Managing Enterprise Cybersecurity
MIS 4596

Unit #23

Case Study 2 – Cyberattack: The Maersk Global Supply-Chain Meltdown

Agenda

- Discussion
  - Why was Maersk attacked?
  - Why was NotPetya attack on Maersk successful?
  - What can companies do to mitigate impacts of cyberattacks on availability?
- Cyber Security Controls: Contingency Planning
  - Business Continuity and Disaster Recovery
- How would you rate Maersk’s InfoSec maturity?

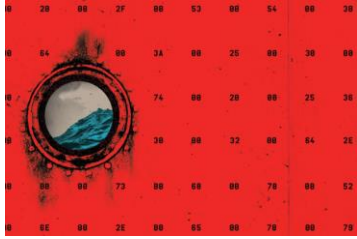
Discussion

- Why was Maersk attacked?
- Why was NotPetya attack on Maersk successful?
- What can companies do to mitigate impacts of ransomware & file encryption attacks?

Why was Maersk attacked?

- Likely collateral damage from an attack by Russia on Ukraine
- NotPetya was likely a warning message sent to international firms not to do business in Ukraine, perhaps to deter foreign investment and/or delay European Union membership
- Hacker accessed and infected systems weeks or months prior to the attack, perhaps leaving evidence of espionage against Ukrainaian government and businesses. Ransomware attack not only disabled computers, but erased evidence of spying

Timeline



2016 – Maersk shipping company's senior system administrators warn company that its network of 80,000+ computers was vulnerable to attack

- Windows 2000 servers and Windows XP computers overdue for replacement
- Leadership approved upgrades, but systems administrators not motivated to implement the upgrades (due to bonuses based on "uptime" and not security)

2017, March – Microsoft issues emergency patch to update systems and protect from NotPetya

2017, June – NotPetya encryption attack

- IT availability loss
  - Active directory domain controllers (network of 150 of them) providing centralized store of usernames and passwords and access control authorization information all wiped out
  - Fall-back to manual business continuity activities
  - 1 domain controller in Ghana protected by power outage and served as a source for restoring domain control and access to restore systems
- 10-days of lost business ($300,000,000 in expenses and lost earnings)
  - **Note: 60% of small companies are unable to sustain their businesses over 6 months after a cyber attack!**

2017, July – System upgraded (4,000 new servers, 45,000 new PC's, with 2,500 applications) and computer-based business processes restored

Why was the NotPetya attack on Maersk successful?

- Systems not upgraded nor patched to protect from NotPetya virus/malware
- All data, backups and systems accessible on the Internet (except Ghana Active Directory server)
- No contingency planning (Business Continuity Plan / Disaster Recovery Plan)

NotPetya

- Arrives as infected e-mail attachments
- Designed to spread automatically, rapidly, and indiscriminately
- Propelled by two powerful hacker exploits working in tandem:
  1. EternalBlue
     - Penetration tool stolen from US NSA that takes advantage of a Windows Server Message Block (SMB) protocol vulnerability (CVE-2017-0144) which allowed hackers to remotely run their own code on any unpatched machine
  2. Mimikatz
     - Windows left users' passwords lingering in computers' memory
     - Once hackers gained initial access to a computer, Mimikatz would pull those passwords out of RAM and use them to hack into other machines accessible with the same credentials. On networks with multiuser computers, it could even allow an automated attack to hop from one machine to the next
  3. Encryption of disk drives (no decryption offered)

Note: Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows–based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting.

What can companies do to mitigate impacts of cyberattacks on availability?

What can companies do to mitigate impacts of cyberattacks?

- Regular operating system, anti-virus, and application updates and patches, training and incentives to keep security capabilities up-to-date
  - Greatest impact is on older unpatched software and systems
- 2-factor authentication to block hackers from infiltrating systems and networks
- Contingency planning
  - Data and system backups, training and practice in backing up and restoring systems

Agenda

- ✓Breakout Groups
  - ✓Why was Maersk attacked?
  - ✓Why was NotPetya attack on Maersk successful?
  - ✓What can companies do to mitigate impacts of cyberattacks on availability?
- Cyber Security Controls: Contingency Planning
  - Business Continuity and Disaster Recovery
- How would you rate Maersk's InfoSec maturity?

To assure resilient response

Business Continuity Plan (BCP)

Documented procedures for recovering and resuming critical operational functions following significant disruption

Source: ISO 22301:2012
Societal security – Business continuity management systems - Requirements

…includes a Disaster Recovery Plan (DRP)

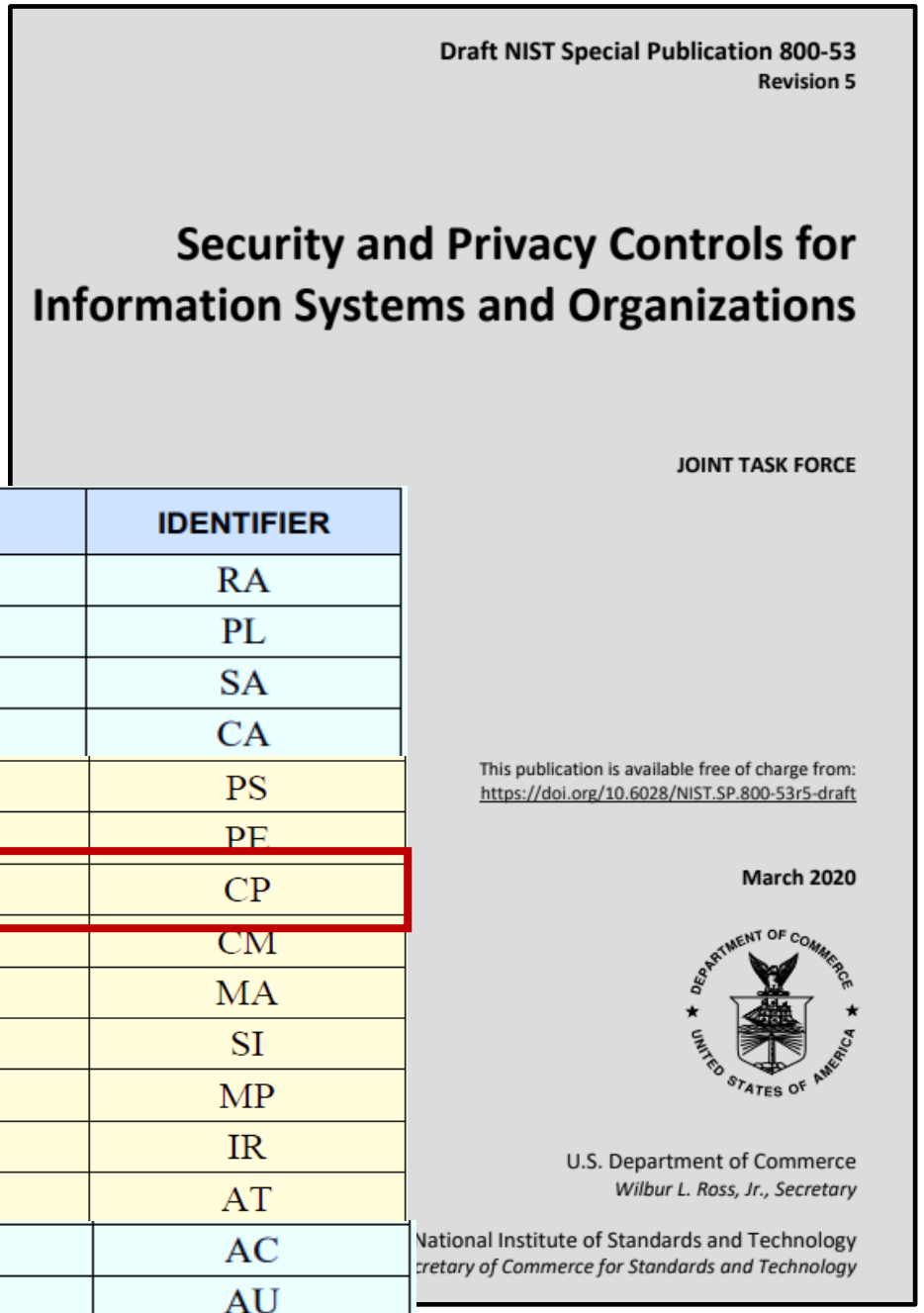
Procedures for recovering critical information systems operations following significant disruption

Catalog of cyber-security controls

for Business Continuity and Resiliency planning focus on Contingency Planning controls

Operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems) with technical expertise and/or management expertise

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	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC


Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5-draft

March 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Secretary of Commerce for Standards and Technology

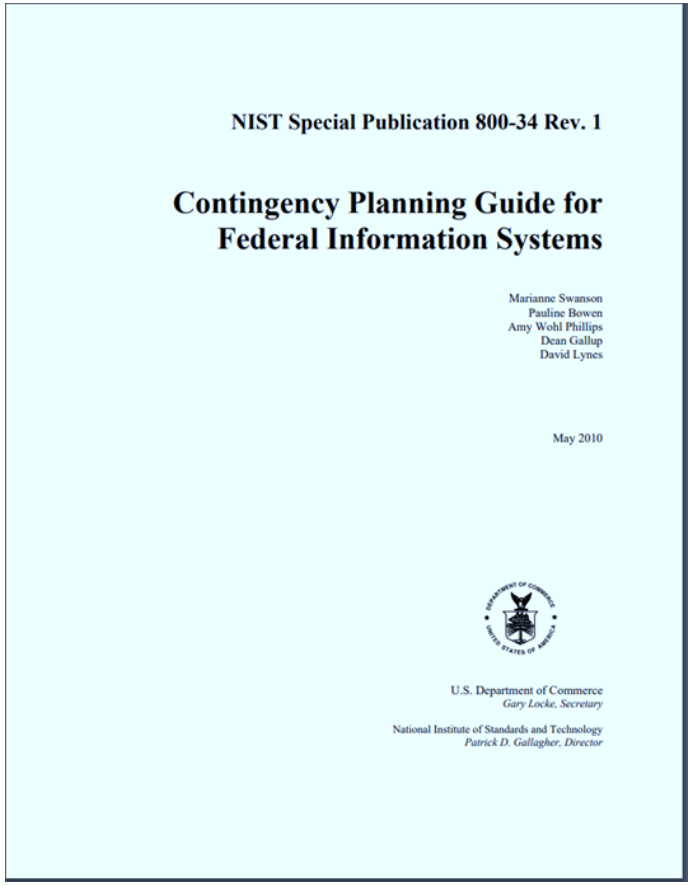
Contingency Planning Controls

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations"

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			

Contingency Plan



NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

May 2010

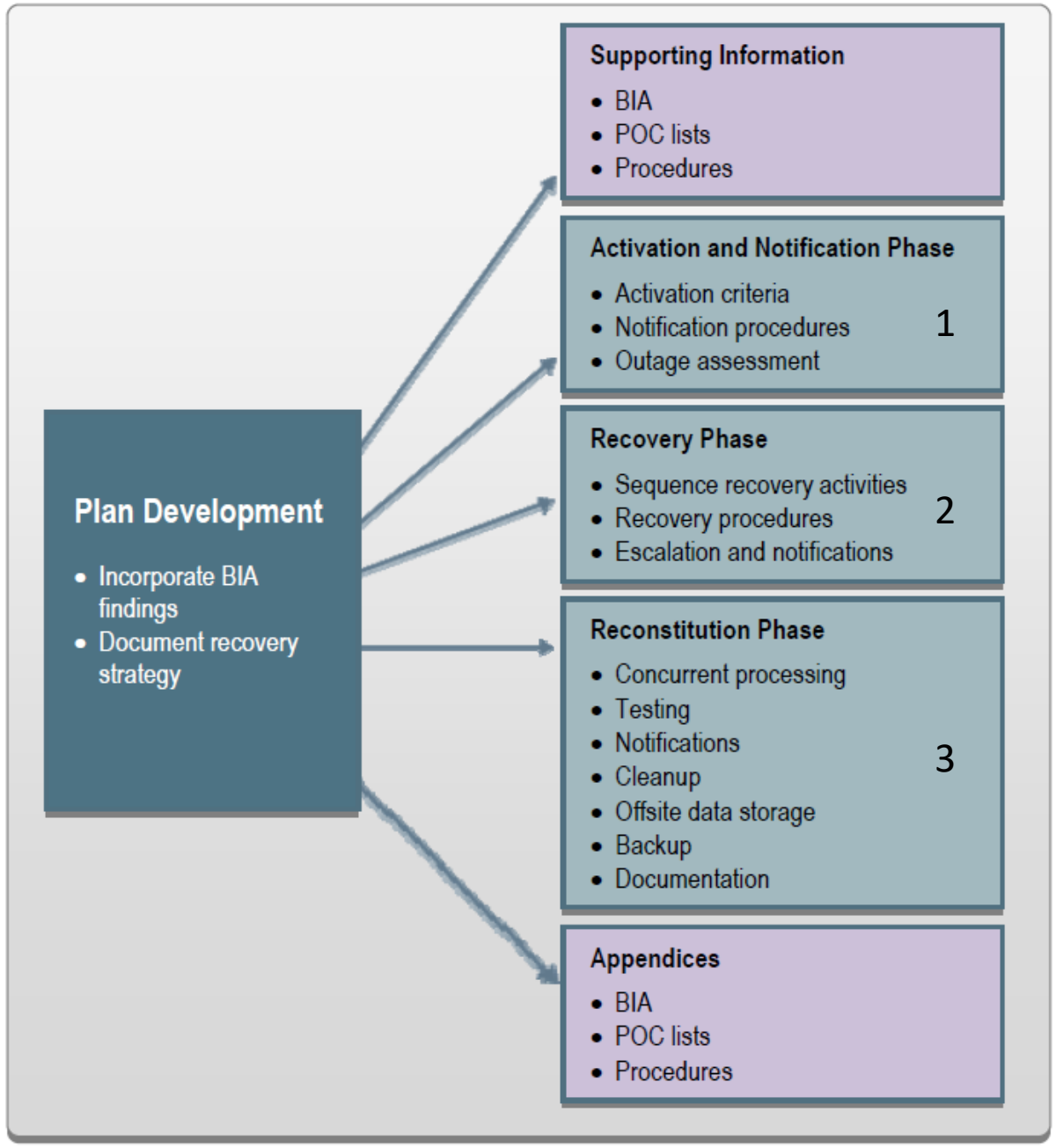
U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

TABLE OF CONTENTS

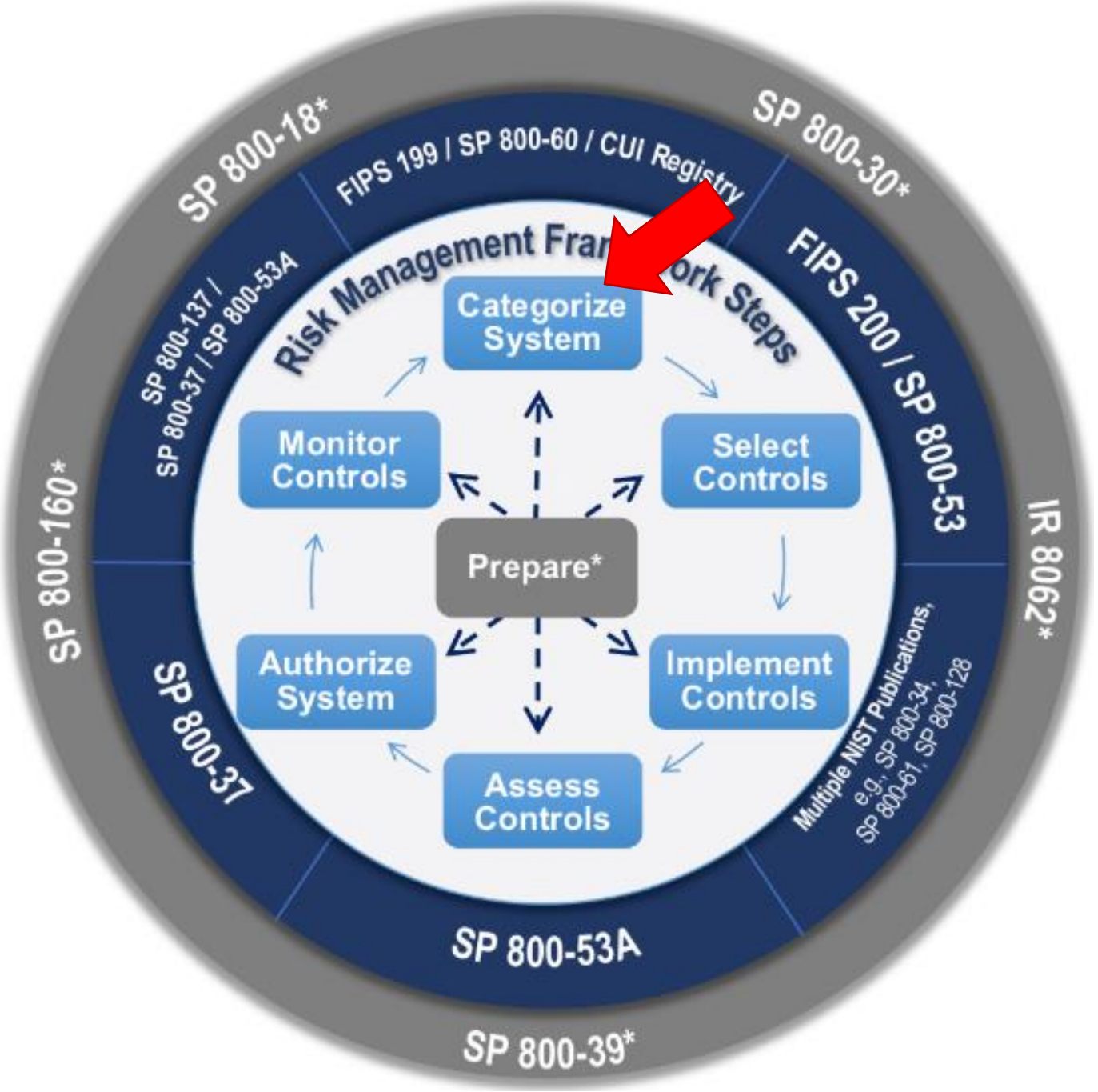
3-Phases in a Contingency Plan

All dependent on a BIA “Business Impact Analysis”



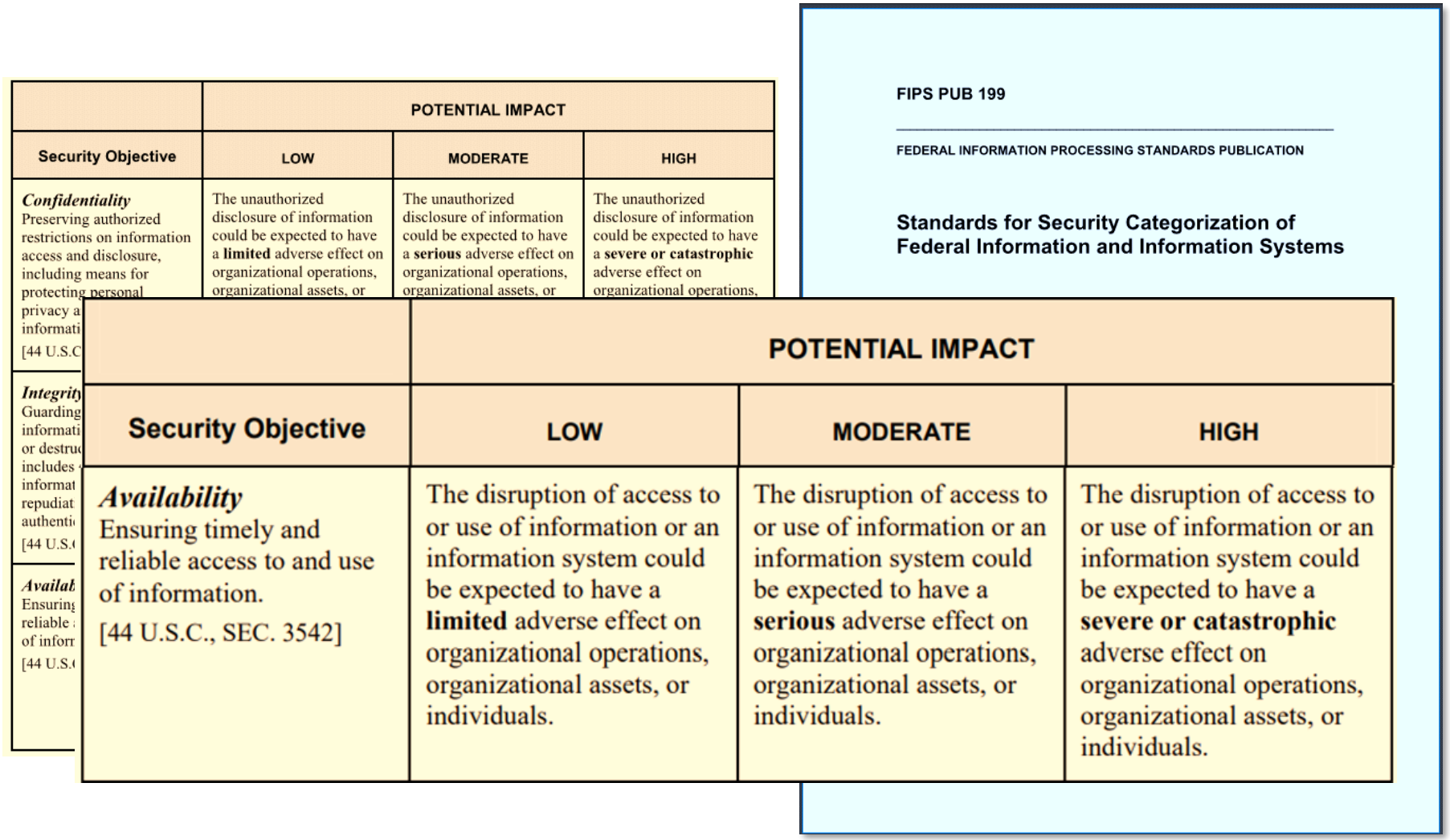
NIST SP 800-34 R1 Contingency Planning Guide for Federal Information Systems

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



Inventorying, categorizing impact of loss of availability of information systems enables us to understand how to prioritize them for recovery…

Impact on which security objective determines priorities for recovery?



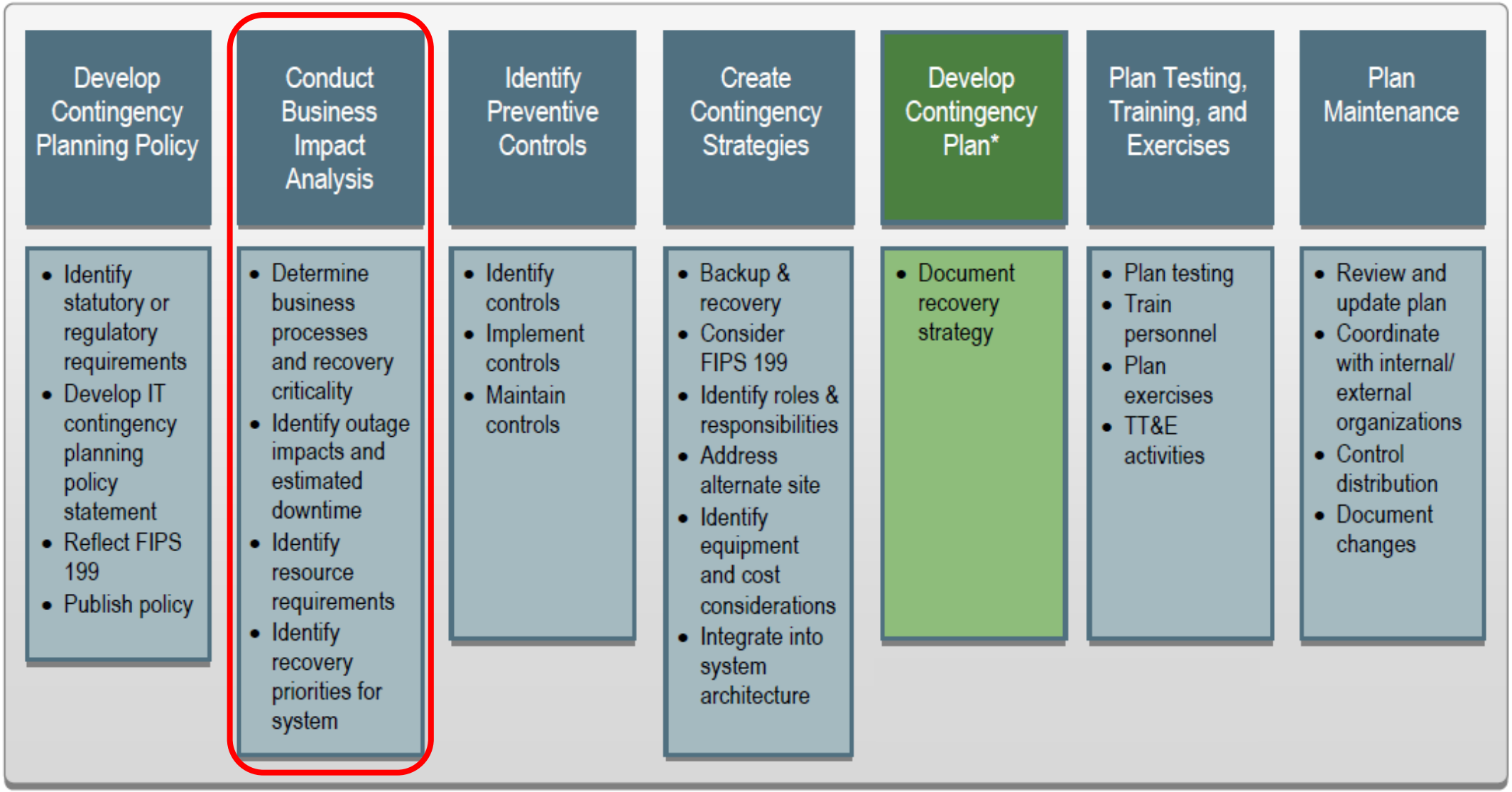
FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
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.

Plan is based on “recovery priorities”



NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems

Business Impact Analysis (BIA) Answers

1. What are the business' work processes ?
2. How critical is each ?
3. What data, applications, and people are needed to run each critical process ?
4. What are the priorities for recovering information systems after disruption ?

5. For each critical IT resource, what are:
   - **Recover time objective** (RTO):

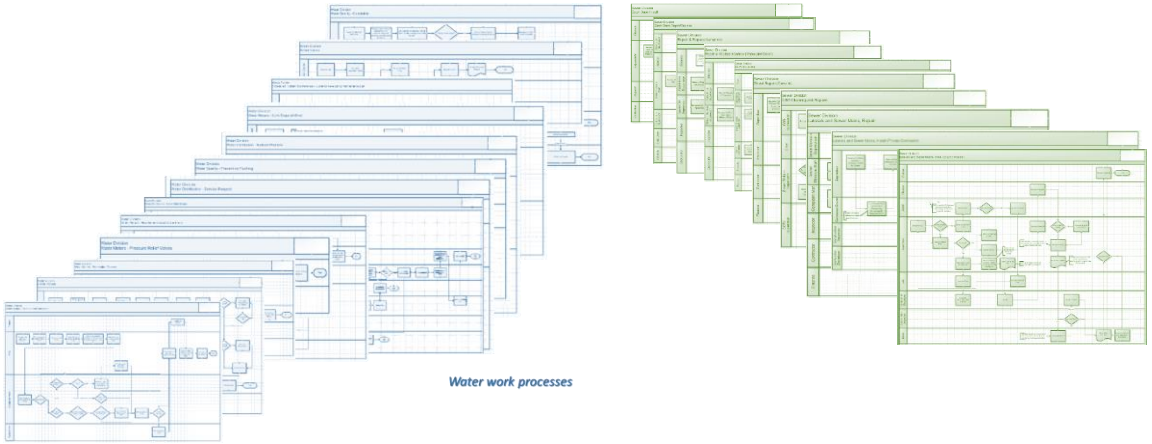
     Maximum acceptable downtime

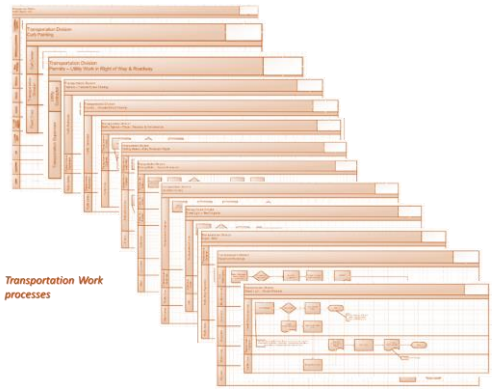
   - **Recovery point objective** (RPO):

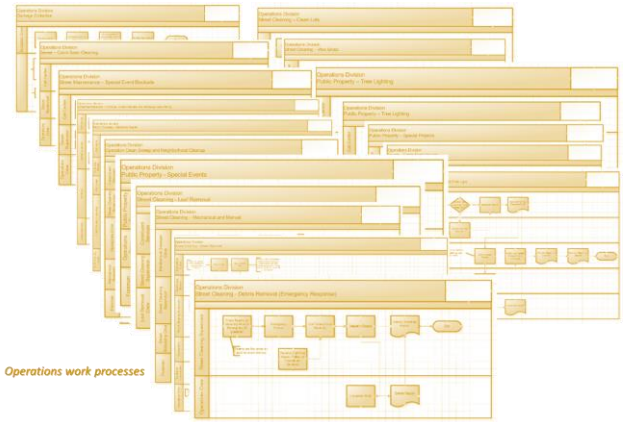
     Maximum acceptable data loss (measured in time, but implies # of data records)

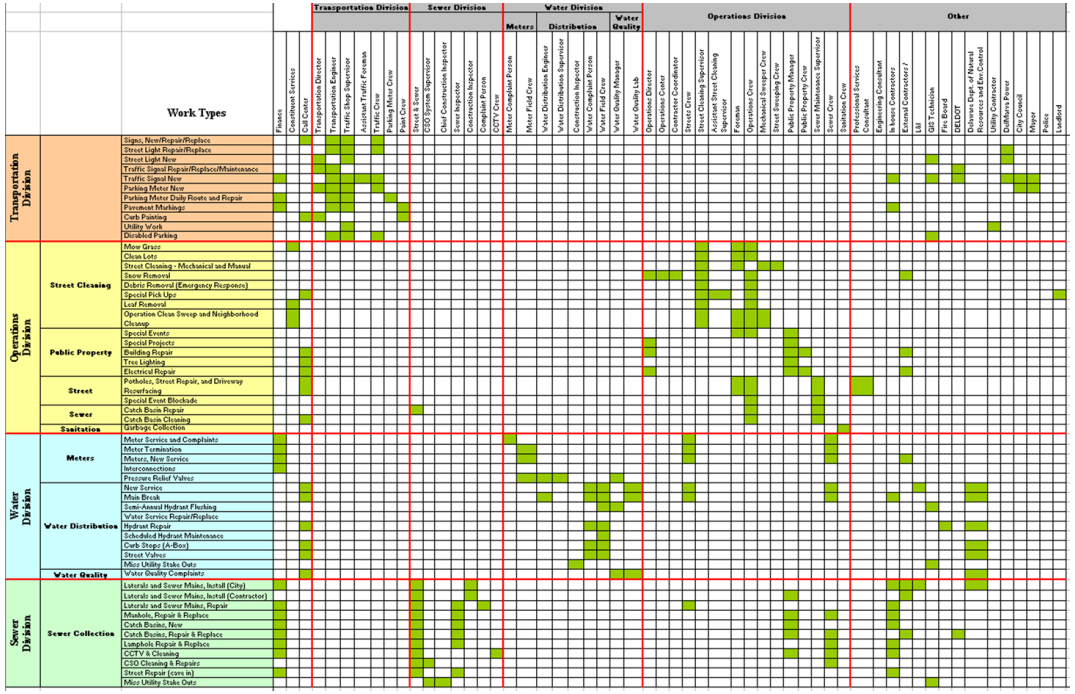
Prerequisite for BIA and contingency planning…

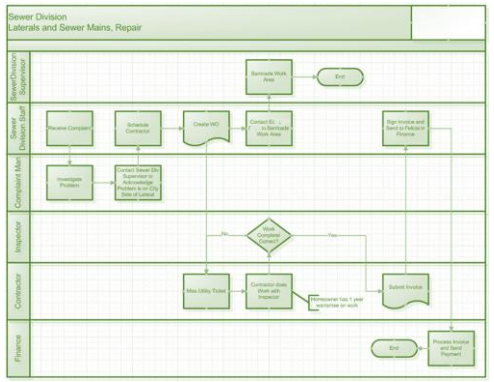
Good work process documentation identifies all people, data, applications, communications and information technologies needed to restore operations





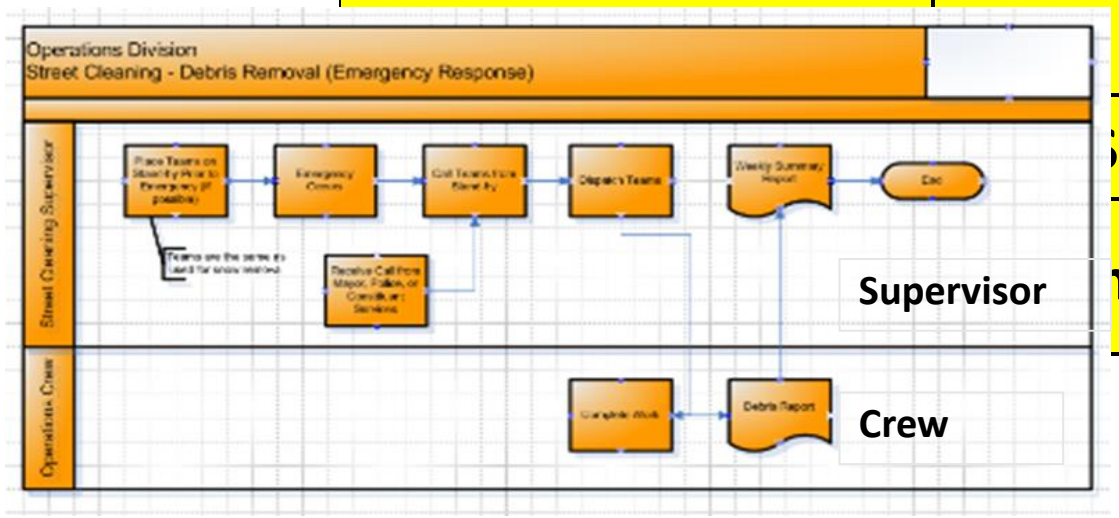






Priorities of business processes for recovery example

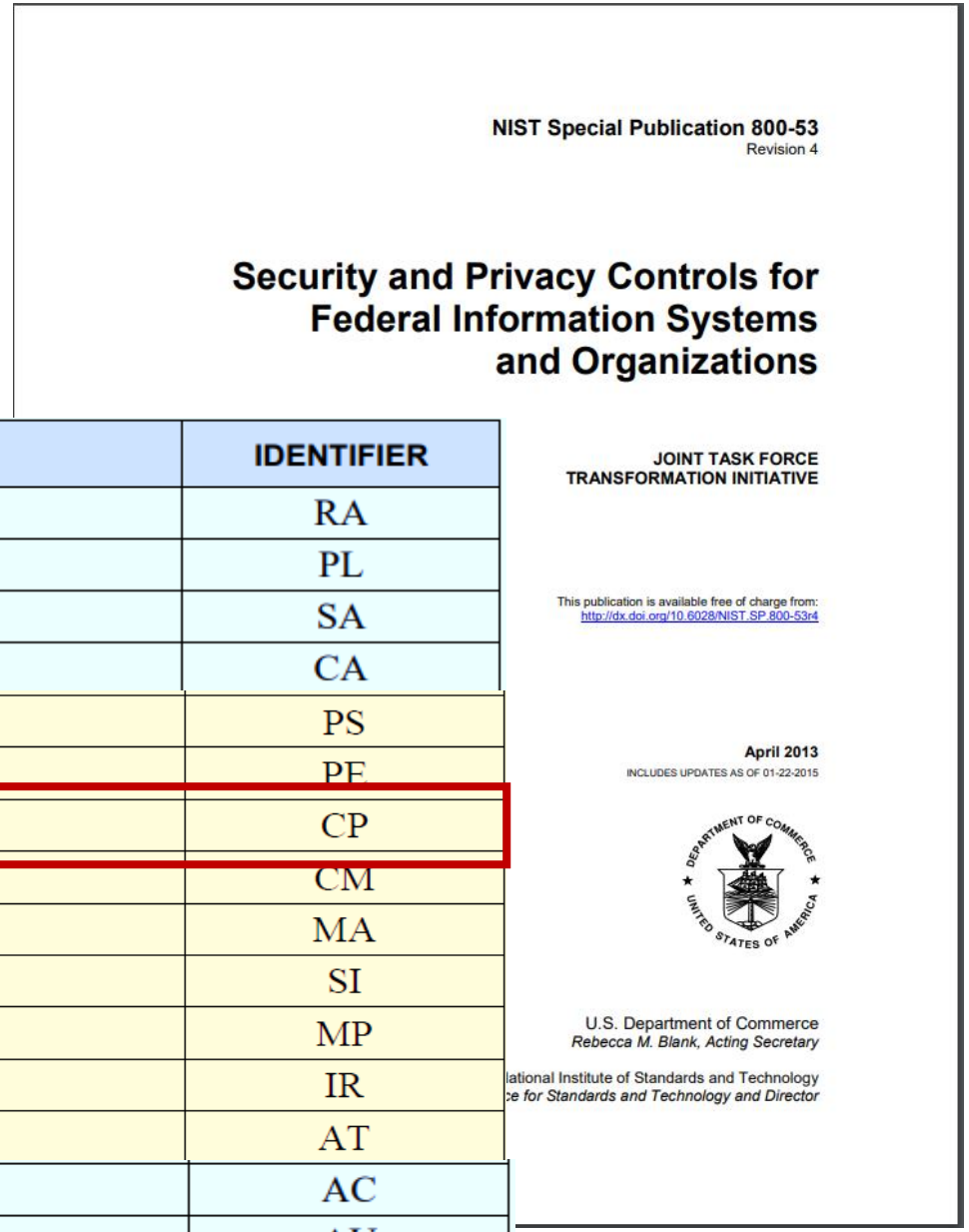
Public Works Dept Operations Division	**Street Cleaning**	**Mow Grass**
		Clean Lots
		Street Cleaning - Mechanical and Manual
		Snow Removal
		Debris Removal (Emergency Response)
		Special Pick Ups
		Leaf Removal
		Neighborhood Cleanup
	Public Property	**Special Events**
		Special Projects
		Building Repair
		Tree Lighting
		Electrical Repair
	treet	**Potholes, Street Repair, and Resurfacing**
		Special Event Blockade
	itation	**Catch Basin Repair**
		Catch Basin Cleaning
		Garbage Collection



Catalog of cyber-security controls

for Business Continuity and Resiliency planning focus on Contingency Planning 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	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC



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

April 2013

INCLUDES UPDATES AS OF 01-22-2015

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

ational Institute of Standards and Technology
ce for Standards and Technology and Director

Contingency Planning Controls

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations"

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			

Options for alternate Data Processing Site

Hot site: A geographically remote facility, fully equipped and ready to power up at a moments notice

Warm site: Includes communications components but computers are not installed – will need to be delivered and setup

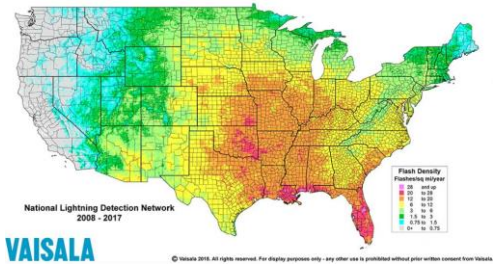
Cold site: Provides only the basic environment that can be outfitted with communication, utilities and computers

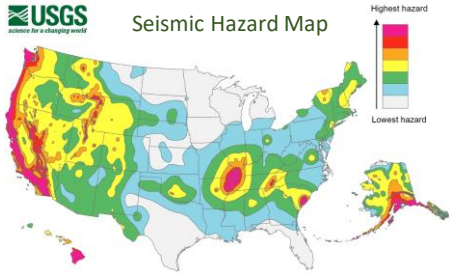
Site	Cost	Hardware Equipment	Telecommunications	Setup Time
Hot Site	High	Full	Full	Short
Warm Site	Medium	Partial	Full / Partial	Medium
Cold Site	Low	None	None	Long

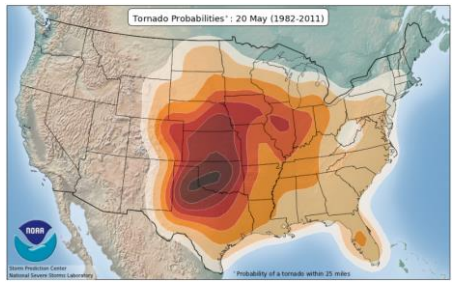
Location of Alternate site

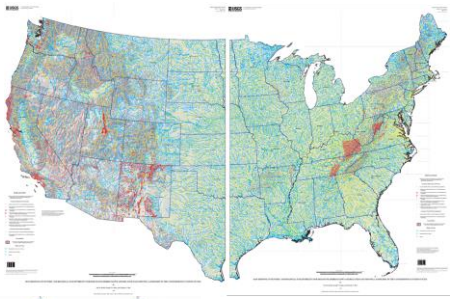
Disaster recovery site should be in a different geophysical area not susceptible to same disaster as the primary operations facility

Note: even the cloud is located somewhere…

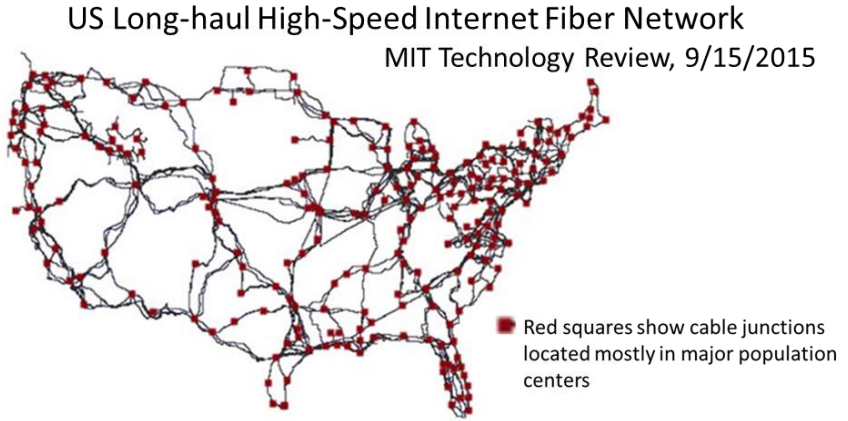








With multiple providers of:



- Telecommunications
- Stable power supply
- Redundant utilities

Contingency Planning Controls

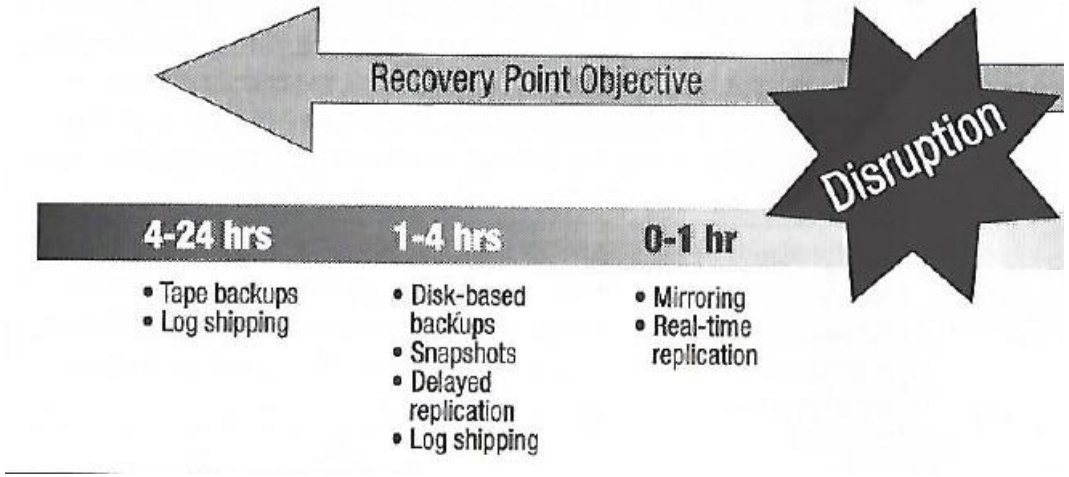
CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

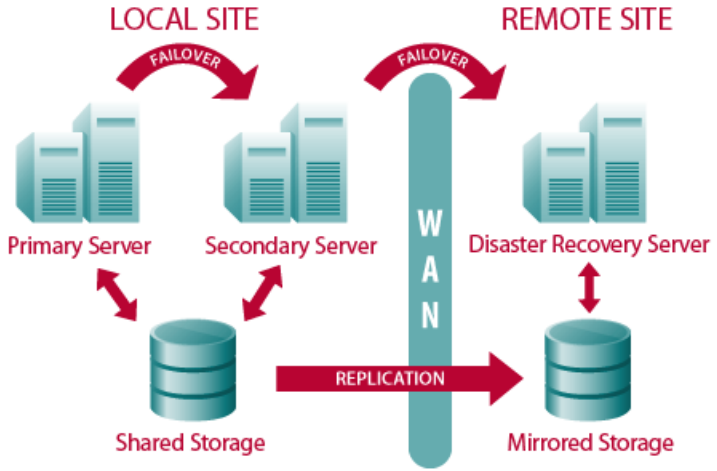
NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations"

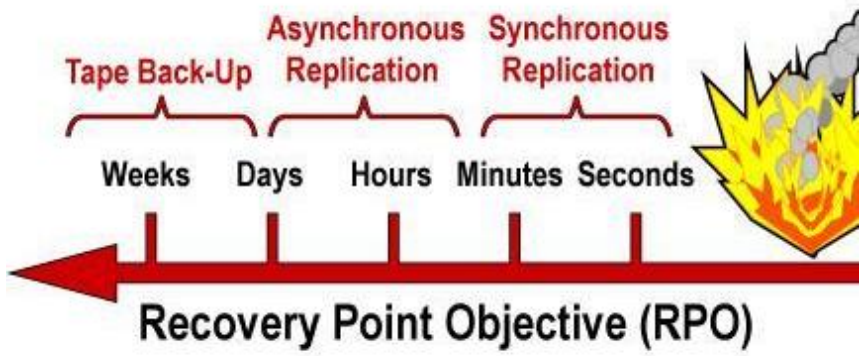
CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			

Data backup systems and redundancies

- **Database shadowing**
- **Electronic vaulting**
- **Remote journaling**
- **Storage area network and hierarchical storage management**
- **Shared storage**
- **RAID**
- **Failover clustering**



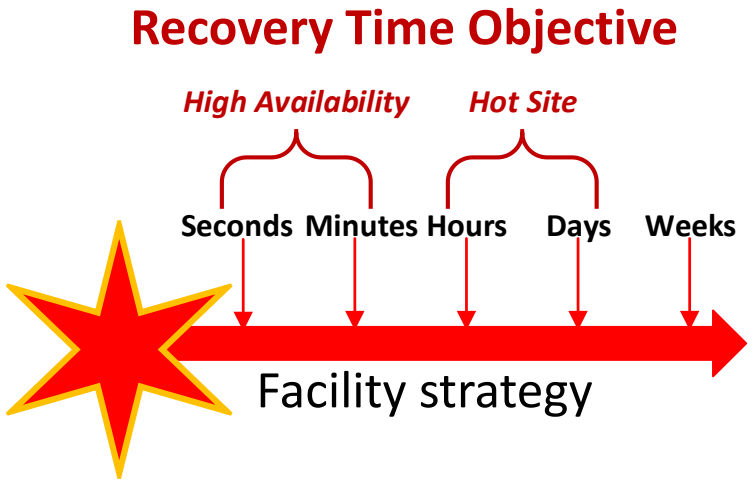


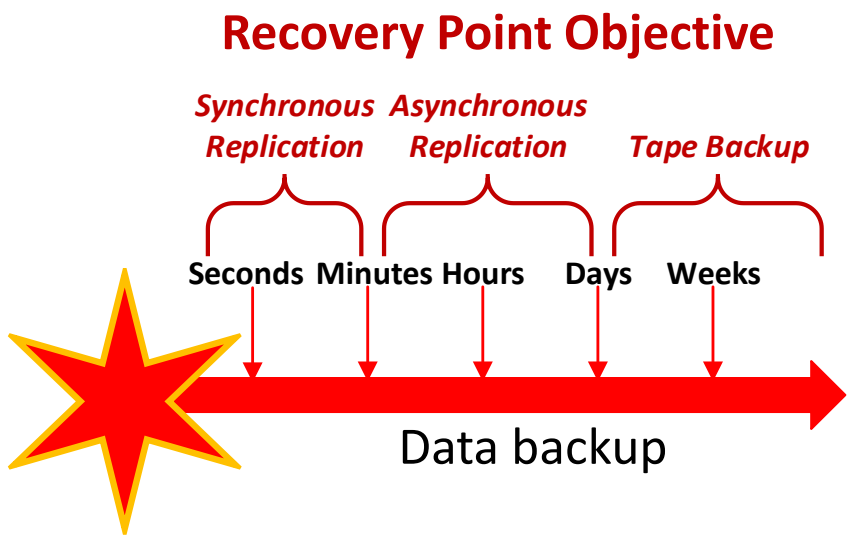


Recovery Options: Location & Backup

Information System Recovery Priority	Backup / Recovery Strategy
High priority	**Backup:** Mirrored systems and disc replication **Strategy:** Hot site $$$
Moderate priority	**Backup:** Optical backup and WAN/VLAN replication **Strategy:** Warm or Cold site $$
Low priority	**Backup:** Tape backup **Strategy:** Cold site $

[NIST SP 800-34 R1](#)
[Planning Guide for Federal Information Systems](#)



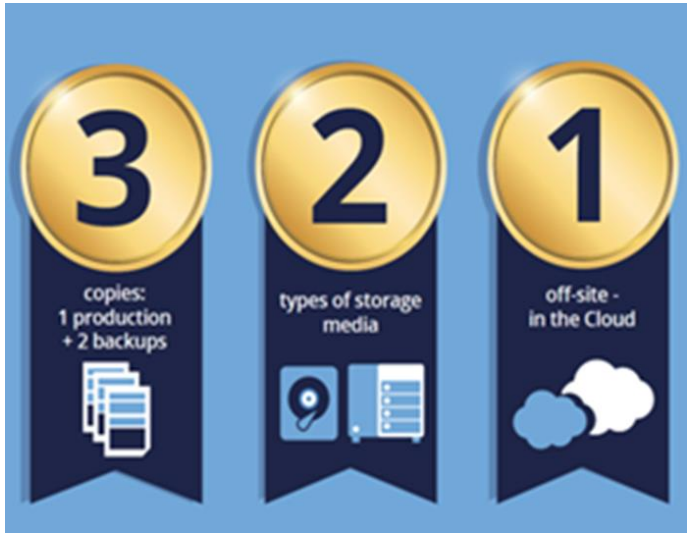


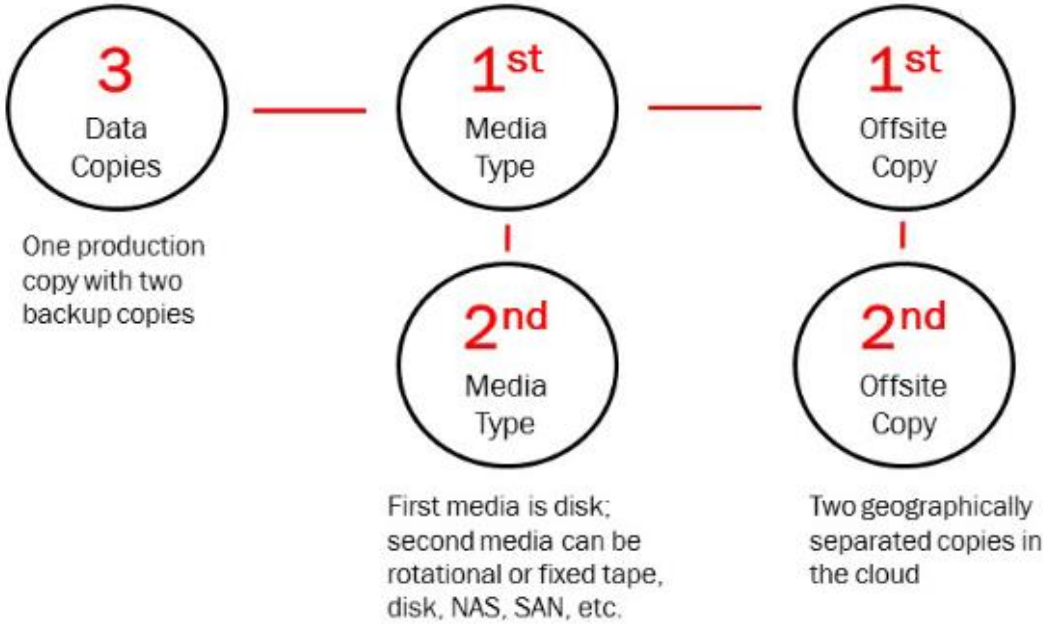
Mitigation – Best Practice

Three-Two-One rule

- Make 3 copies of all mission critical software and corresponding data in 2 different formats (to run on Linux and Windows machines), with 1 copy stored off-site not connected to any network

Maersk had 50 copies of their mission critical software and corresponding data – all in the same format, all on the network

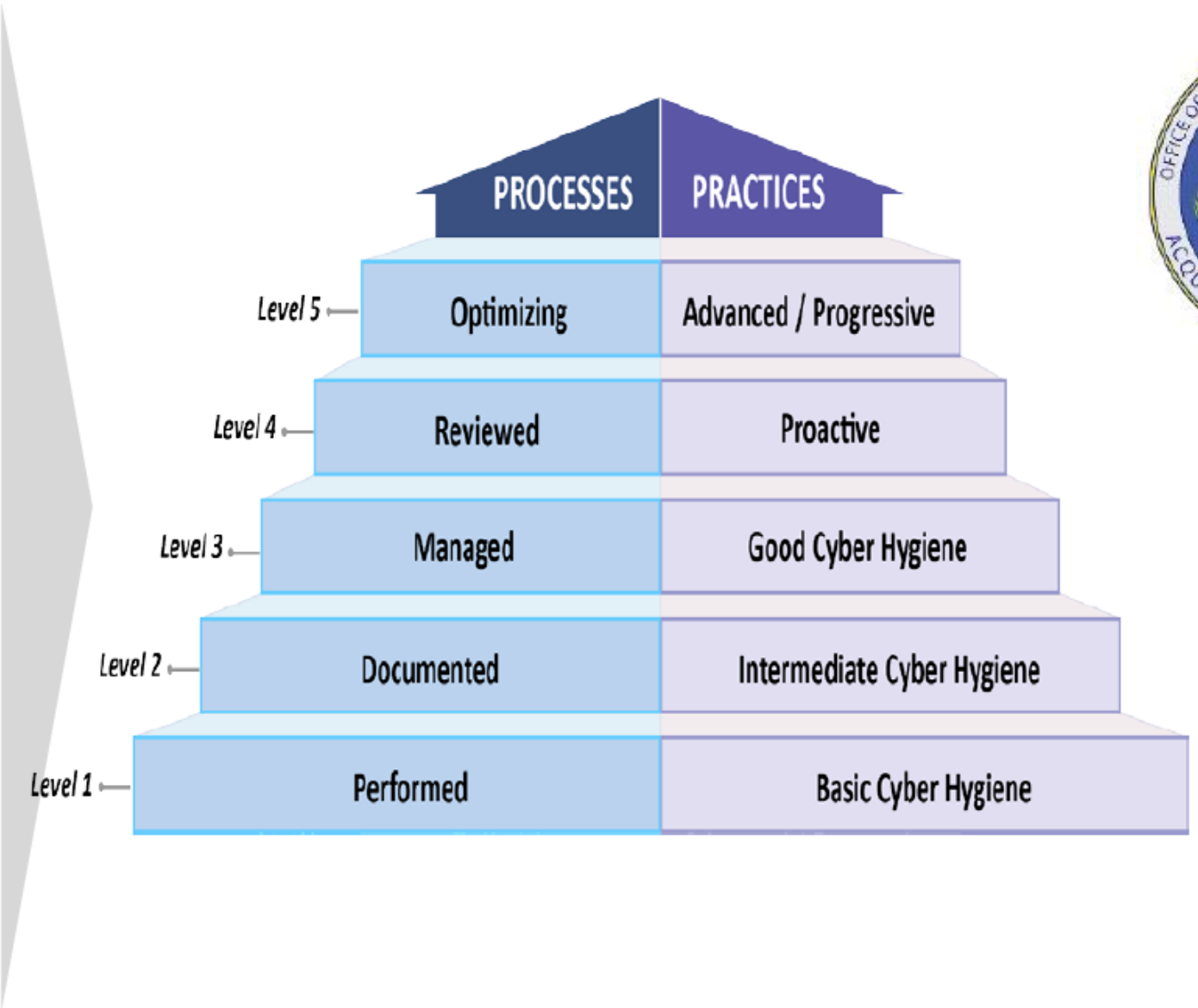




Agenda

- ✓Breakout Groups
  - ✓Why was Maersk attacked?
  - ✓Why was NotPetya attack on Maersk successful?
  - ✓What can companies do to mitigate impacts of cyberattacks on availability?
- ✓Cyber Security Controls: Contingency Planning
  - ✓Business Continuity and Disaster Recovery
- How would you rate Maersk's InfoSec maturity?

How would you rate Maersk's InfoSec maturity?



Agenda

- ✓Breakout Groups
  - ✓Why was Maersk attacked?
  - ✓Why was NotPetya attack on Maersk successful?
  - ✓What can companies do to mitigate impacts of cyberattacks on availability?
- ✓Cyber Security Controls: Contingency Planning
  - ✓Business Continuity and Disaster Recovery
- ✓How would you rate Maersk's InfoSec maturity?