Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Chris Hoover

GRC Strategist, Federal Solutions

10/31/2013

EO 13636 Overview

Executive Order 13636

- Improving Critical Infrastructure Cybersecurity
- Issued February 2013
- What is Critical Infrastructure?

> *"...assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination..."*

Critical Infrastructure

- Chemical Sector
- Commercial Facilities Sector

Critical Infrastructure

- Communications Sector
- Critical Manufacturing Sector

Critical Infrastructure

- Dams Sector
- Defense Industrial Base Sector

Critical Infrastructure

- Emergency Services
- Energy Sector

Critical Infrastructure

- Financial Services Sector
- Food and Agriculture Sector

Critical Infrastructure

- Government Facilities Sector
- Healthcare and Public Health Sector

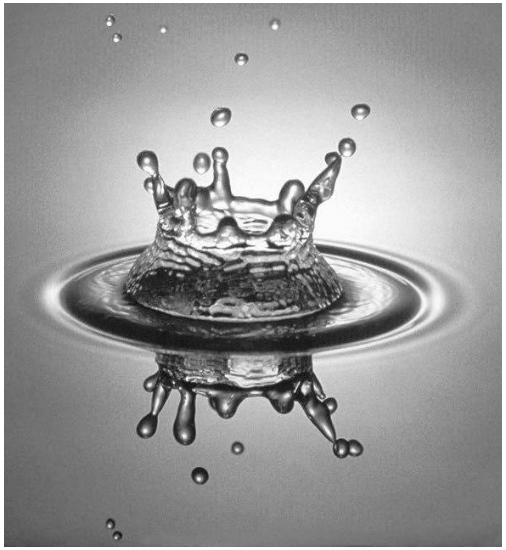
Critical Infrastructure

- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector

```
// _MSC_VER > 1000
#ifndef __AFXWIN_H__
	#error include 'stdafx.h' before including this file for PCH
#endif
#include "resource.h"		// main symbols
// CDMotionApp:
// See DMotion.cpp for the implementation of this class
//
class CDMotionApp : public CWinApp
{
public:
	CDMotionApp();
// Overrides
	// ClassWizard generated virtual function overrides
	//{{AFX_VIRTUAL(CDMotionApp)
	public:
	virtual BOOL InitInstance();
	//}}AFX_VIRTUAL
// Implementation
	//{{AFX_MSG(CDMotionApp)
```

Critical Infrastructure

- Transportation Systems Sector
- Water and Wastewater Systems Sector



What Does It Say? What Does It Do?

Carrot & Stick

Legal liability?

Civic pride?

Patriotism?

Self interest?

Carrot & Stick

EO directs the Executive Branch to:

> "...promote and incentivize the adoption of Cybersecurity practices..."

The Carrots

- EO directs the Executive Branch to:
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Develop a technology-neutral voluntary Cybersecurity framework

Sharing Cyber Threat Information

"…Within 120 days,

- the Attorney General (DOJ),
- the Secretary of DHS, and
- the Director of National Intelligence

shall each issue instructions to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity…"

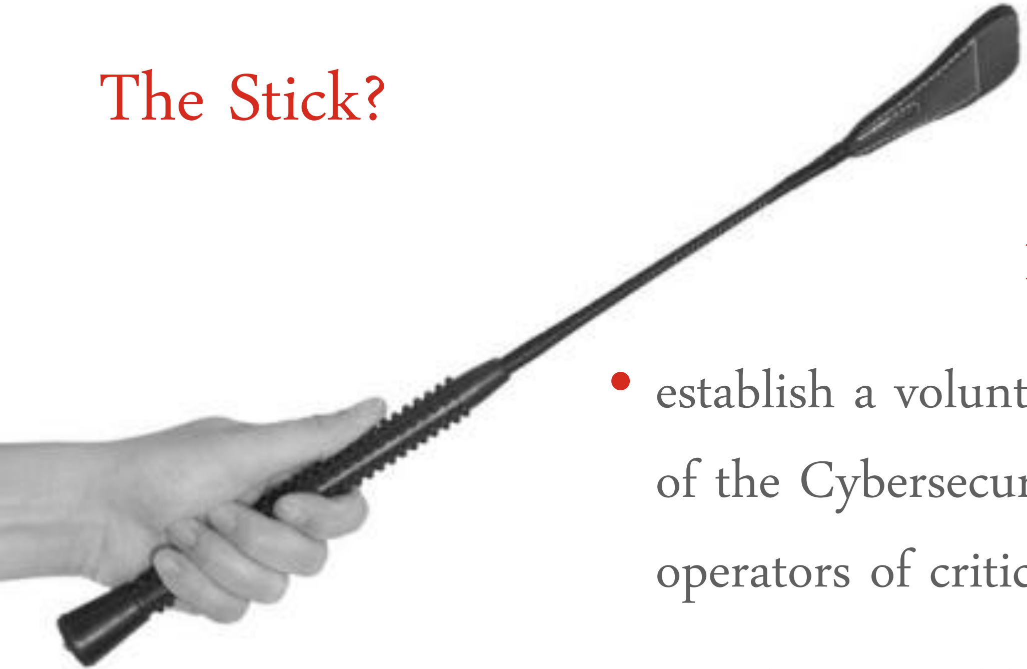
Develop a Cybersecurity Framework

- The Secretary of Commerce shall direct the Director of NIST to lead the development of a framework
- shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

Develop a Cybersecurity Framework

- Within 240 days of the date of this order publish a preliminary version of the Cybersecurity Framework
- Within 1 year of the date of this order publish a final version of the Cybersecurity Framework

The Stick?



Promote & Incentivize

- establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure
- coordinate establishment of a set of incentives designed to promote participation in the Program.

The Stick?

Promote & Incentivize

- include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.
- feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration

NIST Cybersecurity Framework (CSF)

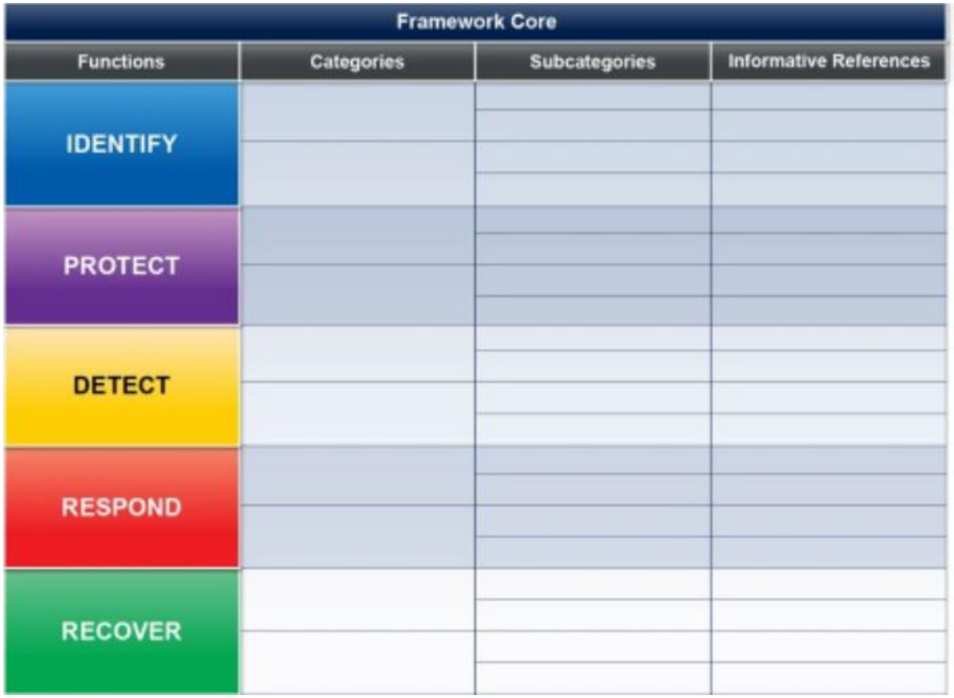
Goals of the Framework

The CSF should enable an organization to:

- describe their current Cybersecurity posture
- describe their target state for Cybersecurity
- identify and prioritize opportunities for improvement within the context of risk management
- assess progress toward the target state
- foster communications among internal and external stakeholders

Framework Core

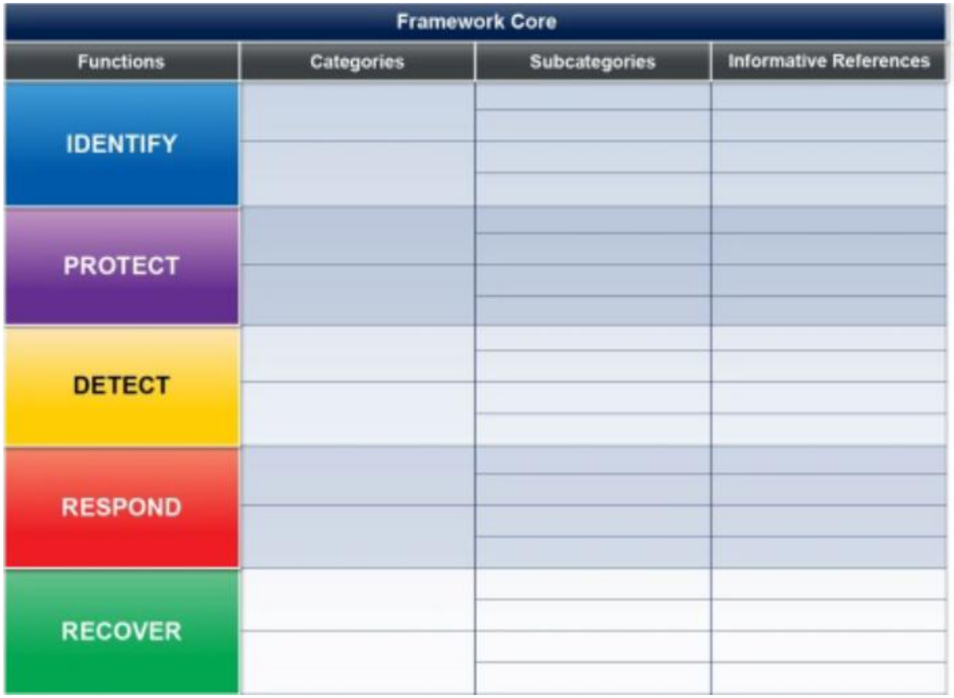
- compilation of Cybersecurity activities and references that are common across critical infrastructure sectors.
- consists of five Functions: Identify, Protect, Detect, Respond, Recover



Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

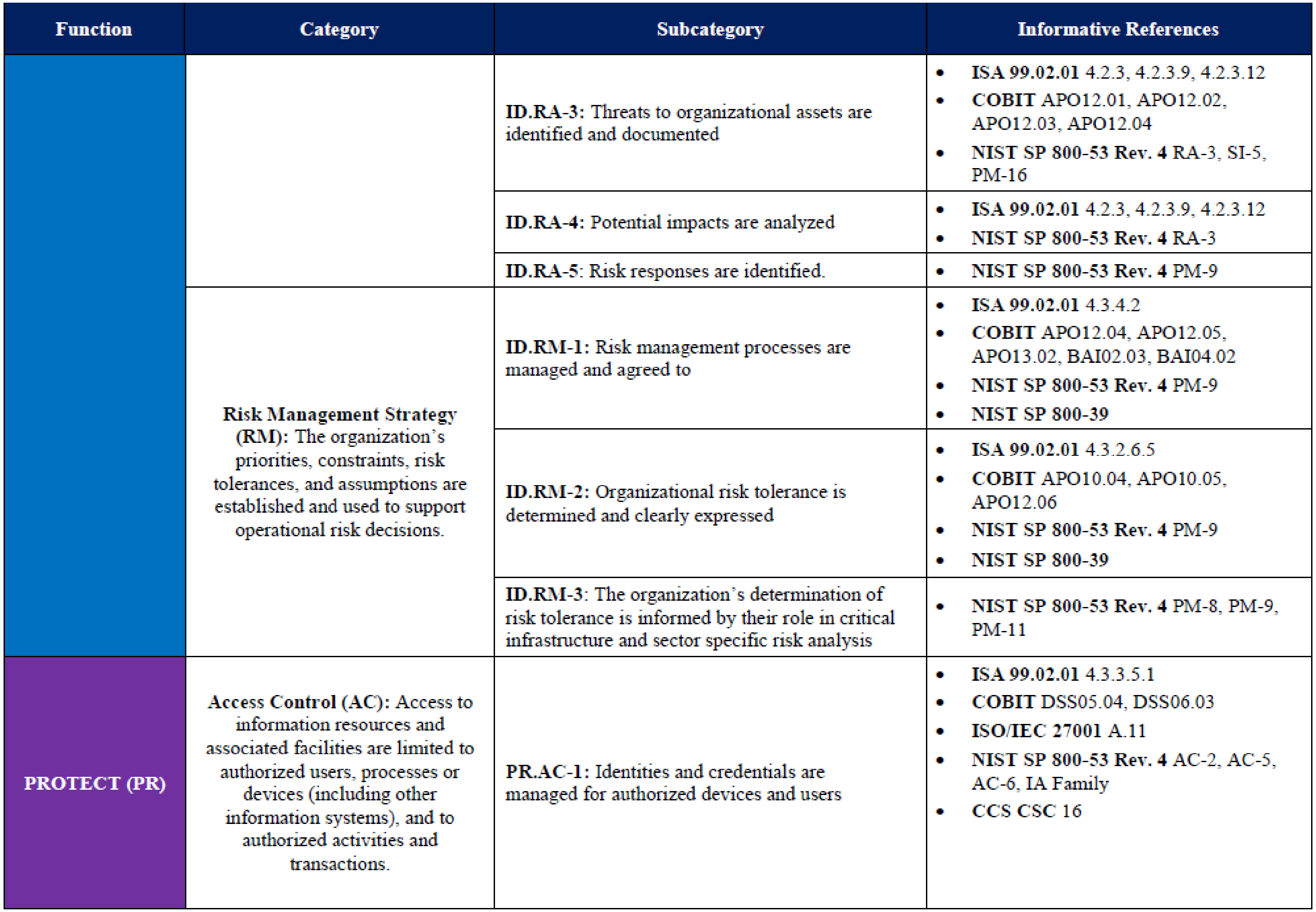
Framework Core

- identifies underlying key Categories and Subcategories for each of these Functions, and matches them with Informative References such as existing standards, guidelines, and practices for each Subcategory



Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Framework Core



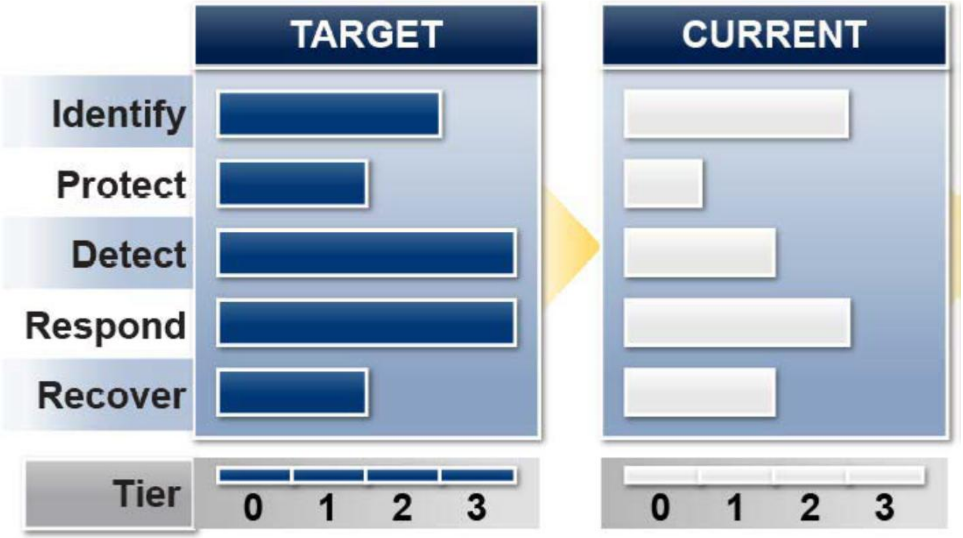
Function	Category	Subcategory	Informative References
		ID.RA-3: Threats to organizational assets are identified and documented	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **COBIT** APO12.01, APO12.02, APO12.03, APO12.04 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-16
		ID.RA-4: Potential impacts are analyzed	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3
		ID.RA-5: Risk responses are identified.	• **NIST SP 800-53 Rev. 4** PM-9
	Risk Management Strategy (RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are managed and agreed to	• **ISA 99.02.01** 4.3.4.2 • **COBIT** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **NIST SP 800-53 Rev. 4** PM-9 • **NIST SP 800-39**
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **ISA 99.02.01** 4.3.2.6.5 • **COBIT** APO10.04, APO10.05, APO12.06 • **NIST SP 800-53 Rev. 4** PM-9 • **NIST SP 800-39**
		ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11
PROTECT (PR)	**Access Control (AC):** Access to information resources and associated facilities are limited to authorized users, processes or devices (including other information systems), and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **ISA 99.02.01** 4.3.3.5.1 • **COBIT** DSS05.04, DSS06.03 • **ISO/IEC 27001** A.11 • **NIST SP 800-53 Rev. 4** AC-2, AC-5, AC-6, IA Family • **CCS CSC** 16

Framework Implementation Tiers ("Tiers")

- describe how an organization manages its Cybersecurity risk
- range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in risk management practices and the extent to which risk management is integrated into an organization's overall practices.
  - Tier 1: Partial
  - Tier 2: Risk-Informed
  - Tier 3: Risk-Informed and Repeatable
  - Tier 4: Adaptive

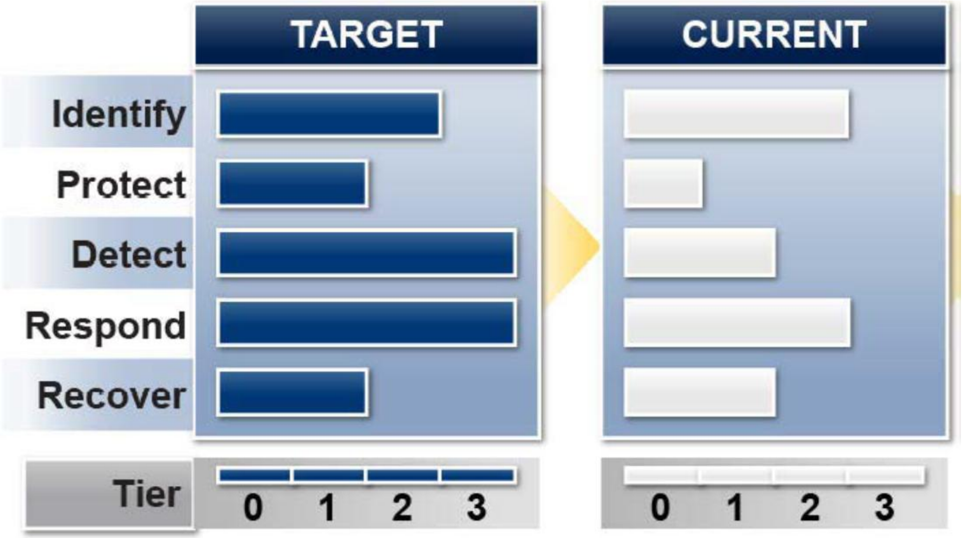
Framework Profile ("Profile")

- conveys how an organization manages Cybersecurity risk in each of the Framework Core Functions and Categories by identifying the Subcategories that are implemented or planned for implementation

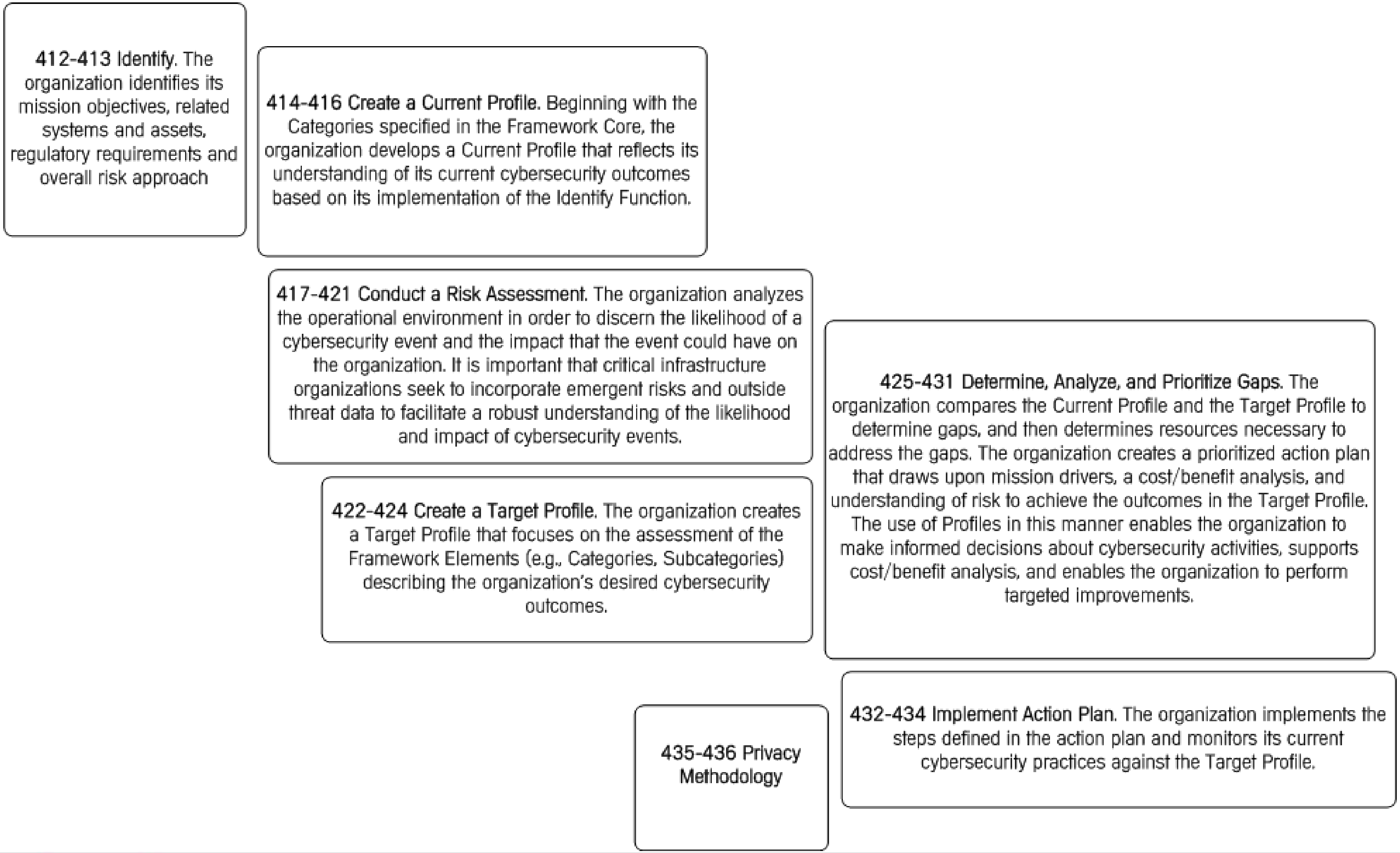


Framework Profile ("Profile")

- also used to identify the appropriate goals for an organization or for a critical infrastructure sector and to assess progress against meeting those goals



Preliminary CSF Workflow



412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

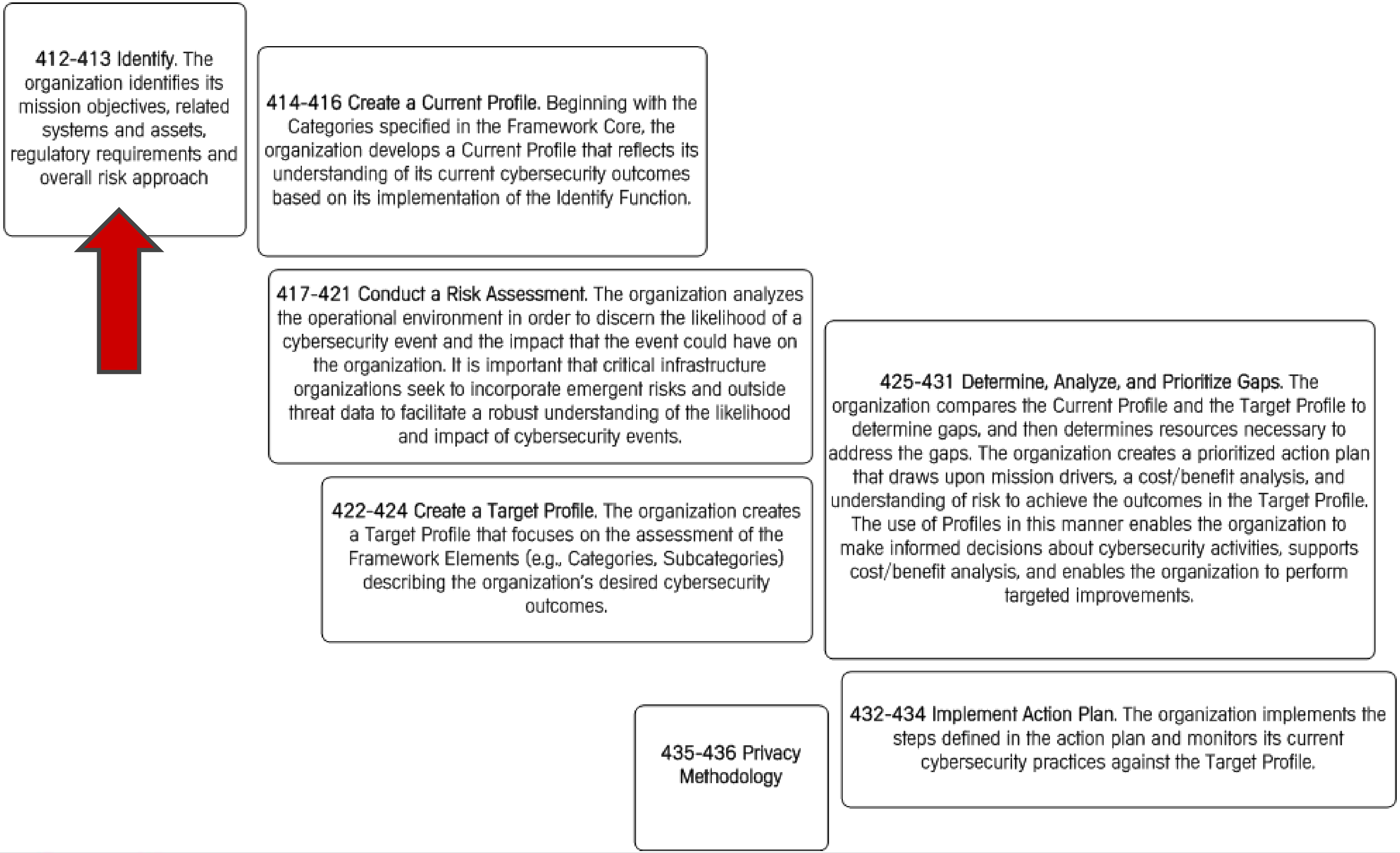
425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

435-436 Privacy Methodology

How RSA Archer Can Help

Preliminary CSF Workflow



412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

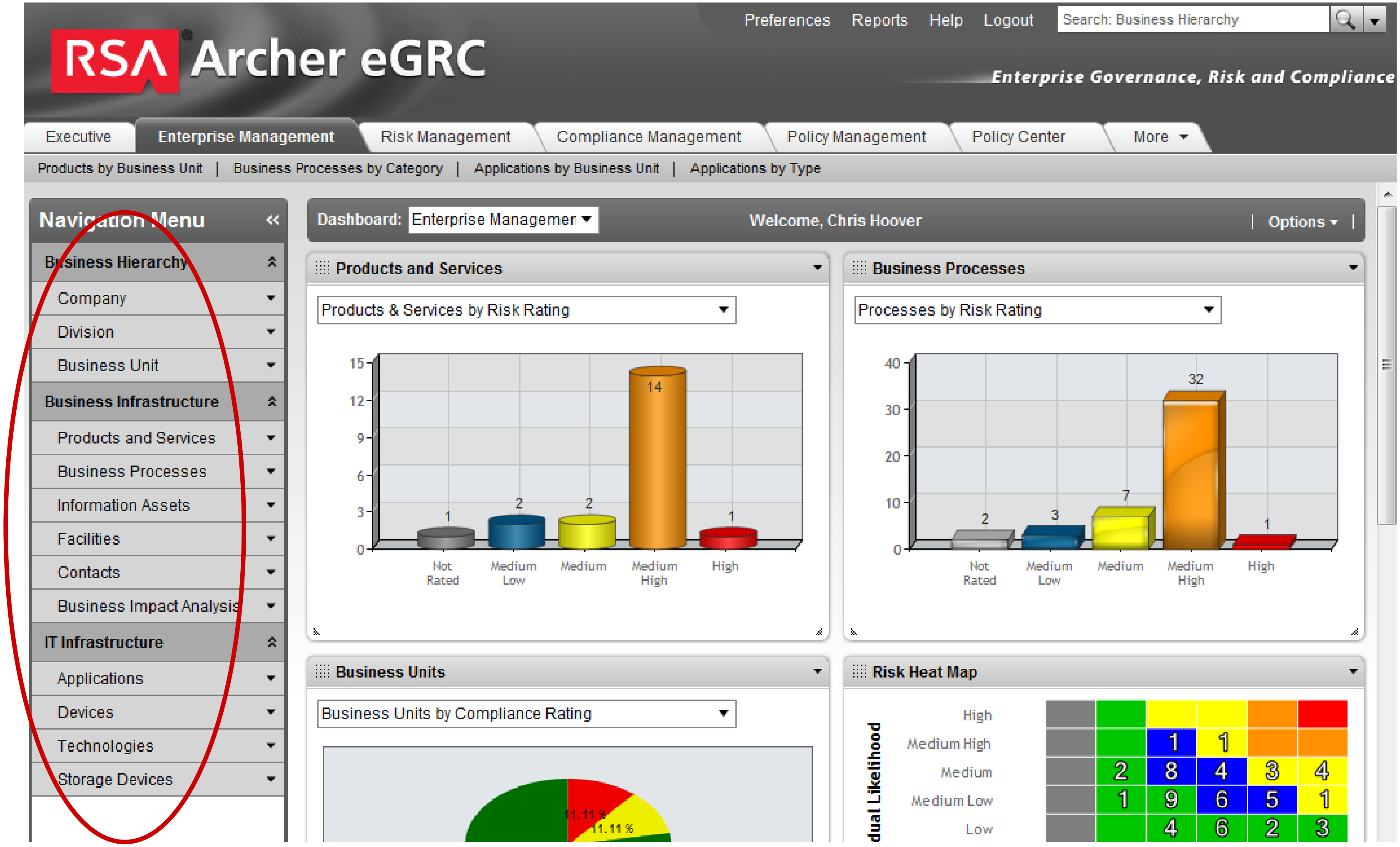
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

435-436 Privacy Methodology

“Identify” Step = RSA Archer Enterprise Mgmt.

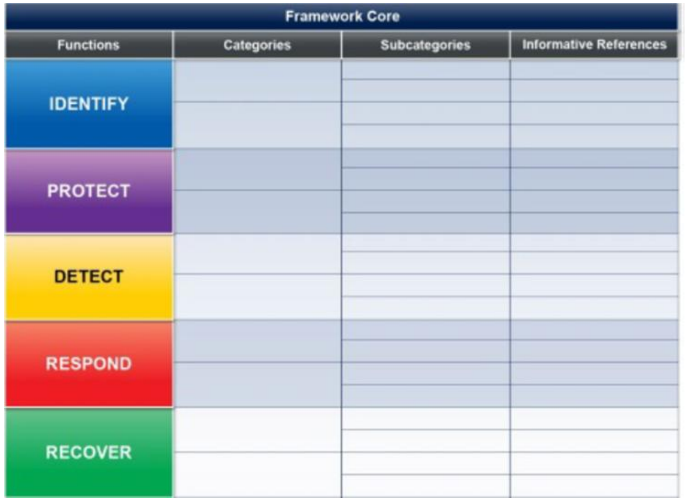


High						
Medium High			1	1		
Medium		2	8	4	3	4
Medium Low		1	9	6	5	1
Low			4	6	2	3

Preliminary CSF Workflow

~~412-413 Identify. The organization identifies its mission objectives, related systems and assets,~~ regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.



Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

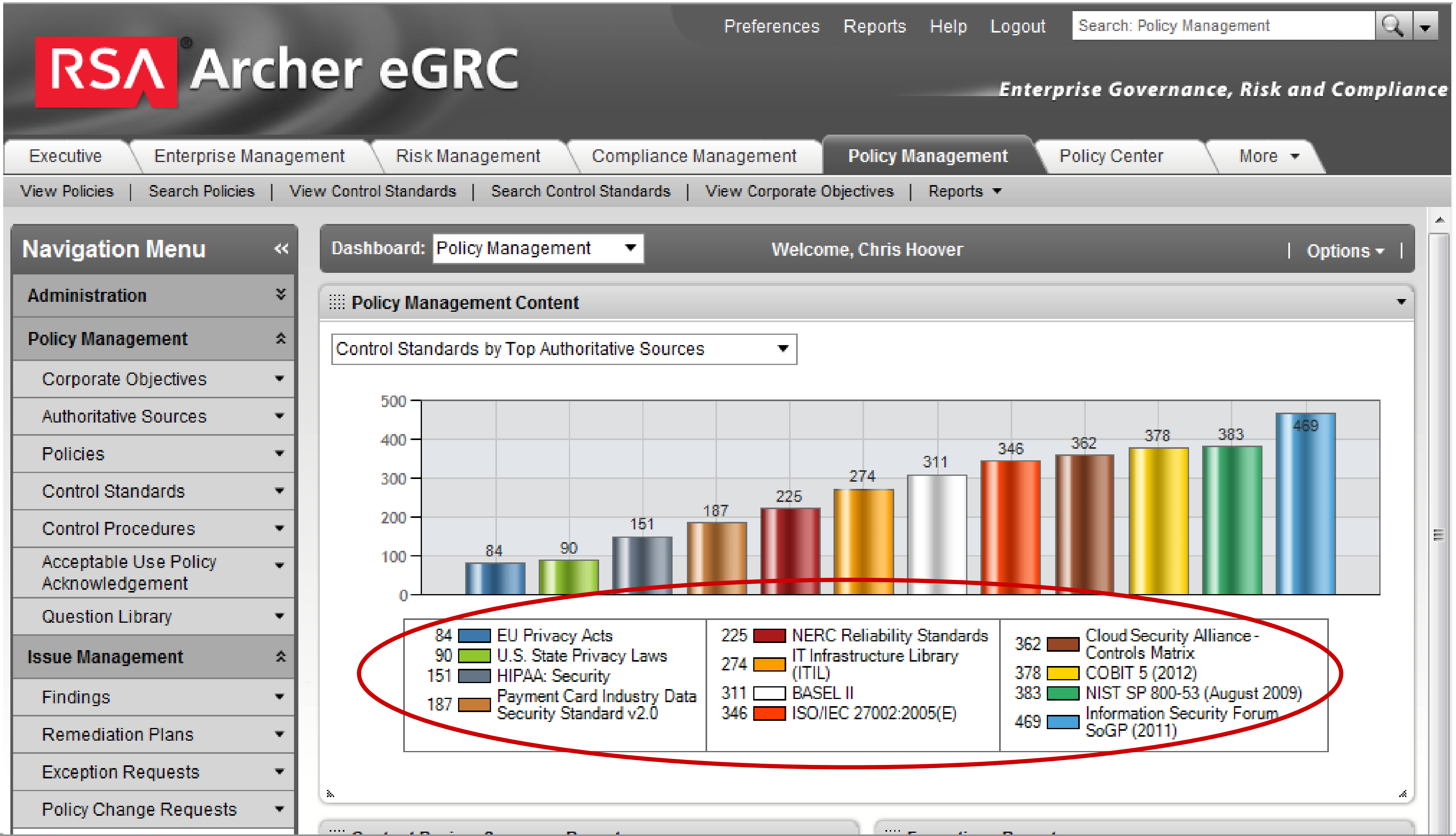
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

435-436 Privacy Methodology

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

Profile Mapping = RSA Archer Policy Mgmt.



Dashboard: Policy Management

Welcome, Chris Hoover

Control Standards by Top Authoritative Sources

84	🟦	EU Privacy Acts
90	🟩	U.S. State Privacy Laws
151	■	HIPAA: Security
187	🟫	Payment Card Industry Data Security Standard v2.0
225	🟥	NERC Reliability Standards
274	🟧	IT Infrastructure Library (ITIL)
311	□	BASEL II
346	🟥	ISO/IEC 27002:2005(E)
362	🟫	Cloud Security Alliance - Controls Matrix
378	🟨	COBIT 5 (2012)
383	🟩	NIST SP 800-53 (August 2009)
469	🟦	Information Security Forum SoGP (2011)

Preliminary CSF Workflow

412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

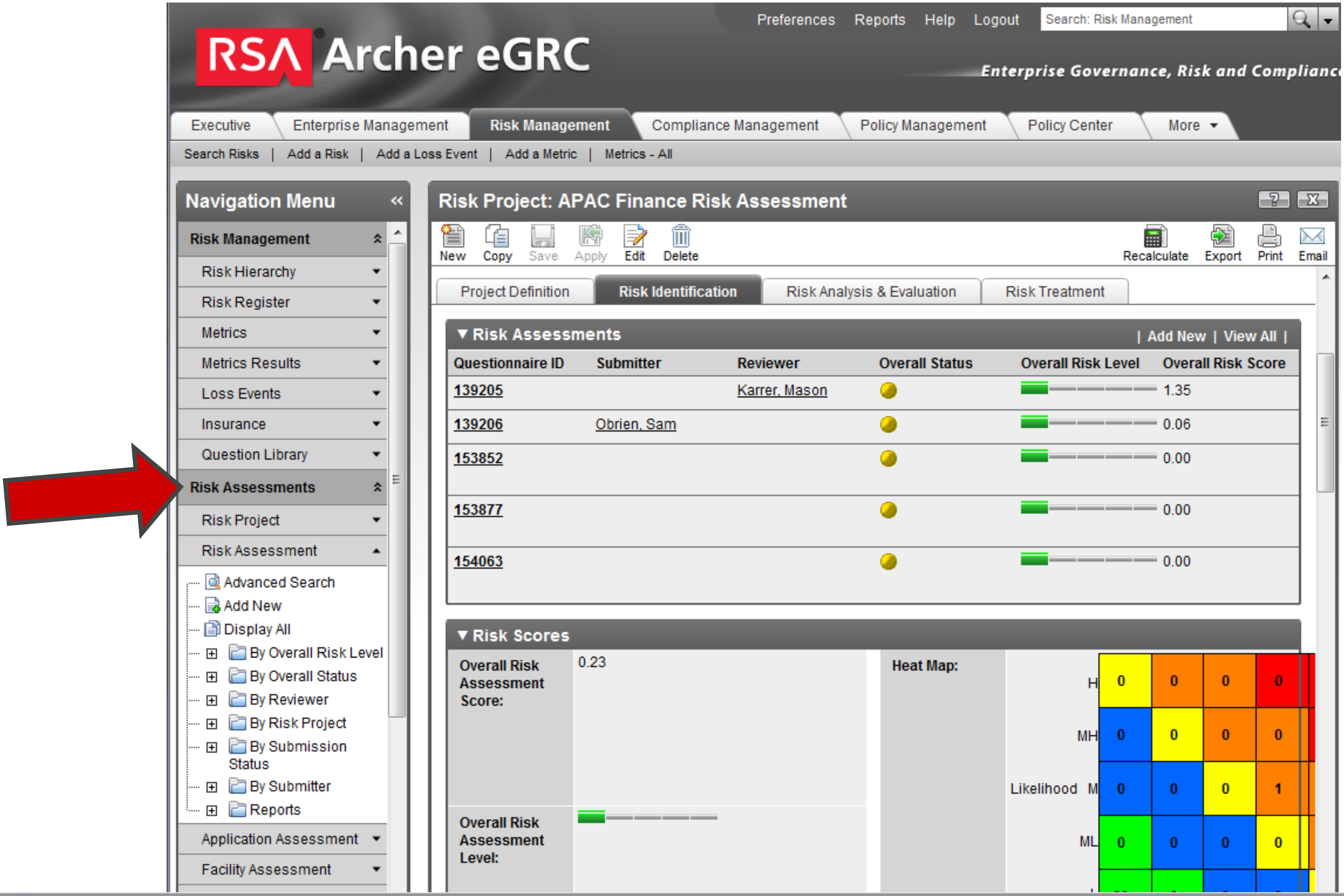
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

435-436 Privacy Methodology

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

Risk Assessment = RSA Archer Risk Mgmt.



Risk Project: APAC Finance Risk Assessment

▼ Risk Assessments

Questionnaire ID	Submitter	Reviewer	Overall Status	Overall Risk Level	Overall Risk Score
139205		Karrer, Mason	●	🟩	1.35
139206	Obrien, Sam		●	🟩	0.06
153852			●	🟩	0.00
153877			●	🟩	0.00
154063			●	🟩	0.00

▼ Risk Scores

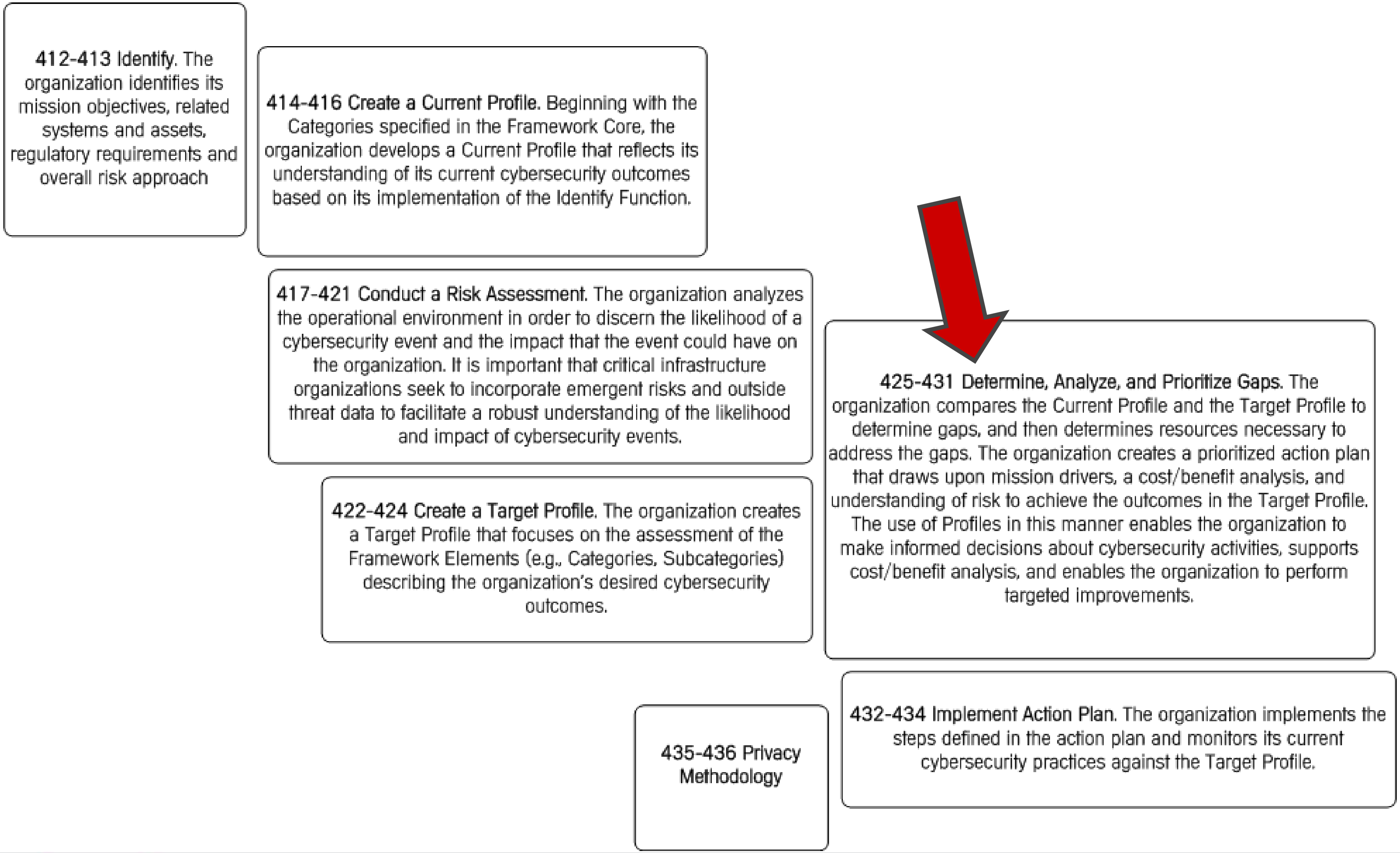
Overall Risk Assessment Score: 0.23

Overall Risk Assessment Level: 🟩

Heat Map:

Likelihood				
H	0	0	0	0
MH	0	0	0	0
M	0	0	0	1
ML	0	0	0	0

Preliminary CSF Workflow



412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

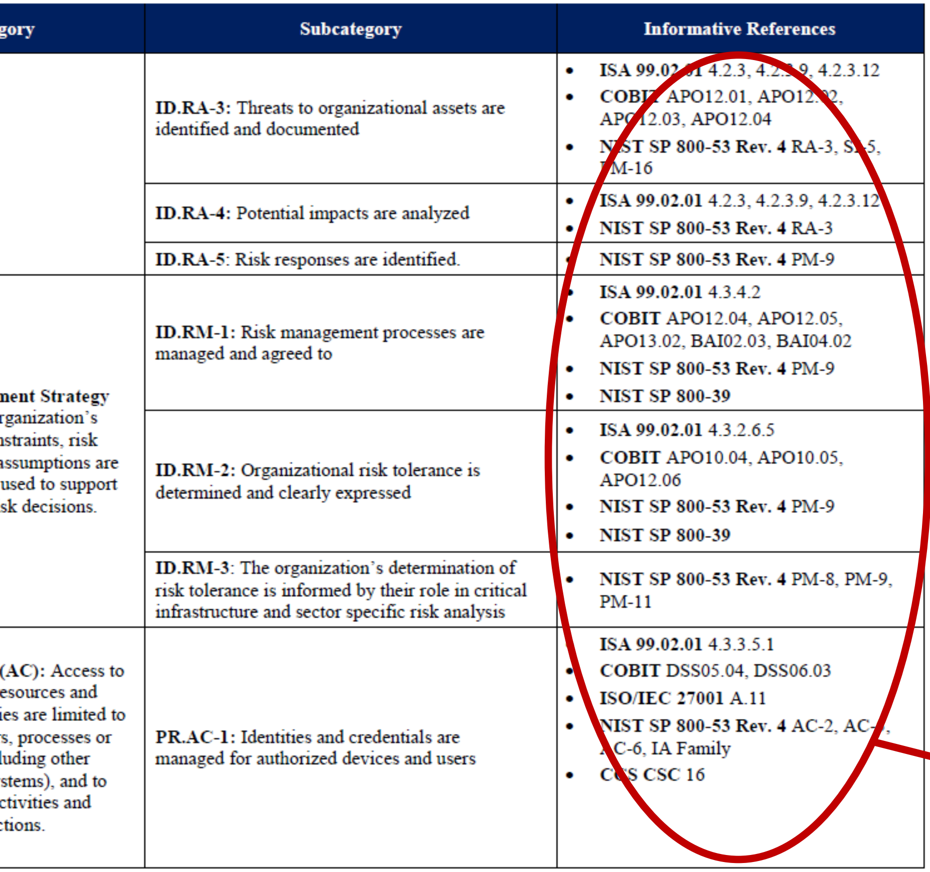
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

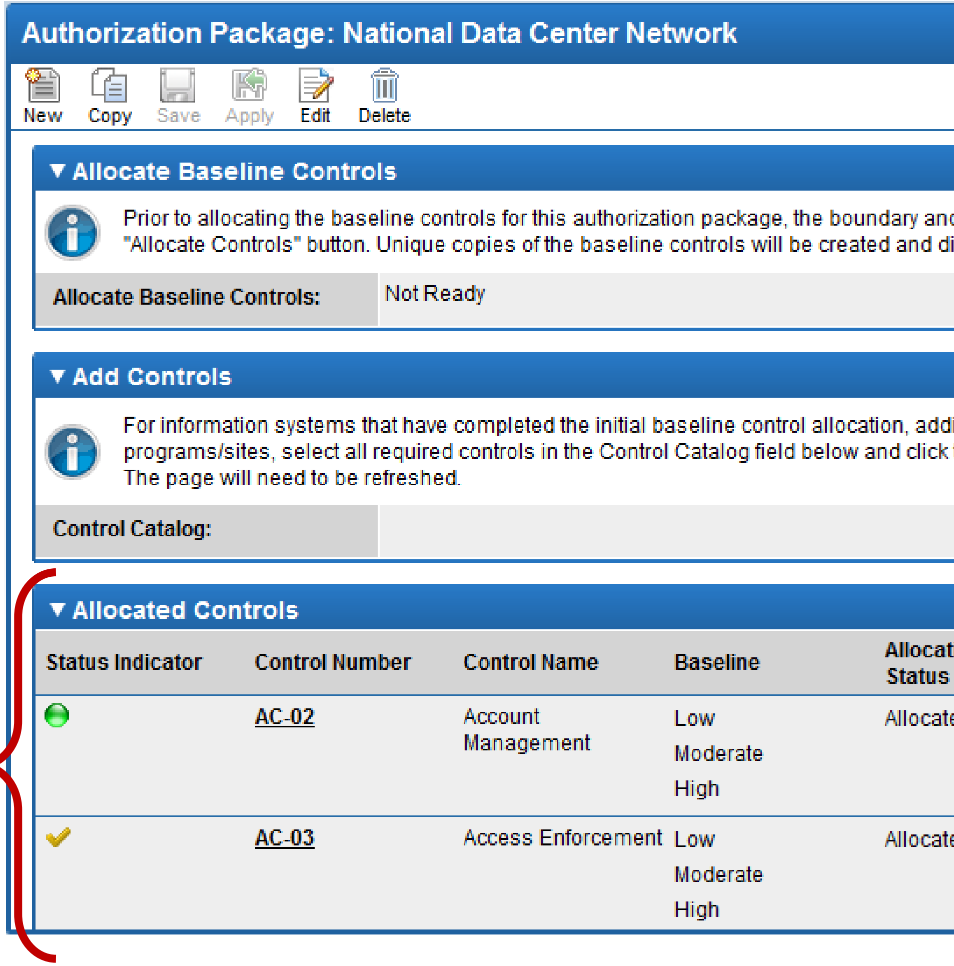
432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

435-436 Privacy Methodology

Allocated Controls



gory	Subcategory	Informative References
	ID.RA-3: Threats to organizational assets are identified and documented	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **COBIT** APO12.01, APO12.02, APO12.03, APO12.04 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-16
	ID.RA-4: Potential impacts are analyzed	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3
	ID.RA-5: Risk responses are identified.	• **NIST SP 800-53 Rev. 4** PM-9
ment Strategy rganization's nstraints, risk assumptions are used to support sk decisions.	**ID.RM-1:** Risk management processes are managed and agreed to	• **ISA 99.02.01** 4.3.4.2 • **COBIT** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **NIST SP 800-53 Rev. 4** PM-9 • **NIST SP 800-39**
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **ISA 99.02.01** 4.3.2.6.5 • **COBIT** APO10.04, APO10.05, APO12.06 • **NIST SP 800-53 Rev. 4** PM-9 • **NIST SP 800-39**
	ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11
(AC): Access to esources and ies are limited to s, processes or luding other stems), and to ctivities and tions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **ISA 99.02.01** 4.3.3.5.1 • **COBIT** DSS05.04, DSS06.03 • **ISO/IEC 27001** A.11 • **NIST SP 800-53 Rev. 4** AC-2, AC-5, AC-6, IA Family • **CCS** CSC 16



Authorization Package: National Data Center Network

▼ Allocate Baseline Controls

Prior to allocating the baseline controls for this authorization package, the boundary and
"Allocate Controls" button. Unique copies of the baseline controls will be created and di

Allocate Baseline Controls: Not Ready

▼ Add Controls

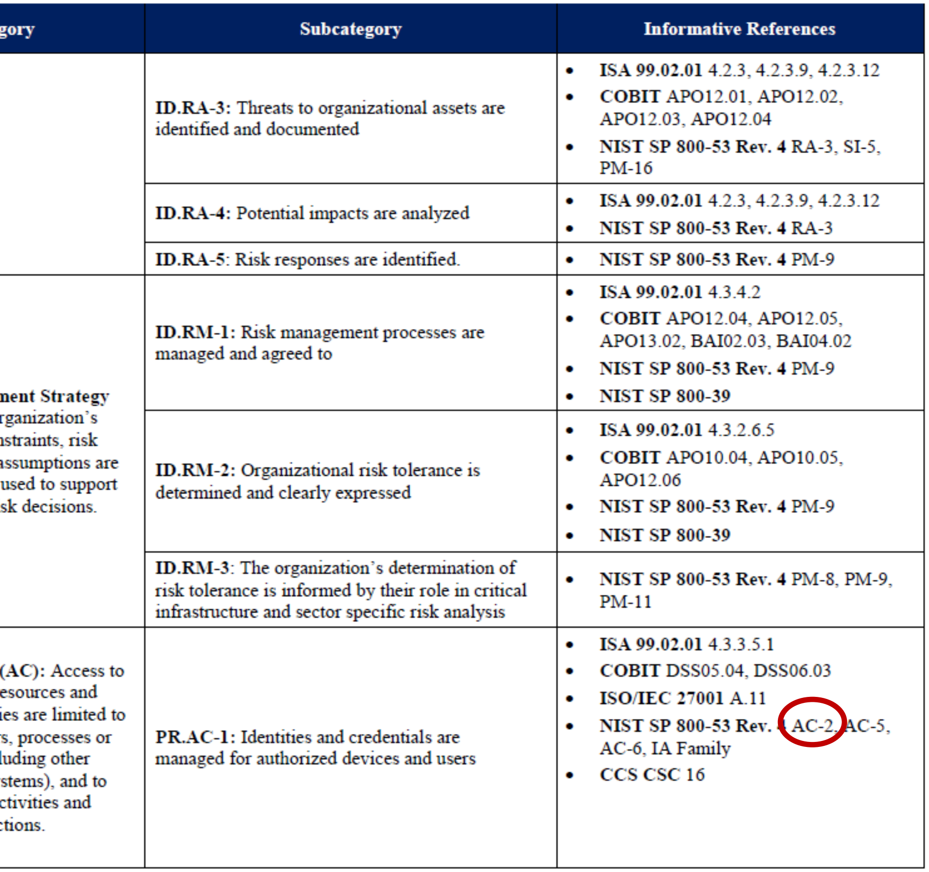
For information systems that have completed the initial baseline control allocation, addi
programs/sites, select all required controls in the Control Catalog field below and click
The page will need to be refreshed.

Control Catalog:

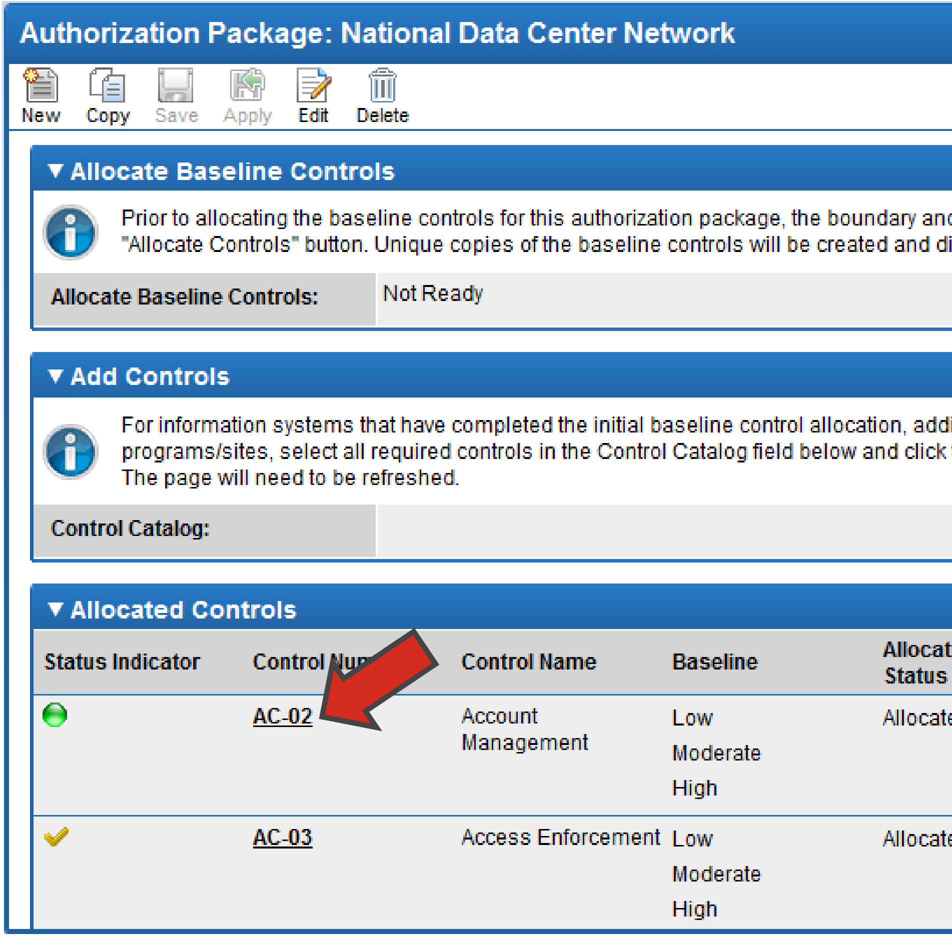
▼ Allocated Controls

Status Indicator	Control Number	Control Name	Baseline	Allocat Status
●	AC-02	Account Management	Low Moderate High	Allocate
✓	AC-03	Access Enforcement	Low Moderate High	Allocate

Tailoring the Control Set - Remove



gory	Subcategory	Informative References
	ID.RA-3: Threats to organizational assets are identified and documented	- **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 - **COBIT** APO12.01, APO12.02, APO12.03, APO12.04 - **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-16
	ID.RA-4: Potential impacts are analyzed	- **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 - **NIST SP 800-53 Rev. 4** RA-3
	ID.RA-5: Risk responses are identified.	- **NIST SP 800-53 Rev. 4** PM-9
nent Strategy rganization's nstraints, risk assumptions are used to support sk decisions.	**ID.RM-1**: Risk management processes are managed and agreed to	- **ISA 99.02.01** 4.3.4.2 - **COBIT** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 - **NIST SP 800-53 Rev. 4** PM-9 - **NIST SP 800-39**
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	- **ISA 99.02.01** 4.3.2.6.5 - **COBIT** APO10.04, APO10.05, APO12.06 - **NIST SP 800-53 Rev. 4** PM-9 - **NIST SP 800-39**
	ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	- **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11
(AC): Access to esources and ies are limited to s, processes or luding other stems), and to ctivities and tions.	**PR.AC-1**: Identities and credentials are managed for authorized devices and users	- **ISA 99.02.01** 4.3.3.5.1 - **COBIT** DSS05.04, DSS06.03 - **ISO/IEC 27001** A.11 - **NIST SP 800-53 Rev. 4** AC-2, AC-5, AC-6, IA Family - **CCS CSC** 16



Authorization Package: National Data Center Network

▼ Allocate Baseline Controls

Prior to allocating the baseline controls for this authorization package, the boundary and "Allocate Controls" button. Unique copies of the baseline controls will be created and di

Allocate Baseline Controls:	Not Ready

▼ Add Controls

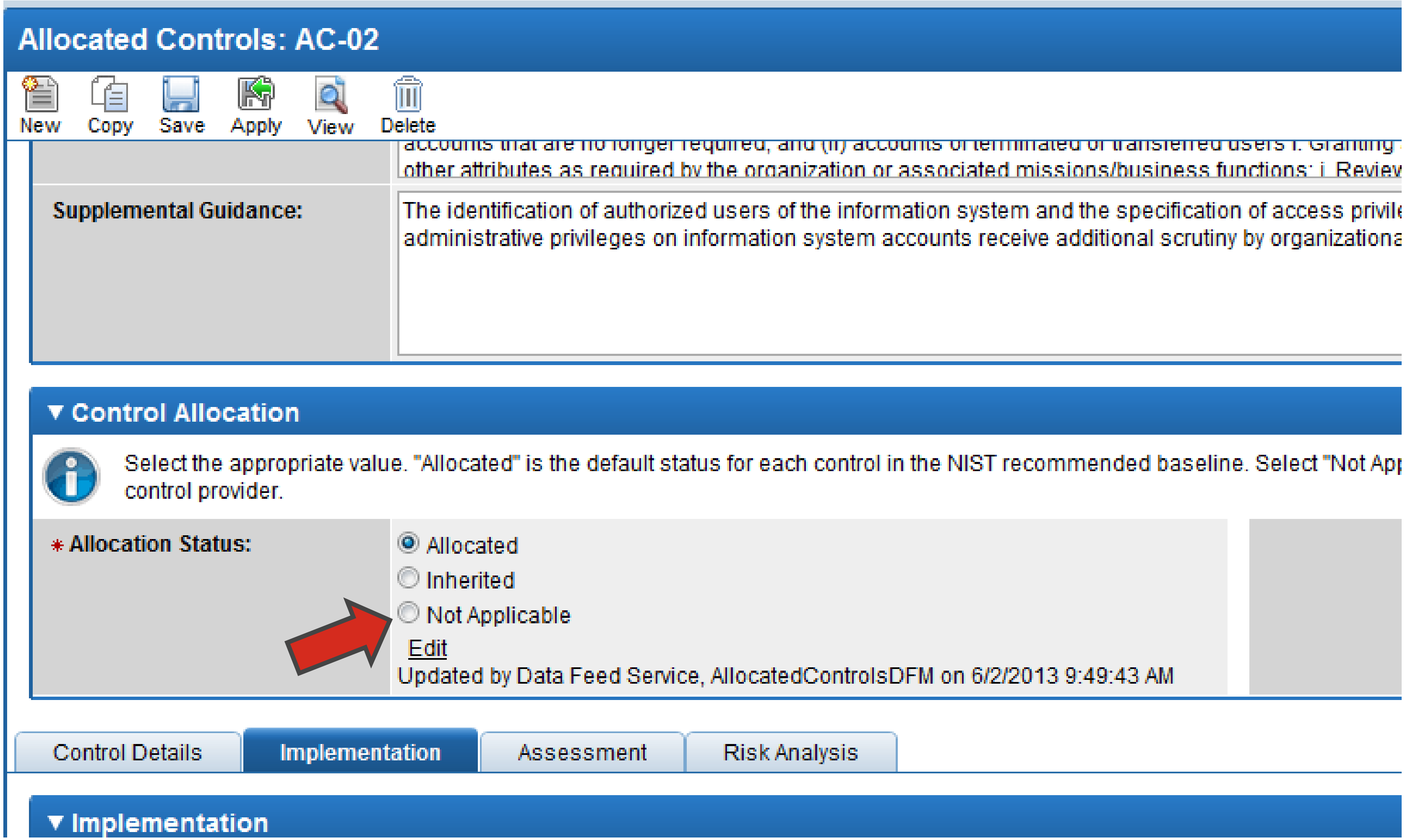
For information systems that have completed the initial baseline control allocation, addi programs/sites, select all required controls in the Control Catalog field below and click The page will need to be refreshed.

Control Catalog:	

▼ Allocated Controls

Status Indicator	Control Num	Control Name	Baseline	Allocat Status
●	AC-02	Account Management	Low Moderate High	Allocate
✓	AC-03	Access Enforcement	Low Moderate High	Allocate

Tailoring the Control Set - Remove



Allocated Controls: AC-02

accounts that are no longer required; and (ii) accounts of terminated or transferred users f. Granting
other attributes as required by the organization or associated missions/business functions; i. Review

Supplemental Guidance: The identification of authorized users of the information system and the specification of access privile
administrative privileges on information system accounts receive additional scrutiny by organizationa

▼ Control Allocation

Select the appropriate value. "Allocated" is the default status for each control in the NIST recommended baseline. Select "Not App
control provider.

* **Allocation Status:**

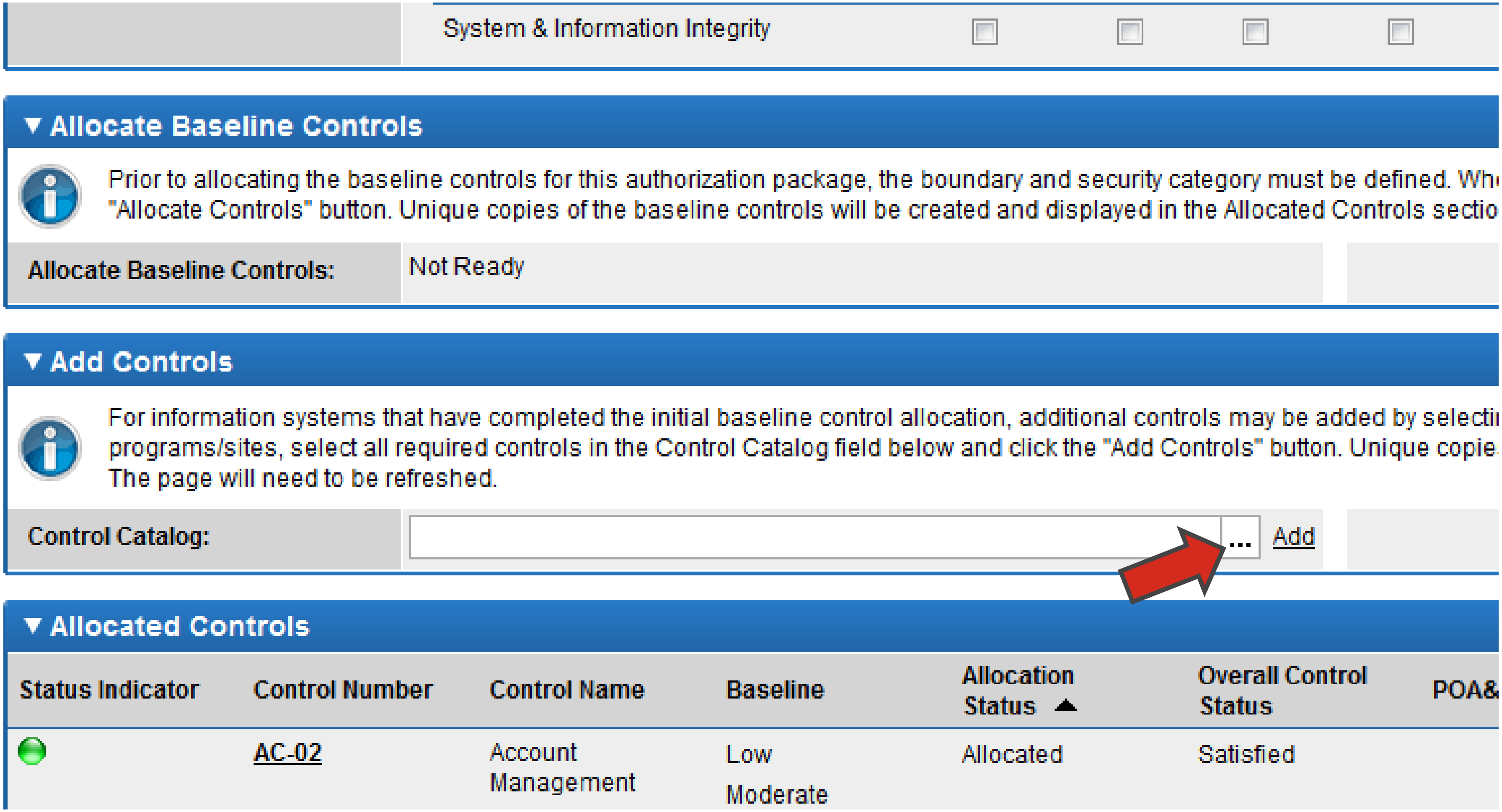
● Allocated
○ Inherited
○ Not Applicable

Edit

Updated by Data Feed Service, AllocatedControlsDFM on 6/2/2013 9:49:43 AM

▼ Implementation

Tailoring the Control Set - Add



System & Information Integrity □ □ □ □

▼ Allocate Baseline Controls

Prior to allocating the baseline controls for this authorization package, the boundary and security category must be defined. Wh "Allocate Controls" button. Unique copies of the baseline controls will be created and displayed in the Allocated Controls sectio

Allocate Baseline Controls:	Not Ready

▼ Add Controls

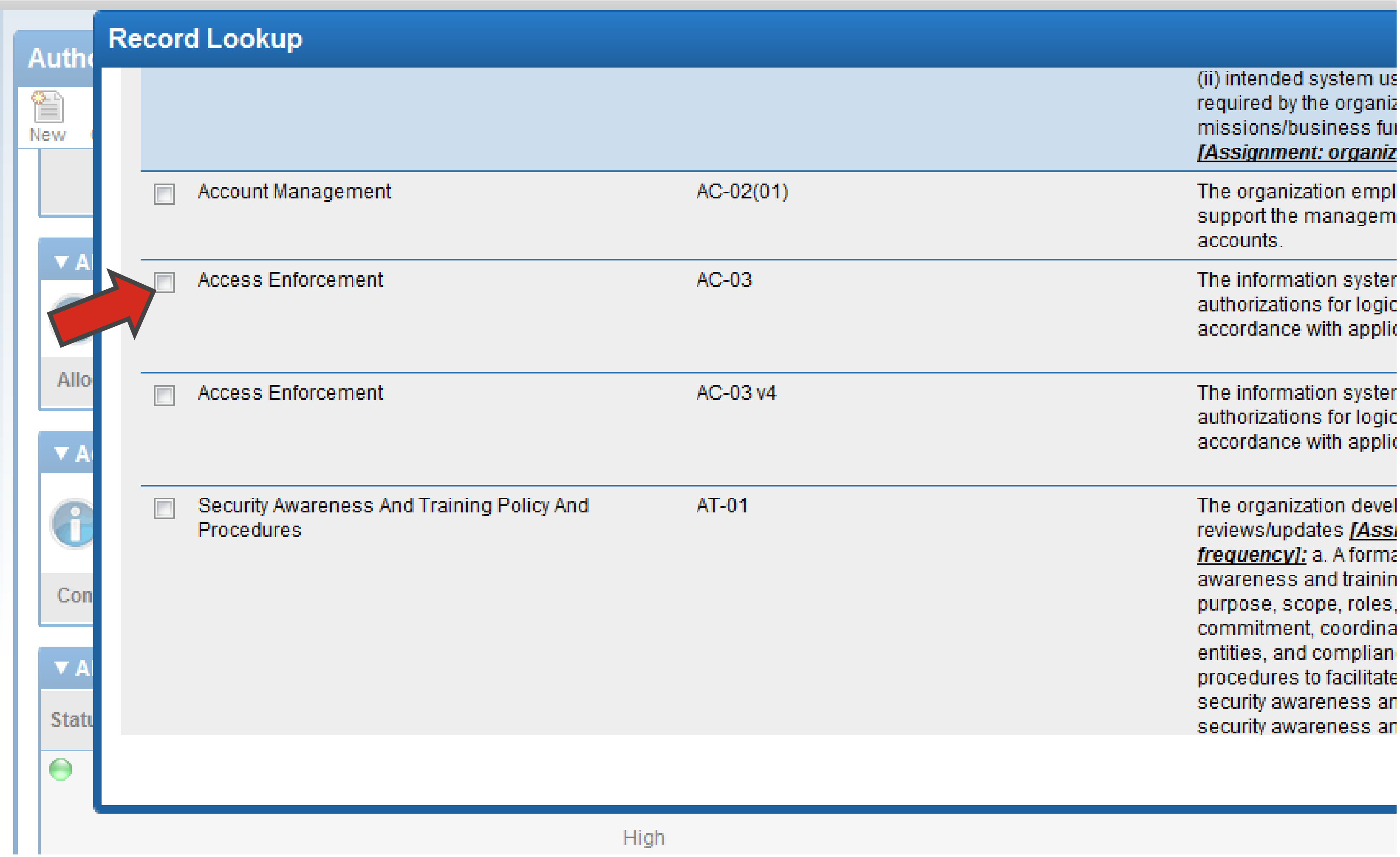
For information systems that have completed the initial baseline control allocation, additional controls may be added by selecti programs/sites, select all required controls in the Control Catalog field below and click the "Add Controls" button. Unique copie The page will need to be refreshed.

Control Catalog:	... Add

▼ Allocated Controls

Status Indicator	Control Number	Control Name	Baseline	Allocation Status ▲	Overall Control Status	POA&
●	AC-02	Account Management	Low Moderate	Allocated	Satisfied	

Tailoring the Control Set - Add



			(ii) intended system us required by the organiz missions/business fu ***[Assignment: organiz***
□	Account Management	AC-02(01)	The organization empl support the managem accounts.
□	Access Enforcement	AC-03	The information syster authorizations for logic accordance with applic
□	Access Enforcement	AC-03 v4	The information syster authorizations for logic accordance with applic
□	Security Awareness And Training Policy And Procedures	AT-01	The organization devel reviews/updates ***[Ass*** ***frequency]:*** a. A forma awareness and trainin purpose, scope, roles, commitment, coordina entities, and complian procedures to facilitate security awareness ar security awareness ar

Preliminary CSF Workflow

412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

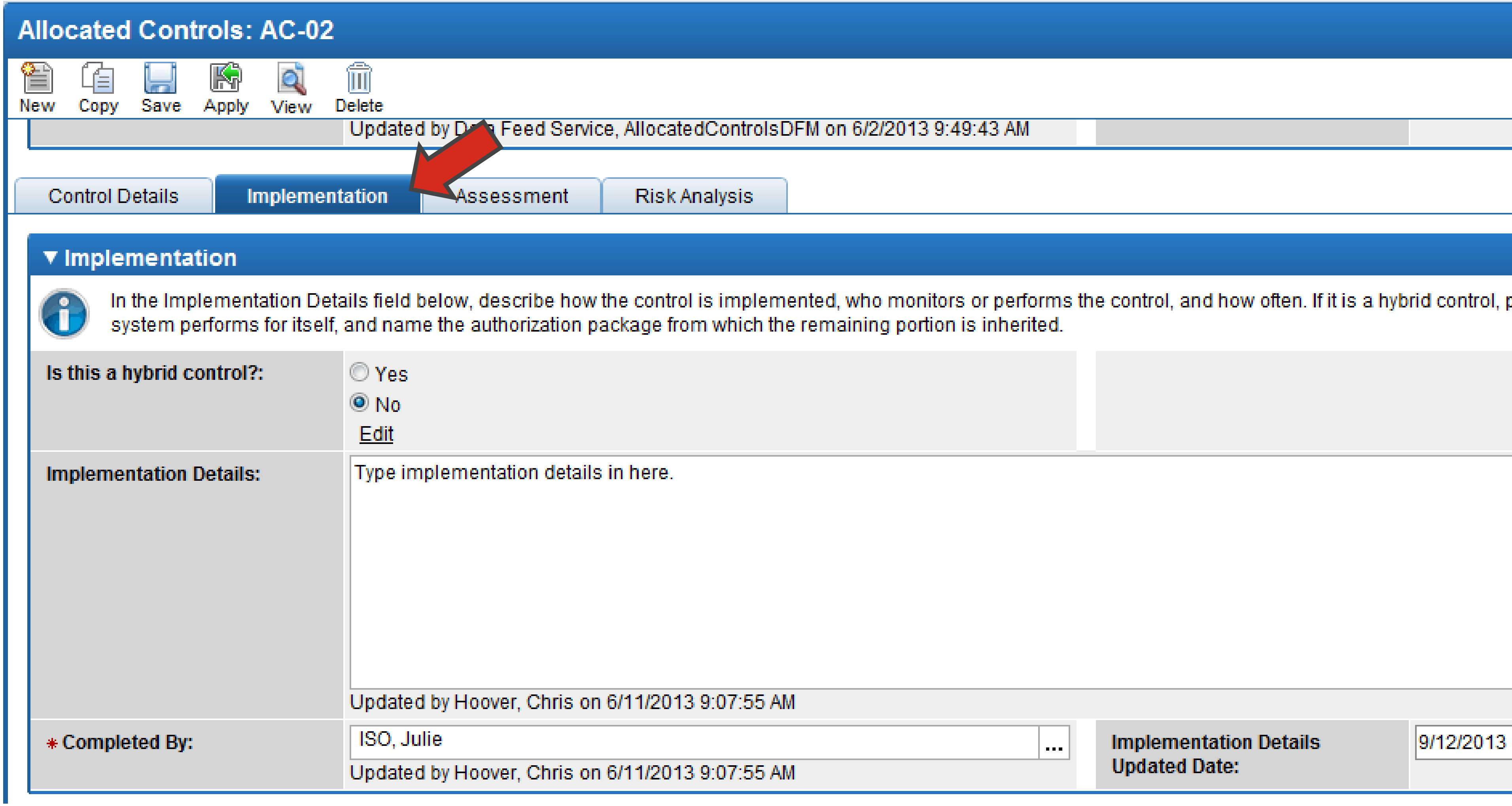
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

435-436 Privacy Methodology

Implementing / Documenting Controls



Allocated Controls: AC-02

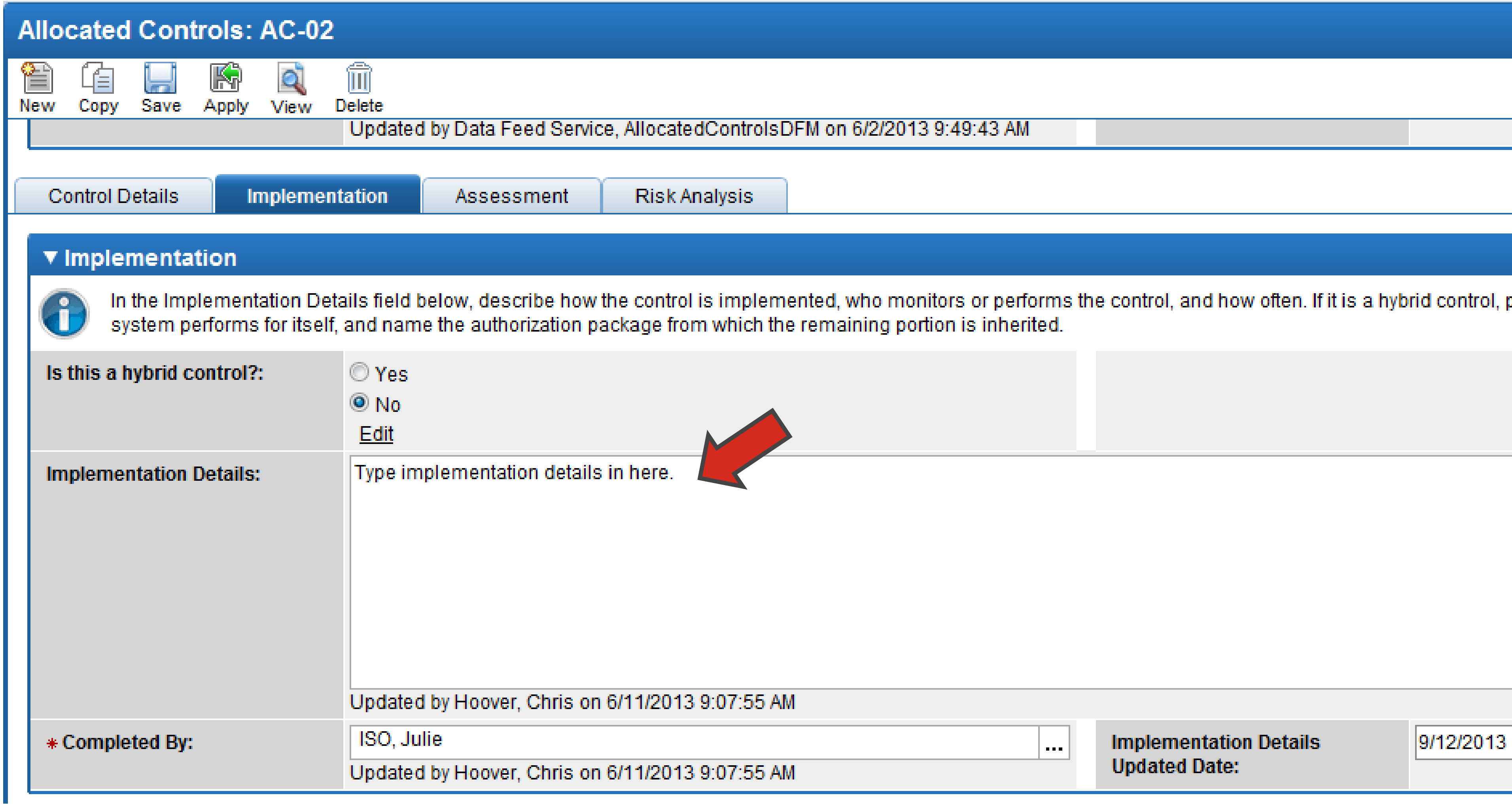
Updated by Data Feed Service, AllocatedControlsDFM on 6/2/2013 9:49:43 AM

▼ Implementation

In the Implementation Details field below, describe how the control is implemented, who monitors or performs the control, and how often. If it is a hybrid control, p
system performs for itself, and name the authorization package from which the remaining portion is inherited.

Is this a hybrid control?:	○ Yes ● No Edit
Implementation Details:	Type implementation details in here. Updated by Hoover, Chris on 6/11/2013 9:07:55 AM
* **Completed By:**	ISO, Julie ... Updated by Hoover, Chris on 6/11/2013 9:07:55 AM
Implementation Details Updated Date:	9/12/2013

Implementing / Documenting Controls

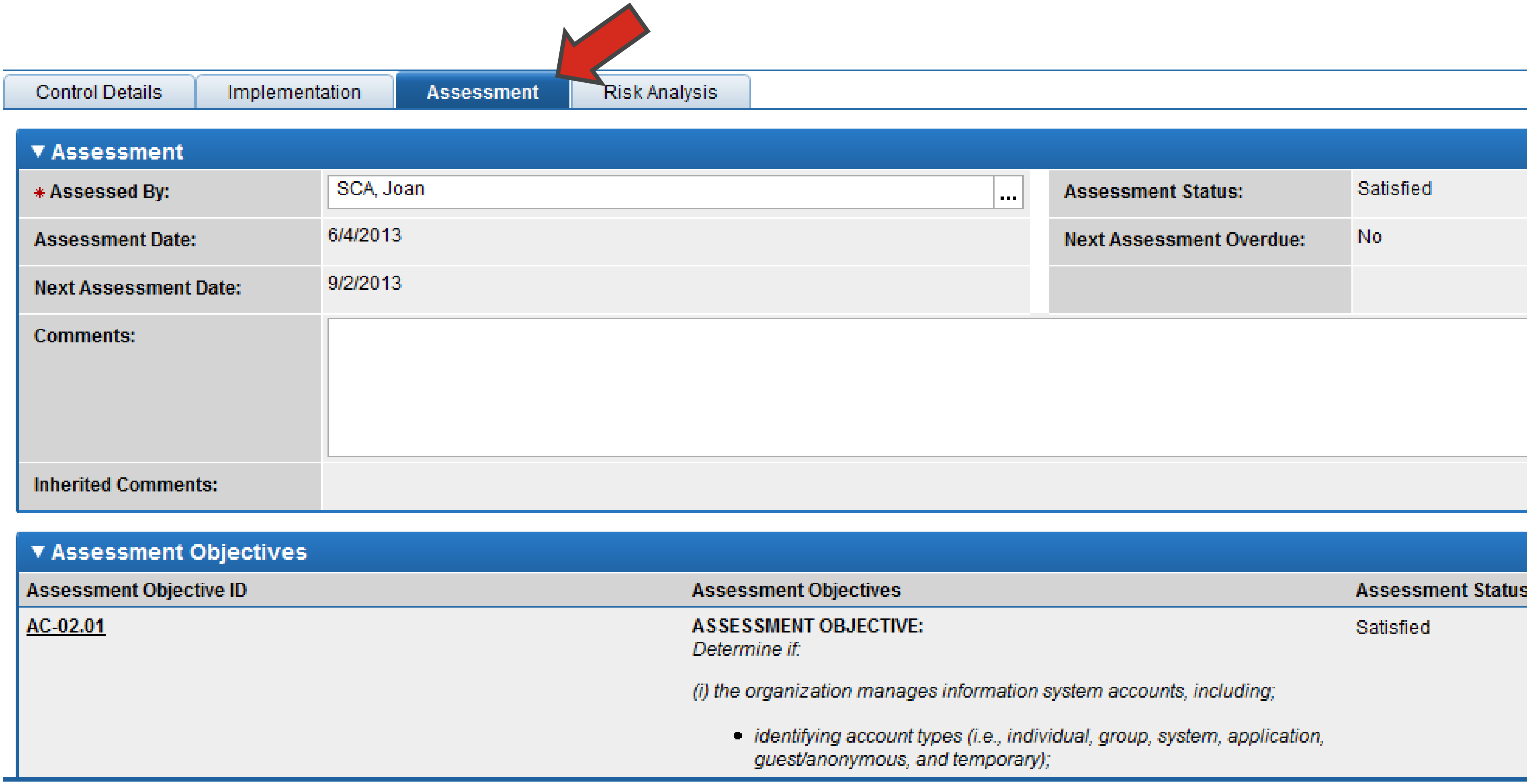


Updated by Data Feed Service, AllocatedControlsDFM on 6/2/2013 9:49:43 AM

In the Implementation Details field below, describe how the control is implemented, who monitors or performs the control, and how often. If it is a hybrid control, p
system performs for itself, and name the authorization package from which the remaining portion is inherited.

Is this a hybrid control?:	○ Yes ● No Edit
Implementation Details:	Type implementation details in here. Updated by Hoover, Chris on 6/11/2013 9:07:55 AM
* **Completed By:**	ISO, Julie ... Updated by Hoover, Chris on 6/11/2013 9:07:55 AM
Implementation Details Updated Date:	9/12/2013

Assessing Controls



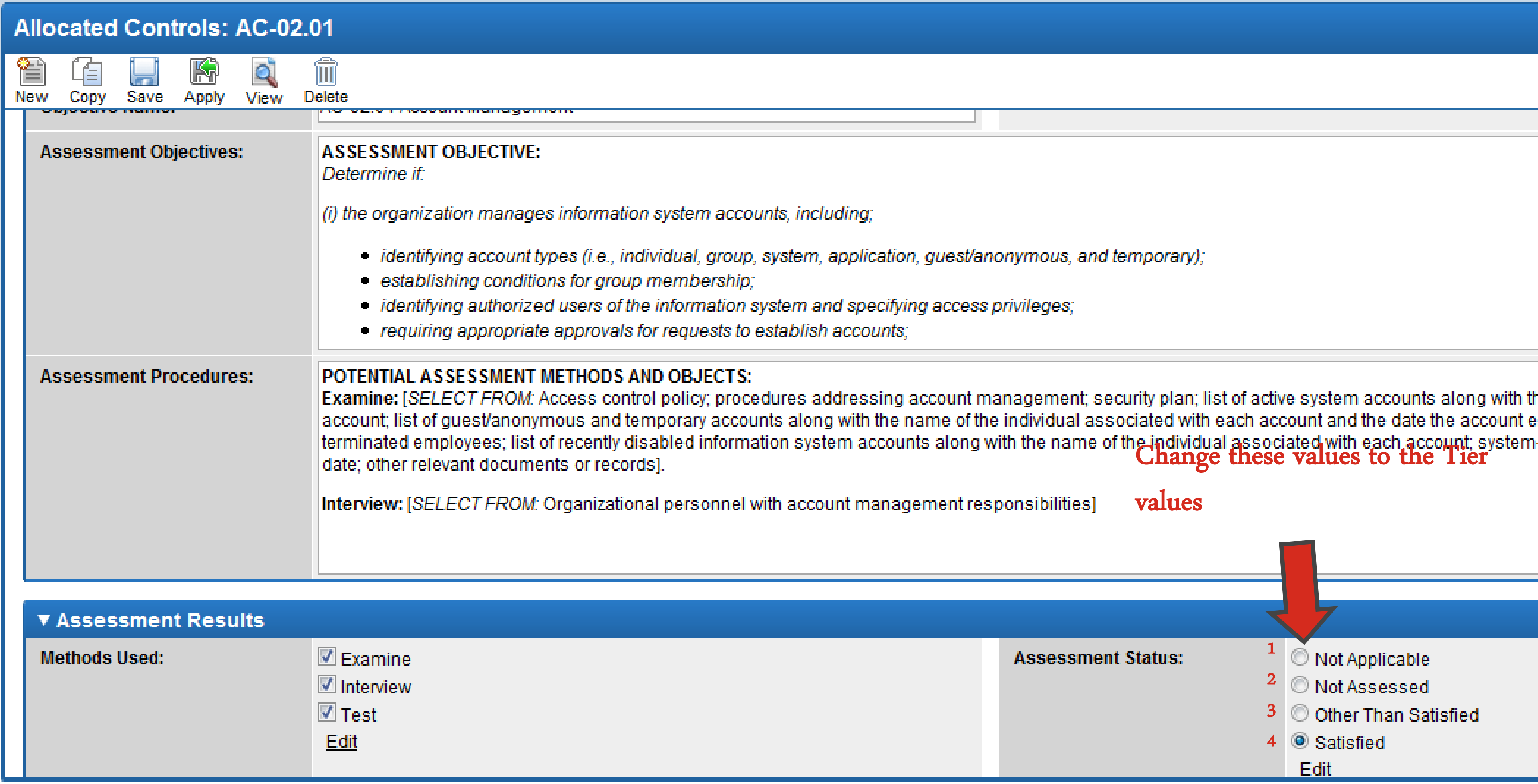
▼ Assessment

* Assessed By:	SCA, Joan ...	Assessment Status:	Satisfied
Assessment Date:	6/4/2013	Next Assessment Overdue:	No
Next Assessment Date:	9/2/2013		
Comments:			
Inherited Comments:			

▼ Assessment Objectives

Assessment Objective ID	Assessment Objectives	Assessment Status
AC-02.01	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages information system accounts, including;* • *identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);*	Satisfied

Assessing Controls



Assessment Objectives:

ASSESSMENT OBJECTIVE:
Determine if:

(i) the organization manages information system accounts, including;

- *identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);*
- *establishing conditions for group membership;*
- *identifying authorized users of the information system and specifying access privileges;*
- *requiring appropriate approvals for requests to establish accounts;*

Assessment Procedures:

POTENTIAL ASSESSMENT METHODS AND OBJECTS:
Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; security plan; list of active system accounts along with th account; list of guest/anonymous and temporary accounts along with the name of the individual associated with each account and the date the account e terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system- date; other relevant documents or records].

Interview: [*SELECT FROM:* Organizational personnel with account management responsibilities]

Change these values to the Tier values

Assessment Results

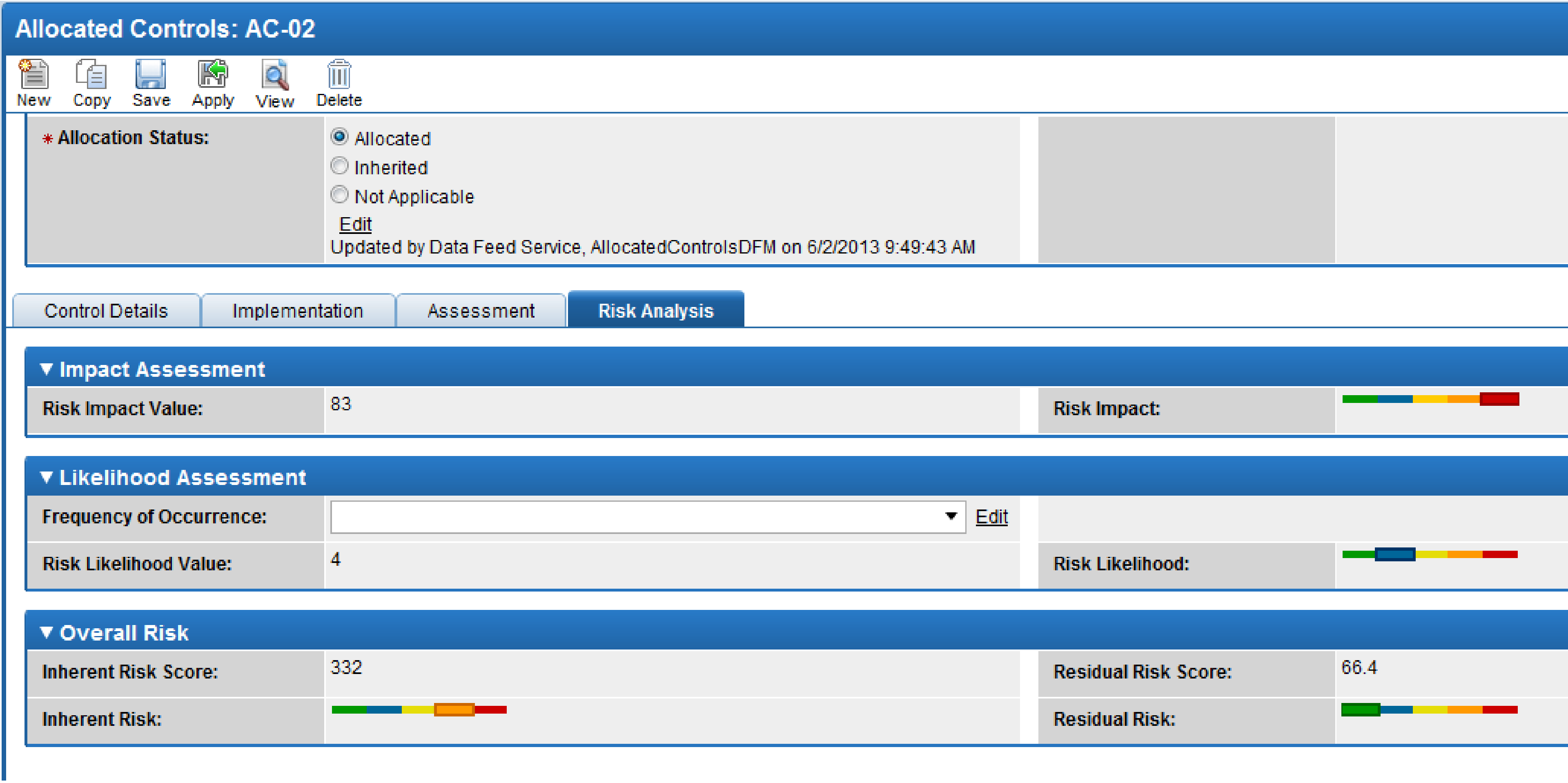
Methods Used:

☑ Examine
☑ Interview
☑ Test
Edit

Assessment Status:

1 ○ Not Applicable
2 ○ Not Assessed
3 ○ Other Than Satisfied
4 ● Satisfied
Edit

Measuring/Scoring Gaps



Allocated Controls: AC-02

* Allocation Status:	● Allocated ○ Inherited ○ Not Applicable Edit Updated by Data Feed Service, AllocatedControlsDFM on 6/2/2013 9:49:43 AM

▼ Impact Assessment

Risk Impact Value:	83	Risk Impact:	

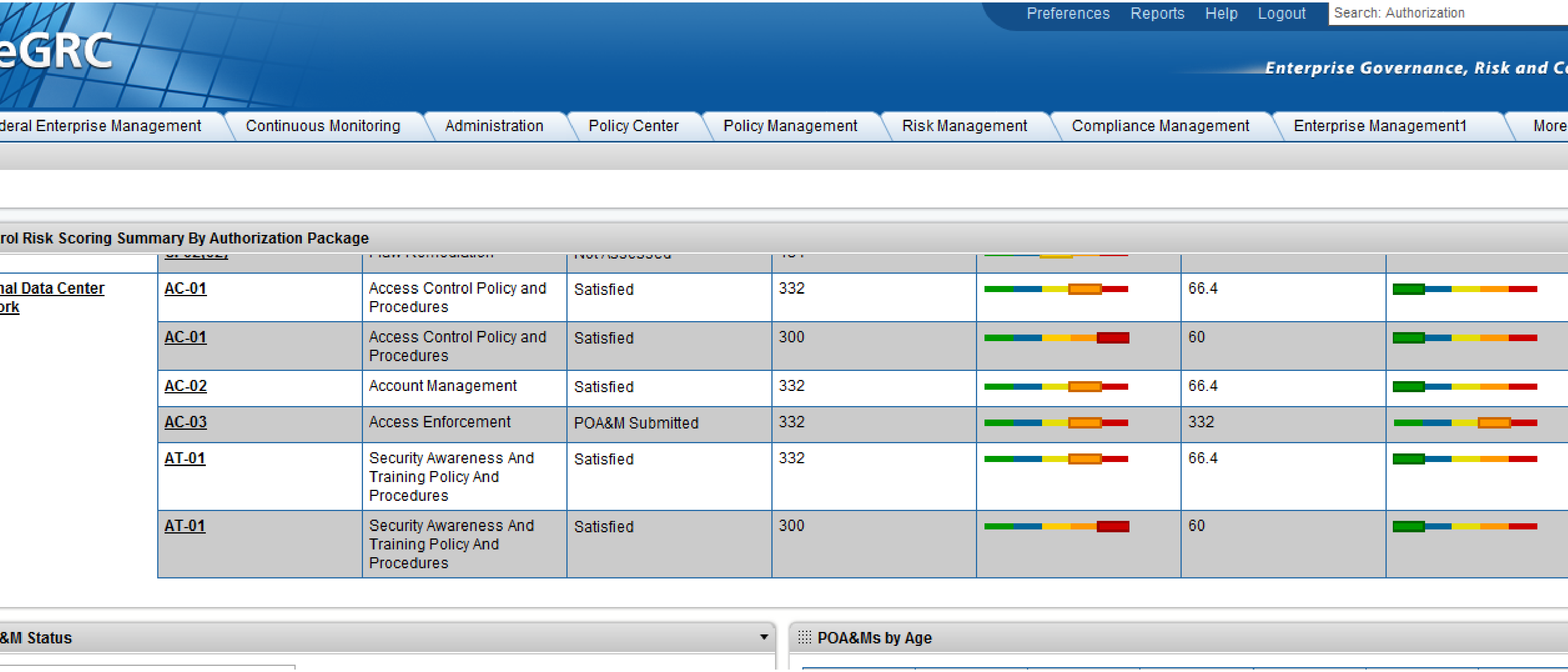
▼ Likelihood Assessment

Frequency of Occurrence:	▾ Edit		
Risk Likelihood Value:	4	Risk Likelihood:	

▼ Overall Risk

Inherent Risk Score:	332	Residual Risk Score:	66.4
Inherent Risk:		Residual Risk:	

Measuring/Scoring Gaps



rol Risk Scoring Summary By Authorization Package

	SI-02(02)	Flaw Remediation	Not Assessed	[illegible]			
nal Data Center ork	AC-01	Access Control Policy and Procedures	Satisfied	332		66.4	
	AC-01	Access Control Policy and Procedures	Satisfied	300		60	
	AC-02	Account Management	Satisfied	332		66.4	
	AC-03	Access Enforcement	POA&M Submitted	332		332	
	AT-01	Security Awareness And Training Policy And Procedures	Satisfied	332		66.4	
	AT-01	Security Awareness And Training Policy And Procedures	Satisfied	300		60	

&M Status

POA&Ms by Age

Preliminary CSF Workflow

412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

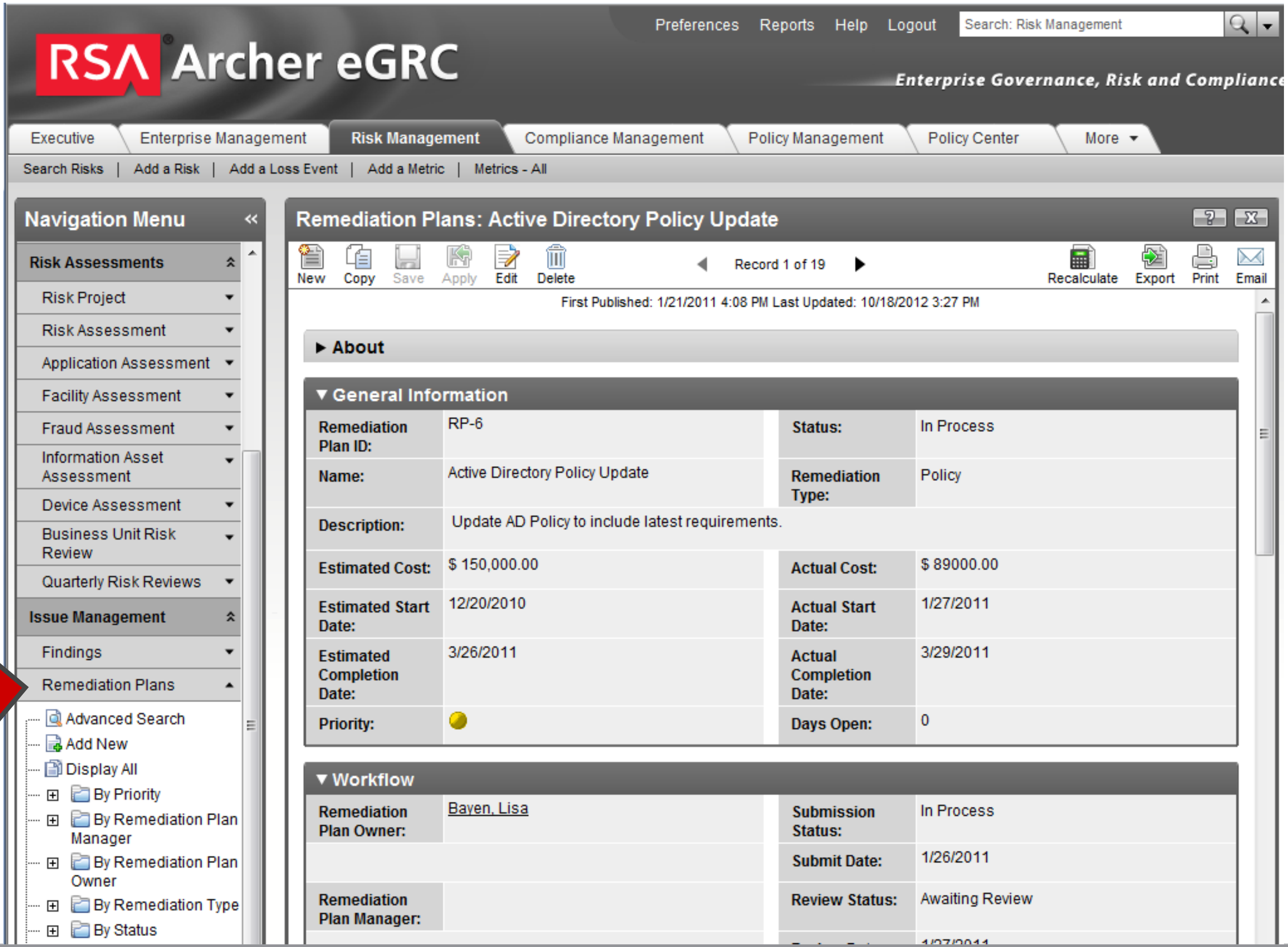
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

435-436 Privacy Methodology

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

Action Plan = RSA Archer Remediation Plan



Remediation Plans: Active Directory Policy Update

First Published: 1/21/2011 4:08 PM Last Updated: 10/18/2012 3:27 PM

▶ About

▼ General Information

Remediation Plan ID:	RP-6	Status:	In Process
Name:	Active Directory Policy Update	Remediation Type:	Policy
Description:	Update AD Policy to include latest requirements.		
Estimated Cost:	$ 150,000.00	Actual Cost:	$ 89000.00
Estimated Start Date:	12/20/2010	Actual Start Date:	1/27/2011
Estimated Completion Date:	3/26/2011	Actual Completion Date:	3/29/2011
Priority:	●	Days Open:	0

▼ Workflow

Remediation Plan Owner:	Bayen, Lisa	Submission Status:	In Process
		Submit Date:	1/26/2011
Remediation Plan Manager:		Review Status:	Awaiting Review

Preliminary CSF Workflow

412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

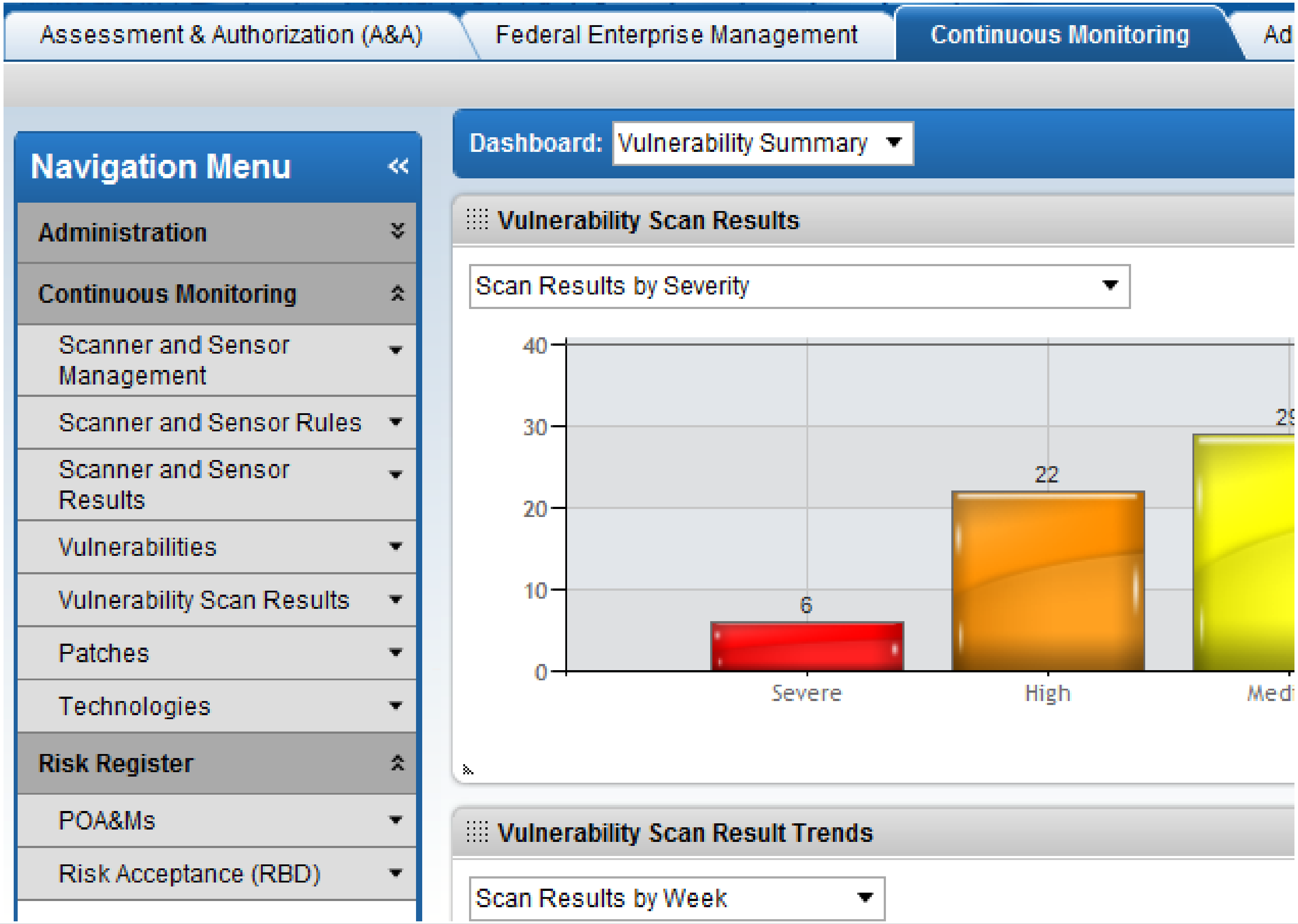
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

435-436 Privacy Methodology

Continuous Monitoring - Automated



Assessment & Authorization (A&A) | Federal Enterprise Management | Continuous Monitoring | Ad

Navigation Menu «

- Administration
- Continuous Monitoring
  - Scanner and Sensor Management
  - Scanner and Sensor Rules
  - Scanner and Sensor Results
  - Vulnerabilities
  - Vulnerability Scan Results
  - Patches
  - Technologies
- Risk Register
  - POA&Ms
  - Risk Acceptance (RBD)

Dashboard: Vulnerability Summary

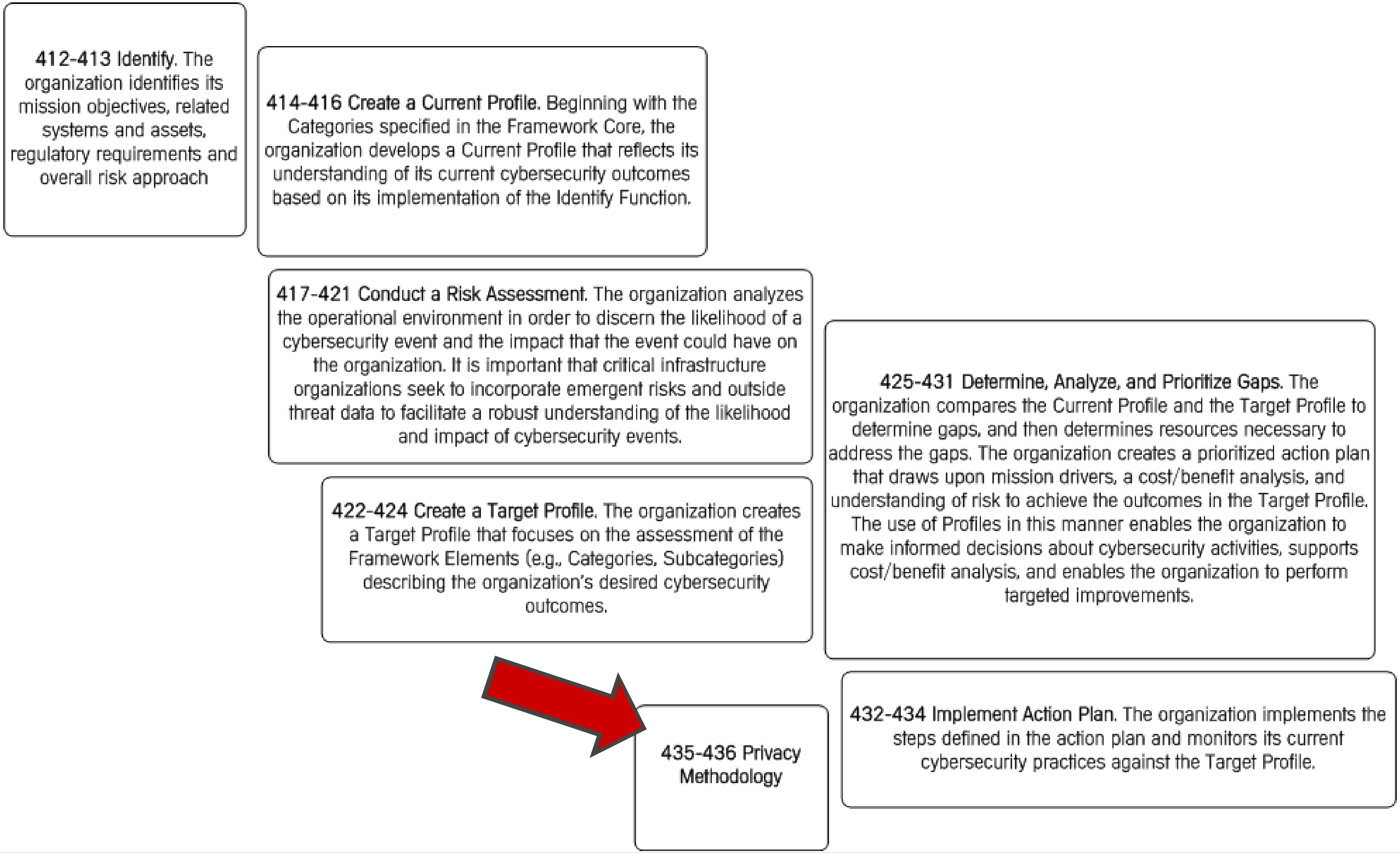
Vulnerability Scan Results

Scan Results by Severity

Vulnerability Scan Result Trends

Scan Results by Week

Preliminary CSF Workflow



412-413 Identify. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach

414-416 Create a Current Profile. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

417-421 Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

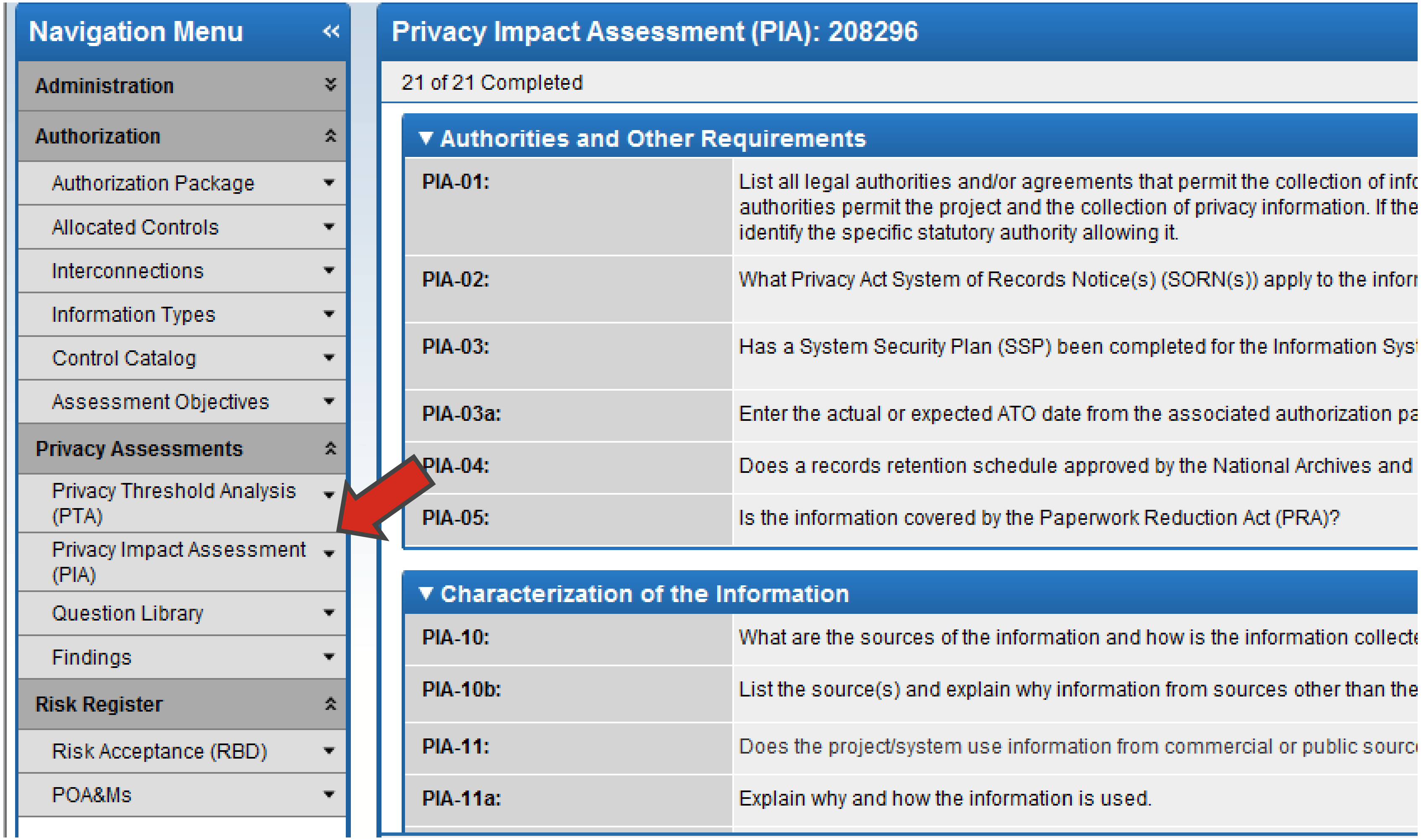
422-424 Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

425-431 Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

435-436 Privacy Methodology

432-434 Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

Augmenting Privacy Controls



Privacy Impact Assessment (PIA): 208296

21 of 21 Completed

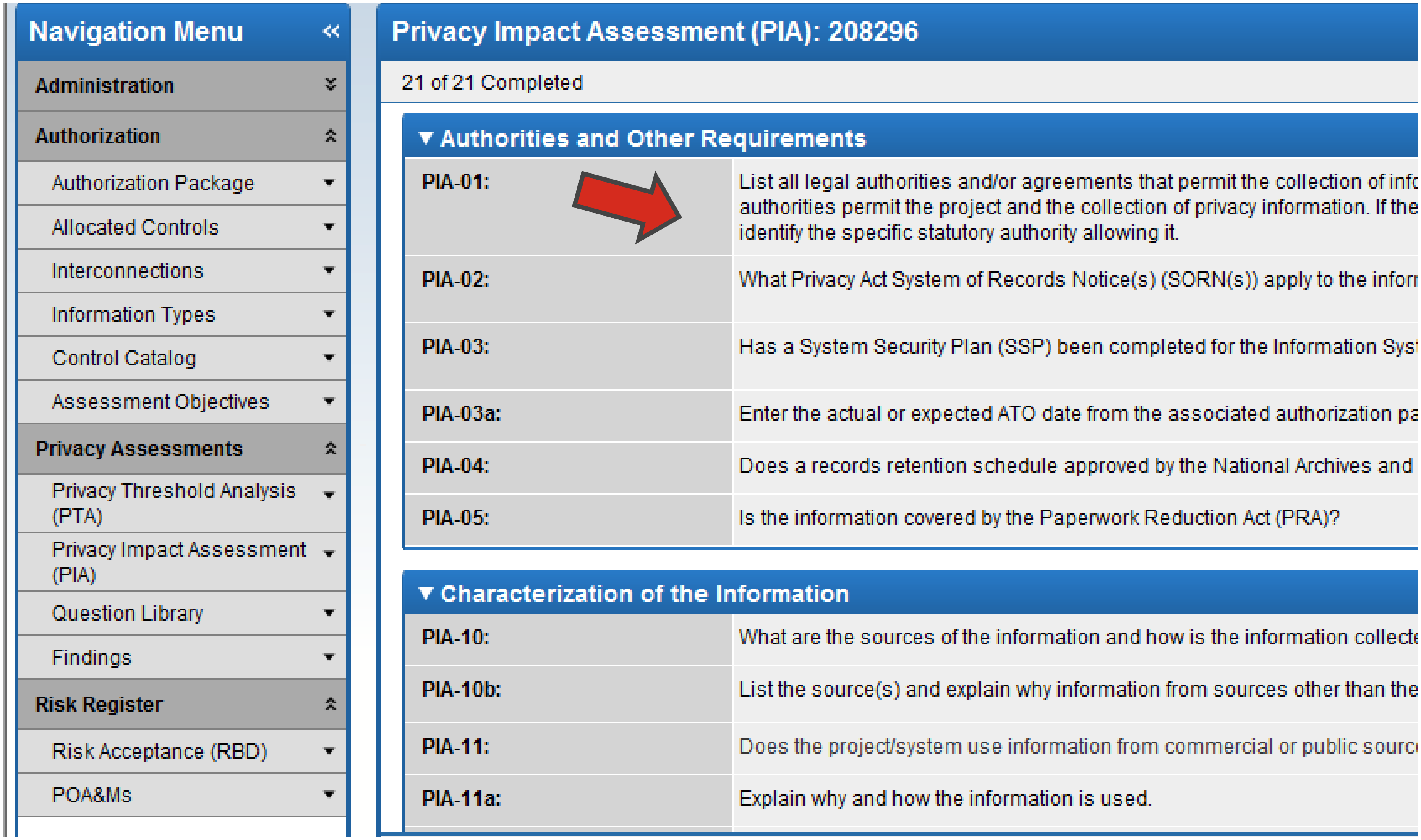
▼ Authorities and Other Requirements

PIA-01:	List all legal authorities and/or agreements that permit the collection of info authorities permit the project and the collection of privacy information. If the identify the specific statutory authority allowing it.
PIA-02:	What Privacy Act System of Records Notice(s) (SORN(s)) apply to the inforr
PIA-03:	Has a System Security Plan (SSP) been completed for the Information Syst
PIA-03a:	Enter the actual or expected ATO date from the associated authorization pa
PIA-04:	Does a records retention schedule approved by the National Archives and
PIA-05:	Is the information covered by the Paperwork Reduction Act (PRA)?

▼ Characterization of the Information

PIA-10:	What are the sources of the information and how is the information collect
PIA-10b:	List the source(s) and explain why information from sources other than the
PIA-11:	Does the project/system use information from commercial or public sourc
PIA-11a:	Explain why and how the information is used.

Augmenting Privacy Controls



Privacy Impact Assessment (PIA): 208296

21 of 21 Completed

▼ Authorities and Other Requirements

PIA-01:	List all legal authorities and/or agreements that permit the collection of info authorities permit the project and the collection of privacy information. If the identify the specific statutory authority allowing it.
PIA-02:	What Privacy Act System of Records Notice(s) (SORN(s)) apply to the inforr
PIA-03:	Has a System Security Plan (SSP) been completed for the Information Sys
PIA-03a:	Enter the actual or expected ATO date from the associated authorization pa
PIA-04:	Does a records retention schedule approved by the National Archives and
PIA-05:	Is the information covered by the Paperwork Reduction Act (PRA)?

▼ Characterization of the Information

PIA-10:	What are the sources of the information and how is the information collect
PIA-10b:	List the source(s) and explain why information from sources other than the
PIA-11:	Does the project/system use information from commercial or public sourc
PIA-11a:	Explain why and how the information is used.

Questions?

chris.hoover@rsa.com

THANK YOU