Unit #3

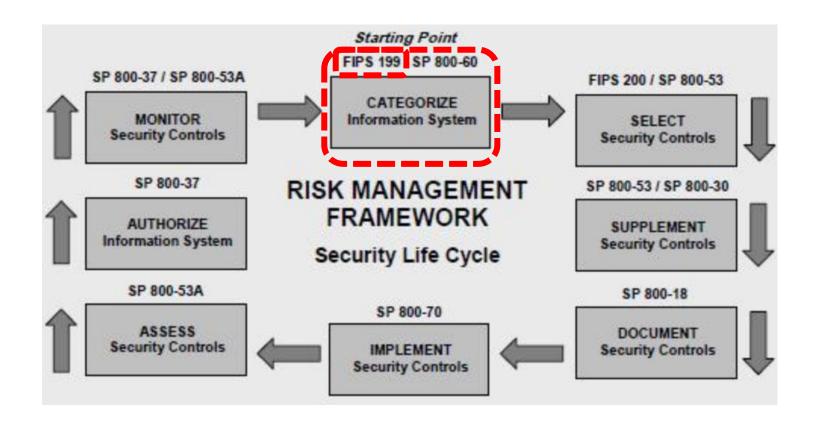
MIS5214

Planning and Policy

Agenda

- Risk Management Framework and IS Security Categorization
- Mapping Information Types to Security Categorizations
- Exercise: How to assess and information security policy?
- Exercise Determine Information and Information System Types and provisional security categorization
- Security Control Baselines review
 - Minimum Security Controls and Security Control Baselines
 - Security Control Families
- Risk Assessment Controls

Risk Management Framework



Risk Assessment based on security objectives and impact ratings for information and information system

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900

February 2004



U.S. DEPARTMENT OF COMMERCE Donald L. Evans, Secretary

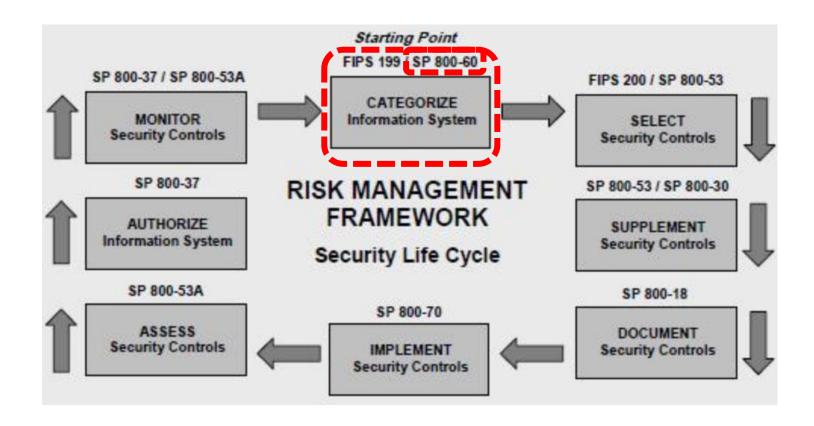
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

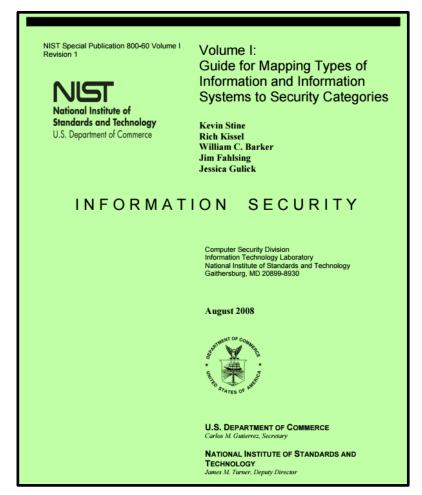
Arden L. Bement, Jr., Director

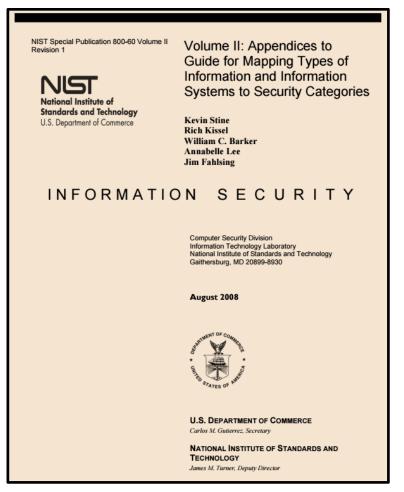
		POTENTIAL IMPACT	
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. 4

Risk Management Framework



Mapping IS Types to Security Categories





https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

NIST Special Publication 800-60 Volume I Revision 1

National Institute of Standards and Technology U.S. Department of Commerce Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Jim Fahlsing Jessica Gulick

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

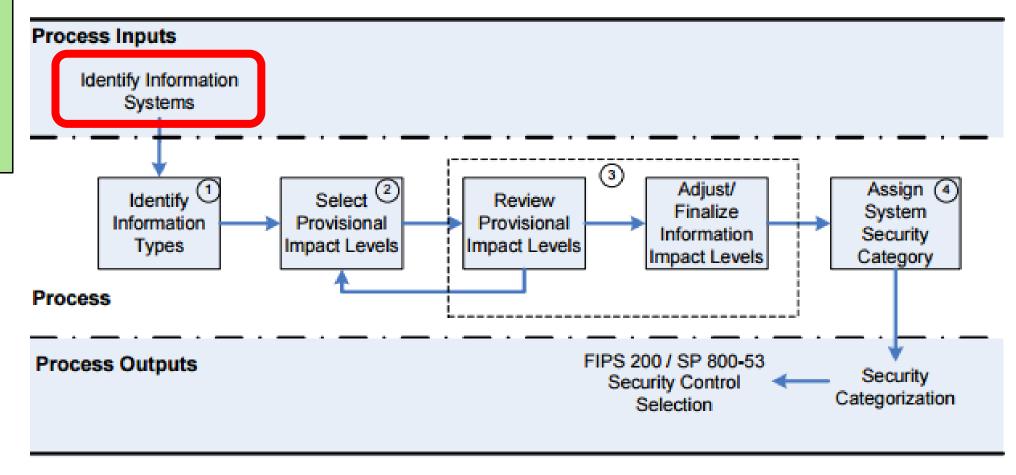
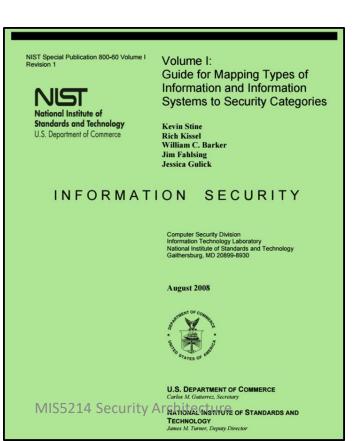


Figure 2: SP 800-60 Security Categorization Process Execution

2 Broad types of Information and Information Systems

1. Mission-based Information & Information Systems

2. Management and Support Information & Information Systems



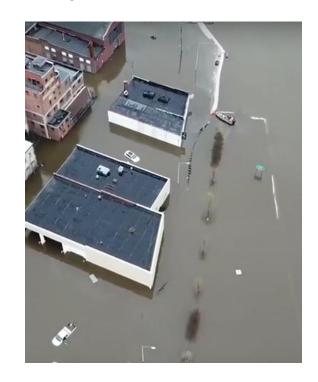
Mission-based Information and Information Systems

- 1. Defense and National Security
- 2. Homeland Security
- 3. Intelligence Operations
- 4. Disaster Management
- 5. International Affairs and Commerce
- 6. Natural Resources
- 7. Energy
- 8. Environmental Management
- 9. Economic Development
- 10. Community and Social Services
- 11. Transportation
- 12. Education
- 13. Workforce Management

- 14. Health
- 15. Income Security
- 16. Law Enforcement
- 17. Litigation and Judicial Activities
- 18. Federal Correctional Activities
- 19. General Sciences and Innovation
- 20. Knowledge Creation and Management
- 21. Regulatory Compliance and Enforcement
- 22. Public Goods Creation and Management
- 23. Federal Financial Assistance
- 24. Credit and Insurance
- 25. Transfers to State/Local Governments
- 26. Direct Services for Citizens

Disaster Management Information System Example











Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Jim Fahlsing Jessica Gulick

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg. MD 20899-8930

August 200



U.S. DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AN TECHNOLOGY

2 Broad Types of Information and Information Systems

1. Mission-based Information & Information Systems

- 2. Management and Support Information & Information Systems
 - i. Services Delivery Support Functions
 - ii. Government Resource Management Functions

Services Delivery Support Functions and Information Types

- 1. Controls and Oversight
- 2. Regulatory Development
- 3. Planning and Budgeting
- 4. Internal Risk Management and Mitigation
- 5. Revenue Collection
- 6. Public Affairs
- 7. Legislative Relations
- 8. General Government

Example Management & Support Information & Information Systems

Table 5: Service	es Delivery Support Functions and In	formation Types ¹⁵
C.2.1 Controls and Oversight	C.2.4 Internal Risk Management &	C.2.8 General Government
Corrective Action (Policy/Regulation)	Mitigation	Central Fiscal Operations
Program Evaluation	Contingency Planning	Legislative Functions
Program Monitoring	Continuity of Operations	Executive Functions
C.2.2 Regulatory Development	Service Recovery	Central Property Management
Policy & Guidance Development	C.2.5 Revenue Collection	Central Personnel Management
Public Comment Tracking	Debt Collection	Taxation Management
Regulatory Creation	User Fee Collection	Central Records & Statistics
Rule Publication	Federal Asset Sales	Management
C.2.3 Planning & Budgeting	C.2.6 Public Affairs	Income Information
Budget Formulation	Customer Services	Personal Identity and Authentication
Capital Planning	Official Information Dissemination	Entitlement Event Information
Enterprise Architecture	Product Outreach	Representative Payee Information
Strategic Planning	Public Relations	General Information
Budget Execution	C.2.7 Legislative Relations	
Workforce Planning	Legislation Tracking	
Management Improvement	Legislation Testimony	
Budgeting & Performance Integration	Proposal Development	
Tax & Fiscal Policy	Congressional Liaison Operations	

Example Resource Management Functions & Information Types

- 1. Administrative Management
- 2. Financial Management
- 3. Human Resources Management
- 4. Supply Chain Management
- 5. Information and Technology Management

Example Management and Support Information and Information Systems

C.3.1 Administrative Management	C.3.3 Human Resource Management	C.3.5 Information & Technology
Facilities, Fleet, and Equipment	HR Strategy	Management
Management	Staff Acquisition	System Development
Help Desk Services	Organization & Position Mgmt	Lifecycle/Change Management
Security Management	Compensation Management	System Maintenance
Travel	Benefits Management	IT Infrastructure Maintenance
Workplace Policy Development &	Employee Performance Mgmt	Information Security
Management	Employee Relations	Record Retention
C.3.2 Financial Management	Labor Relations	Information Management
Accounting	Separation Management	System and Network Monitoring
Funds Control	Human Resources Development	Information Sharing
Payments	C.3.4 Supply Chain Management	
Collections and Receivables	Goods Acquisition	
Asset and Liability Management	Inventory Control	
Reporting and Information	Logistics Management	
Cost Accounting/ Performance	Services Acquisition	
Measurement	-	

1. Identify Information Types

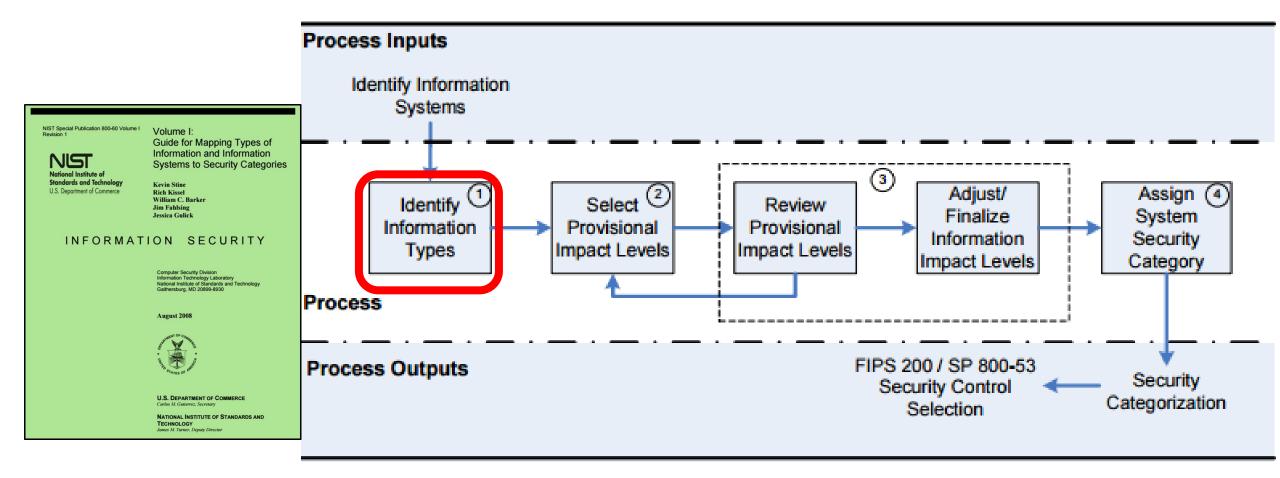


Figure 2: SP 800-60 Security Categorization Process Execution

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

Disaster Management Information Types

Table 4: Mission-Based Information

Mission Areas and Information

D.1 Defense & National Security

Strategic National & Theater Defense Operational Defense

Tactical Defense

D.2 Homeland Security

Border and Transportation Security Key Asset and Critical Infrastructure Protection

Catastrophic Defense

Executive Functions of the Executive Office of the President (EOP)

D.3 Intelligence Operations

Intelligence Planning

Intelligence Collection

Intelligence Analysis & Production Intelligence Dissemination

Intelligence Processing

D.4 Disaster Management

Disaster Monitoring and Prediction Disaster Preparedness and Planning Disaster Repair and Restoration Emergency Response

D.S International Atlairs &

Commerce

Foreign Affairs International Development and Humanitarian Aid Global Trade

D.6 Natural Resources

Water Resource Management Conservation, Marine and Land Management

Recreational Resource Management and Tourism

Apricological/Indevation and Services ture Worker Safety

D.7 Enc

Energy Supply
Energy Conservation a
Energy Resource Mana
Energy Production

D.8 Environmenta

Environmental Monito Forecasting

Environmental Remed Pollution Prevention a

D.9 Economic D

Business and Industry Intellectual Property P Financial Sector Overs

Industry Sector Income Stabilization

D.10 Community & Social Services

Homeownership Promotion

Community and Regional Development

Social Services

Postal Services

D.11 Transportation

Ground Transportation

Water Transportation

Air Transportation

Space Operations

D.12 Education

Elementary, Secondary, and Vocational Education

Higher Education

Cultural and Historic Preservation

Cultural and Historic Exhibition D.13 Workforce Management

Training and Employment Labor Rights Management

D.4 Disaster Management

Disaster Monitoring and Prediction Disaster Preparedness and Planning Disaster Repair and Restoration Emergency Response

Mode of Delivery

D.24 Credit and Insurance

Direct Loans Loan Guarantees

General Insurance

D.25 Transfers to State/ Local

Governments

Formula Grants

Project/Competitive Grants

Earmarked Grants

State Loans

D.26 Direct Services for Citizens

Military Operations Civilian Operations

D.16 Law Enforcement

Criminal Apprehension

Criminal Investigation and Surveillance

Citizen Protection

Leadership Protection

Property Protection

Substance Control

Crime Prevention

Trade Law Enforcement

D.17 Litigation & Judicial Activities

Judicial Hearings

Legal Defense

Legal Investigation

Legal Prosecution and Litigation

Resolution Facilitation

D.18 Federal Correctional Activities

Criminal Incarceration

Criminal Rehabilitation

D.19 General Sciences & Innovation

Scientific and Technological Research and Innovation

Space Exploration and Innovation

NIST Special Publication 800-60 Volume I Revision 1

National Institute of Standards and Technology Guide for Mapping Types of Information and Information

Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Jim Fahlsing

INFORMATION SECURITY

Computer Security Unision Information Technology Laboratory National Institute of Standards and Technolog Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

• 17

NIST Special Publication 800-60 Volume II Revision 1

National Institute of Standards and Technology U.S. Department of Commerce Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE

Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

James M. Turner, Deputy Director

2. Select Provisional Impact Levels for the identified information system

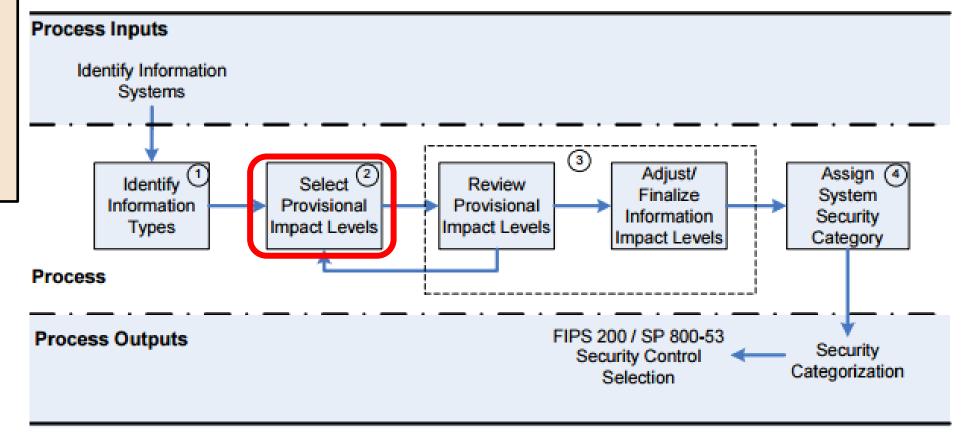


Figure 2: SP 800-60 Security Categorization Process Execution

NIST Special Publication 800-60 Volume II Revision 1



Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

James M. Turner, Deputy Director



Disaster Management Information Types

APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS	102
D.1 Defense and National Security	107
D.2 Homeland Security	108
D.2.1 Border and Transportation Security Information Type	
D.2.2 Key Asset and Critical Infrastructure Protection Information Type	110
D.2.3 Catastrophic Defense Information Type	111
D.2.4 Executive Functions of the Executive Office of the President (EOP) Information	
Туре	112
D.3 Intelligence Operations	113
D.4 Disaster Management	115
D.4.1 Disaster Monitoring and Prediction Information Type	
D.4.2 Disaster Preparedness and Planning Information Type	117
D.4.3 Disaster Repair and Restoration Information Type	
D.4.4 Emergency Response Information Type	119

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Disaster Management Information Impact

D.4 Disaster Management

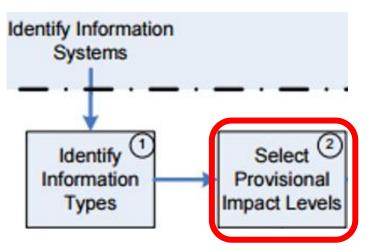
Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all physical and humanitarian disasters whether natural or man-made. Compromise of much information associated with any of the missions within the disaster management mission area may seriously impact the security of a broad range of critical infrastructures and key national assets.

Can you use...

• <u>NIST SP 800-60 V.2 R1</u> to determine the Impact Levels for the Disaster Information Types ?

Disaster Management Information Systems					
				Summary Impact	
Information Types	Confidentiality	Integrity	Availability	Level	
Disaster Monitoring and Prediction	?	?	?		
Disaster Preparedness and Planning	,	?	?		
Disaster Repair and Restoration	Ş	?	Ş		
Emergency Response Information Type	5	?	,		

Disaster Management Information Types



D.4.1 Disaster Monitoring and Prediction Information Type

Disaster monitoring and prediction involves the actions taken to predict when and where a disaster may take place and communicate that information to affected parties. [Some disaster management information occurs in humanitarian aid systems under the International Affairs and Commerce line of business (e.g., State Department disaster preparedness and planning).] The recommended provisional categorization of the disaster monitoring and protection information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

D.4.2 Disaster Preparedness and Planning Information Type

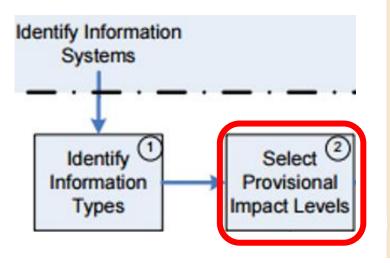
Disaster preparedness and planning involves the development of response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The recommended provisional categorization of the disaster preparedness and planning information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

D.4.3 Disaster Repair and Restoration Information Type

Disaster repair and restoration involves the cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The recommended provisional categorization of the disaster repair and restoration information type follows:

Disaster Management Information Types



D.4.4 Emergency Response Information Type

Emergency Response involves the immediate actions taken to respond to a disaster (e.g., wildfire management). These actions include providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions. Impacts to emergency response information and the information systems that process and store emergency response information could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions. The recommended provisional categorization of the emergency response information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

Question

• Can you determine Summary Impact Levels for Disaster Information Types?

Disaster Management Information Systems					
				Summary Impact	
Information Types	Confidentiality	Integrity	Availability	Level	
Disaster Monitoring and Prediction	Low	High	High	5	
Disaster Preparedness and Planning	Low	Low	Low	?	
Disaster Repair and Restoration	Low	Low	Low	?	
Emergency Response Information Type	Low	High	High	5	

Answer...

• Summary Impact Levels for the Disaster Information Types

Disaster Management Information Systems					
				Summary Impact	
Information Types	Confidentiality	Integrity	Availability	Level	
Disaster Monitoring and Prediction	Low	High	High	High	
Disaster Preparedness and Planning	Low	Low	Low	Low	
Disaster Repair and Restoration	Low	Low	Low	Low	
Emergency Response Information Type	Low	High	High	High	

Question -

• Can you determine Overall Impact Levels for Disaster Information Types?

Disaster Management Information Systems					
				Summary	
Information Types	Confidentiality	Integrity	Availability	Impact Level	
Disaster Monitoring and Prediction	Low	High	High	High	
Disaster Preparedness and Planning	Low	Low	Low	Low	
Disaster Repair and Restoration	Low	Low	Low	Low	
Emergency Response Information Type	Low	High	High	High	
Information System Impact Ratings:	?	?	?		

Answer

• Overall Impact Levels for the Disaster Information Types

Disaster Management Information Systems					
1	C		A! - L !!!	Summary	
Information Types	Confidentiality		Availability	Level	
Disaster Monitoring and Prediction	Low	High	High	High	
Disaster Preparedness and Planning	Low	Low	Low	Low	
Disaster Repair and Restoration	Low	Low	Low	Low	
Emergency Response Information Type	Low	High	High	High	
Information System Impact Ratings:	Low	High	High		

Question

• Can you determine overall Impact Level of a system of Disaster Information Systems?

Disaster Management Information Systems					
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level	
Disaster Monitoring and Prediction	Low	High	High	High	
Disaster Preparedness and Planning	Low	Low	Low	Low	
Disaster Repair and Restoration	Low	Low	Low	Low	
Emergency Response Information Type	Low	High	High	High	
Information System Impact Ratings:	Low	High	High	?	

Answer

• Overall Impact Level of Disaster Information Systems

Disaster Management Information Systems					
Information Tunes	Confidentiality	Intogritu	Availability	Summary Impact	
Information Types Disaster Monitoring and Prediction	Confidentiality Low	Integrity High	Availability High	Level High	
Disaster Preparedness and Planning	Low	Low	Low	Low	
Disaster Repair and Restoration	Low	Low	Low	Low	
Emergency Response Information Type	Low	High	High	High	
Information System Impact Ratings:	Low	High	High	High	
Information System Impact Ratings:	Low	High	High	High	

NIST Special Publication 800-60 Volume II Revision 1

National Institute of Standards and Technology U.S. Department of Commerce Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE

Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

James M. Turner, Deputy Director

3. Adjust Information Impact Level

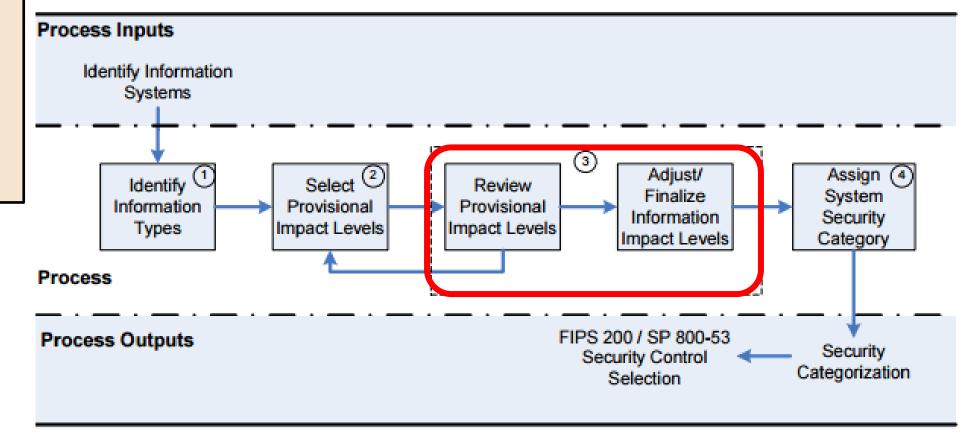


Figure 2: SP 800-60 Security Categorization Process Execution

To adjust preliminary impact levels...

Use NIST SP 800 60 V2R1

- ...looking at the "Special Factors" affecting CIA impact levels for each Disaster Management information type
- How might we adjust the impact levels?

Disaster Management Information Systems					
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level	
Disaster Monitoring and Prediction	Low	High	High	High	
Disaster Preparedness and Planning	Low	Low	Low	Low	
Disaster Repair and Restoration	Low	Low	Low	Low	
Emergency Response Information Type	Low	High	High	High	
Information System Impact Ratings:	Low	High	High	High	

NIST Special Publication 800-60 Volume II Revision 1

National Institute of Standards and Technology U.S. Department of Commerce Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE

Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY James M. Turner, Deputy Director

U.S. Denomination of Con-

2. Select Provisional Impact Levels for the identified information system

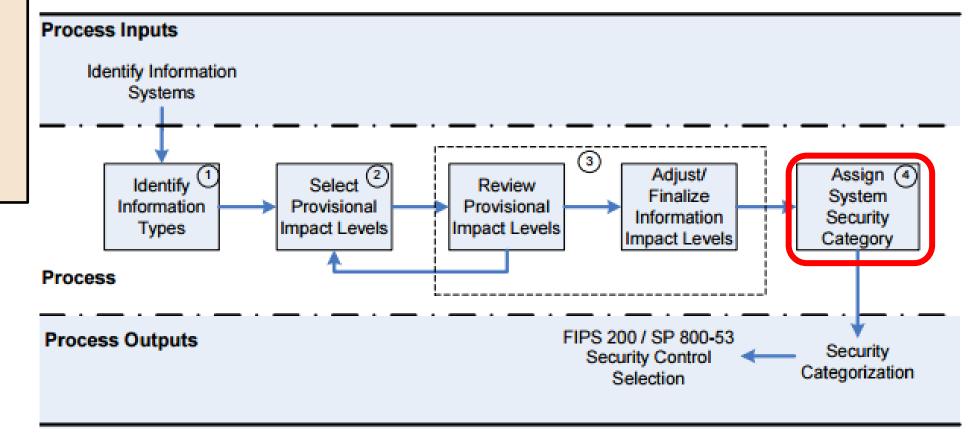
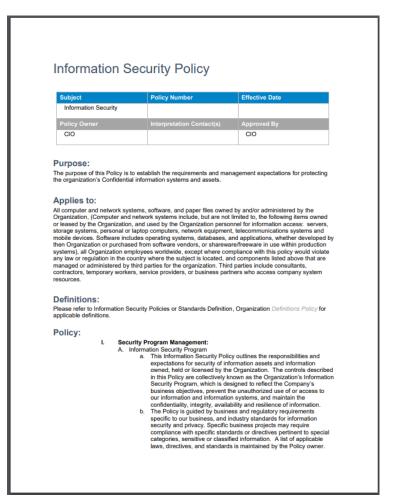


Figure 2: SP 800-60 Security Categorization Process Execution

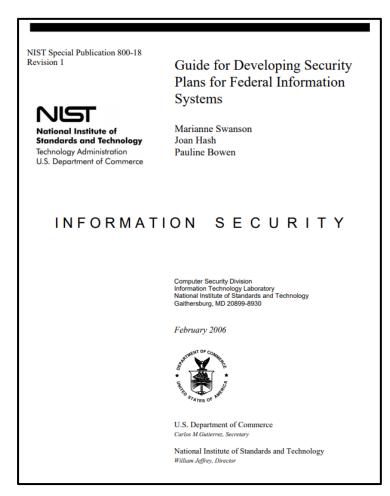
Exercise: How would you approach assessing the completeness (breadth & depth) of the <u>Generic Information Security Policy</u> example?





Teams in Breakout Rooms

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 classes of NIST SP 800-18 provide a good framework for assessing completeness of Information Security Policies and controls



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 Control Classes of NIST SP 800-18 provide a framework for assessing completeness of Information Security Policies and controls

Control	Control Family	Implemented	Partial	Planned	Alternate	NA	System	Empty	FedRamp	Completeness?
Class	Control value	implemented	Faitiai	Flamed	Aitemate	1965	System	Linkty	reunamp	
Management	Risk Assessment	2	5	1	2	1	11		10	
Management	Planning	1	2	1			4	2	6	
Management	System & Service Acquisition						0	22	22	
Management	Security Assessments & Authorization				1		1	14	15	
Technical	Identification & Authentication	9	3	8		9	29		27	
Technical	Access Control	4	3	28	1	13	49		43	
Technical	Audit & Accountability	1	3	13		4	21		19	
Technical	System & Communication Protection	17	8	9	1	5	40		32	
Operational	Personnel Security	6	1			2	9		9	
Operational	Physical & Environmental Protection					19	19	1	20	
Operational	Contingency Planning	1	2	24	II.		27		24	
Operational	Configuration Management	8	6	11		5	30	1	26	
Operational	Maintenance						0	11	11	
Operational	System & Information Integrity		5	16		8	33		28	
Operational	Media Protection	2				3	5	7	10	
Operational	Incident Response						0	18	18	
Operational	Awareness & Training			5			5		5	
	Total:	55	38	116	5	69	283	76	325	

Exercise

Using NIST SP 800-60, find a preliminary categorization for the following information system and adjust the categorization based on your analysis – present justifications for both preliminary and adjusted categorizations

Purpose: The system has two overarching purposes:

- 1. For clients it is a system intended to help understand sewage and storm water collection and treatment systems (i.e. pipe networks, pump stations, and treatment plants) and their capacities, overflow characteristics and controls
- 2. For the firm the system is intended to provide revenue through pay by clients for direct use of the service(s) of the system

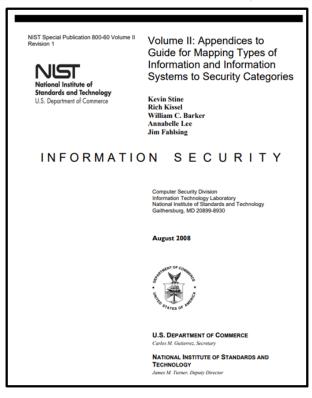
Users:

- 1. Municipal and regional water and sewer utilities and governmental organizations will use the system to help plan capital improvement, operations, and maintenance of sewer systems (i.e. treatment plants and sewage collection networks)
- 2. External consultants helping municipal and regional water and sewer utilities plan capital improvement, operations, and maintenance of sewer systems
- 3. The firm's technical information system development staff will work directly on the information system to provide, maintain, enhance and extend the services of the information system

Below is a preliminary categorization for the information system based on NIST SP 800-60 Vol

Business Area	Information Type ID	Information Type	Confidentiality	Integrity	Availability	Information Type Categorization	,	System Categorization
Environmental Management	D.8.3	Pollution Prevention and Control	Low	Low	Low	Low		
Public Goods Creation & Management	D.22.3	Public Resources, Facility and Infrastructure Management	Low	Low	Low	Low	Low	
		Tenant Data	Low	Low	Low	Low		
Information & Technology Management	C.3.5.5	Information Security	Low	Moderate	Low	Moderate		Moderate
Information & Technology Management	C.3.5.6	Record Retention	Low	Low	Low	Low	Moderate	Woderate
Information & Technology Management	C.3.5.7	Information Management	Low	Moderate	Low	Moderate	Moderate	
Information & Technology Management	C.3.5.8	System and Network Monitoring	Moderate	Moderate	Low	Moderate		
		System Data	Moderate	Moderate	Low	Moderate		

NIST Special Publication 800-60 Volume I Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories National Institute of Standards and Technology Kevin Stine U.S. Department of Commerce Rich Kissel William C. Barker Jim Fahlsing Jessica Gulick INFORMATION SECURITY Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 August 2008 U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND

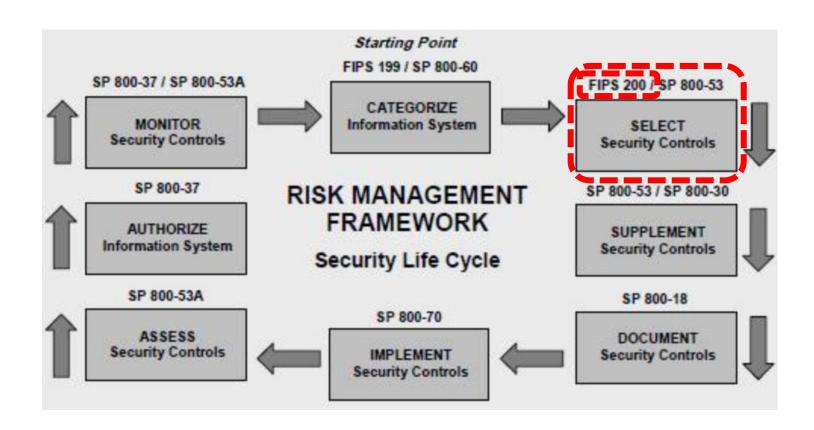




Agenda

- ✓ Risk Management Framework and IS Security Categorization
- ✓ Mapping Information Types to Security Categorizations
- ✓ Exercises Determine and finalize impact levels
- ✓ Exercise Determine Information and Information System Types and provisional security categorization
- Security Control Baselines review
 - Minimum Security Controls and Security Control Baselines
 - Security Control Families
- Risk Assessment Controls
- Team Exercise Find and assess risk assessment policy

Risk Management Framework

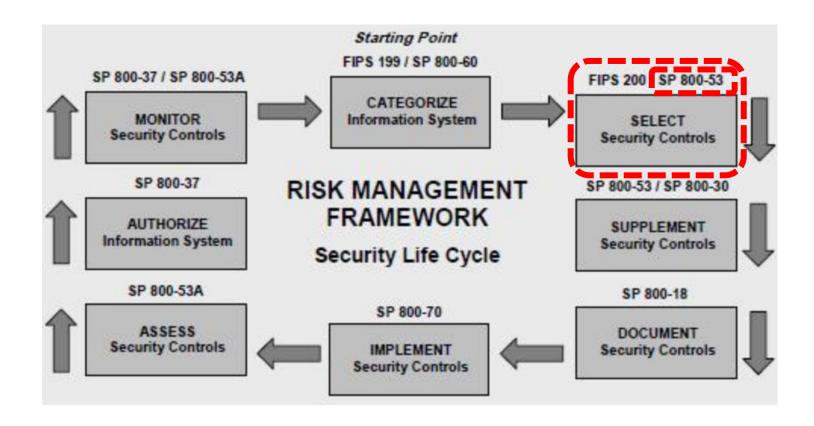


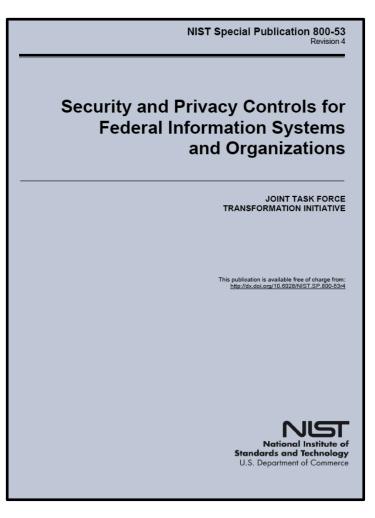
Minimum Security Control Requirements

- Access Control (AC)
- 2. Awareness and Training (AT)
- 3. Audit and Accountability (AU)
- 4. Certification, Accreditation, and Security Assessment (CA)
- 5. Configuration Management (CM)
- 6. Contingency Planning
- 7. Identification and Authentication
- 8. Incident Response (IR)
- 9. Maintenance (MA)

- 10. Media Protection (MP)
- 11. Physical and Environmental Protection *PE)
- 12. Planning (PL)
- 13. Personal Security (PS)
- 14. Risk Assessment (RA)
- 15. System and Services Acquisition(SA)
- 16. System and Communications Protection (SC)
- 17. System and Information Integrity (SI)

Risk Management Framework





												CNTI					E		INITIAL C	ONTROL BASE	LINES
												NO.		CONTR	ROL N	AME	PRIO	L	LOW	MOD	HIG
												SC-2	5 Th	nin Nodes			PO	Not S	Selected	Not Selected	Not Sele
												SC-2		oneypots			PO			Not Selected	Not Sele
												SC-2	7 PI	atform-Independe	nt Appli	cations	PO	Not S	Selected	Not Selected	Not Sele
												SC-2		otection of Inform			P1	Not S	Selected	SC-28	SC-2
										-			- 1				1			1 t Selected	Not Sele
											CNTL				È	INITIAL C	ONTROL	L BASEL	LINES	t Selected	Not Sele
											NO.	CONTR	OL N	AME	PRIORTY					t Selected	Not Sele
															_	LOW	MOD		HIGH	Selected	Not Sele
												eveloper Configura			P1	Not Selected	SA-10		SA-10	- Cenedico	1401.041
											SA-11 D	eveloper Security	Testing :	and Evaluation	P1	Not Selected	SA-1		SA-11	Selected	Not Sel
												upply Chain Protec	tion				Not Sele		SA-12		
											SA-13 T	rustworthiness			P0	Not Selected	Not Sele	cted	Not Selected	t Selected	Not Sel
														INITIAL CONTR	OL BAS	ELINES	ot Sele	cted	Not Selected	t Selected	Not Sel
								CNTL NO.		CONTROL	NAME	PRIORITY				1	ot Sele	cted	SA-15	t Selected	Not Sel
								NO.				8	LC	OW MC	OD	HIGH	ot Sele		SA-16	t Selected	Not Sel
								PE-17	Alterna	te Work Site		P2	Not Se	elected PE-	-17	PE-17	ot Sele		SA-10	SC-39	SC-
										n of Information S	vetem Con			elected Not Se		PE-18	ot Sele		Not Selected	t Selected	Not Sel
										ation Leakage	yatem out	P0		elected Not Se		Not Selected	ot Sele		Not Selected Not Selected	! Selected	Not Sel
										Monitoring and Tra	okina	P0			lected		ot Sele		Not Selected	! Selected	Not Sel
								1 5-20	Maaet II	nontoning and Tra	cking	Planning	NOL DE	elected Not Se	iecteu	Not Selected	Dt Sele	cted	Not Selected	Selected	Not Sel
					-			-								PL-1	ot Sele	cted	Not Selected	Selected	Not Sel
						CNTL				È		INITIAL CONTRO	L BASI	ELINES	(3)		ot Sele		Not Selected		Hot Sei
						NO.	C	ONTROL NA	AME	Sion					(3)	PL-2 (3)					
										2	LOV	V MO	D	HIGH	(1)	PL-4 (1)	SC-1		SC-1	SI-1	SI-
						IR-3 II	ncident Resp	onse Testing		P2	Not Sel			IR-3 (2)	(1)	PL-4 (1)	1			SI-2 (2)	SI-2 (1
					H	IR-4 II	ncident Hand	ling		P1	IR-			IR-4 (1) (4)	-	-	SC-2		SC-2	- '	
					H		ncident Monit			P1	IR-			IR-5 (1)		Net Calcut.	ot Sele	cted	SC-3	-3 (1) (2)	SI-3 (
					H		ncident Repo			P1	IR-			IR-6 (1)	ected	Not Selected	SC-4		SC-4	(2) (4) (5)	SI-4 (2)
													1)	IR-7 (1)	8	PL-8	SC-5		SC-5	SI-5	SI-5
				CNTI				La		INITIAL CONT	TROL BAS	ELINES		IR-8	lected	Not Selected	ot Sele		Not Selected	t Selected	SI-
				NO.	CC	NTROL I	NAME	PRIORITY					ted	Not Selected			-7 (3) (4) (5)	SC-7 (3) (4) (5	-7 (1) (7)	SI-7 (1)
								ž.	L	_ow	MOD	HIGH	ted	Not Selected	-1	PS-1	(7)		(7) (8) (18) (21)	(7) (
				CM-6	Configuration S	Settings		P1	0	CM-6	CM-6	CM-6 (1) (2)		- Tenedied	-2	PS-2	SC-8 (1)	SC-8 (1)	-8 (1) (2)	SI-8 (1
				CM-7	Least Function	ality		P1	0	CM-7 CM-7	(1) (2) (4)	CM-7 (1) (2) (5)			-3	PS-3					_
				CM-8	Information Sy	stem Comp	onent Invento	ry P1	0		(1) (3) (5)	CM-8 (1) (2) (3)		MA-1	-4	PS-4 (2)	SC-10		SC-10	SI-10	SI-1
					1							(4) (5)	_	MA-2 (2)	-5	PS-5	ot Sele		Not Selected	SI-11	SI-1
						F	INIT	IAL CONTRO	L BASI	ELINES	A-9 I-10	CM-10	(2)	MA-3 (1) (2) (3)	-6	PS-6	SC-12	2	SC-12 (1)	SI-12	SI-1
		CNTL NO.	CON	ITROL	NAME	8 -							2)	MA-4 (2) (3)	-7	PS-7	SC-13	2	SC-13	Selected	Not Sel
		NO.				8	LOW	MOE	D	HIGH	1-11	CM-11		MA-5 (1)	-8	PS-8	30-1	3	30-13		
					Awaren	ess and Tra	aining			-	1			MA-6			SC-18	-	SC-15	t Selected	Not Sel
		AT-1	Security Awaren	oee and	Training Policy and	P1	AT-1	AT-		AT-1	2-1	CP-1			-1	RA-1	ot Sele		Not Selected	Selected	Not Sel
		0111	Procedures	CJS GIIU			0111	A1-		21-1) (3) (8)	CP-2 (1) (2) (3)		MP-1	-2	RA-2				SI-16	SI-1
		AT-2	Security Awaren	ess Trair	ing	P1	AT-2	AT-2	(2)	AT-2 (2)	,,(3)(0)	(4) (5) (8)		MP-2	-3	RA-3	SC-18		SC-17 SC-18	Selected	Not Sel
		AT-3	Role-Based Seco	urity Trai	ning	P1	AT-3	AT-		AT-3	2-3	CP-3 (1)		MP-3			SC-18		SC-18 SC-19	+	
		AT-4	Security Training	Record	5	P3	AT-4	AT-4		AT-4	4 (1)	CP-4 (1) (2)		MP-4	(2) (5)	RA-5 (1) (2) (4)	SC-19		SC-19 SC-20	+	
		TABL	E D-2: SECURIT	Y CON	TROL BASELINES	S**							1)	MP-5 (4)		(5) Not Selected	30-20		30-20		
				7,00					1		(1) (3)	CP-6 (1) (2) (3)		MP-6 (1) (2) (3)	lected	Not Selected	SC-2	1	SC-21		
NTL IO.				PRIORITY	INITIAL	CONTRO	L BASELINI	ES		AU-1) (2) (3)	CP-7 (1) (2) (3)	1)	MP-7 (1)			1	_		-	
10.	0011	TDO: N.		1 2 1	LOW		_					(4)			4	SA-1	SC-2	2	SC-22		
	CON	TROL NA		F					1 —			CP-7 (1) (2) (3) (4)	:ted	Not Selected			002			-	
	CON	TROL NA		-		MOI	D	HIGH]=	AU-2 (3)	(1) (2)	CP-8 (1) (2) (3)	ted	Not Selected	-1			2	SC 22		
	CON	TROL NA		ss Con		MOI	D	HIGH		AU-3 (1) (2)		CP-8 (1) (2) (3) (4)	ted	Not Selected PE-1	-2	SA-2	SC-23		SC-23		
			Acce	-		MOI AC-		AC-1		AU-3 (1) (2) AU-4	(1) (2) 9 (1)	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5)	ated	PE-1	-2	SA-2 SA-3			SC-23 SC-24		
		olicy and P	Acce	ss Con	trol	AC-2 (1)	-1 (2) (3) AC	AC-1		AU-3 (1) (2) AU-4 AU-5 (1) (2)	9 (1)	CP-8 (1) (2) (3) (4)	xted	PE-1 PE-2	-2 -3 (2) (9)	SA-2 SA-3 SA-4 (1) (2) (9)	SC-23				
	Access Control Po	olicy and P	Acce	ss Con	AC-1	AC-	-1 (2) (3) AC	AC-1	1)	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5)	9 (1)	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5) CP-10 (2) (4)	xted	PE-1 PE-2 PE-3 (1)	-2 -3 (2) (9)	SA-2 SA-3 SA-4 (1) (2) (9) (10)	SC-23				
2-2	Access Control Po Account Managen	olicy and P	Acce	P1	AC-1 AC-2	AC-2 (1) (4)	1 (2) (3) AC (4)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13)	1)	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6)	(1) (2) 9 (1) 10 (2)	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5) CP-10 (2) (4) Not Selected	ted	PE-1 PE-2 PE-3 (1) PE-4	-2 -3 (2) (9)))	SA-2 SA-3 SA-4 (1) (2) (9)	SC-23				
C-2 C-3	Access Control Po Account Managen Access Enforcement	olicy and P ment ent	Acce rocedures	P1 P1	AC-1 AC-2 AC-3	AC-2 (1) (4)	-1 (2) (3) AC (4)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) AC-3	1)	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (8) AU-7 (1)	(1) (2) 9 (1) 10 (2) elected	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5) CP-10 (2) (4) Not Selected Not Selected	sted	PE-1 PE-2 PE-3 (1) PE-4 PE-5	-2 -3 (2) (9))) -5	SA-2 SA-3 SA-4 (1) (2) (9) (10)	SC-23				
C-2 C-3 C-4	Access Control Po Account Managen Access Enforceme	olicy and P ment ent Enforceme	Acce rocedures	P1 P1 P1 P1	AC-1 AC-2 AC-3 Not Selected	AC-2 (1) (4) AC-AC-	-1 (2) (3) AC (4)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4	1)	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (0) AU-7 (1) AU-8 (1)	(1) (2) 9 (1) 10 (2)	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5) CP-10 (2) (4) Not Selected	sted	PE-1 PE-2 PE-3 (1) PE-4	-2 -3 ((2) (9))) -5	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 	SC-23				
C-2 C-3 C-4 C-5	Access Control Pc Account Managen Access Enforceme Information Flow B Separation of Duti	olicy and P ment ent Enforceme	Acce rocedures	P1 P1 P1 P1 P1	AC-1 AC-2 AC-3 Not Selected Not Selected	AC-2 (1) (4) AC-AC-AC-	-1 (2) (3) AC (4) 3 4 5	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4 AC-5		AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (8) AU-7 (1)	(1) (2) 9 (1) 10 (2) elected elected elected	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5) CP-10 (2) (4) Not Selected Not Selected	sted 1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5)) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5	Access Control Po Account Managen Access Enforceme	olicy and P ment ent Enforceme	Acce rocedures	P1 P1 P1 P1	AC-1 AC-2 AC-3 Not Selected	AC-2 (1) (4) AC-AC-AC-	-1 (2) (3) AC (4) 3 4 5	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3)	i)	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10	(1) (2) 9 (1) 10 (2) elected	CP-8 (1) (2) (3) (4) CP-9 (1) (2) (3) (5) CP-10 (2) (4) Not Selected Not Selected	sted	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1)	-2 -3 ((2) (9))) -5	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 	SC-23				
C-2 C-3 C-4 C-5 C-6	Access Control Po Account Managen Access Enforceme Information Flow & Separation of Duti Least Privilege	olicy and P ment ent Enforceme ies	Acce rocedures	P1 P1 P1 P1 P1	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected	AC-2 (1) (4) AC- AC- AC- AC- AC- (9) (1	-1 (2) (3) AC (4) 3 4 4 5 (2) (5) AC (10)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10)		AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11	(1) (2) 9 (1) 10 (2) Plected Plected Plected	CP-8 (1) (2) (3) (4) (P-9 (1) (2) (3) (5) (5) (CP-10 (2) (4) (P-10 (2) (2) (P-10 (2) (2) (P-10 (2) (ited	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9)) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6	Access Control Pc Account Managen Access Enforcem Information Flow 6 Separation of Duti Least Privilege Unsuccessful Log	ent Enforceme ies	Acce rocedures	P1 P1 P1 P1 P1 P2	AC-1 AC-2 AC-3 Not Selected Not Selected AC-7	AC-2 (1) (4) AC-2 (1) (4) AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-A	-1 (2) (3) AC (4) 3 4 4 -5 (2) (5) AC (77	AC-12 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4 AC-56 (1) (2) (3) (5) (9) (10) AC-7	id	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3)	(1) (2) 9 (1) 10 (2) elected elected elected	CP-8 (1) (2) (3) (4) (P-9 (1) (2) (3) (5) (5) (CP-10 (2) (4) (P-10 (2) (2) (P-10 (2) (2) (P-10 (2) (ited	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10)) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8	Access Control Pc Account Managen Access Enforcem Information Flow to Separation of Duti Least Privilege Unsuccessful Log System Use Notifi	ent Enforceme ies ion Attemptication	Acce rocedures	P1 P1 P1 P1 P2 P1	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected AC-7 AC-8	AC-2 (1) (4) AC-2 (1) AC- AC- AC- AC- AC- AC- AC- AC- AC- AC-	-1 (2) (3) AC (4) 3 4 5 (2) (5) AC (10) (77 8	AC-12 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4 AC-56 (1) (2) (3) (5) (9) (10) AC-7 AC-8		AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11	(1) (2) 9 (1) 10 (2) Plected Plected Plected Plected Plected (-1) (2) (3) 1) (12)	CP-8 (1) (2) (3) (6) (7) (7) (8) (7) (7) (8) (7) (7) (7) (7) (8) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	ted	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-10 PE-11 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9	Access Control PC Account Managen Access Enforcem Information Flow & Separation of Duti Least Privilege Unsuccessful Log System Use Notifi Previous Logon (A	ent Enforceme ies ion Attemptication Access) No	Acce rocedures	P1 P1 P1 P1 P2 P1 P0	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected	AC-2 (1) (4) AC-2 (AC-2 (AC))))))))))))))))))))))))))))	-1 (2) (3) AC (4) 3 4 4 5 (2) (5) AC (10) 7 8 ected N	AC-12 (1) (2) (3) (5) (11) (12) (13) AC-3 AC-4 AC-56 (1) (2) (3) (5) (9) (10) AC-7 AC-8 ot Selected	d	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected	(1) (2) 9 (1) 10 (2) Plected Plected Plected	CP-8 (1) (2) (3) (4) (5) (7) (9) (7) (9) (7) (9) (7) (9) (7) (9) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	ted	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12)) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10	Access Control Pc Account Managen Access Enforcem Information Flow to Separation of Duti Least Privilege Unsuccessful Log System Use Notifi Previous Logon (& Concurrent Session	ent Enforceme ies ion Attemptication Access) No	Acce rocedures	P1 P1 P1 P1 P2 P1 P0 P3	AC-1 AC-2 AC-3 Not Selected Not Selected AC-7 AC-8 Not Selected	AC-2 (1) (4) AC-2 (1) AC- AC- AC-6 (1) (9) (1 AC- AC- Not Sele Not Sele	-1 (2) (3) AC (4) (4) (4)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (6) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10) AC-7 AC-8 ot Selected AC-10	d d	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected	(1) (2) 9 (1) 10 (2) Plected Plecte	CP-8 (1) (2) (3) (6) (7) (7) (8) (7) (8) (7) (8) (7) (8) (7) (9) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-3 (1) PE-4 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
D-2 D-3 D-4 D-5 D-6 D-7 D-8 D-9 D-10	Access Control Pc Account Managen Access Enforcem Information Flow to Separation of Dutil Least Privilege Unsuccessful Log System Use Notifi Previous Logon (A Concurrent Sessio Session Lock	ent Enforceme les Ion Attempt ication Access) No	Acce rocedures	P1 P1 P1 P1 P1 P2 P1 P0 P3 P3	AC-1 AC-2 AC-3 Not Selected Not Selected AC-7 AC-8 Not Selected AC-7 AC-8 Not Selected Not Selected Not Selected	AC-2 (1) (4) AC-2 (1) AC- AC- AC-6 (1) (9) (1) AC- AC- Not Sele Not Sele	-1 (2) (3) AC (4) 3 4 4 -5 5 (2) (5) AC (10) (7.7 8 8 ected N ected I (1)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10) AC-7 AC-8 Of Selected AC-10 AC-11 (1)	d d	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected	(1) (2) 9 (1) 10 (2) Plected Plected Plected Plected Plected (-1) (2) (3) 1) (12)	CP-8 (1) (2) (3) (4) (5) (7) (9) (7) (9) (7) (9) (7) (9) (7) (9) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-12 (1) (2))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11	Access Control Pc Account Managen Access Enforcem Information Flow Is Separation of Duti Least Privilege Unsuccessfu Log System Use Notifi Previous Logon (& Concurrent Sessic Session Lock Session Terminati	ent Enforceme les Ion Attempt ication Access) No	Acce rocedures	P1 P1 P1 P1 P2 P1 P0 P3	AC-1 AC-2 AC-3 Not Selected Not Selected AC-7 AC-8 Not Selected	AC-2 (1) (4) AC-2 (1) AC- AC- AC-6 (1) (9) (1 AC- AC- Not Sele Not Sele	-1 (2) (3) AC (4) 3 4 4 -5 5 (2) (5) AC (10) (7.7 8 8 ected N ected I (1)	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (6) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10) AC-7 AC-8 ot Selected AC-10	d d	AU-3 (1) (2) AU-4 AU-5 (1) (3) (5) (6) AU-6 (1) (3) (5) (6) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected Not Selected	(1) (2) 9 (1) 10 (2) Plected Plecte	CP-8 (1) (2) (3) (6) (7) (7) (8) (7) (8) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-6 PE-6 (1) (4) PE-9 PE-10 (1) PE-11 (1) PE-12 PE-13 (1) (2) PE-14)) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12	Access Control Pc Account Managen Access Enforcem Information Flow & Separation of Duti Least Privilege Unsuccessful Log System Use Notifi Previous Logon (A Concurrent Separation Concurrent Concurrent Separation Concurrent Separation Concurrent Separation Concurrent Separation Concurrent Concurre	ent Enforceme les ion Attempt ication Access) No on Control	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P0 P3 P3 P2	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected	AC-2 (1) (4) AC-2 (1) (4) AC-AC-C (1) (9) (1 AC-C (1) (1 AC-C (1 AC-C (1) (1 AC-C (1 AC-	-1 (2) (3) (4) (4) (3) (4) (4) (5) (6) (6) (7) (7) (8) (9) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (15) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) 5) (9) (10) AC-7 AC-8 of Selected AC-10 AC-10 AC-11 AC-12	d d	AU-3 (1) (2) AU-4 AU-5 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) AU-8 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected Not Selected Not Selected	(1) (2) 9 (1) 10 (2) slected slected slected slected 10 (2) (3) 11 (12) 13 (2) (3) 1 (12) (3)	CP-8 (1) (2) (3) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (8) (7) (8) (8) (8) (8) (8) (8) (8) (8) (9) (11) (12) (14) (14) (15) (15) (15) (15) (15) (15) (15) (15	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-1 C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13	Access Control Pc Account Managen Access Enforcem Information Flow 8 Separation of Duti Least Privilege Unsuccessful Log System Use Notifi Previous Logon (A Concurrent Session Terminati Withdrawn Permitted Actions Permitted Actions	ent Enforceme les ion Attempt ication Access) No on Control	Acce rocedures nt ts	P1 P1 P1 P1 P1 P2 P1 P0 P3 P3	AC-1 AC-2 AC-3 Not Selected Not Selected AC-7 AC-8 Not Selected AC-7 AC-8 Not Selected Not Selected Not Selected	AC-2 (1) (4) AC-2 (1) AC- AC- AC-6 (1) (9) (1) AC- AC- Not Sele Not Sele	-1 (2) (3) (4) (4) (3) (4) (4) (5) (6) (6) (7) (7) (8) (9) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10) AC-7 AC-8 Of Selected AC-10 AC-11 (1)	d d	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) AU-7 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-11 AU-12 (1) (3) Not Selected Not Selected Not Selected CA-1 CA-2 (1) (2)	(1) (2) 9 (1) 10 (2) slected slected slected slected 10 (2) (3) 11 (12) 13 (2) (3) 1 (12) (3)	CP-8 (1) (2) (3) (4) (4) (7) (4) (7) (7) (8) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-6 PE-6 (1) (4) PE-9 PE-10 (1) PE-11 (1) PE-12 PE-13 (1) (2) PE-14)) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 2-10 2-11 2-12 2-13 2-14	Access Control Pc Account Managen Access Enforcem Information Flow It Separation of Duff Least Privilege Unsuccessful Log System Use Notifi Previous Logon (& Concurrent Session Lock Session Terminati Withdrawn Permitted Actions Authentication	ent Enforceme les ion Attempt ication Access) No on Control	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P0 P3 P3 P2	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected	AC-2 (1) (4) AC-2 (1) (4) AC-AC-C (1) (9) (1 AC-C (1) (1 AC-C (1 AC-C (1) (1 AC-C (1 AC-	-1 (2) (3) (4) (4) (3) (4) (4) (5) (6) (6) (7) (7) (8) (9) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (15) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) 5) (9) (10) AC-7 AC-8 of Selected AC-10 AC-10 AC-11 AC-12	d d	AU-3 (1) (2) AU-4 AU-5 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) AU-8 (1) AU-8 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected Not Selected Not Selected	(1) (2) 9 (1) 10 (2) slected slected slected 10 (2) (3) 11 (12) 13 (4) 12 (3) 13 (2) (3) 14 (2) (3) 16 (2) (3) 17 (2) (3) 18 (2) (3) 19 (2) (3) 19 (2) (3) 19 (3) 19 (3) 19 (3) 19 (3) 19 (4) 19 (4) 19 (5) 19 (6) 19 (6) 19 (7) 19	CP-6 (1) (2) (3) (4) (7) (2) (6) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
0-2 0-3 0-4 0-5 0-6 0-7 0-8 0-9 0-10 0-11 0-12 0-13	Access Control Pc Account Managen Access Enforcem Information Flow to Separation of Dutil Least Privilege Unsuccessful Log System Use Notifie Previous Logon (A Concurrent Session Terminati Withdrawn Permitted Actions Autheritication Autheritication Withdrawn Withdrawn	ent ent Enforceme ies jon Attempt ication Access) No on Control ion	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P3 P3 P2 P3	AC-1 AC-2 AC-3 AC-3 AC-3 AC-3 AC-8 AC-8 AC-7 AC-8 AC-7 AC-8 Not Selected AC-7 AC-8 Not Selected AC-7 AC-8 AC-8 AC-8 AC-8 AC-8 AC-8 AC-8 AC-14 ——	AC-2 (1) (4) AC-2 (1) (4) AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-A	-1 (2) (3) AC (4) (4) 3 3 4 4 5 5 (22) (5) AC (10) (7.7 8.8 ected N (1.11) 112 112	AC-1 -2 (1) (2) (3) (5) (11) (12) (13) (15) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10) AC-7 AC-8 ot Selected AC-10 AC-11 (1) AC-14	d d	AU-3 (1) (2) AU-4 AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-9 (2) (3) (4) AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected CA-1 CA-2 (1) (2) CA-3 (5)	(1) (2) 9 (1) 10 (2) slected slected slected 1) (2) (3) 1) (12) 13 14 1 (2) (3) 1) 10 10 10 10 10 10 10 10 10 10	CP-8 (1) (2) (3) (4) (9) (1) (2) (3) (4) (9) (9) (9) (1) (2) (3) (9) (9) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16	Access Control Pc Account Managen Access Enforcem Information Flow & Separation of Duti Least Privilege Unsuccessful Log System Use Notifi Previous Logon (& Concurrent Sessic Session Lock) Session Terminal Withdrawn Permitted Actions Authentication Withdrawn Security Attrobutes	ent ent Enforceme ies jon Attempt ication Access) No on Control ion	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P0 P3 P3 P2 P0 P0	AC-1 AC-2 AC-3 AC-3 AC-3 AC-3 Not Selected Not Selected Not Selected AC-7 AC-8 AC-8 AC-7 AC-8 AC-14 Not Selected	AC-2 (1) (4) AC-2 (1) (4) AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-A	-1 (2) (3) AC (4) (4) AC (4) A	AC-1 (2) (3) (5) (11) (12) (3) (5) (11) (12) (13) AC-3 AC-4 AC-5 -6 (1) (2) (3) (5) (9) (10) AC-7 AC-8 ot Selected AC-10 AC-11 (1) AC-12	d d	AU-3 (1) (2) AU-4 (1) (2) AU-5 (1) (2) AU-5 (1) (3) (5) (8) AU-7 (1) AU-8 (1) (3) (5) AU-7 (1) AU-8 (2) (3) (4) AU-10 AU-10 AU-10 AU-11 AU-12 (1) (3) AU-11 AU-12 (1) (3) AU-11 CA-2 (1) (2) CA-3 (5) — CA-3 CA-5	(1) (2) 9 (1) 10 (2) slected slected slected 1) (2) (3) 1) (12) 13 14 1) (2) (3) 1) 10 (2) (3) 1) (2) (3) 1) slected slecte	CP-6 (1) (2) (3) (4) (9) (1) (2) (3) (6) (7) (7) (1) (2) (4) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
0-2 0-3 0-4 0-5 0-6 0-7 0-8 0-9 0-10 0-11 0-12 0-13 0-14 0-15 0-16	Access Control Pc Account Managen Access Enforcem Information Flow to Separation of Dutil Least Privilege Unsuccessful Log System Use Notifie Previous Logon (A Concurrent Session Terminati Withdrawn Permitted Actions Autheritication Autheritication Withdrawn Withdrawn	ent ent Enforceme ies jon Attempt ication Access) No on Control ion	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P3 P3 P2 P3	AC-1 AC-2 AC-3 AC-3 AC-3 AC-3 AC-8 AC-8 AC-7 AC-8 AC-7 AC-8 Not Selected AC-7 AC-8 Not Selected AC-7 AC-8 AC-8 AC-8 AC-8 AC-8 AC-8 AC-8 AC-14 ——	AC-2 (1) (4) AC-2 (1) (4) AC-AC-C-C-C-C-C-C-C-C-C-C-C-C-C-C-C-C-	-1 (2) (3) AC (4) 3 3 4 4 5.5 (2) (5) AC (2) (5) AC (10) (1) (1) 4 7.7 8.8 8 ected N e	AC-1 -2-(1)(2)(3) (5)(11)(12) (13) AC-3 AC-4 AC-5 -6-(1)(2)(3) 5)(9)(10) AC-7 AC-8 AC-10 AC-11(1) AC-12 AC-14	d d	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) (6) AU-7 (1) AU-9 (2) (3) (4) AU-10 AU-10 AU-11 AU-12 (1) (3) Not Selected Not Selected Not Selected CA-1 CA-2 (1) (2) CA-3 (5) CA-6 CA-6	(1) (2) 9 (1) 10 (2) slected slected slected 1) (2) (3) 1) (12) 13 14 1 (2) (3) 1) 10 10 10 10 10 10 10 10 10 10	CP-8 (1) (2) (3) (4) (9) (1) (2) (3) (4) (9) (9) (1) (2) (3) (9) (9) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16 C-17	Access Control P. Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Information Flow Information Inform	ent ent Enforceme ies jon Attempt ication Access) No on Control ion	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P3 P3 P3 P2 P1	AC-1 AC-2 AC-3 AC-3 AC-3 Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 AC-8 AC-7 AC-8 AC-14 AC-14 Not Selected AC-17	AC-2 (1) (4) AC-2 (1) (4) AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-A	-1 (2) (3) AC (4) (4) 3 3 4 4 5.5 AC (2) (5) AC (10) (10) (10) (11) (11) 4 14 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	AC-1 -2-(1) (2) (3) (5) (11) (12) (13) (5) (11) (12) (13) AC-3 AC-4 AC-5 -6-(1) (2) (3) (5) (9) (10) AC-7 AC-8 AC-10 AC-11 (1) AC-12 AC-14 Of Selected C-17 (1) (2) (3) (3) (4)	d d	AU-3 (1) (2) AU-4 (1) (2) AU-5 (1) (2) AU-5 (1) (3) (5) (8) AU-7 (1) AU-9 (1) AU-10 AU-11 AU-12 (1) (3) (4) AU-12 (1) (4) (4) (4) (4) (4)	(1) (2) 9 (1) 10 (2) Plected Plecte	CP-8 (1) (2) (3) (4) (6) (7) (6) (7) (8) (8) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16 C-17	Access Control Pc Account Managen Access Enforcem Information Flow & Separation of Duti Least Privilege Unsuccessful Log System Use Notifi Previous Logon (& Concurrent Sessic Session Lock) Session Terminal Withdrawn Permitted Actions Authentication Withdrawn Security Attrobutes	ent ent Enforceme ies jon Attempt ication Access) No on Control ion	Acce rocedures nt ts	P1 P1 P1 P1 P2 P1 P0 P3 P3 P2 P0 P0	AC-1 AC-2 AC-3 AC-3 AC-3 AC-3 Not Selected Not Selected Not Selected AC-7 AC-8 AC-8 AC-7 AC-8 AC-14 Not Selected	AC-2 (1) (4) AC-2 (1) (4) AC-AC-C-C-C-C-C-C-C-C-C-C-C-C-C-C-C-C-	-1 (2) (3) AC (4) (4) 3 3 4 4 5.5 AC (2) (5) AC (10) (10) (10) (11) (11) 4 14 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	AC-1 -2-(1)(2)(3) (5)(11)(12) (13) AC-3 AC-4 AC-5 -6-(1)(2)(3) 5)(9)(10) AC-7 AC-8 AC-10 AC-11(1) AC-12 AC-14	d d	AU-5 (1) (2) AU-6 (1) (2) AU-6 (1) (3) (5) AU-7 (1) AU-7 (1) AU-7 (1) AU-7 (1) AU-7 (1) AU-7 (1) AU-10 AU-11 AU-12 (1) (3) (4) AU-11 AU-12 (1) (3) (4) AU-12 (1) (3) (4) AU-13 (1) AU-14 AU-14 (1) (2) AU-15 (1) (2) AU-16 (1) (3) (4) AU-17 (1) (2) AU-18 (1) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	0 (1) (2) 0 (1) 10 (2)	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16 C-17 C-18	Access Control P. Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Information Flow Information Inform	ent ent Enforceme les ion Attempt ication Access) No on Control ion without Ide	Accedures nt ss entification	P1 P1 P1 P1 P2 P1 P3 P3 P3 P2 P1	AC-1 AC-2 AC-3 AC-3 AC-3 Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 AC-8 AC-7 AC-8 AC-14 AC-14 Not Selected AC-17	AC-2 (1) (4) AC-2 (1) (4) AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-AC-A	-1 (2) (3) AC (4) (4) (4) (4) (4) (5) AC (10) (7) AC (10) (10) (10) (10) (10) (10) (10) (10)	AC-1 -2-(1) (2) (3) (5) (11) (12) (13) (15) (11) (12) (13) AC-3 AC-4 AC-5 -6-(1) (2) (3) (3) (5) (9) (10) AC-7 AC-8 OI Selected AC-10 AC-11 AC-12 OI Selected C-17 (1) (2) (3) (4) (2) (3) (4) (2) (3) (4)	id i	AU-3 (1) (2) AU-4 (1) (2) AU-5 (1) (2) AU-5 (1) (3) (5) (8) AU-7 (1) AU-9 (1) AU-10 AU-11 AU-12 (1) (3) (4) AU-12 (1) (4) (4) (4) (4) (4)	(1) (2) 9 (1) 10 (2) Plected Plecte	CP-8 (1) (2) (3) (4) (6) (7) (6) (7) (8) (8) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16 C-17 C-18 C-18 C-19	Access Control R Account Managem Access Enforcem Information Flow to Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Information Informat	olicy and P ment ent Enforcement Enforcement eles eles eles eles eles eles eles ele	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P2 P3 P3 P2 P1	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected AC-7 AC-8 Not Selected AC-14 AC-14 AC-18	AC-2 (1) (4) AC-2 (1) (4) AC-2 (1) (9) (1) AC-1	-1 (2) (3) AC (4) 3 4 4 5 5 (2) (5) AC (10) 7 7 8 8 ected N (11) 12 12 14 14 14 14 14 14 14 15 15 (11) AC (11)	AC-1 -2-(1) (2) (3) (5) (11) (12) (3) (13) (13) (13) (13) (13) (13) (13)	id i	AU-5 (1) (2) AU-6 (1) (2) AU-6 (1) (2) AU-6 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (3) (4) AU-10 AU-11 AU-12 (1) (3) (4) AU-12 (1) (3) (4) AU-13 (1) (4) AU-14 (1) (2) (3) (4) AU-15 (1) (3) (4) AU-16 (1) (3) (4) AU-17 (1) (4)	0 (1) (2) 0 (1) 10 (2)	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
0-2 0-3 0-4 0-5 0-6 0-7 0-8 0-9 0-10 0-11 0-12 0-13 0-14 0-15 0-16 0-17 0-18 0-19 0-10 0-	Access Control P. Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Information Flow Information Inform	ent	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P1 P3 P3 P3 P2 P1	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected Not Selected AC-17 AC-8 AC-14 AC-17 AC-18 AC-18 AC-19 AC-19	AC-220(1) AC-2(1)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)	-1 (2) (3) AC (4) (4)	AC-1 -2(1)(2)(3) (13) -2(1)(2)(3) (13) -2(1)(3)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(13) -2(13)(13)(1	id i	AU-5 (1) (2) AU-6 (1) (2) AU-6 (1) (3) (5) AU-7 (1) AU-7 (1) AU-7 (1) AU-7 (1) AU-7 (1) AU-7 (1) AU-10 AU-11 AU-12 (1) (3) (4) AU-11 AU-12 (1) (3) (4) AU-12 (1) (3) (4) AU-13 (1) AU-14 AU-14 (1) (2) AU-15 (1) (2) AU-16 (1) (3) (4) AU-17 (1) (2) AU-18 (1) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	0 (1) (2) 0 (1) 10 (2)	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
0-2 0-3 0-4 0-5 0-6 0-7 0-8 0-9 0-10 0-11 0-12 0-13 0-14 0-15 0-16 0-17 0-18 0-19 0-	Access Control Pc Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Access Enforcem Information Flow Info	ent lend to le	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P3 P3 P3 P2 P1 P1 P1 P1 P1 P1 P1 P1 P2 P2 P1 P2 P3 P3 P3 P2 P3 P3 P3 P2 P3 P3 P3 P2 P3 P3 P3 P2 P1 P2	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected AC-7 AC-8 AC-1 AC-8 Not Selected AC-1 AC-8 AC-14 AC-17 AC-18 AC-19 AC-19 AC-19 AC-10 AC-10	AC-20 (1) AC-21(1) AC-21(1) AC-21(1) AC-21(1) AC-32(1) AC	-1 (2) (3) ACC (4) (4) (4) (5) ACC (5) ACC (7)	AC-1 -2-(1)(2)(3)(3)(5)(11)(12)(3)(5)(11)(12)(3)(3)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)	1d 1	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) AU-7 (1) AU-7 (1) AU-12 (1) AU-12 (1) (2) AU-12 (1) (3) Not Selected Not Selected Not Selected CA-1 CA-2 (1) (2) CA-3 (5) CA-6 CA-6 CA-6 CA-6 CA-6 CA-9 CA-9	9 (1) (2) 9 (1) 10 (2) 1ected slected	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 10 11 12 13 14 15 17 18 19 20 22	Access Control P. Account Managem Access Enforcem Information Flow to Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Information Information Flow Information Information Information Information Information Information Information Share Informat	colley and P P P P P P P P P P P P P P P P P P P	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P3 P3 P2 P1 P1 P1 P1 P1 P1 P1 P1 P1 P2 P2 P3 P3 P3 P3 P2 P3 P3 P3 P2 P3 P3 P3 P3 P3 P2 P3	AC-1 AC-2 AC-3 Not Selected Not Selected Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected Not Selected Not Selected Not Selected Not Selected Not Selected AC-14 Not Selected AC-17 AC-8 Not Selected AC-17 AC-19 AC-19 AC-20 Not Selected	AC-20 (1) (AC-20	-1 (2) (3) (4) (3) (4) (3) (4) (3) (4) (4) (5) (5) (6) (7) (7) (8) (10) (10) (10) (10) (10) (10) (10) (10	AC-1 -C-2(1)(2)(3)(3)(5)(11)(12)(3)(6)(11)(12)(3)(4)(3)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)	id i	AU-3 (1) (2) AU-4 AU-5 (1) (2) AU-6 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) AU-7 (1) AU-7 (1) AU-12 (1) AU-12 (1) (2) AU-12 (1) (3) Not Selected Not Selected Not Selected CA-1 CA-2 (1) (2) CA-3 (5) CA-6 CA-6 CA-6 CA-6 CA-6 CA-9 CA-9	9 (1) (2) 9 (1) 10 (2) 1ected slected	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 >-10 >-11 >-12 >-13 >-14 >-15 >-16 >-17 >-18 >-19 >-20 >-21 >-22 >-23	Access Control P. Account Managem Access Enforcement Access Enforcement Information Flow to Least Privilege Unsuccessful Log System Use Notice Previous Logon (# Concurrent Session Session Lock Session Terminal Withdrawn Permitted Actions Autheritacian Recurrent Artification Access Wireless Access Les of External in Information Sharin Puticity Accessible Loss Mining Profession Loss Mining Privilege Loss Mining Min	control of the content of the conten	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P3 P3 P2 P1 P2 P2 P3 P3 P5	AC-1 AC-3 Not Selected Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected AC-17 AC-18 AC-19 AC-10 AC-	AC-17 (3) (4) AC-20 (AC-20 Not Selection AC-20 (Not	-1 (2) (3) (4) (4) (4) (5) (6) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (7) (8) (7) (7) (7) (8) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	AC-1 -22 (1) (2) (3) (6) (11) (12) (13) (15) (11) (12) (13) AC-3 -AC-4 -AC-5 (1) (2) (3) 5) (9) (10) AC-7 -AC-8 -AC-8 -AC-10 -AC-10 -AC-11 (1) -AC-12	1d 1	AU-3 (1) (2) AU-4 AU-5 (1) (3) (5) AU-6 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (4) AU-10 AU-11 AU-12 (1) (2) AU-13 (1) AU-12 (1) (2) AU-13 (1) AU-14 AU-12 (1) (2) AU-15 (1) (2) AU-16 AU-17 (1) (2) AU-17 (2) (2) AU-18 (2) (2) (2) (2) AU-18 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	9 (1) (2) 9 (1) 10 (2) 1ected slected	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16 C-17 C-18 C-20 C-21 C-22 C-23 C-24	Access Control P. Account Managem Access Enforcem Information Flow to Account Managem Access Enforcem Information Flow to Access Enforcem Information Flow to Access Enforcem Information Flow Information Informa	ent Endouge and Person and Endouge and En	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P3 P0 P1	AC-1 AC-2 AC-3 Not Selected AC-14 AC-18 AC-17 AC-19 AC-20 Not Selected AC-19 AC-20 Not Selected AC-22 Not Selected AC-22 Not Selected	AC-2 (1) (1) (1) (2) (1) (2) (1) (2) (1) (2) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	1 (2) (3) AC (4) (4) Ad (4) Ad (5) AC (6) AC (7) AC	AC-1 -2(1)(2)(3)(3)(5)(11)(12)(3)(3)(11)(12)(3)(3)(3)(4)(3)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)	1d 1	AU-3 (1) (2) AU-4 AU-6 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (3) (5) AU-10 (1) AU-10 (1) AU-11 (1) (3) Not Selected Not Selected Not Selected Not Selected CA-1 CA-2 (1) (2) CA-3 (5) — — CA-6 CA-6 CA-6 CA-7 CA-7 CA-8 CA-9 CA-9 CA-9 CA-9 CA-9 CA-1 CM-1 CM-2 (1) (2) (3) CM-3 (1) (2) CM-3 (1) (2) CM-3 (1) (2) CM-3 (1) (2)	9 (1) (2) 9 (1) 10 (2) 1ected slected	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				
C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-12 C-13 C-14 C-15 C-16 C-17 C-18 C-19 C-20 C-21 C-22 C-23	Access Control P. Account Managem Access Enforcement Access Enforcement Information Flow to Least Privilege Unsuccessful Log System Use Notice Previous Logon (# Concurrent Session Session Lock Session Terminal Withdrawn Permitted Actions Autheritacian Recurrent Artification Access Wireless Access Les of External in Information Sharin Puticity Accessible Loss Mining Profession Loss Mining Privilege Loss Mining Min	ent Endouge and Person and Endouge and En	Acce orocedures Int Its diffication entification or	P1 P1 P1 P2 P3 P3 P2 P1 P2 P2 P3 P3 P5	AC-1 AC-3 Not Selected Not Selected Not Selected Not Selected Not Selected AC-7 AC-8 Not Selected AC-17 AC-18 AC-19 AC-10 AC-	AC-17 (3) (4) AC-20 (AC-20 Not Selection AC-20 (Not	1 (2) (3) AC (4) (4) Ad (4) Ad (5) AC (6) AC (7) AC	AC-1 -22 (1) (2) (3) (6) (11) (12) (13) (15) (11) (12) (13) AC-3 -AC-4 -AC-5 (1) (2) (3) 5) (9) (10) AC-7 -AC-8 -AC-8 -AC-10 -AC-10 -AC-11 (1) -AC-12	1d 1	AU-3 (1) (2) AU-4 AU-5 (1) (3) (5) AU-6 (1) (3) (5) AU-6 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (3) (5) AU-7 (1) (4) AU-10 AU-11 AU-12 (1) (2) AU-13 (1) AU-12 (1) (2) AU-13 (1) AU-14 AU-12 (1) (2) AU-15 (1) (2) AU-16 AU-17 (1) (2) AU-17 (2) (2) AU-18 (2) (2) (2) (2) AU-18 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	(1) (2) (3) (1) (1) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	CP-6 (1) (2) (3) (4) (4) (7) (2) (6) (6) (7) (7) (7) (8) (7) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	1)	PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) PE-8 (1) PE-9 PE-10 PE-11 (1) PE-12 PE-13 (1) (2) PE-14 PE-15 (1))) -5 -	SA-2 SA-3 SA-4 (1) (2) (9) (10) SA-5 SA-8	SC-23				

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

NIST Special Publication 800-53 Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

CNTL	CONTROL WINE	IORITY	INITIA	L CONTROL BASE	ELINES
NO.	CONTROL NAME	PRIO	LOW	MOD	HIGH
	Awarenes	s and	Training		
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Withdrawn				
	Audit and	Accou	intability		
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
	Security Assessn	nent ar	nd 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	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn				
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
	Configurati	on Ma	nagement		
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) (7)	CM-2 (1) (2) (3) (7)
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)

									CNTL						YIM		INITIAL	CON	NTROL BASE	LINES
									NO.		CONT	ROI	L NA	AME	PRIORITY		LOW		MOD	HIGH
									SC-25		in Nodes				P0		Selected		t Selected	Not Selected
									SC-26		neypots				P0		Selected		t Selected	Not Selected
									SC-27		tform-Independ				P0		Selected	No	t Selected	Not Selected
									SC-28	Pro	tection of Infor	natio	n at l	Rest	P1	Not	Selected		SC-28	SC-28
												-		INITIAL	CONTRO	DACE	TIME		Selected	Not Selected
						(CNTL		CONTR	OL NA	ME	Ped	L	MITTAL	CONTRO	L DAGE	LINES		Selected	Not Selected
							NO.					E		LOW	MOI	0	HIGH		Selected	Not Selected
						9	SA-10	Developer (onflourat	on Mar	nagement	P1	1	Not Selected	SA-1	0	SA-10		Selected	Not Selected
											and Evaluation	P1		Not Selected	SA-1		SA-11			
								Supply Cha		on		P1		Not Selected	Not Sele		SA-12		Selected	Not Selected
						5	SA-13	Trustworthin	ess			P0		Not Selected	Not Sele		Not Select		Selected Selected	Not Selected Not Selected
				CNTL					E		INITIAL CONT	ROL	BASE	ELINES	ot Sele		Not Select	ted	Selected	Not Selected
				NO.	CON	TROL	NAME		PRIORT					T	ot Sele	ected	SA-15		Selected	Not Selected
									_	LO		IOD		HIGH	ot Sele	ected	SA-16		SC-39	SC-39
				PE-17	Alternate Work Si					Not Se		E-17		PE-17	ot Sele		SA-17		Selected	Not Selected
				PE-18	Location of Inform		ystem Co	mponents		Not Se		elect		PE-18	ot Sele		Not Select		Selected	Not Selected
				PE-19 PE-20	Asset Monitoring		alian.			Not Se Not Se		elect		Not Selected Not Selected	ot Sele		Not Select Not Select		Selected	Not Selected
				PE-20	Asset Monitoring :	and Ira	uxing	DI	anning	not Se	recued Not 5	refect	D90	/vot Selected	ot Sele	ected	Not Select	ted	Selected	Not Selected
	1								_			14		PL-1	ot Sele	ected	Not Select		Selected	Not Selected
		CNTL		urner :		IORTY		INITIAL	ONTROL	BASE	LINES	(3))	PL-2 (3)	ot Sele	ected	Not Select	ted		
		NO.	CO	NTROL N	IAME	PRIOF		ow	MOD		HIGH		_		1				SI-1	SI-1
		-				-	_					(1))	PL-4 (1)	SC-	1	SC-1			
		IR-3 IR-4	Incident Respon			P2 P1		elected R-4	IR-3 (IR-3 (2) IR-4 (1) (4)	+		-	SC-	2	SC-2		31-2 (2)	SI-2 (1) (2)
		IR-5	Incident Monitor			P1		₹-5	IR-5		IR-5 (1) (+)	-			ot Sele		SC-3		-3 (1) (2)	SI-3 (1) (2)
		IR-6	Incident Reporti			P1		₹-8	IR-6 (IR-6 (1)	ect	ted	Not Selected	SC-	4	SC-4		(2) (4) (5)	SI-4 (2) (4) (5)
)	IR-7 (1)	8		PL-8	SC-	5	SC-5		SI-5	SI-5 (1)
CNTL		ONTRO		F F	INITIA	L CONT	TROL BA	SELINES			IR-8	ect	ted	Not Selected	ot Sele		Not Select		Selected	SI-6
NO.	0	ONTRO	LNAME	88	LOW	,	MOD	ни		ted	Not Selected	١,		PS-1	;-7 (3) (7)	(4) (5)	SC-7 (3) (4) (7) (8) (18)		-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
CM-6	0	0.00		P1	CM-6	-	CM-6	CM-6	40.000	ted	Not Selected	2		PS-2	SC-8	(1)	SC-8 (1)		-8 (1) (2)	SI-8 (1) (2)
CM-7	Configuration Least Function	nality		P1	CM-0		(1) (2) (4					-3		PS-3		1-7		_	-0 (1)(2)	51-0 (1) (2)
CM-8			mponent Inventory		CM-8		(1) (3) (5			_	MA-1	4		PS-4 (2)	SC-1	0	SC-10		SI-10	SI-10
								(4)	(5)		MA-2 (2)	-5		PS-5	ot Sele	ected	Not Select	ted	SI-11	SI-11
CM-10	Configuration			P1	Not Selected CM-10		CM-9 CM-10	CM		(2)	MA-3 (1) (2) (3	-8		PS-6	SC-1	2	SC-12 (1	1)	SI-12	SI-12
CM-10	Software Usa User-Installer			P1	CM-10 CM-11		M-10 M-11	_		2)	MA-4 (2) (3)	-7		PS-7			SC-13	\dashv	Selected	Not Selected
CM*II																				
						C	M-11	CM	-11		MA-5 (1)	-8		PS-8	SC-1	3	SU-13	\dashv	Selected	Not Selected
CP-1	Contingency	Planning F	Con	tingency P			OP-1	CM			MA-5 (1) MA-6	-8			SC-1		SC-13			Not Selected Not Selected
	Contingency Procedures		Con	tingency P	CP-1		CP-1	CF	ч		MA-6	-1		RA-1	SC-1 ot Sele	5 ected	SC-15 Not Select		Selected	
CP-1 CP-2			Con	tingency P	lanning			CF	v1) (2) (3)		MA-6 MP-1	-1 -2 -3			SC-1	5 ected 7	SC-15 Not Select SC-17		Selected Selected	Not Selected
	Procedures	Plan	Con	tingency P	CP-1	CP-2	CP-1	OF-2 (1	-1) (2) (3)) (8)		MP-1 MP-2	1 2 3		RA-1 RA-2	SC-1 ot Sele SC-1	5 ected 7	SC-15 Not Select SC-17 SC-18		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4	Procedures Contingency Contingency Contingency	Plan Training	Con Policy and	P1	CP-1 CP-2	CP-2	CP-1 (1) (3) (8	CP-2 (1 (4) (5	·1) (2) (3)) (8)		MA-6 MP-1	3 (2)) (5)	RA-1 RA-2 RA-3 RA-5 (1) (2) (4)	SC-1 ot Sele SC-1 SC-1	5 ected 7 8	SC-15 Not Select SC-17 SC-18 SC-19		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5	Procedures Contingency Contingency Contingency Withdrawn	Plan Training Plan Testi	Con Policy and	P1 P1 P2 P2	CP-1 CP-2 CP-3 CP-4	CP-2	CP-1 (1) (3) (8 CP-3 P-4 (1)	CP-2 (1 (4) (5 CP-3 CP-4	(2) (3) (8) (1) (1)	4)	MP-1 MP-2 MP-3 MP-4 MP-5 (4)	-		RA-1 RA-2 RA-3 RA-5 (1) (2) (4) (5)	SC-1 ot Sele SC-1 SC-1 SC-2	5 ected 7 8 9	SC-15 Not Select SC-17 SC-18 SC-19 SC-20		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto	Plan Training Plan Testi rage Site	Con Policy and	P1 P1 P2 P2 P2 P1	CP-1 CP-2 CP-3 CP-4 Not Selected	CP-2	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3)	CP-2 (1 (4) (5 CP-4 CP-4 CP-8 (1	(2) (3) (8) (8) (1) (2) (4)	MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3	-8 -1 -2 -3 (2)		RA-1 RA-2 RA-3 RA-5 (1) (2) (4)	SC-1 ot Sele SC-1 SC-1	5 ected 7 8 9	SC-15 Not Select SC-17 SC-18 SC-19		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5	Procedures Contingency Contingency Contingency Withdrawn	Plan Training Plan Testi rage Site	Con Policy and	P1 P1 P2 P2	CP-1 CP-2 CP-3 CP-4	CP-2	CP-1 (1) (3) (8 CP-3 P-4 (1)	CP-2 (1 (4) (5 CP-4 CP-4 CP-8 (1	(2) (3) (8) (8) (1) (2) (4)	MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-8 (1) (2) (3 MP-7 (1)	-		RA-1 RA-2 RA-3 RA-5 (1) (2) (4) (5)	SC-1 ot Sele SC-1 SC-1 SC-2 SC-2	5 ected 7 8 9 10	SC-15 Not Select SC-17 SC-18 SC-19 SC-20		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto	Plan Training Plan Testi rage Site ressing Si	Con Policy and ng	P1 P1 P2 P2 P2 P1	CP-1 CP-2 CP-3 CP-4 Not Selected	CP-2 CP-7	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3)	CP-2 (1 (4) (5 CP-4 CP-4 (1) CP-7 (1 (4 CP-8 (1 CP-8 ((2) (3) (8) (1) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3)	4) 1)	MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3	-		RA-1 RA-2 RA-3 RA-5 (1) (2) (4) (5)	SC-1 ot Selv SC-1 SC-1 SC-2 SC-2 SC-2	5 ected	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro	Plan Training Plan Testi rage Site rosssing Si ications Si	Con Policy and ing ite envices	P1 P1 P2 P2 P2 P1 P1 P1 P1	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected	CP-2 CP- CP- CP-7	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3) (1) (2) (3 8 (1) (2)	CP-2 (1 (4) (5 CP-4 CP-4 (1) CP-7 (1) CP-8 (1	(2) (3) (8) (1) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3)		MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3 MP-7 (1) Not Selected	-		RA-1 RA-2 RA-3 RA-5 (5) (2) (4) (5) Not Selected	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro	Plan Training Plan Testi rage Site rosssing Si ications Si	Con Policy and ing ite envices	P1 P1 P2 P2 P2 P1 P1 P1	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-0	CP-2 CP-7 CP-7 CP-	CP-1 (1) (3) (8 CP-3 P-4 (1) 6 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1)	CP-2 (1 (4) (5 CP-4 CP-4 (1) CP-7 (1 (4 CP-8 (1 CP-8 ((2) (3) (8) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3)		MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-8 (1) (2) (3 MP-7 (1)	-		RA-1 RA-2 RA-3 RA-5 (1) (2) (4) (5) Not Selected	SC-1 ot Selv SC-1 SC-1 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Information S	Plan Training Plan Testi rage Site scessing Si scations Se System Bar System Re	Con Policy and ng teleses teleses teleses teleses teleses teleses teleses teleses	P1 P1 P2 P2 P2 P1 P1 P1 P1	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected	CP-2 CP-7 CP-7 CP-	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3) (1) (2) (3 8 (1) (2)	CP-2 (1 (4) (5 CP-2 (1 (5 (1 (5 (1 (5 (1 (5 (1 (5))))))))))	(2) (3)) (8) (1) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3)		MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3 MP-7 (1) Not Selected	1 2 3		RA-1 RA-2 RA-3 	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7 CP-8 CP-9 CP-10	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Reconstitutio	Plan Training Plan Testi rage Site scessing Si sications Se System Bar System Re	Con Policy and Ing Ite Envices Skup Covery and	P1 P1 P2 P2 P2 P1 P1 P1 P1 P1 P1	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-9 CP-10	CP-2 CP-7 CP-7 CP- CP- CP- CP-	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1) 2-10 (2)	CP-8 (1 CP-9 ((2) (3) (8) (1) (1) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3)		MA-6 MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3 MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1)	1 2 3	ted	RA-1 RA-2 RA-3 RA-5 (1) (2) (4) Not Selected SA-1 SA-2 SA-3 SA-4 (1) (2) (9) (10)	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7 CP-8 CP-9 CP-10	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Information S Reconstitutio Alternate Cor	Plan Training Plan Testi rage Site scessing Si sications Se System Bar System Re	Con Policy and Ing Ite Envices Skup Covery and	P1 P1 P2 P2 P2 P1	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected	CP-2 CP- CP- CP- CP- CP- CP- CP- CP-	CP-1 (1) (3) (8 CP-3 P-4 (1)8 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1) P-10 (2) Selected	CP-8 (1 (4) (5) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	(2) (3) (8) (1) (1) (1) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) (2) (4)		MA-6 MP-1 MP-2 MP-3 MP-4 MP-6 (1) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4	1 2 3	ted	RA-1 RA-2 RA-3 	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7 CP-8 CP-9 CP-10	Procedures Contingency Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Reconstitution Alternate Cor Safe Mode	Plan Training Plan Testi rage Site scessing Si ications Si System Bai System Re in	Con Policy and Ing Ing Ing Ing Ing Ing Ing I	P1 P1 P2 P2 P2 P1 P1 P1 P1 P1 P1	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-9 CP-10	CP-2 CP-7 CP-7 CP-7 CP-Not:	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1) 2-10 (2)	CP-8 (1 (4 (5 CP-8 (1 CP-10 Not See No	(2) (3) (8) (1) (8) (1) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) (2) (4) (4)		MA-6 MP-1 MP-2 MP-3 MP-3 MP-4 MP-6 (1) (2) (3 MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-5	1 2 3	ted	RA-1 RA-2 RA-3 RA-5 (1) (2) (4) Not Selected SA-1 SA-2 SA-3 SA-4 (1) (2) (9) (10)	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-10 CP-11 CP-12	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Information S Reconstitutio Alternate Cor	Plan Training Plan Testi rage Site scessing Si ications Si System Bai System Re in	Con Policy and Ing Ing Ing Ing Ing Ing Ing I	P1 P1 P2 P2 P2 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected Not Selected	CP-2 CP-7 CP-7 CP-7 CP-Not:	CP-1 (1) (3) (8 CP-3 P-4 (1)8 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1) P-10 (2) Selected Selected	CP-8 (1 (4 (5 CP-8 (1 CP-10 Not See No	(2) (3) (8) (1) (8) (1) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) (2) (4) (4)		MA-6 MP-1 MP-2 MP-3 MP-4 MP-6 (1) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4	1 2 3	ted	RA-1 RA-2 RA-3 RA-5 (1) (2) (4) Not Selected SA-1 SA-2 SA-3 SA-4 (1) (2) (9) (10)	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-10 CP-11 CP-12	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Reconstitution State Mode Alternative S Identification	Plan Training Plan Testi rage Site rosessing Si idications Si System Bai System Re in mmunicati ecurity Me	Con Policy and Ing Re ervices ciklup covery and covery and chanisms	P1 P1 P2 P2 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P1	Inning CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected And Selected CP-10 Not Selected Not Selected Not Selected OP-10	CP-2 CP-7 CP-7 CP-7 CP-1 CP-1 CP-1 CP-1 CP-1 CP-1 CP-1 CP-1	CP-1 (1) (3) (8 CP-3 P-4 (1)8 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1) P-10 (2) Selected Selected	CP-8 (1 (4 (5 CP-8 (1 CP-10 Not See No	(2) (3) (8) (1) (1) (2) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) (2) (4)		MA-6 MP-1 MP-2 MP-3 MP-3 MP-4 MP-5 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4)	1 2 3	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-10 CP-10 CP-11 CP-12 CP-13	Procedures Contingency Contingency Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Reconstitutio Alternate Cot Safe Mode Alternates Identification Procedures	Plan Training Plan Testi rage Site rocessing Si ications Si System Bai System Rein mmunicati ecurity Me and Auther	Con Policy and te te te te covery and covery and covery and covery and leantifica	P1 P	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected Not Selected Not Selected Not Selected Into Selected	CP-2 CP-7 CP-7 CP-Not: Not:	CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3) (1) (2) (3 8 (1) (2) P-9 (1) 2-10 (2) Selected Selected IA-1	CP-2 (1 (4) (5) (7) (4) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	(2) (3) (8) (1) (1) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) (2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4		MA-6 MP-1 MP-2 MP-3 MP-3 MP-4 MP-6 (1) (2) (3 MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-5	ect	ted) (9)	RA-1 RA-2 RA-3 RA-5 (1) (2) (4) (5) Not Selected SA-1 SA-2 SA-3 SA-4 (1) (2) (9) (1) SA-5 	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-0 CP-10 CP-11 CP-12 CP-13	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Reconstitution State Mode Alternative S Identification	Plan Training Plan Testi rage Site coessing Si ications Si System Bai System Rein mmunicati ecurity Me and Auther	Con Policy and te te te te covery and covery and covery and covery and leantifica	P1 P1 P2 P2 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P1	Ianning CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected Not Selected Not Selected CP-0 CP-10 Not Selected	CP-2 CP-7 CP-7 CP-7 CP-1 CP-Not: Not:	CP-1 (1) (3) (8 CP-3 P-4 (1)	CP-2 (1 (4)) (5 (4)) (6 (4)) (7 (4)) (.1 (2) (3)) (8) (1) (1) (2) (3)) (9) (1) (1) (2) (3)) (2) (3)) (2) (3)) (2) (4) lected lected		MA-6 MP-1 MP-2 MP-3 MP-8 (1) (2) (3) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-8 (1) (4) PE-8 (1) (4)	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7 CP-8 CP-9 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2	Procedures Contingency Contingency Contingency Withdrawn Albernate Sto Alternate Pro Telecommun Information S Information S Information S Safe Mode Albernative S: Identification Procedures Identification (Organization (Organization)	Plan Training Plan Testi rage Site coessing Si cications Si system Bai System Rein mmunicati ecurity Me and Auther and Auther and Auther and Auther and Auther	Con Policy and ng the the the the the the the the the th	P1 P1 P2 P2 P1	Lanning CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected CP-10 Not Selected Land Selected Lan	CP-2 (CP-7 CP-7 CP-7 CP-7 CP-1 LA-2 (8) (CP-1 (1) (3) (8 CP-3 P-4 (1)	CF-2 (1 (4) (5) (P-2) (P-2) (P-2) (P-3) (P	(2) (3) (3) (6) (6) (7) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7		MA-6 MP-1 MP-2 MP-3 MP-4 MP-5 (4) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-6 (1) (4) PE-8 (1) PE-9 PE-9 (1) (4)	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-8 CP-7 CP-8 CP-9 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information S Information S Safe Mode Alternate Cot Safe Mode Alternate Cot Safe Mode Alternate Cot Safe Mode Alternate Cot Safe Mode Device Identification Corganization Device Identification Device Identification	Plan Training Plan Testi rage Site coessing Si idications Si System Bai System Rein mmunicati ecurity Me and Auther and System Se in fication an	Con Policy and te te te te covery and covery and covery and covery and leantifica	P1 P	CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected Not Selected Not Selected Not Selected Into Selected	CP-2 CP-7 CP-7 CP-1 CP-1 CP-1 CP-1 CP-1 CP-1 CP-1 CP-1	CP-1 (1) (3) (8 CP-3 P-4 (1)6 (1) (2) (3 8 (1) (2) P-9 (1) P-9 (1) Selected Selected IA-1 (1) (2) (3) (3)	CP-2 (1 (4)) (5 (4)) (6 (4)) (7 (4)) ((2) (3) (6) (6) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5 (4) MP-5 (4) MP-5 (1) (2) MP-7 (1) Not Selected PE-1 PE-2 PE-3 PE-6 (1) (4) PE-6 (1) (9) PE-10 PE-10 PE-11 (1) PE-11 (1) PE-11 (1) PE-10 PE-11 (1)	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-6 CP-6 CP-7 CP-8 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3	Procedures Contingency Contingency Contingency Withdrawn Albernate Sto Alternate Pro Telecommun Information S Information S Information S Safe Mode Albernative S: Identification Procedures Identification (Organization (Organization)	Plan Training Plan Testi rage Site soessing Si sications Si system Bai system Re in mmunicati and Auther and Auther and Auther all Users) infeation ann nagement	Con Policy and The telescope of the telescope of the telescope of tel	P1 P1 P2 P2 P2 P1 P0 P0 P0 P0 F0 P1	Lanning CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected CP-0 CP-0 CP-0 LA-1 LA-2 LA-2 LA-2 LA-2 LA-2 LA-2 LA-2 LA-2	CP-2 CP-7 CP-7 CP-7 CP-1 CP-1 CP-1 LA-2 (8) (1) LA-5	CP-1 (1) (3) (8 CP-3 P-4 (1)	CP-2 (1 (4 (4 (8)) (4	(2) (3) (6) (6) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1		MA-6 MP-1 MP-2 MP-3 MP-4 MP-5 (4) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-6 (1) (4) PE-8 (1) PE-9 PE-9 (1) (4)	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-0 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-5	Procedures Contingency Contingency Contingency Withdrawn Alternate So Alternate Pro Telecommun Information S Information S Reconstitution Alternate Contingency Identification J Identification Corporation Lidentification Device Identification	Plan Training Plan Testi Plan Testi rage Site coessing Si cications Si cystem Ba- coessing Si yystem Ba- and Author and A	Con Policy and Ing Ing Ing Ing Ing Ing Ing I	P1	Ianning CP-1 CP-2 CP-3 CP-4 Not Selected Not Selected Not Selected Not Selected Not Selected LP-1 Not Selected	CP-2 CP- CP- CP- CP- CP- CP- CP- CP- (P- (P- (P- (P- (P- (P- (P- (P- (P- (CP-1 (1) (3) (8 CP-3 P-4 (1) 8 (1) (3) (1) (2) (3 8 (1) (2) (3 8 (1) (2) Selected Selected (1) (2) (3 (11) (12) (3 (14) (12) (3 (14) (12) (3 (15) (14) (15) (15) (15) (15) (15) (15) (15) (15	CP-2 (1 (4) (8) (6) (8) (8) (8) (8) (8) (8) (8) (8) (8) (8	(2) (3) (9) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	1)	MA-6 MP-1 MP-2 MP-3 MP-3 MP-4 MP-5 (4) (3) MP-7 (1) Not Selected PE-2 PE-3 (1) PE-4 PE-6 PE-6 (1) (4) PE-9 PE-9 PE-10 (1) PE-11 (1) PE-12	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-6 CP-7 CP-8 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-6 IA-6	Procedures Contingency Contingency Contingency Withdrawn Alternate Sto Alternate Sto Alternate Fro Telecommun Information S Information S Sate Mode Alternate Cot Sate Mode Alternate Cot Granification (Organization (Organization Ledentification (Organization Authenticato Authent	Plan Training Plan Testing Plan	Con Policy and The telescope of the telescope of the telescope of tel	P1	Internation	CP-2 CP- CP- CP- CP- CP- CP- CP- CP- LA-2 (8) (1) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	CP-1 (1) (3) (8 CP-3 CP-3 CP-4 (1)	CP-3 (1 (4) (8) (4) (4) (8) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	-1 (2) (3) (8) (1) (1) (1) (2) (3) (8) (1) (1) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) lected lected lected lected lected lected (2) (3) (3) (2) (4) (2) (3) (3) (4) (4) (4) (5) (6) (6) (6) (6) (6) (6) (6) (6) (6) (6	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5(1) (2) (3) MP-7 (1) Not Selected PE-3 (1) PE-4 PE-6 PE-6 (1) (4) PE-10 PE-10 PE-10 PE-12 PE-12 (3)	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-6 CP-6 CP-6 CP-7 CP-8 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-6 IA-7	Procedures Contingency Contingency Contingency Contingency Contingency Contingency Contingency Contingency Mithdraws Alternate Pro Telecommun Information S Information S Sate Mode Alternative S Sate Mode Alternative S Identification (Organization Unganization Unganization Levice Identifier Mar Authenticator	Plan Training Plan Testing Plan	Con Policy and The control of the c	P1	Invaring	CP-2 CP-7 CP-7 CP-7 CP-1 Not: Not: Not: 1A-2 (8) (1	CP-1 (1) (3) (8 CP-3 P-4 (1)	CP-01 (14) (14) (14) (14) (14) (14) (14) (14	(2) (3) (6) (7) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	1)	MA-6 MP-1 MP-2 MP-3 MP-8 MP-5 (4) MP-5 (9) MP-6 (1)(2)(3 MP-6 (1)(2)(3 MP-7 (1)(3 MP-7 (1)(ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-6 CP-6 CP-6 CP-7 CP-7 CP-8 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-6 IA-7 IA-8	Procedures Contingency Contingency Contingency Contingency Contingency Contingency Contingency Contingency Mithdraws Alternate Pro Telecommun Information S Information S Sate Mode Alternative S Sate Mode Alternative S Identification (Organization Unganization Unganization Levice Identifier Mar Authenticator	Plan Training Plan Testing Plan	Con Policy and The telescope of the telescope of the telescope of tel	P1	Invaring	CP-2 CP-7 CP-7 CP-7 CP-1 Not: Not: Not: IA-2 (8) (1	CP-1 (1) (3) (8 CP-3 P-4 (1)	CP-2 (1) (4) (1) (4) (2) (4) (2) (4) (2) (4) (2) (4) (2) (4) (2) (4) (2) (4) (2) (4) (2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	(2) (3) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5(1) (2) (3 MP-7 (1) Not Selected PE-2 PE-3 (1) PE-6 PE-6 (1) (4) PE-10 PE-10 PE-11 PE-12 PE-14 PE-14	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-6 IIA-6 IIA-9	Procedures Contingency Contingency Contingency Contingency Contingency Contingency Contingency Contingency Contingency Alternate Sto Alternate Sto Alternate Sto Alternate Sto Information S Reconstitution Safe Mode Alternate Co Safe Mode Alternate Co Safe Mode Identification Cyganization Device Identi Identification Cygnization Authenticator Cryptographi Identification Cygnization Service Identi	Plan Training Plan Testition Training Plan Testition Training Plan Testition	Con Policy and The te The te	P1	Invarience	CP-2 CP-7 CP-7 CP-7 CP-1 CP-1 IA-2 (8) (1) IA-5 (1) IA-8 (1	CP-1 (1) (3) (8 CP-3 P-4 (1) (3) (8 CP-3 P-4 (1) (3) (1) (2) (3 (4) (2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	CP-0 (4)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)	(2) (3) (1) (1) (2) (3) (1) (1) (1) (1) (1) (2) (3) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (4) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5(1)(2)(3 MP-7(1) Not Selected PE-2 PE-3(1) PE-4 PE-5 PE-6(1)(4) PE-10 PE-10 PE-11 PE-12 PE-14 PE-14	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-6 CP-7 CP-8 CP-10 CP-11 CP-11 IA-1 IA-2 IA-3 IA-6 IA-6 IA-7 IA-8 IA-9 IA-9	Procedures Contingency Contingency Contingency Contingency Contingency Withdrawn Albernate Pro Telecommuni Information S Information Informati	Plan Training Plan Testit Plan	Con Con Con Colory and Tog Tog Tog Tog Tog Tog Tog To	P1	Tanning CP-1 CP-2 CP-3 CP-3 CP-8 CP-8 CP-8 CP-8 CP-9 Not Selected	CP-2 CP-7 CP-7 CP-1 Not: Not: Not: IA-2 (8) (1) IA-8 Not: Not: Not: Not: Not: Not: Not: Not:	CP-1 (1) (3) (8 CP-3 P-4 (1)	CFF (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)	(2) (3) (1) (2) (3) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (4) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5(1)(2)(3 MP-7(1) Not Selected PE-2 PE-3(1) PE-4 PE-5 PE-6(1)(4) PE-10 PE-10 PE-11 PE-12 PE-14 PE-14	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-3 CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-6 IIA-6 IIA-9	Procedures Contingency Contingency Contingency Contingency Contingency Contingency Contingency Contingency Contingency Alternate Sto Alternate Sto Alternate Sto Alternate Sto Information S Reconstitution Safe Mode Alternate Co Safe Mode Alternate Co Safe Mode Identification Cyganization Device Identi Identification Cygnization Authenticator Cryptographi Identification Cygnization Service Identi	Plan Training Plan Testit Plan	Con Colory and C	P1	Inaming CP-1 CP-2 CP-3 CP-3 CP-3 CP-3 CP-3 Not Selected Not Selected Not Selected Not Selected Local Selected Not Selected Local Selected Not Selected Local	CP-2 CP-7 CP-7 CP-1 Not: Not: Not: IA-2 (8) (1) IA-8 Not: Not: Not: Not: Not: Not: Not: Not:	CP-1 (1) (3) (8 CP-3 P-4 (1) (3) (8 CP-3 P-4 (1) (3) (1) (2) (3 (4) (2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	CFF (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)	(2) (3) (1) (2) (3) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (4) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5(1)(2)(3 MP-7(1) Not Selected PE-2 PE-3(1) PE-4 PE-5 PE-6(1)(4) PE-10 PE-10 PE-11 PE-12 PE-14 PE-14	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16
CP-2 CP-3 CP-4 CP-5 CP-6 CP-6 CP-7 CP-8 CP-10 CP-11 CP-11 IA-1 IA-2 IA-3 IA-6 IA-6 IA-7 IA-8 IA-9 IA-9	Procedures Contingency Contingency Contingency Contingency Withdrawn Albernate Pro Telecommuni Information S Information Information S Information Information Information S Information Informati	Plan Training Plan Testing Plan	Con Colory and C	P1	Inaming CP-1 CP-2 CP-3 CP-3 CP-3 CP-3 CP-3 Not Selected Not Selected Not Selected Not Selected Local Selected Not Selected Local Selected Not Selected Local	(CP-2 (CP-2 (CP-7	CP-1 (1) (3) (8 CP-3 P-4 (1)	CFF (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)	(2) (3) (1) (2) (3) (1) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	1)	MA-6 MP-1 MP-2 MP-3 MP-4 MP-5(1)(2)(3 MP-7(1) Not Selected PE-2 PE-3(1) PE-4 PE-5 PE-6(1)(4) PE-10 PE-10 PE-11 PE-12 PE-14 PE-14	ect	ted) (9)	RA-1 RA-2 RA-3	SC-1 ot Sele SC-1 SC-1 SC-1 SC-2 SC-2 SC-2 SC-2 SC-2	5 ected 7 8 9 10 11 11 12 13	SC-15 Not Select SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23		Selected Selected SI-16	Not Selected SI-16

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

	TABLE D-2: SECURI	TY CON	TROL BASELINE	S ⁹²	
CNTL		RITY	INITIA	L CONTROL BASE	ELINES
NO.	CONTROL NAME	PRIORITY	LOW	MOD	HIGH
	Acc	ess Con	trol		
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn			-	-
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	Withdrawn				
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

											_	_			_		_	_			
											CN	.					È		INITIAL	CONTROL BA	ASELINES
											NO		CON	TROL	NA	ME	наонт	L	ow	MOD	HIGH
											SC-		hin Nodes				PO		elected	Not Selected	
											SC-		oneypots latform-Indepen				PO PO		elected elected	Not Selected	
											SC-		ratection of Info				P1		elected	SC-28	SC-28
															П	INITIAL C	ONTRO	BARRI	wee	: Selected	
									CNI	n.	CONT	ROL P	AME	PROBITY	H		UNINU	- UMBELL	int.	Selected Selected	
																LOW	MOG		HISH	Selected	
									S.A.	10 0	leveloper Configu leveloper Security	ation M	anagement	P1		Not Selected Not Selected	SA-1	0	SA-10 SA-11		
											leveloper security luggly Chain Prote		and Evaluation	PI			Not Sele		SA-11	Selected	Not Selecte
									SA	13 T	rustworthiness			PO	1	Not Selected	Not Sele		Not Selecte	d ! Selected	
						CNTL					È		INITIAL CON	TROL B	ASE	LINES	ot Sele		Not Selecte SA-15	Selected Selected	
						NO.		CONTR	OL NA	ME	PROBLEY	_	OW	MOO	П	нен	1			Selected	
					- 1	DC.17	Alterna	te Work Site			P2			PE-17	-	PE-17	ot Sele		SA-16 SA-17	SC-39	SC-39
						PE-18	Locatio	n of Informati	ion Syste	em Con	rponents P3	Not:	lelected Not	Selecte	d	PE-18	zt Sele		Not Selecte	Selected	
						PE-19	Informa	rion Leakage	•		P0	Not 2		Selecte		Not Selected	xt Sele		Not Selecte		
					-	PE-20	Asset 1	donitoring and	d Trackin	ng	Po		lelected Not	Selecte	d	Not Selected	ot Sele	cted	Not Selecte	Selected	
									-		INITIAL CONTR		ri nere	-1		PL/1	x Sele		Not Selecte		
				CNTL NO.	cor	UTROL	NAME		PRICHTY				_	(3)	П	PL-2 (3)	ot Sele	cted	Not Selecte		_
										LO		00	HISH	(1)	-	PL4 (1)	80-1	T	SC-1	\$1-1	\$1-1
				R-3	Incident Respon	se Testin	9	-	P2 P1	Not Sal	lected IR-	3 (2) 5 (1)	IR-3 (2) IR-4 (1) (4)	ď		-	500		50-2	31-2 (2)	\$1-2 (1) (2)
				R4	Incident Monitor	ing			P1	IR-	6 F	16	IR-5 (1)	lecte.		Not Selected	ot Sele	cted	80-3	-3 (1) (2)	SI-3 (1) (2) SI-4 (2) (4) (3
				R4	Incident Reports	10			P1	IR-	d IRA	(1)	IR4 (1)	A	0	PLA	504		SC-4 SC-6	(2) (4) (5	SI-5 (1)
		CNTL				E		INITIAL (CONTRO	OL BAS	ELINES	1	IR-7 (1)	ecte	d	Not Selected	x Sele		Not Selecte		
		NO.		ONTRO	LNAME	MCGRT		ow	MO		HIGH	fed	Not Selected		_		-7 (35)	41(%) 2	SC-7 (%) (4) I	51 (7.01)(7)	\$1,7 (1) (2) (
		CHA	Configuration	- Control		P		OM-0	CM		CM-8 (1) (2)	fed	Not Selected	7	-	PS-1 PS-2	(7) SC-8 (10	7) (0) (10) (2 SC-8 (1)	-8 (1) (2)	(7) (14) SI-8 (1) (2)
		CM-7	Least Functi	onality		P		M-7	CM-T (1)	(2)(4)	CM-7 (1) (2) (5)		-3		PS-3	***				
		CM-8	Information 5	System Co	mponent Inventory	P		M-8	CM-8 (1)	(3) (5)	CM-8 (1) (2) (3 (4) (5))	MA-1	4-5	_	PS-4 (2) PS-5	SC-1 xt Sele		SC-10 Not Selecte	SI-10	SI-10
					DATE:	LCONT	BOI BAS	EL MARIE		1.0	CM-9	(2)	MA-3 (1) (2) (PS-6	30-1		SC-12 (1)	\$1-11	SI-11
CNTL	CON	TROL N	AME	PROSTY		1		T		10	CM-10 CM-11	1)	MA-4 (2) (3)	-7		PS-7	90-1		90-13	SI-12 Selected	SI-12 I Not Selecte
					LOW	h	100	HIGH		-11	CM-11	Η=	MA-5 (1)	-	_	PS-8	-	-	2012	Selected	
AT-1			Aware	eness and	Training AT-1		T-1	AT-1		4	CP-1	1-	MA-6	-1		RA-1	80-1		SC-15	Selected	
	Security Awarene Procedures									(2) (3)	CP-2 (1) (2) (3	-	MP-1	- 2		RA-2	X Sele		Not Selecte SC-17	3710	SI-16
AT-2	Security Awarene Role-Based Secu			P1	AT-2		(2 (2) (E.3)	AT-2 G	2)	9	(4) (5) (8)		MP-2	-3		RA-3	30-1		90-18	Selected	i Not Selecte
AT-4	Security Training		9	P3	AT-4		T-4	AT-4		im im	CP-3 (1) CP-4 (1) (2)	1—	MP-3	(2)	(5)	RA-5 (1) (2) (4)	SC-1		SC-19		
AT-5	Withdrawn			-	-		-	-				1)	MP-5 (4)	lecte		(5) Not Selected	80-2		SC-20		
AU.1	Audit and Accoun		Audit	and Accor	antability ALL1		44.1	AU.1		1) (3)	CP-8 (1) (2) (3 CP-7 (1) (2) (3		MP-8 (1) (2) () ***	۰	MIT DENEURO	80-2	1	80-21		
	Procedures	samily Po	cy and								(4)		MP-7 (1) Not Selected	-	-	SA-1	50-2	2	SC-22		
AU-2	Audit Events Contract of Audit F	Records		P1	AU-2 AU-3		(2 (3) (3 (1)	AU-2 (I	(2)	1) (2)	CP-8 (1) (2) (3 (4)						SC-2	3	SC-23		
AU-4	Audit Storage Cap	pacity		P1	AU4		U4	AU-4	,	(1)	CP-9 (1) (2) (3		PE-1	-2	-	SA-2 SA-3	at Sele		SC-24		
AU-6	Response to Audi Audit Review, And	t Processi	ng Failures	P1	AU-S AU-A		U-8 1 (1) (3)	AU-5 (1) AU-6 (1) (1		0 (2)	CP-10 (2) (4)	1=	PE-2	(2)	(9)	SA-4 (1) (2) (9)	1				
				1				(0)		lected	Not Selected	1-	PE-3 (1)	- 1	-	(10) SA-5	1				
AU-7	Audit Reduction a	nd Report	Generation	P2 P1	Not Selected ALLR		17 (1) 18 (1)	AU-7 (lected	Not Selected	1-	PE-5	Ė		-	1				
AU-9	Time Stamps Protection of Audi	t Informati	on.	PI	AU-9		1-2 (4)	AU-9 (2) (2		lected	Not Selected	9	PE-8 (1) (4)	7-	_	5A-8					
AU-10	Non-repudiation			P2	Not Selected		elected	AU-10		-1	14-1	1-	PE-8 (1)	(2)	-	SA-8 (2)	1				
AU-11 AU-12	Audit Record Ren Audit Generation			P3 P1	AU-11 AU-12		U-11 U-12	AU-11 AU-12 (1)	1/20	(2) (5)	14-2 (1) (2) (3)	-	PE-0	_	_		•				
AU-13	Monitoring for Info		isclosure	PO	Not Selected		elected	Not Selec	ited)(12)	(4) (0) (9) (11) (12)	11-	PE-10 PE-11 (1)	-							
AU-14 AU-15	Session Audit Alternate Audit Co			PO	Not Selected Not Selected		elected	Not Selec		3	IA-3	1-	PE-11 (1)	-							
AU-15	Cross-Organizatio			PO	Not Selected		elected	Not Selec		(2)(3)	IA-6 (1) (2) (3)	3)	PE-13 (1) (2								
			Security Asse	essment a	nd Authorization	-				0	(11)	4-	(a) PE-14	-							
CA-1	Security Assessm Policies and Proo	ent and Ar edures	thorization	P1	CA-1		A-1	CA-1	- 1	0 2	IA-6 IA-7	+=	PE-15 (1)								
CA-2	Security Assessm	rent's		P2	CA/2		·2 (1)	CA/2 (1)		(2) (3)	W-8 (1) (2) (3)	1-	PE-16								
CA-8	System Interconn Withdrawn	ections		P1	CA-3	CA	A (5)	CA-3 (5	5)	lected	(4) Not Selected	+									
CA-5	Plan of Action and		15	P3	CA-6		A-5	CA-5		lected	Not Selected										
CA-6	Security Authoriza			P2	CA-6		A-6	CA-6		lected	Not Selected	4									
CA-7	Continuous Monit Penetration Testin			P2 P2	CA-7 Not Selected		7 (1) lelected	CA-7 (1			18.1	-									
	Internal System C			P2	CA-9		A4	CAG		2	IR-2 (1) (2)										
CA-8 CA-9				aration Ma																	
CA-0				P1	CM-1		M-1	CM-1													
CM-1	Configuration Mar Procedures		only and			_		_													
CA-9	Configuration Mar Procedures Baseline Configur		- OLY BIO	PI	CM-2	CM-2	(1) (2) (7)	CM-2 (1) (2	2) (3)												
CM-1 CM-2 CM-3	Procedures Baseline Configur Configuration Cha	ration ange Contr		P1	CM-2 Not Selected	CN	1-3 (2)	CM-2 (1) (2 (7) CM-3 (1)	(2)												
CM-1 CM-2	Procedures Baseline Configur	ration ange Contr	ol	PI	CM-2 Not Selected CM-4	CN			(2)												

45

AC-1

NIST Special Publication 800-53 **Security and Privacy Controls for Federal Information Systems** and Organizations JOINT TASK FORCE TRANSFORMATION INITIATIVE This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-53r4 Standards and Technology

U.S. Department of Commerce

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

- a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
 - An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Procedures to facilitate the implementation of the access control policy and associated access controls; and
- b. Reviews and updates the current:
 - Access control policy [Assignment: organization-defined frequency]; and
 - Access control procedures [Assignment: organization-defined frequency].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1 LOW AC-1 MOD AC-1 HIGH AC-1 46

What kind of control is Access Control?

NIST Special Publication 800-18 Revision 1

National Institute of Standards and Technology Technology Administration U.S. Department of Commerce Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson Joan Hash Pauline Bowen

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

February 2006



U.S. Department of Commerce Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

NIST Special Publication 800-18 Revision 1

National Institute of Standards and Technology Technology Administration U.S. Department of Commerce Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson Joan Hash Pauline Bowen

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

February 2006



U.S. Department of Commerce Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Risk Assessment (RA) Controls

	Risk Assessment											
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1							
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2							
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3							
RA-4	Withdrawn											
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)							
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected							

FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

- Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
 - A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
- b. Reviews and updates the current:
 - 1. Risk assessment policy [Assignment: organization-defined frequency]; and
 - 2. Risk assessment procedures [Assignment: organization-defined frequency].

scope, roles, responsibilities, rganizational entities, and compliance;

risk assessment policy and associated

n-defined frequency]; and zation-defined frequency].

iment of policy and procedures for the control enhancements in the RA family. cutive Orders, directives, regulations, es and procedures at the organization procedures unnecessary. The policy can icy for organizations or conversely, can nature of certain organizations. The general and for particular information

systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.

Priority and Baseline Allocation:

P1 LOW RA-1 MOD RA-1 HIGH RA-1 50

RA-2 SECURITY CATEGORIZATION

Control: The organization:

- Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Documents the security categorization results (including supporting rationale) in the security

RA-2 SECURITY CATEGORIZATION

Control: The organization:

- Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

ntative reviews

for effective
e impacts to
information and
vailability
activity with
information
nizations also
ith the USA
national-level

development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	LOW RA-2	MOD RA-2	HIGH RA-2	51

RA-3 RISK ASSESSMENT

Control: The organization:

- Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];

RA-3 RISK ASSESSMENT

Control: The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
- Reviews risk assessment results [Assignment: organization-defined frequency];
- d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
- e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Ennancements. INOIE.

References: OMB Memorandum 04-04; NIST Special Publications 800-30, 800-39;

Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1 LOW RA-3 MOD RA-3 HIGH RA-3

r there ig the

ive

ion unt

on

rcing ition of c or

access

on

ilso be ecurity

ol must

t role

ice,

Exercise

- 1. Using your favorite search engine...
 - Find an organization's IT risk assessment policy and procedures
 - Assess how well the policy meets requirements of RA-1
 - Assess how well the procedures meet RA2 and RA3
- 2. Return to class discussion
- 3. Present your findings

Agenda

- ✓ NIST Risk Management Framework and FIPS 199
- ✓ Use of NIST SP 800-60 Volume 1 and Volume 2
- ✓ Exercise Determine and finalize impact levels
- ✓ Exercise Determine Information and Information System Types and provisional security categorization
- ✓ Security Control Baselines review
 - ✓ FIPS 200 and NIST 800-53 Security Control Baselines
 - ✓ Security Control Families
- ✓ Risk Assessment Controls
- ✓ Team Exercise Find and assess risk assessment policy

Unit #3

MIS5214

Planning and Policy