CSAM Support for C&A Transformation

Cyber Security Assessment and Management (CSAM)

Five Services, One Complete C&A Solution

1 Mission/Risk-Based Policy & Implementation/Test Guidance

2 Program Management Plan

Enterprise vs System Solutions:
Cost – Schedule - Responsibilities

3 System Security Planning and Implementation

SSP 95% Documented
Emphasis on Implementation & Validation

4 Management Reporting (fully automated)

Enterprise – System – Regulatory – Ad Hoc

5 Training & Quarterly Workshops

C&A Web
Authoring Tool
& Knowledge Base

Annual Computer Security Applications Conference (ACSAC) 2007
December 13, 2007

Cyber Security Assessment & Management

CSAM Partnership

Shared Service Center

CSAM PARTNERSHIP

USAID
DOC
DOE
DOI
DOL
DOT
NSF
Treasury
SEC

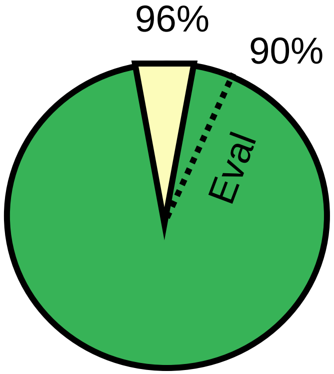
FTC
IMLS
USDA
DOJ

Others
Pending

IT Security Performance Dashboard

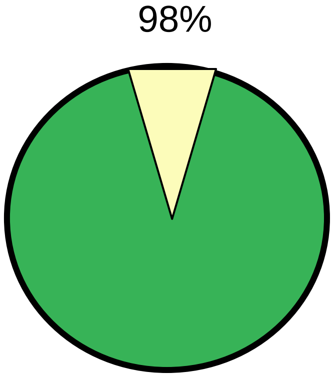
(Executive Level)

% Controls Implemented



Control Category	% Impl	POA&M
Risk & IT Security Mgmt	96	96
Vulnerability Mgmt	85	94
Incident Response & Cont Planning	100	N/A
Awareness & Training	97	100

% Critical Controls Implemented



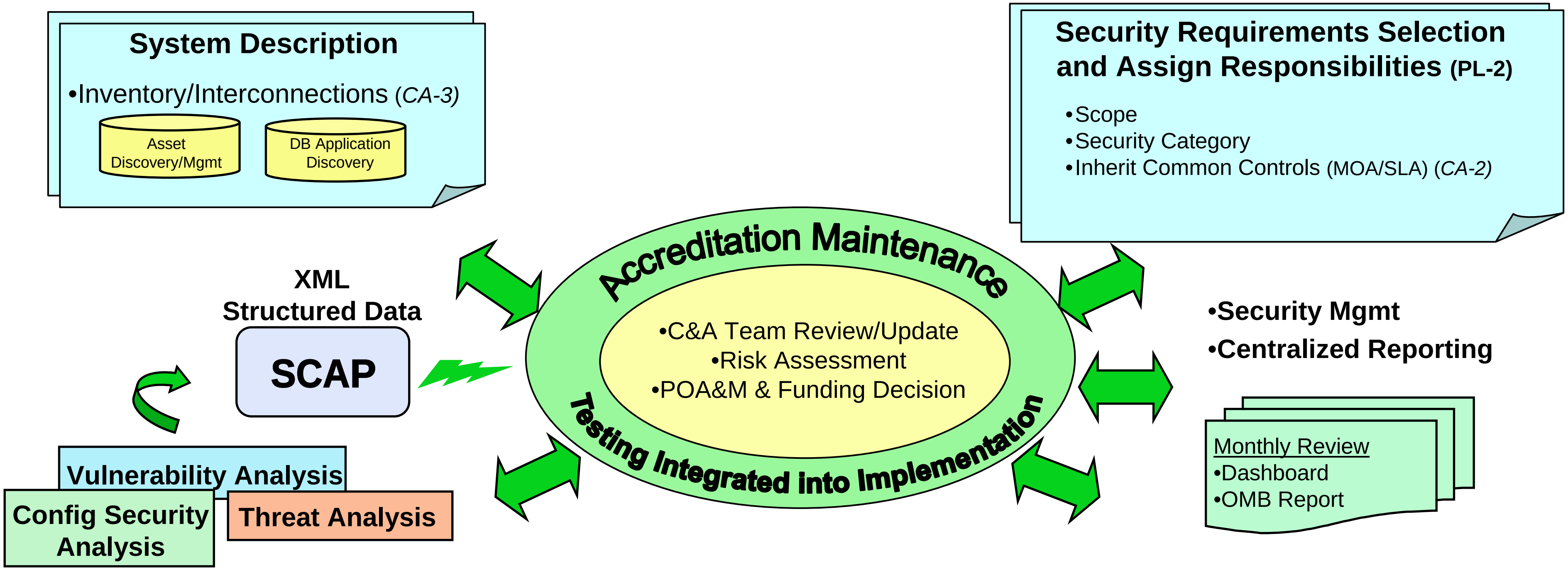
Control Category	% Impl	POA&M
Risk & IT Security Mgmt	98	96
Vulnerability Mgmt	96	96
Incident Response & Cont Planning	100	N/A
Awareness & Training	96	100

Mission Based IT Security Priorities

IT Security Program Initiatives Strategic Goals/ Objectives	Risk & IT Security Mgmt			Vulnerability Mgmt			Incident Mgmt & Contingency Mgmt		Awareness Trng & Security Trng for IT Professionals	
	Risk Assessment & Mgmt; RA, PL, CA	Acquisition Config Mgmt; SA, CM	Personnel/Physical& Environ Security; PS, & PE	Access Control; AC	Systems & Comm Protect, Integrity; SC, SI, MA,AU	Media Protection; MP	Incident Response: IR	Contingency Planning: CP	Security Awareness & ROB	IT Security Trng for IT Professionals
I. Prevent Terrorism and Promote the Nation's Security	**Very High**			**Critical**			**Very High**		**High**	
Supporting Objectives & Programs	VH	M	VH	C	C	VH	VH	VH	H	H
	VH	VH	H	C	C	VH	VH	VH	H	H
	VH	VH	H	C	VH	VH	VH	H	H	H
II. Prevent Crime, Enforce the Law and Represent the Rights and Interests of the American People	**Very High**			**Critical**			**Very High**		**High**	
Supporting Objectives & Programs	VH	VH	VH	C	C	VH	VH	VH	H	H
	VH	VH	VH	C	C	VH	VH	H	H	H
	VH	H	H	C	C	H	VH	VH	H	M
III. Ensure the Fair and Efficient Operation of the Federal Justice System	**High**			**High**			**High**		**High**	
Supporting Objectives & Programs	H	H	H	H	H	H	H	H	H	H
	H	H	H	H	H	M	H	H	H	H
	H	M	M	H	H	M	H	H	H	M

CSAM Certification & Accreditation

(DOJ IT Security Standards (FISCAM/FIPS 200/NIST 800-53)



System Description

- Inventory/Interconnections *(CA-3)*

Asset Discovery/Mgmt

DB Application Discovery

Security Requirements Selection and Assign Responsibilities (PL-2)

- Scope
- Security Category
- Inherit Common Controls (MOA/SLA) *(CA-2)*

XML Structured Data

SCAP

Accreditation Maintenance

- C&A Team Review/Update
- Risk Assessment
- POA&M & Funding Decision

Testing Integrated into Implementation

- **Security Mgmt**
- **Centralized Reporting**

Monthly Review
- Dashboard
- OMB Report

Vulnerability Analysis

Config Security Analysis

Threat Analysis

Standardizing Specifications of Content

1. Vulnerability Mgmt Plan

- Access Controls (AC 2-20)
- Vulnerability Mgmt (RA-5)
- Audit and Accountability (AU 2- 11)
- Identification and Authentication (IA 2-7)
- Systems & Communications Protection (SC 2-19)
- System and Information Integrity (SI 2-12)

Content Repositories

Asset Inventory

- Config Guides
- Vulner Analysis
- Threat Analysis
- Incident
- Response

2.
- Life Cycle Mgmt (SA-3)
- Configuration Management (PL-1)
- Exercise & Update Incident Response Plan (IR-7)
- Exercise & Update Contingency Plan (CP-10)
- Awareness & Training (AT- 2 & 3)

3.
- Physical/Environ Protection (PE-4)
- Personnel Security *(PS-8)*
- Media Protection *(MP-7)*

Cyber Security Assessment and Management (CSAM)

PRESIDENTS MANAGEMENT AGENDA
FISMA, DCID 6/3
DOJ IT SECURITY STDS
FISCAM, FIPS/NIST 800-53,

Risk-based

Management Controls

Cost + Implementation Guidance

RA-1 Risk Assessment and Procedures
PL-1 Security Planning Policy and Procedures.
SA-1 System & Services Acquisition Policy & Procedures
CA-1 Certification & Accreditation & Security Assessment Policies and Procedures.

Operational Controls

Cost + Implementation Guidance

PS-1 Personnel Security Policy & Procedures
PE-1 Physical Environmental Protection Policy & Procedures
CP-1 Contingency Planning Policy & Procedures
CM-1 Configuration Management Policy & Procedures.

Technical Controls

Cost + Implementation Guidance

IA-1 Identification and Authentication Policy & Procedures
AC-1 Access Control Policy & Procedures
AU-1 Audit & Accountability Policy & Procedures
SC-1 System & Comm Protection Policy & Procedures.

Implementation Requirements

Risk	System Controls			Common Controls		
Priority	L	M	H	L	M	H
4	X			X		
2	X	X		X	X	
2	X		X	X		X
5				X		
4	X			X		
2		X			X	
2		X			X	
2		X			X	
4	X			X		
2	X	X		X	X	
4	X			X		
2	X	X	X	X	X	X
4	X			X		
2		X	X		X	
2	X			X		
2	X			X		
2		X			X	
2		X			X	
4				X		
2		X			X	
2	X	X		X	X	
4	X			X		
2				X		
5				X		
4	X			X		
3				X		
2	X		X	X		X
3	X	X		X	X	

Test Case for Each Requirement

(SCAP where available)

Test Case nn.n.n.
Test Case CA-1.3
Test Case SA-1.1
Test Case PL-1.8

Test Case RA-1.1

- **Control Objective**
(Subordinate Objective)
- **Control Techniques**
- **Specific Criteria**
- **Prerequisite Controls**
- **Test Objective**
- **Test Set Up**
- **Test Steps**
- **Expected Results:**
- **Actual Results:**
- **Cost**

□ PASS 🟥 FAIL

Risk Assessment

Vulner Control | Vulner Level X Threat Level X Signif Level = Total Risk

Plans of Action & Milestones (POA&M)

OMB
FISMA
Reporting

Cyber Security Assessment & Mgmt

(CSAM)

Vulnerabilities Requiring Correction

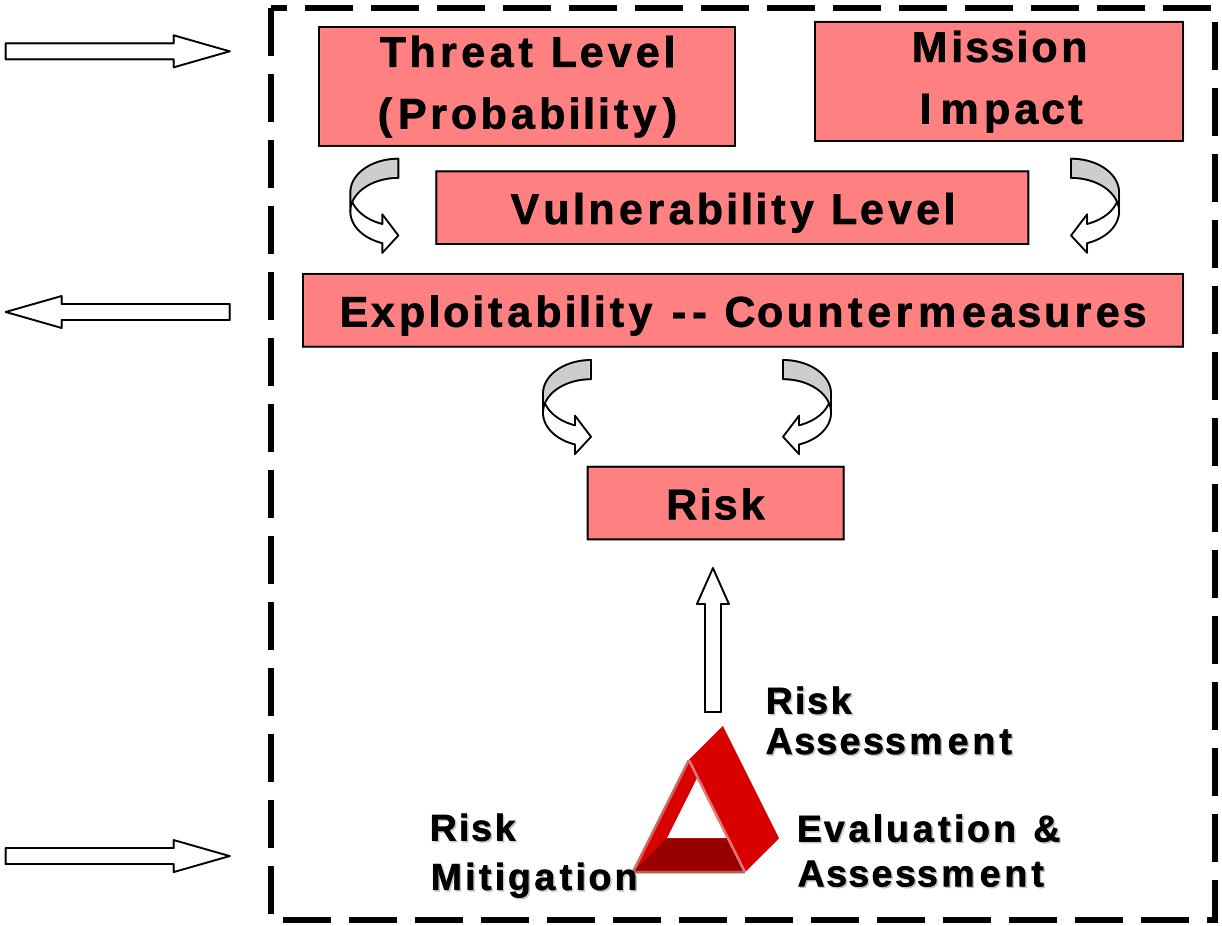
- Risk Impact: ____
- Plan Start: ____
- Actual Start: ____
- Planned Finish: ____
- Actual Finish: ____
- Validation Date:____
- Cost: ______

Risk Management Framework

- Categorize

- Select
- Supplement
- Document
- Implement

- Assess
- Authorize
- Monitor



Threat Level (Probability)

Mission Impact

Vulnerability Level

Exploitability -- Countermeasures

Risk

Risk Assessment

Risk Mitigation

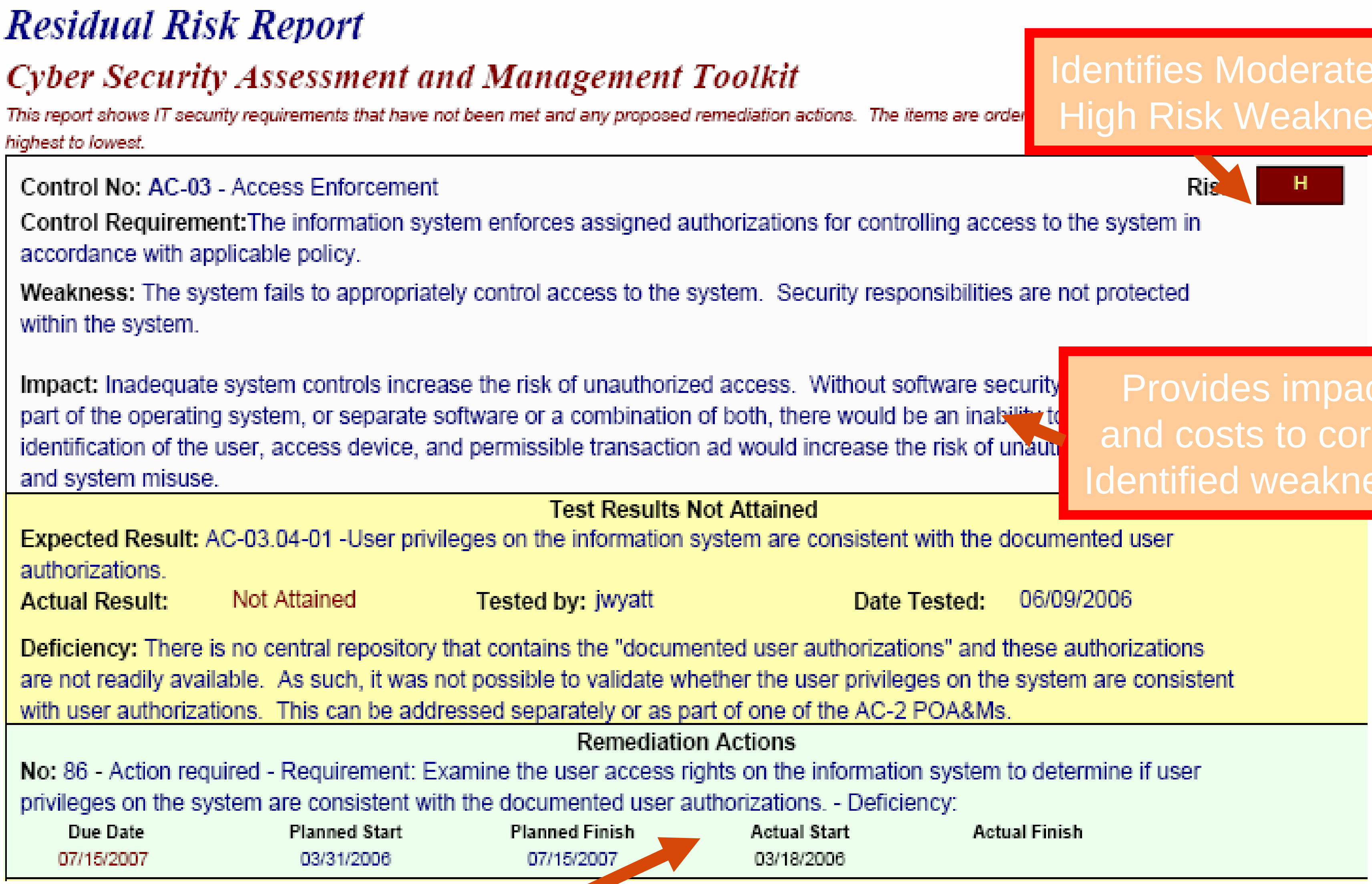
Evaluation & Assessment

Risk Assessment

Vulnerability/ Countermeasures and Threat Pairing (Security Countrols)		Vulnerability Level			X Threat Level				X Significance Level					= Total Risk
		EX-CT = Total			C+H+G-A-D = Total				DL+Ops+Equip = Total					
Vulnerability/ Countermeasures	Threat/s	Exploitability (Hi=5 Low=1)	(Actual) Counter Measures (Weak=0 Very Strong=2)	**Total (0-5)**	Capability (Hi=2 Low=1)	History/Gain (Hi=2 Low=1)	Attributable/Detectable (Easy=2 Difficult=0)	**Total (0-6)**	Loss of Life (Yes=4 No=0)	Sensitivity (Yes=4 No=0)	Ops Impact (Yes=2 No=0)	Equipment Loss (Yes=2 No=0)	**TOTAL (0-4)**	**RISK TOTAL (VL*TL*SL) (0-120) RISK Ranking**
Logical Access Controls														
Security controls can detect unauthorized access attempts.	8.1, 11.1, 12.1, 13.1, 16.1	5	3	2	2	2	0	**4** (Med)	0	2	2	0	**4**	32 (medium)
Access control software prevents fraudulent activity without collusion.	6.1, 8.1, 11.1, 12.1, 13.1, 16.1	4	2	2	2	2	0	4 (Med)	0	2	2	0	**4**	32 (medium)

Vulnerability Level	
Very High	**5**
High	**4**
Medium	**3**
Low	**2**
Very Low	**1**

Risk Scale	
Very High	**> 75**
High	**55 to 75**
Medium	**19 to 54**
Low	**6 to 18**
Very Low	**< 6**



Residual Risk Report

Cyber Security Assessment and Management Toolkit

This report shows IT security requirements that have not been met and any proposed remediation actions. The items are order highest to lowest.

Control No: AC-03 - Access Enforcement

Ris H

Control Requirement: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Weakness: The system fails to appropriately control access to the system. Security responsibilities are not protected within the system.

Impact: Inadequate system controls increase the risk of unauthorized access. Without software security part of the operating system, or separate software or a combination of both, there would be an inability to identification of the user, access device, and permissible transaction ad would increase the risk of unaut and system misuse.

Test Results Not Attained

Expected Result: AC-03.04-01 -User privileges on the information system are consistent with the documented user authorizations.

Actual Result: Not Attained **Tested by:** jwyatt **Date Tested:** 06/09/2006

Deficiency: There is no central repository that contains the "documented user authorizations" and these authorizations are not readily available. As such, it was not possible to validate whether the user privileges on the system are consistent with user authorizations. This can be addressed separately or as part of one of the AC-2 POA&Ms.

Remediation Actions

No: 86 - Action required - Requirement: Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations. - Deficiency:

Due Date	Planned Start	Planned Finish	Actual Start	Actual Finish
07/15/2007	03/31/2006	07/15/2007	03/18/2006	

Identifies Moderate and High Risk Weaknesses

Provides impacts and costs to correct Identified weaknesses

Documents POA&M to correct weaknesses

SCAP

Security Content Automation Program

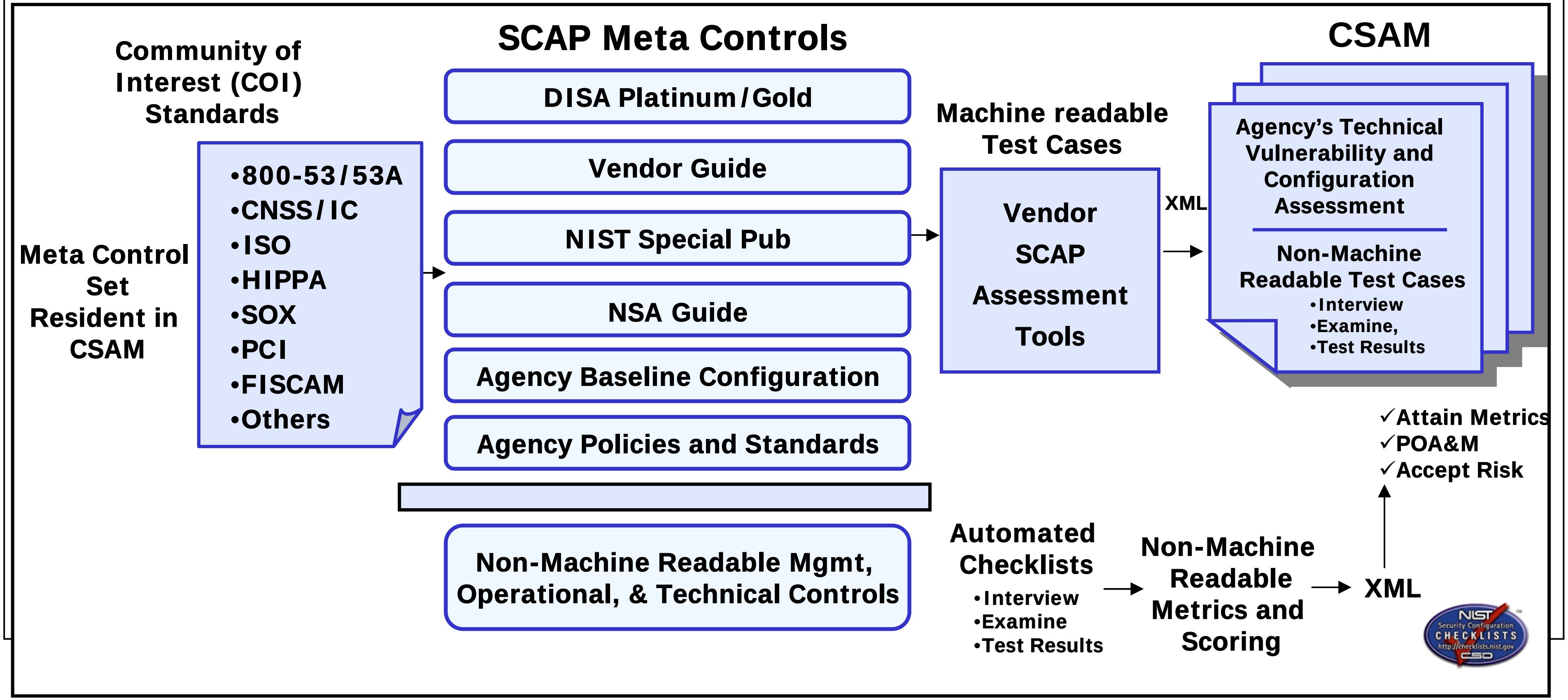
Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

Security Content Automation Program

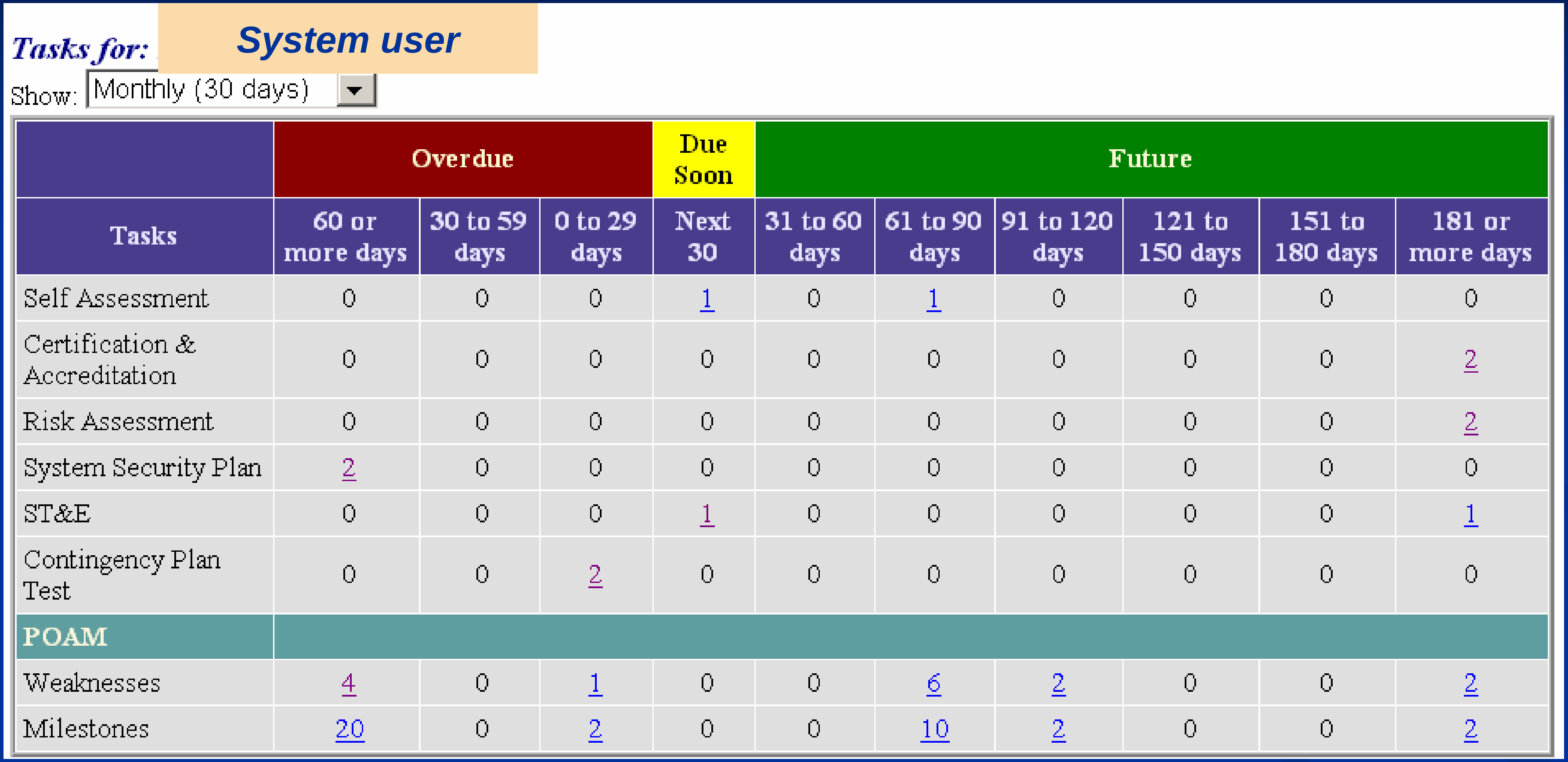
automating compliance checking, vulnerability management, and security measurement

Address http://nvd.nist.gov/scap/scap.cfm



Community of Interest (COI) Standards
•800-53/53A
•CNSS/IC
•ISO
•HIPPA
•SOX
•PCI
•FISCAM
•Others
Meta Control Set Resident in CSAM
SCAP Meta Controls
DISA Platinum/Gold
Vendor Guide
NIST Special Pub
NSA Guide
Agency Baseline Configuration
Agency Policies and Standards
Non-Machine Readable Mgmt, Operational, & Technical Controls
Machine readable Test Cases
Vendor SCAP Assessment Tools
XML
CSAM
Agency's Technical Vulnerability and Configuration Assessment
Non-Machine Readable Test Cases
•Interview
•Examine,
•Test Results
✓Attain Metrics
✓POA&M
✓Accept Risk
Automated Checklists
•Interview
•Examine
•Test Results
Non-Machine Readable Metrics and Scoring
XML
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

My Schedule – Tasking Synopsis



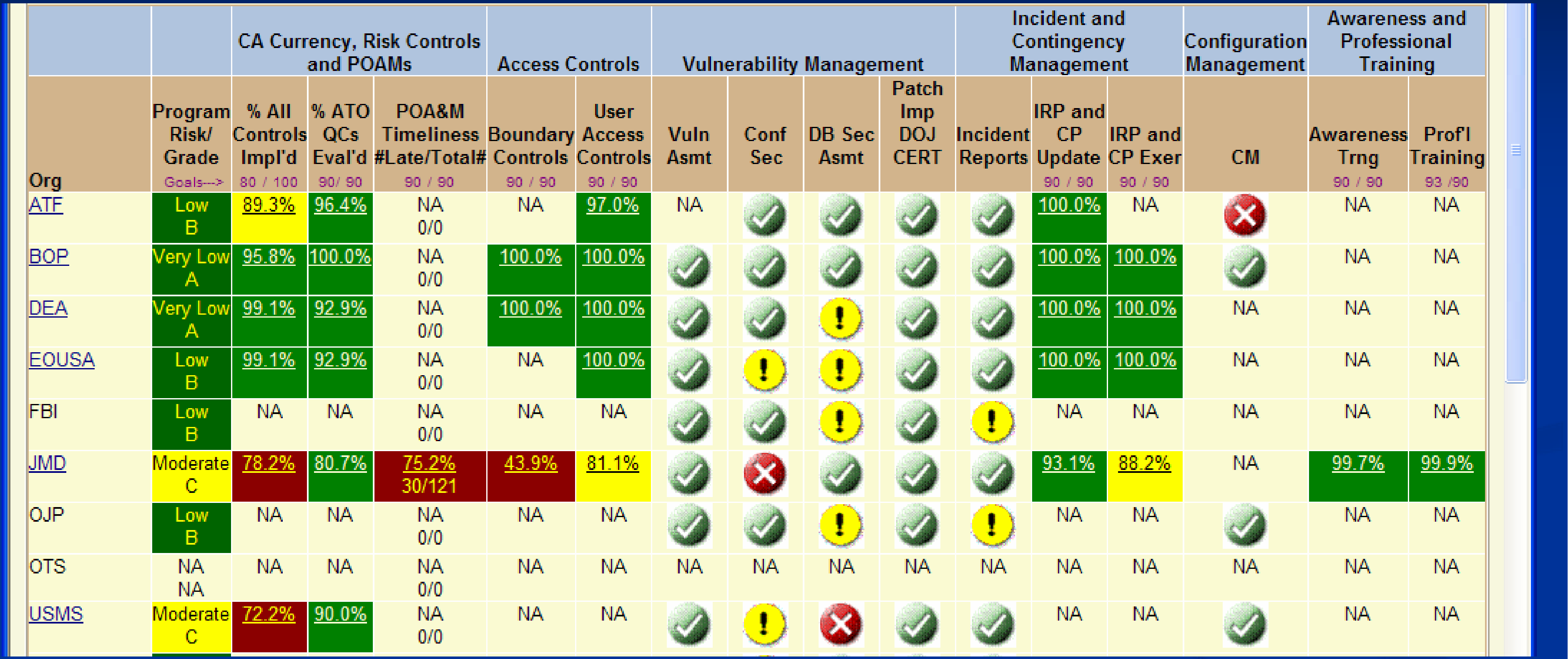
Tasks for: **System user**

Show: Monthly (30 days) ▼

	Overdue			Due Soon	Future					
Tasks	**60 or more days**	**30 to 59 days**	**0 to 29 days**	**Next 30**	**31 to 60 days**	**61 to 90 days**	**91 to 120 days**	**121 to 150 days**	**151 to 180 days**	**181 or more days**
Self Assessment	0	0	0	1	0	1	0	0	0	0
Certification & Accreditation	0	0	0	0	0	0	0	0	0	2
Risk Assessment	0	0	0	0	0	0	0	0	0	2
System Security Plan	2	0	0	0	0	0	0	0	0	0
ST&E	0	0	0	1	0	0	0	0	0	1
Contingency Plan Test	0	0	2	0	0	0	0	0	0	0
POAM										
Weaknesses	4	0	1	0	0	6	2	0	0	2
Milestones	20	0	2	0	0	10	2	0	0	2

Drill-down links you directly to the point of interest.

Performance Dashboard



		CA Currency, Risk Controls and POAMs			Access Controls		Vulnerability Management				Incident and Contingency Management			Configuration Management	Awareness and Professional Training	
Org	Program Risk/ Grade	% All Controls Impl'd	% ATO QCs Eval'd	POA&M Timeliness #Late/Total#	Boundary Controls	User Access Controls	Vuln Asmt	Conf Sec	DB Sec Asmt	Patch Imp DOJ CERT	Incident Reports	IRP and CP Update	IRP and CP Exer	CM	Awareness Trng	Prof'l Training
	Goals--->	80 / 100	90/ 90	90 / 90	90 / 90	90 / 90						90 / 90	90 / 90		90 / 90	93 /90
ATF	Low B	89.3%	96.4%	NA 0/0	NA	97.0%	NA	✓	✓	✓	✓	100.0%	NA	✗	NA	NA
BOP	Very Low A	95.8%	100.0%	NA 0/0	100.0%	100.0%	✓	✓	✓	✓	✓	100.0%	100.0%	✓	NA	NA
DEA	Very Low A	99.1%	92.9%	NA 0/0	100.0%	100.0%	✓	✓	!	✓	✓	100.0%	100.0%	NA	NA	NA
EOUSA	Low B	99.1%	92.9%	NA 0/0	NA	100.0%	✓	!	!	✓	✓	100.0%	100.0%	NA	NA	NA
FBI	Low B	NA	NA	NA 0/0	NA	NA	✓	✓	!	✓	!	NA	NA	NA	NA	NA
JMD	Moderate C	78.2%	80.7%	75.2% 30/121	43.9%	81.1%	✓	✗	✓	✓	✓	93.1%	88.2%	NA	99.7%	99.9%
OJP	Low B	NA	NA	NA 0/0	NA	NA	✓	✓	!	✓	!	NA	NA	✓	NA	NA
OTS	NA NA	NA	NA	NA 0/0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
USMS	Moderate C	72.2%	90.0%	NA 0/0	NA	NA	✓	!	✗	✓	✓	NA	NA	✓	NA	NA

- Clicking on the green, green checkmark, the yellow exclamation point, or the red X pops up the explanation of why they were given that grade.

- Clicking on the POAMS columns give a list of POA&Ms that are late for the org selected.

- Clicking on the Training % shows the Comments and the actual numbers that make up the percentages.