AC-2
PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7

My perspective…

NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

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

DRAFT

MANUFACTURING PROFILE

NIST Cybersecurity Framework

A Manufacturing-Sector tailored approach to protecting against cyber risk
April 2016

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

Mission 4 - Production Goals

ID.AM-1
ID.AM-2
ID.AM-3
ID.AM-4
ID.AM-5
ID.AM-6
ID.BE-1
ID.BE-2
ID.BE-3
ID.BE-4
ID.BE-5
ID.GV-1
ID.GV-2
ID.GV-3
ID.GV-4
ID.RA-1
ID.RA-2
ID.RA-3
ID.RA-4
ID.RA-5
ID.RA-6
ID.RM-1
ID.RM-2
ID.RM-3
PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AT-1
PR.AT-2

Awareness and Training

Manufacturing Profile for Cyber Security Framework 12

The problem: using two guidance specifications together

Cybersecurity Framework

- Top-down
- High-level
- Emphasis on business/mission goals
- Usable/understandable by all

No structured data format

NIST Special Pub 800-53

- Bottom-up
- Granular
- Emphasis on risk management
- Intended for security professionals

XML format for catalog, but no structured representation of tailoring

Objectives

- Make it easier to create and document Cybersecurity Framework Profiles, tailored security control baselines, overlays
- Enforce NIST SP 800-53 tailoring constraints
- Promote interoperability and reuse
- Improve traceability of security automation to requirements
  - By representing Profiles, baselines in a structured, unambiguous manner

Outline

- NIST SP 800-53, the Cybersecurity Framework, and my integration problem
- **A general XML-centric approach**
- Application to my integration problem
- Demo
- Discussion

The more general problem

- Develop common UI for viewing and manipulating information from disparate sources
- Assumptions
  - Sources may be tables in a document
  - Generally not structured XML
  - Small Arcane Nontrivial Datasets
  - UI should produce structured XML output

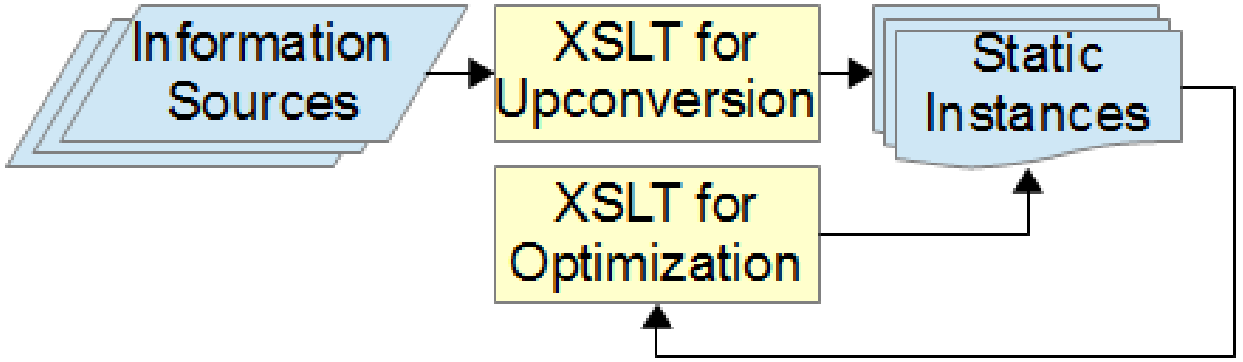
XML Technologies Used: XForms

- XML language for specifying web-based UIs
- Adopts Model-View-Controller software pattern
- XForms model
  - Instances - well-formed XML documents, some static and some dynamic
  - Bindings - define UI constraints, compute instance data values from other instance data, manage display of UI widgets
- Why XForms?
  - W3C standard
  - Good fit for lightweight, data-driven applications
  - Great for generating XML output
  - Platform independence

XSLT and XPath

- XSLT
  - Generates static XForms model instances from native information sources
  - Creates multiple alternatively-structured XForms instances to speed up UI
- XPath – used by XForms and XSLT
  - XForms
    - Bindings within the model
    - Specifying interactions between the user interface widgets and the model
  - XSLT
    - Data model
    - Library of functions and operators

XML Transformation Pipeline



Handling Poorly-structured Data

Semi-automated approach

1. If document not in Office Open XML Spreadsheet (.xlsx) format, save it as .xlsx
2. Determine how the information should be represented as structured XML
3. Open up saved result in Excel or equivalent and partition the file into separate simple tabular spreadsheets

   No split cells or cells spanning multiple rows or columns
4. Create XML map for each spreadsheet document and convert to structured XML.
5. Use XSLT to combine the XML documents, upconvert ill-structured data within cells

Outline

- NIST SP 800-53, the Cybersecurity Framework, and my integration problem
- A general XML-centric approach
- **Application to my integration problem**
- Demo
- Discussion

Baseline Tailor

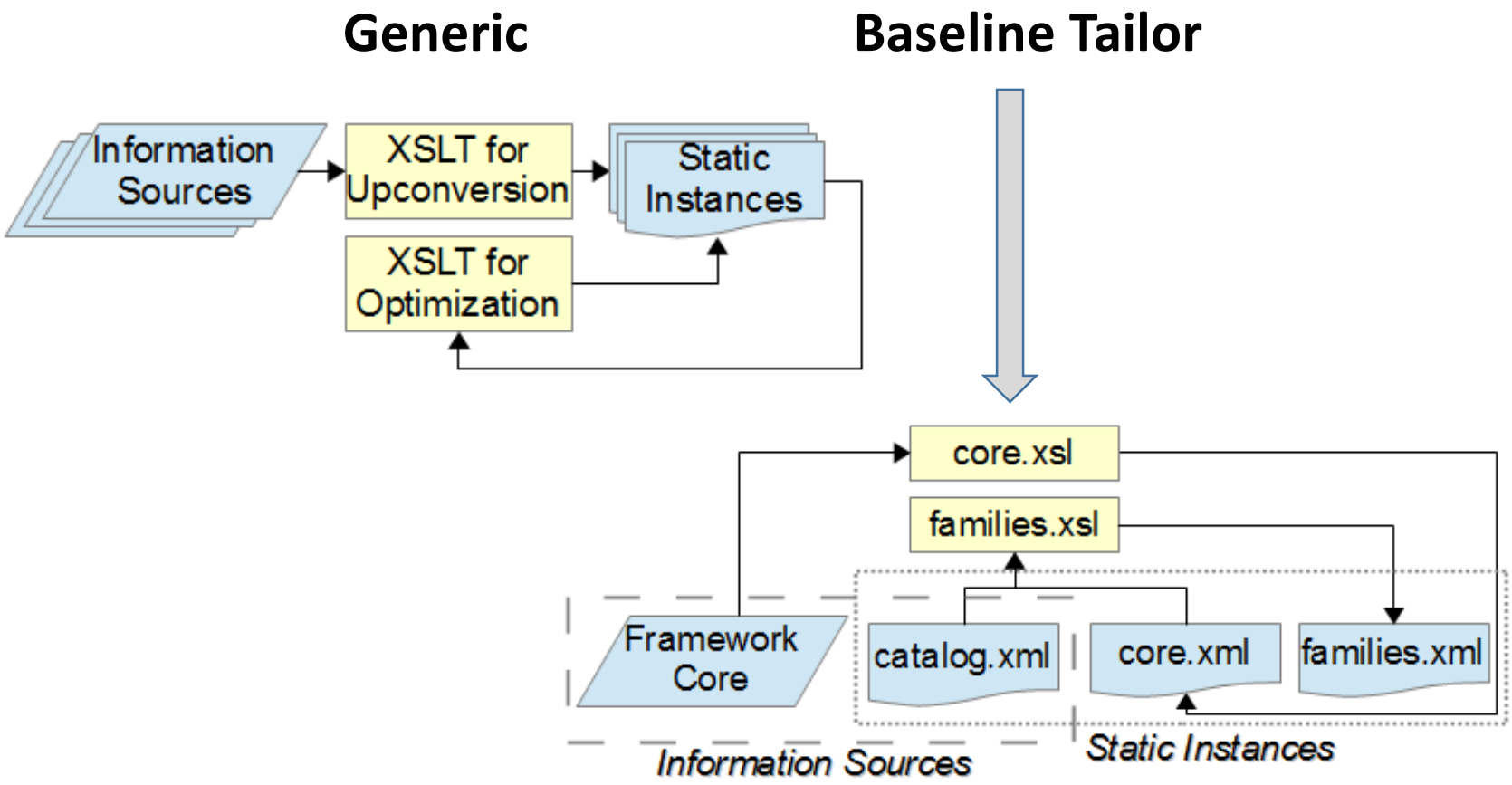
Experimental open source software for:

- Developing Cybersecurity Framework Profiles
- Tailoring NIST SP 800-53 security controls
- Generating XML output
- Using Cybersecurity Framework and NIST SP 800-53 together

Potential Users

- People responsible for:
  - Information system development
  - Cybersecurity implementation and operation
- Developers of:
  - Industry sector-specific cybersecurity guidance
  - Cybersecurity-related software applications
- Organizations wishing to improve communication of cybersecurity information

Transformation Pipeline: Baseline Tailor



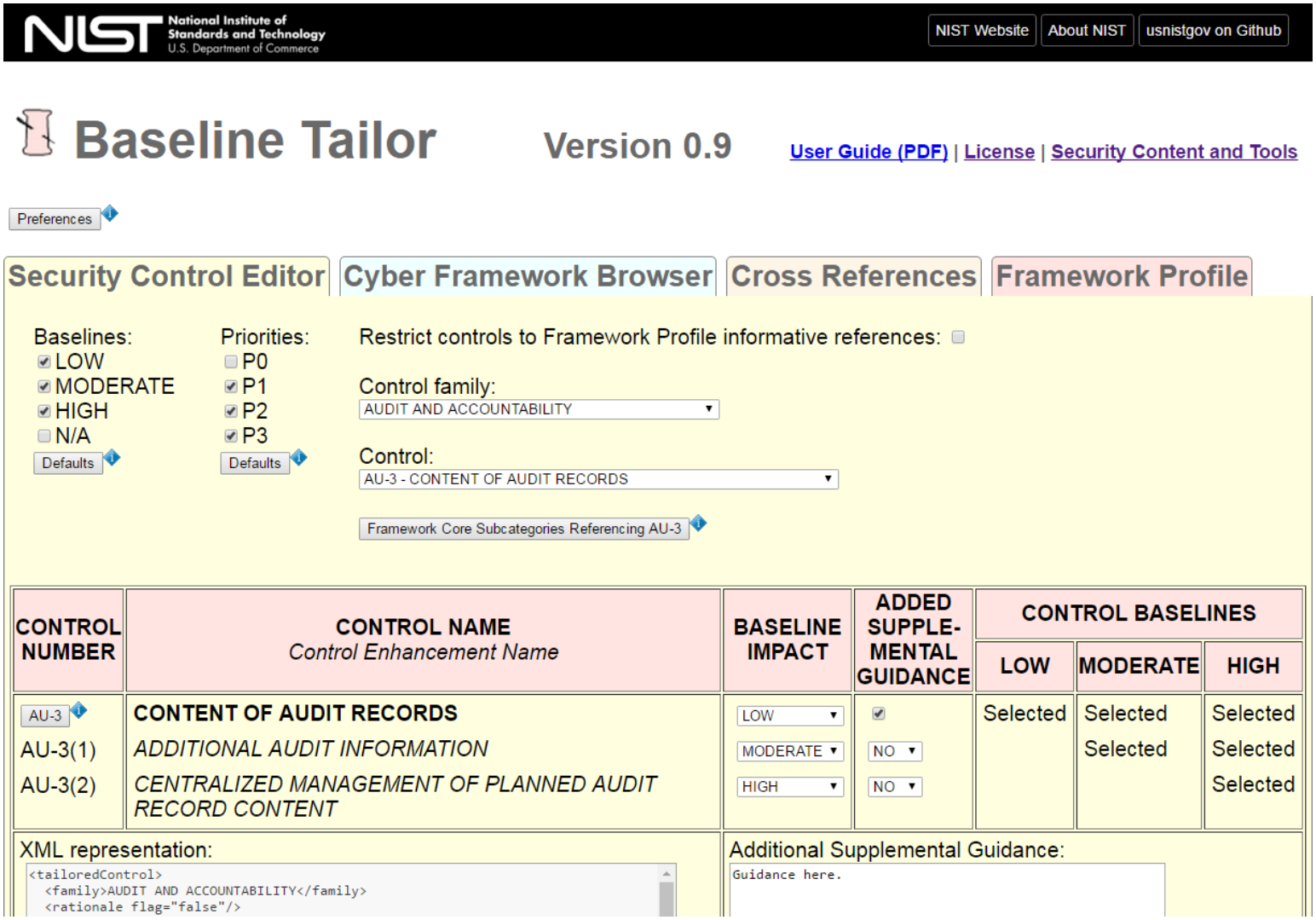
core.xml (category PR.AC)

```
<category id="PR.AC">
  <name>Access Control</name>
  <description>Access to assets…</description>
  <subcategory id="PR.AC-1">
    <description>Identities and credentials…</description>
    <sp800-53>
      <control>AC-2</control><family>IA</family>
    </sp800-53>
  </subcategory>
  <subcategory id="PR.AC-2">…</subcategory>
  <subcategory id="PR.AC-3">…</subcategory>
  <subcategory id="PR.AC-4">
    <description>Access permissions are…</description>
    <sp800-53>
      <control>AC-2</control><control>AC-3</control>
      <control>AC-5</control><control>AC-6</control>
      <control>AC-16</control>
    </sp800-53>
  </subcategory>
  <subcategory id="PR.AC-5">…</subcategory>
</category>
```

families.xml (Access Control)

```
<family name="ACCESS CONTROL">
  <control number="AC-1">…</control>
  <control number="AC-2">
    <title>ACCOUNT MANAGEMENT</title>
    <default>1</default>
    <priority>1</priority>
    <subcategory number="PR.AC-1"/>
    <subcategory number="PR.AC-4"/>
    <subcategory number="DE.CM-1"/>
    <subcategory number="DE.CM-3"/>
  </control>
  …
</family>
```

Tabbed User Interface



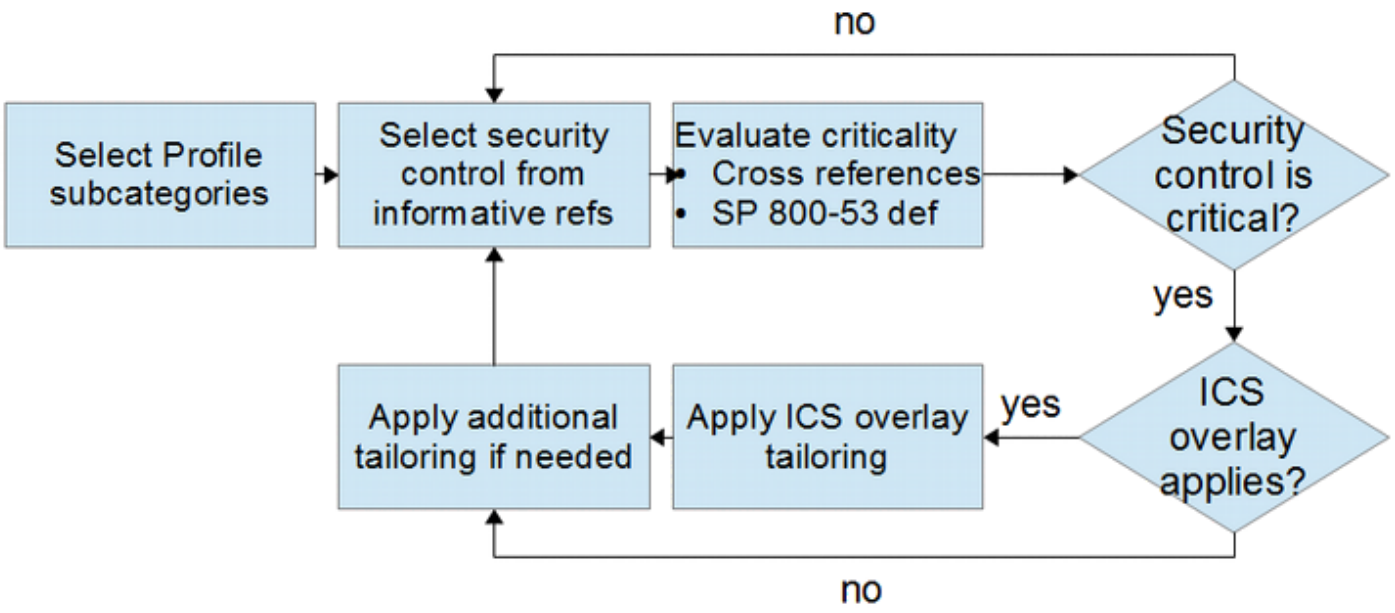
What You Can Do With the Tabs

Tab	Operations
Security Control Editor	• Navigate security control catalog and Industrial Control System (ICS) overlay • Modify baselines • Add to supplemental guidance
Cyber Framework Browser	• Navigate Core • Modify Profile
Cross References	• Show all Core subcategories referencing a control *Helpful for using Cybersecurity Framework to support security control selection*
Framework Profile	• Modify Profile • View subcategory details

Baseline Tailor Implementation

- Source code is 100 % XML (XForms, XSLT, XHTML)
  - Eases leveraging of NIST SP 800-53 XML data
  - Reduces dependence on programming/scripting languages
- All processing client side
  - Using XSLTForms XForms implementation
- Runs in common browsers (Chrome, Firefox, Safari, Opera, …)
- Can be run from local file system without HTTP server

Workflow synthesizing Framework Core, NIST SP 800-53, SP 800-82 guidance



Outline

- NIST SP 800-53, the Cybersecurity Framework, and my integration problem
- A general XML-centric approach
- Application to my integration problem
- **Demo**
- Discussion

Demo!

- Common XForms-authored UI for using Framework Core, SP 800-53, SP 800-82
- Framework Profile can aid in security control selection
- Cross References tab can help prioritize security control implementation

Outline

- NIST SP 800-53, the Cybersecurity Framework, and my integration problem
- A general XML-centric approach
- Application to my integration problem
- Demo
- **Discussion**

Related Research Efforts

- Integrating top-down and bottom-up risk management guidance
  - Linkov, Igor, Elke Anklam, Zachary A. Collier, Daniel DiMase, and Ortwin Renn. 2014. “Risk-Based Standards: Integrating Top–down and Bottom–up Approaches.” *Environment Systems and Decisions* 34 (1).
- Spreadsheet issues and their mitigation
  - Durusau, Patrick, and Sam Hunting. “Spreadsheets - 90+ million End User Programmers With No Comment Tracking or Version Control.” In *Proceedings of Balisage: The Markup Conference 2015.*
  - Kohlhase, Andrea, Michael Kohlhase, and Ana Guseva. 2015. “Context in Spreadsheet Comprehension.” In *Proceedings of the Second Workshop on Software Engineering Methods in Spreadsheets*.
  - Hung, Vu, Boualem Benatallah, and Regis Saint-Paul. 2011. “Spreadsheet-Based Complex Data Transformation.” In *Proceedings of the 20th ACM International Conference on Information and Knowledge Management.*
  - Cunha, Jacome, Joao Saraiva, and Joost Visser. 2009. “Discovery-Based Edit Assistance for Spreadsheets.” In *Symposium on Visual Languages and Human-Centric Computing (VL/HCC).*
- XPath for integrating information from distributed sources
  - Pedersen, Torben Bach, Dennis Pedersen, and Karsten Riis. 2013. “On-Demand Multidimensional Data Integration: Toward a Semantic Foundation for Cloud Intelligence.” *The Journal of Supercomputing* 65 (1).
  - Rennau, Hans-Jürgen, and Christian Grün. “XQuery as a data integration language.” In *Proceedings of Balisage: The Markup Conference 2015*. Balisage Series on Markup Technologies, vol. 15 (2015).

Summary

- Baseline Tailor is experimental open source software for Cybersecurity Framework and SP 800-53 users
- Usage scenarios
  - Tailoring a security control
  - Browsing and using the Framework Core
  - Creating structured XML
  - Using the Core and 800-53/800-82 together
  - *More likely to emerge*
- Was useful in creating Manufacturing Profile employing SP 800-53 and 800-82 guidance

Limitations

- Baseline Tailor
  - Implementation tied to current versions on NIST specifications
    - New versions will require software updates
  - Framework Profile XML could include more information
  - Cannot import an existing tailored control
    - Needed for composability (e.g., tailoring an overlay)
  - UI not “baseline-centric”
- Overall integration approach relies on hand-editing for semi-automated conversion
  - Hung, Cunha research results could improve automation
  - But would require more disciplined spreadsheet authoring

How Baseline Tailor Evolved

- First Baseline Tailor incarnation limited to security control tailoring
- Framework Core browsing added later, but without bidirectional subcategory/control traversal
- Manufacturing Profile development experience led to need for bidirectional traversal
  - Cross References tab added
  - Applied Linkov's hybrid top-down/bottom-up approach

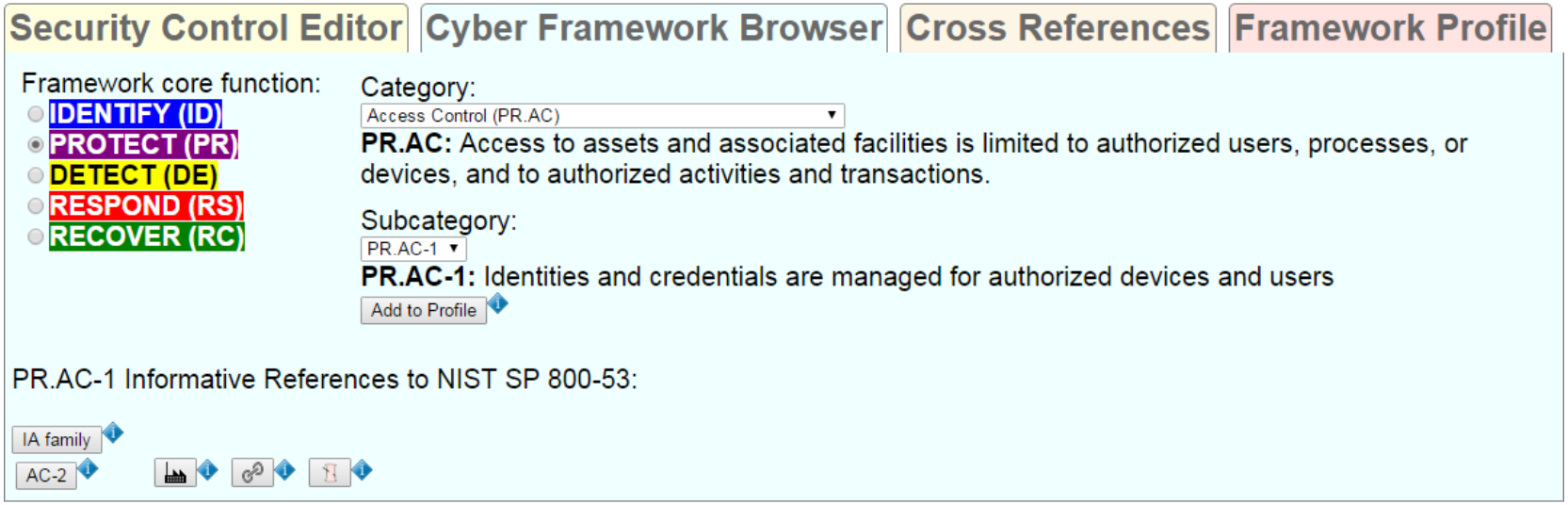
For More Information

- NIST Pages site: https://pages.nist.gov/sctools
  - Baseline Tailor online application
  - XML schemas and data
  - User Guide
  - GitHub repository
- Baseline Tailor information page: http://go.usa.gov/cuxq3
- My email: lubell@nist.gov

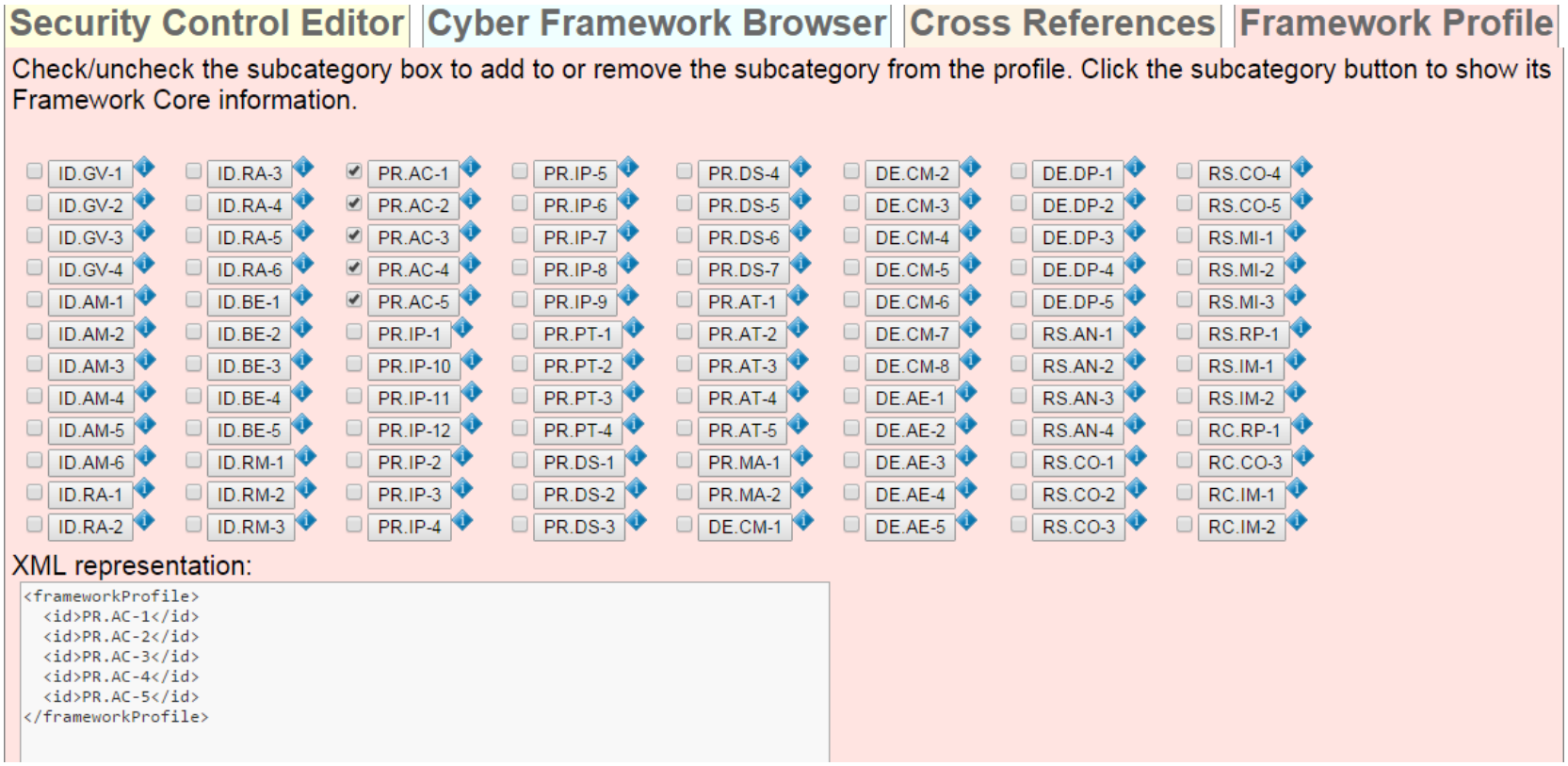
Backup Slides

Preferences Dialog

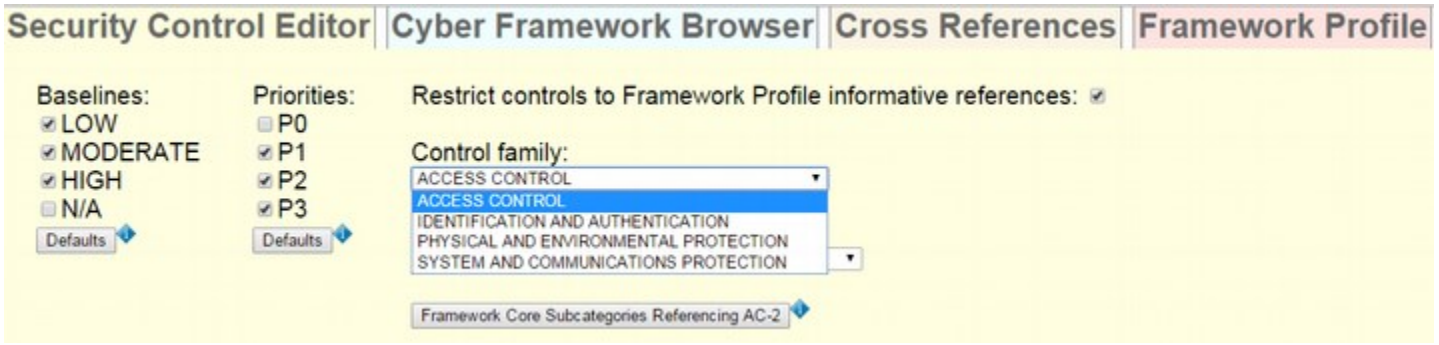
Cyber Framework Browser Tab

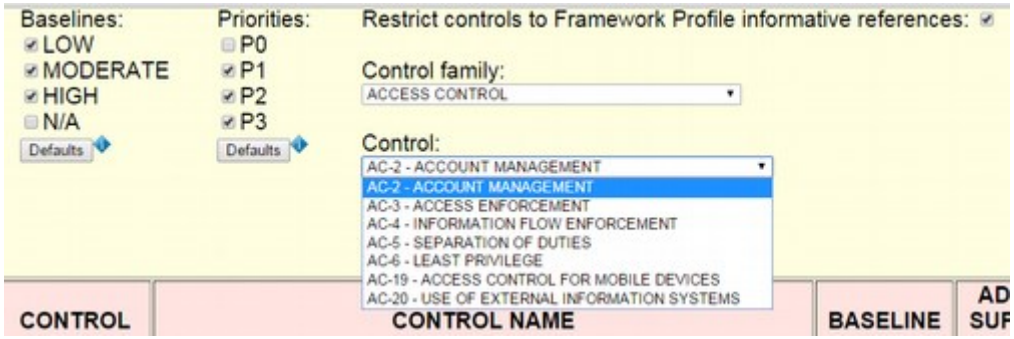


Framework Profile Tab



Controls Referenced by PR.AC Subcategories

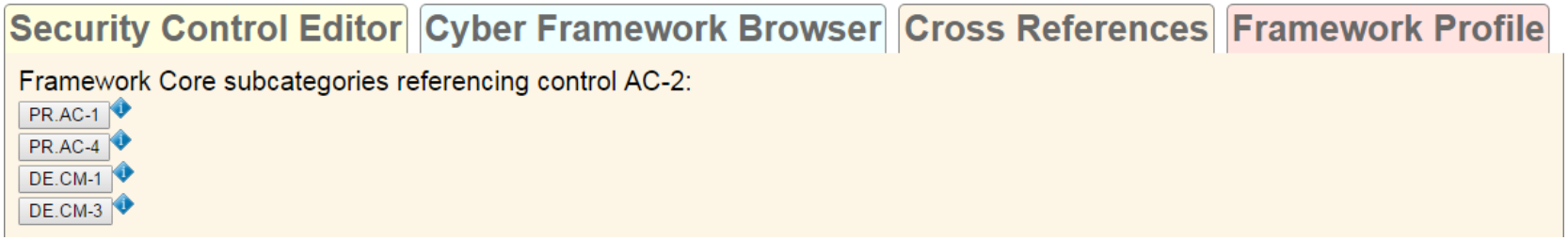




Security Control AC-2

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
AC-2	**ACCOUNT MANAGEMENT**	LOW		Selected	Selected	Selected
AC-2(1)	*AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	MODERATE	NO		Selected	Selected
AC-2(2)	*REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	MODERATE	NO		Selected	Selected
AC-2(3)	*DISABLE INACTIVE ACCOUNTS*	MODERATE	NO		Selected	Selected
AC-2(4)	*AUTOMATED AUDIT ACTIONS*	MODERATE	NO		Selected	Selected
AC-2(5)	*INACTIVITY LOGOUT*	HIGH	NO			Selected
AC-2(6)	*DYNAMIC PRIVILEGE MANAGEMENT*	N/A	NO			
AC-2(7)	*ROLE-BASED SCHEMES*	N/A	NO			
AC-2(8)	*DYNAMIC ACCOUNT CREATION*	N/A	NO			
AC-2(9)	*RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*	N/A	NO			
AC-2(10)	*SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*	N/A	NO			
AC-2(11)	*USAGE CONDITIONS*	HIGH	NO			Selected
AC-2(12)	*ACCOUNT MONITORING / ATYPICAL USAGE*	HIGH	NO			Selected
AC-2(13)	*DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*	HIGH	NO			Selected

Cross References Tab



NIST SP 800-53 Database Lookup

AC-2 - ACCOUNT MANAGEMENT

Family: AC - ACCESS CONTROL

Priority: P1 - Implement P1 security controls first.

Baseline Allocation:

Low	Moderate	High
AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

Jump To:
Revision 4 Statements
Control Description
Supplemental Guidance
References

Control Description

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of information system accounts;

h. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

NIST SP 800-82 ICS

AC-2 ACCOUNT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	Selected	Selected	Selected
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Selected	Selected
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*		Selected	Selected
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*		Selected	Selected
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Selected	Selected
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT / TYPICAL USAGE MONITORING*			Selected
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Selected
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*			Selected
AC-2 (13)	*ACCOUNT MANAGEMENT | ACCOUNT REVIEWS*			Selected

ICS Supplemental Guidance: Example compensating controls include providing increased physical security, personnel security, intrusion detection, auditing measures.
Control Enhancement: (1, 3, 4) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (11, 12, 13) No ICS Supplemental Guidance.

Framework Core: Database Export

```
<RESULTSET FOUND="96">
  <ROW MODID="0" RECORDID="420">
    <COL>
      <DATA>IDENTIFY (ID)</DATA>
    </COL>
    <COL>
      <DATA>Governance (ID.GV): The policies, procedures, and processes to
manage and monitor the organization's regulatory, legal, risk, environmental,
and operational requirements are understood and inform the management of
cybersecurity risk.</DATA>
    </COL>
    <COL>
      <DATA>ID.GV-1: Organizational information security policy is
established</DATA>
    </COL>
    <COL>
      <DATA>·_____ NIST SP 800-53 Rev. 4 -1 controls from all families </DATA>
    </COL>
  </ROW>
  <ROW MODID="0" RECORDID="428">
    <COL>
      <DATA>IDENTIFY (ID)</DATA>
    </COL>
    <COL>
      <DATA>Governance (ID.GV): The policies, procedures, and processes to
manage and monitor the organization's regulatory, legal, risk, environmental,
and operational requirements are understood and inform the management of
cybersecurity risk.</DATA>
```

Structured XML via XSLT 2.0

```
   <function id="ID">
      <name>IDENTIFY</name>
      <category id="ID.GV">
         <name>Governance</name>
         <dropDownLabel>Governance (ID.GV)</dropDownLabel>
         <description>The policies, procedures, and processes to manage and
monitor the organization's regulatory, legal, risk, environmental, and
operational requirements are understood and inform the management of
cybersecurity risk.</description>
         <subCategory id="ID.GV-1">
            <description>Organizational information security policy is
established</description>
            <sp800-53 all="true"/>
         </subCategory>
         <subCategory id="ID.GV-2">
            <description>Information security roles &amp;amp; responsibilities are
coordinated and aligned with internal roles and external partners</description>
            <sp800-53>
               <control>PM-1</control>
               <control>PS-7</control>
            </sp800-53>
         </subCategory>
         <subCategory id="ID.GV-3">
            <description>Legal and regulatory requirements regarding
cybersecurity, including privacy and civil liberties obligations, are
understood and managed</description>
            <sp800-53 all="true">
               <except>PM-1</except>
```