Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6500.8
Transmittal Sheet
April 6, 2011

INFORMATION SYSTEM CONTINGENCY PLANNING

1. REASON FOR ISSUE: To establish operational requirements and provide specific procedures for the implementation of Information System (IS) Contingency Planning as required by the Department of Veterans Affairs (VA) Directive and Handbook 6500, *Information Security Program*, dated August 4, 2006 and September 18, 2007, respectively.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Handbook provides the specific procedures and operational requirements for implementing IS contingency planning in accordance with VA Directive and Handbook 6500*, Information Security Program*, ensuring Department-wide compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549 and the security of VA information and information systems administered by or on behalf of VA. This handbook applies to all VA organizations, their employees, and contractors working for or on behalf of VA.

This Handbook includes revisions based on the NIST SP 800-34 (Rev. 1) *Contingency Planning Guide for Federal Information Systems*. The most prevalent update is the terminology change from “Information Technology” to “Information System” and from “IT” to “IS.” It also contains the minor additions of collection of recovery point objective (RPO) and recovery time objective (RTO) data and associated definitions and descriptions.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005), Office of Information Security (005R), Office of Business Continuity (BC) (005R4).

4. RELATED DIRECTIVE: VA Directive 6500, *Information Security Program*.

5. RESCISSIONS: VA Handbook 6500.8, Information Technology Contingency Planning dated November 4, 2009.

CERTIFIED BY:

/s/
Roger W. Baker
Assistant Secretary
for Information and Technology

BY DIRECTION OF THE SECRETARY of VETERANS AFFAIRS:

/s/
Roger W. Baker
Assistant Secretary
for Information and Technology

Distribution: Electronic Only

INFORMATION SYSTEM CONTINGENCY PLANNING

CONTENTS

PARAGRAPH PAGE

APPENDICES

INFORMATION SYSTEM CONTINGENCY PLANNING

1. **PURPOSE:** The purpose of this handbook is to describe the procedures for implementing and administering the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T) information system contingency planning process. The primary objectives of this process are to:

a. Ensure VA information technology services supporting VA critical business functions can be recovered and restored following a disruption within the time parameters and the required levels established by business/service lines, either at a primary or alternate location.

b. Produce effective, auditable information system contingency plans (ISCPs) and disaster recovery plans (DRPs).

c. Refine policies, plans, and procedures and continually improve IS contingency planning by employing an iterative program management cycle.

d. Support the performance of VA's mission essential functions within the National Response Framework.

2. **SCOPE:** This Handbook addresses the procedural elements of OI&T IS contingency planning activities and provides prescriptive guidance for all OI&T personnel – VA Central Office (VACO) and field alike – supporting the resilience of VA critical business processes.

3. **ASSUMPTIONS**

a. VA IS contingency plans will be compliant with:

(1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 (Rev. 1), *Contingency Planning Guide for Federal Information Systems*;

(2) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*; and

(3) NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*.

b. Other NIST, Federal (e.g., Government Accountability Office), and industry guidance (e.g., SANS Institute, Carnegie Mellon CERT; etc., also should be considered in the development of IS contingency plans.

c. OI&T staff operating in VA Administrations and Staff Offices outside of VACO OI&T ("tenants" in other facilities) will adhere to the policies and procedures outlined in this handbook, but have broad latitude in determining, in coordination with the Administrations/Staff Offices they support, the manner in which the procedures are implemented.

4. RESPONSIBILITIES

a. **Deputy Assistant Secretary for Office of Information Security (OIS)** is responsible for advising and assisting the AS/IT on matters related to information security, including IS and business continuity planning.

b. **Director, Business Continuity (OIS/BC)** is responsible for:

(1) Developing and maintaining the IS Contingency Planning Assessment (ISCPA) process and associated ISCP and DRP templates and standards for their completion.

(2) Provision of ISCPA "train-the-trainer" education to specific OI&T personnel, as identified by local Chief Information Officers (CIOs).

c. **Information System Owners (Regional Directors) and Datacenter Directors** are responsible for ensuring compliance with the ISCPA process; and reviewing, updating, and testing ISCPs and DRPs on an annual basis and when one or more significant changes are made to a system (either the general support system or major application).

d. **Program Directors/Facility Directors**, through the Information Security Officer (ISO), are responsible for:

(1) Ensuring business/service line personnel are fully and appropriately engaged in the ISCPA process through participation in the business impact assessment (BIA); and

(2) Engaging in exercises to validate results of the process.

e. **ISOs** are responsible for:

(1) Coordinating, advising, and participating in the development and maintenance of IT contingency and DRP plans for all systems under their responsibility; and

(2) Ensuring completed and updated information system contingency plans (ISCPs) and disaster recovery plans (DRPs) are uploaded into the Security Management and Reporting Tool (SMART) database.

f. **Local CIO/System Administrators/Network Administrators** are accountable for assisting in the development and maintenance of ISCPs and DRPs for all systems under their responsibility.

5. IS CONTINGENCY PLANNING PROCEDURES

a. VA requires a robust, collaborative IS contingency planning process. For a full understanding of VA IS contingency planning policy, refer to VA Directive 6500, *Information Security Program*, dated September 18, 2007.

b. VA IT contingency planning will be conducted in the following five stages, as shown in Figure 1:

(1) IS Contingency Planning Assessment: Using the ISCPA methodology, identify and map IS contingency planning requirements through development of a Business Impact Analysis (BIA) and threat and vulnerability analyses;

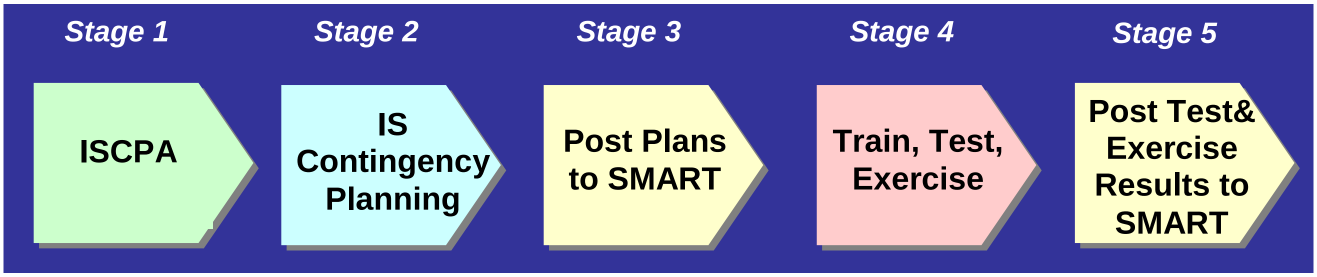
(2) IS Contingency Planning: Build ISCPs and DRPs to meet those requirements;

(3) Post Plans to SMART: Post IS contingency and DR plans to the SMART database;

(4) Train, Test, and Exercise: Train operations staff in ISCP and DRP roles/responsibilities, test individual components of plans, and exercise complete IS contingency and DR plans to validate plans work and update as necessary

(5) Post Test and Exercise Results to SMART: Post test/exercise results to the SMART database.

Figure 1: Five Stages of VA IS Contingency Planning



a. The VA IS Contingency Planning will be conducted in the following five stages as shown in Figure 1.

(1) Stage 1 – IS Contingency Planning Assessment (ISCPA) identifies and maps IS Contingency Planning requirements through development of a BIA and threat and vulnerability analyses;

(2) Stage 2 – IS Contingency Planning builds ISCPs and DRPs to meet those requirements;

(3) Stage 3 – Post Plans to SMART: Post IS Contingency and DR plans to the SMART database;

(4) Stage 4 – Train, Test, and Exercise: Train operations staff in ISCP and DRP roles/responsibilities, test individual components of plans, and exercise complete IS Contingency and DR Plans to validate plans works and update as necessary;

(5) Stage 5 – Post Test & Exercise Results to SMART: Post test/exercise results to the SMART database.

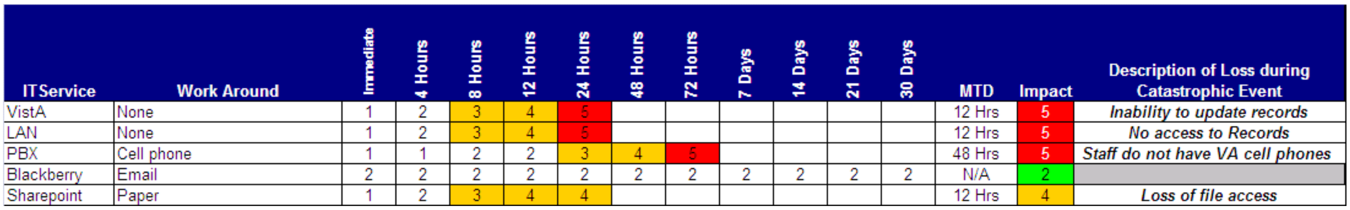
c. **STAGE 1: ISCPA.** The ISCPA is a 4-step process that collects data necessary for actual IS contingency planning. Refer to Table 1. Following Step 4, a report will be generated that identifies and prioritizes the exposures and risks for critical IS services (both general support systems and major applications) that must be accounted for in the site IS Contingency Plan (ISCP) and/or Disaster Recovery Plan (DRP).

Table 1: IS Contingency Planning Assessment Process

Step 1	***Step 2***	***Step 3***	***Step 4***
Gather Business Requirements	***Map IS Components to IS Services***	***Conduct IS Threat Assessment***	***Conduct IS Vulnerability Assessment***
Respondents: Business/Service Line Personnel	***Respondents: IS Personnel***	***Respondents: IS Personnel/ EM Personnel/Facility Management Personnel***	***Respondents: IS Personnel/ EM Personnel/Facility Management Personnel***
Substeps – *ID Critical Business Processes* – *ID Supporting IS Services* – *Determine Maximum Tolerable Downtime (MTD) for IS Services* – *ID Workarounds* – *Assign Business Impact to Loss of IS Service* – *Analyze the Impact of the Loss of IS Services on Critical Business Processes*	***Substep*** – *Map IS Components to IS Services* – *Document the Recovery Time Objective for each IS Component* – *Document the RTO for each IS Service*	***Substeps*** – *ID Threats to IS Services* – *Prioritize Threat Value to each Threat*	***Substeps*** – ***By Threat:*** – *ID Vulnerabilities of IS Services and Current Mitigation Strategies* – *Assign Vulnerability Values (V) to IS Services* – *Prioritize IS Services by Critical Exposure*
Output – ***CBP Listing*** – ***Report of IS Services Supporting Business/ Service Lines*** – ***Business Impact Analysis*** – ***MTD Listing for IS Services*** – ***Map of IS Services to CBPs***	***Output*** – ***IS Components Map*** – ***RTOs for IS Services*** – ***MTD/RTO Analysis***	***Output*** – ***Threat Assessment***	***Outputs*** – ***Vulnerability Assessment*** – ***Prioritized Critical Exposure Assessment of IS Services***

(1) **ISCPA Step 1: Business Impact Analysis (BIA), Gather Business Requirements -** The purpose of this step is to identify service/business line's critical business processes (CBPs), the IS services that support them, business recovery time expectations for those IS services, and the impact to business/service lines if an IS service if it is not available. Refer to Figure 2 for illustration of ISCPA Step 1 instructions.

Figure 2: Notional IS Service Outage Impact Sample Table for Pharmacy



ITService	Work Around	Immediate	4 Hours	8 Hours	12 Hours	24 Hours	48 Hours	72 Hours	7 Days	14 Days	21 Days	30 Days	MTD	Impact	Description of Loss during Catastrophic Event
VistA	None	1	2	3	4	5							12 Hrs	5	*Inability to update records*
LAN	None	1	2	3	4	5							12 Hrs	5	*No access to Records*
PBX	Cell phone	1	1	2	2	3	4	5					48 Hrs	5	*Staff do not have VA cell phones*
Blackberry	Email	2	2	2	2	2	2	2	2	2	2	2	N/A	2	
Sharepoint	Paper	1	2	3	4	4							12 Hrs	4	*Loss of file access*

a. This sample table lists IS Services with workarounds for that IS Service. (A viable workaround is one that is documented as an alternative process, and has been used during an actual outage.) For each of the IS Services, the appropriate impact of loss of the IS Services to the business processes must be determined over various timeframes. Impact values range from 1 to 5, where 5=Catastrophic, 4=Major, 3=Moderate, 2=Minor, and 1=Insignificant (refer to Table 2 for definitions of impact). The timeframes are: Immediate, 4 hours, 8 hours, 12 hours, 24 hours, 48 hours, 72 hours, 7 days, 14 days, 21 days, and 30 days. The MTD column is the earliest timeframe that the first 4 or 5 first appears in the row. The Impact column is the highest number that appears in the row. Finally a description of the loss is noted in the last column. This tabular process continues until all IS Services are listed.

(a) OI&T personnel will interview respondents from all business/service lines in the facilities they support, since the latter understand the mission of the business, essential functions, and the impact on mission when IS services are disrupted. Examples of business/service lines include Pharmacy, Nursing Services, Eligibility Determination, Headstones and Markers; etc. Business/service line personnel will identify all CBPs* for all service/business lines resident within a facility and the IS services that support them.

(b) **CBPs are the critical operational and/or business support functions that cannot be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization.* They include logical groupings of processes/activities that produce a product and/or service. Examples of CBPs include scheduling appointments, performing surgery, patient follow-up, dispensing pharmaceuticals, patient admittance/discharge, eligibility determination, processing financials, ordering supplies, educational counseling, vocational training; etc.

(c) During the interviews with business/service line respondents, OI&T personnel will assist business/service line personnel to determine the IS services that support **each CBP** and identify known workarounds. Examples of IS services include telecommunications, data communications, helpdesk, Web applications, email, telephones, the network, and telephone services. *A workaround is defined as an alternate way to operate or manage without IT hardware, software, or communications when they are not available.* A workaround can be used to avoid risk for a period of time, but is not a permanent solution or mitigation of a risk. Workarounds include, but are not limited to, paper processing, alternate work areas, or manual input of data to a text file. In some cases, no workarounds will be in place.

(d) Business/service line respondents will determine outage impacts. An outage impact quantifies how a loss or disruption of a given IS services affects the ability of a business/service line to continue performing CBPs over time. Impacts are shown in Table 2.

Table 2: Impact Descriptions and Values

Impact Description	Impact Value
Indicates that a compromise to the IS service would have grave consequences leading to loss of life, serious injury to people, mission failure, or serious damage to the reputation of the VA as determined by the business line or service line. Workarounds are not in place or are not effective.	Catastrophic = 5
Indicates that a compromise to the IS service would have serious consequences resulting in loss of highly sensitive data, functions, equipment/facilities, or the reputation of the VA that could impair operations for an indefinite amount of time or put employees or customers at high risk for adverse health, financial or other consequences. Workarounds may be in place preventing further impact.	Major = 4
Indicates that a compromise to the IS service would have moderate consequences resulting in loss of sensitive information, functions, data, or costly equipment/facilities that would impair operations for a limited period of time or put employees or customers at moderate risk for adverse health or financial consequences. Workarounds may be in place preventing further impact.	Moderate = 3
Indicates little impact on human life or the continuation of operations. Workarounds may be in place preventing further impact.	Minor = 2
Indicates no impact on human life or the continuation of operations. Workarounds may be in place preventing further impact.	Insignificant = 1

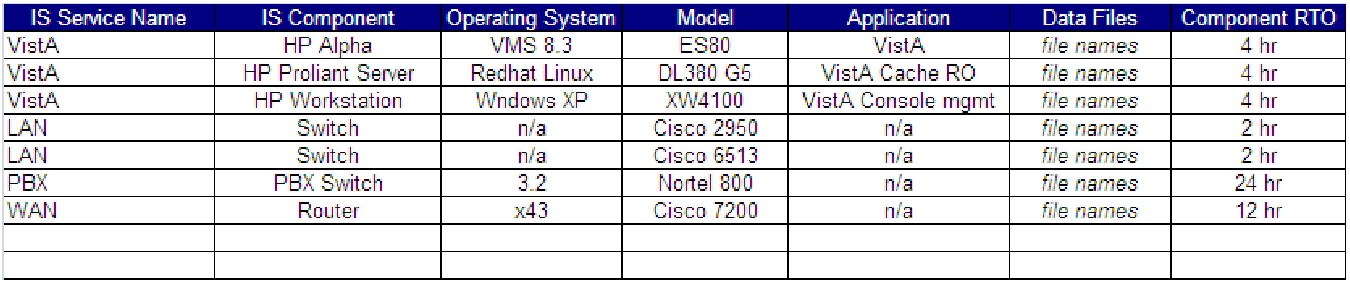
(e) Next, business/service line personnel will determine maximum tolerable downtime (MTD) for IS services supporting their business or service line. An MTD is the amount of time a business can be disrupted without causing significant harm to the organization's mission.

(f) Review the example in Table 1. If "Pharmacy" determines that the loss of the LAN is a 1 immediately but progressively becomes a 4 at 48 hours, the MTD is listed as 48 hours. If an IS service line's impact value, in this case the help desk, does not reach an impact value of 4 or 5, an MTD is not required in the MTD field. Enter a description of the *meaning* of the loss for impacts of 4 and 5.

(g) MTDs can vary widely, depending on the high availability technologies employed for recovery, including the point in time in which backup data resources can be recovered and restored. MTD should not be confused with service response time by OI&T personnel or vendors. It is expected that the business/service line will have multiple IS services and impacts.

(2) **<u>ISCPA Step 2</u>:** Map IS Components to IS Services. The purpose of this step is to map all IS components to all IS service(s) identified in Step 1 having the two highest impact ratings. The recovery time objective (RTO) for each IS Service and IS component is also to be documented. Refer to Table 3 for illustration of Step 1 data collected.

Table 3: IS Component Mapping Sample Table with Notional Data



IS Service Name	IS Component	Operating System	Model	Application	Data Files	Component RTO
VistA	HP Alpha	VMS 8.3	ES80	VistA	*file names*	4 hr
VistA	HP Proliant Server	Redhat Linux	DL380 G5	VistA Cache RO	*file names*	4 hr
VistA	HP Workstation	Wndows XP	XW4100	VistA Console mgmt	*file names*	4 hr
LAN	Switch	n/a	Cisco 2950	n/a	*file names*	2 hr
LAN	Switch	n/a	Cisco 6513	n/a	*file names*	2 hr
PBX	PBX Switch	3.2	Nortel 800	n/a	*file names*	24 hr
WAN	Router	x43	Cisco 7200	n/a	*file names*	12 hr

Note: Not all of the fields are applicable for all IT [IS] components. An IT [IS] component is a subset of a larger information system and is used to process, store or transmit information.

(a) For each IS Service identified in Step 1 as having an impact level of 4 or 5, all of the IS components that deliver the IS Service must be documented. IS can include, but are not limited to, mainframes, servers, workstations, network components, operating systems (OS), middleware, and applications. Network components can include firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers can include database servers, authentication servers, electronic mail and Web servers, proxy servers, domain name servers, and network time servers. For each component documented, applicable data to be collected should include:

1. *Model*: The hardware and descriptor “model” differentiates one hardware model or type from another. Different model types may appear outwardly similar, but are comprised of different internal components.

2. *OS Operating System*: The program that after being initially loaded into the computer by a boot program, manages all the other programs in a computer.

3. *Application*: A program designed to perform a specific function directly for the user or, in some cases, for another application program. Application programs use the services of the computer's OS and other supporting programs. Applications can be word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs. Please identify all critical applications for each IS Service.

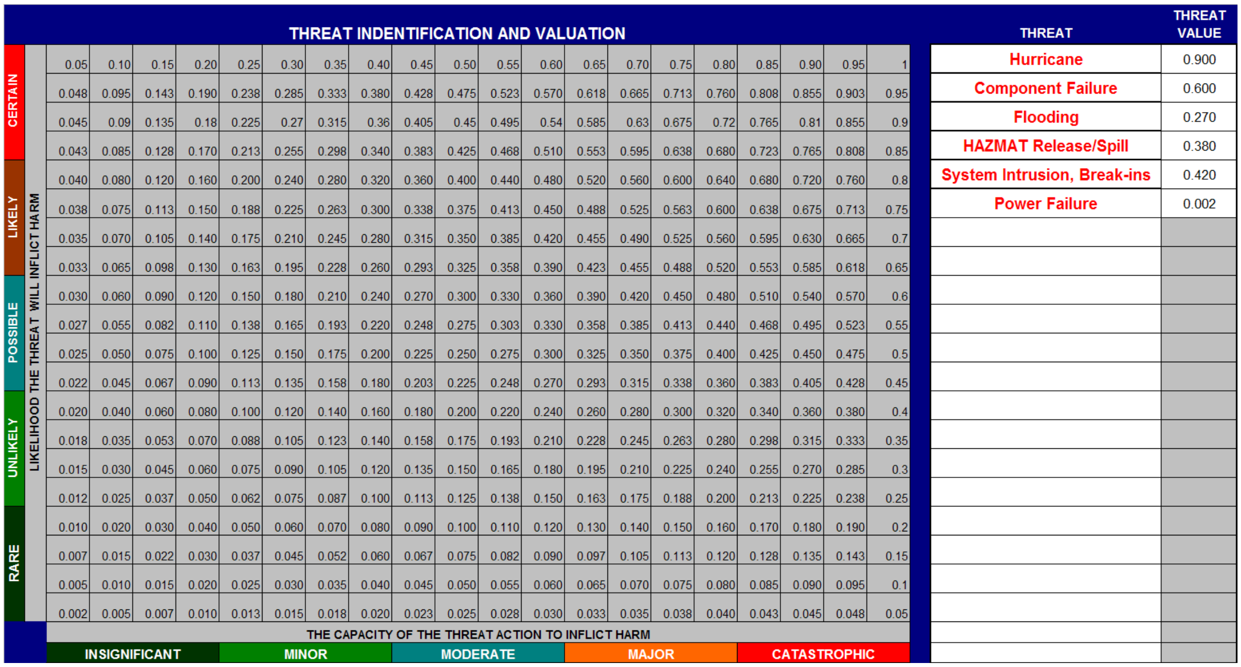
4. *Data Files*: Data files are any electronic information required to restore the IS Service to full functionality. Data files can be information processed and backed up on the system such as user files, electronic vital records or databases as well as scripts, logs, or programming code needed to ensure full operations of the IS system.

5. *RTO*: The time available to recover disrupted systems and resources (systems recovery time). It is typically one segment of the total MTD. For example, if it takes 48 hours from the loss of an IS Component or Service to recover, then the RTO is listed as 48 hours.

(b) The output of this step is a prioritized listing of all of the IS services together with the components that are known to support them. Also, the RTO’s for both the IS Services and each IT [IS] Component. To complete analysis for this step, first compare the RTO for the IT [IS] Service against the MTD specified for that IT [IS] Service in Step 1. If the RTO is greater than the MTD, then a new Contingency or Disaster Recovery plan needs to be developed to meet the IT [IS] Service MTD goal. Second, compare the RTO’s for each IT [IS] Service against the RTO’s of the IT [IS] Components that deliver the IT [IS] Service. If the component RTO’s exceed the RTO for the IS Service, then a new Contingency or Disaster Recovery plan needs to be developed to meet the IS Service RTO goals.

(3) **ISCPA Step 3:** Threat Assessment. The purpose of this step is to identify and prioritize threats to IS infrastructure. Refer to Figure 3 for illustration of Step 3 instructions.

Figure 3: Threat Identification and Value (Data Notional)



		THREAT INDENTIFICATION AND VALUATION																			
CERTAIN	LIKELIHOOD THE THREAT WILL INFLICT HARM	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50	0.55	0.60	0.65	0.70	0.75	0.80	0.85	0.90	0.95	1
		0.048	0.095	0.143	0.190	0.238	0.285	0.333	0.380	0.428	0.475	0.523	0.570	0.618	0.665	0.713	0.760	0.808	0.855	0.903	0.95
		0.045	0.09	0.135	0.18	0.225	0.27	0.315	0.36	0.405	0.45	0.495	0.54	0.585	0.63	0.675	0.72	0.765	0.81	0.855	0.9
		0.043	0.085	0.128	0.170	0.213	0.255	0.298	0.340	0.383	0.425	0.468	0.510	0.553	0.595	0.638	0.680	0.723	0.765	0.808	0.85
LIKELY		0.040	0.080	0.120	0.160	0.200	0.240	0.280	0.320	0.360	0.400	0.440	0.480	0.520	0.560	0.600	0.640	0.680	0.720	0.760	0.8
		0.038	0.075	0.113	0.150	0.188	0.225	0.263	0.300	0.338	0.375	0.413	0.450	0.488	0.525	0.563	0.600	0.638	0.675	0.713	0.75
		0.035	0.070	0.105	0.140	0.175	0.210	0.245	0.280	0.315	0.350	0.385	0.420	0.455	0.490	0.525	0.560	0.595	0.630	0.665	0.7
		0.033	0.065	0.098	0.130	0.163	0.195	0.228	0.260	0.293	0.325	0.358	0.390	0.423	0.455	0.488	0.520	0.553	0.585	0.618	0.65
POSSIBLE		0.030	0.060	0.090	0.120	0.150	0.180	0.210	0.240	0.270	0.300	0.330	0.360	0.390	0.420	0.450	0.480	0.510	0.540	0.570	0.6
		0.027	0.055	0.082	0.110	0.138	0.165	0.193	0.220	0.248	0.275	0.303	0.330	0.358	0.385	0.413	0.440	0.468	0.495	0.523	0.55
		0.025	0.050	0.075	0.100	0.125	0.150	0.175	0.200	0.225	0.250	0.275	0.300	0.325	0.350	0.375	0.400	0.425	0.450	0.475	0.5
		0.022	0.045	0.067	0.090	0.113	0.135	0.158	0.180	0.203	0.225	0.248	0.270	0.293	0.315	0.338	0.360	0.383	0.405	0.428	0.45
UNLIKELY		0.020	0.040	0.060	0.080	0.100	0.120	0.140	0.160	0.180	0.200	0.220	0.240	0.260	0.280	0.300	0.320	0.340	0.360	0.380	0.4
		0.018	0.035	0.053	0.070	0.088	0.105	0.123	0.140	0.158	0.175	0.193	0.210	0.228	0.245	0.263	0.280	0.298	0.315	0.333	0.35
		0.015	0.030	0.045	0.060	0.075	0.090	0.105	0.120	0.135	0.150	0.165	0.180	0.195	0.210	0.225	0.240	0.255	0.270	0.285	0.3
		0.012	0.025	0.037	0.050	0.062	0.075	0.087	0.100	0.113	0.125	0.138	0.150	0.163	0.175	0.188	0.200	0.213	0.225	0.238	0.25
RARE		0.010	0.020	0.030	0.040	0.050	0.060	0.070	0.080	0.090	0.100	0.110	0.120	0.130	0.140	0.150	0.160	0.170	0.180	0.190	0.2
		0.007	0.015	0.022	0.030	0.037	0.045	0.052	0.060	0.067	0.075	0.082	0.090	0.097	0.105	0.113	0.120	0.128	0.135	0.143	0.15
		0.005	0.010	0.015	0.020	0.025	0.030	0.035	0.040	0.045	0.050	0.055	0.060	0.065	0.070	0.075	0.080	0.085	0.090	0.095	0.1
		0.002	0.005	0.007	0.010	0.013	0.015	0.018	0.020	0.023	0.025	0.028	0.030	0.033	0.035	0.038	0.040	0.043	0.045	0.048	0.05
		THE CAPACITY OF THE THREAT ACTION TO INFLICT HARM																			
		INSIGNIFICANT				MINOR				MODERATE				MAJOR				CATASTROPHIC			

THREAT	THREAT VALUE
Hurricane	0.900
Component Failure	0.600
Flooding	0.270
HAZMAT Release/Spill	0.380
System Intrusion, Break-ins	0.420
Power Failure	0.002

(a) This is an x-y chart. First, moving along the x-axis is a range of threat capacity values from insignificant to catastrophic with results from low values to high values. Second, along the y-axis is a range of threat likelihood values from rare to certain.

(b) Threat assessment guidance is given in the form of an example that explains in detail the following sub-steps:

1. Threat Identification

2. Evaluation of Threat Capacity to Inflict Harm

3. Evaluation of the Likelihood the Threat will Inflict Harm

4. Assignment of Threat Value and Description

(c) The example assumes the location of the site under consideration is located in central Florida.

(d) Threat Identification. List potential site-specific threats to the IS infrastructure. Threats include, but are not limited to, those listed in Table 4.

Table 4: Threat List (Not Inclusive)

NATURAL	
Blizzard	Storm classified by the National Weather Service as a blizzard with significant snow, ice, wind, and cold
Earthquake	Earthquake at or near the facility
Extreme Outdoor Cold	Extremely low temperatures outside of the facility
Extreme Outdoor Heat	Extremely high temperatures outside of the facility
Fire	Fire affecting a portion of or the entire facility (may also be categorized under Human)
Flood	A rising level of water outside or near a facility
Hail	Storm classified by the National Weather Service as hail
Hurricane	Storm classified by the National Weather Service as a hurricane
Landslide	Movement of earth’s surface that can cause damage to a facility
Lightning Strike	Lightning strike on the facility
Thunderstorm	Storm classified by the National Weather Service as a thunderstorm
Tornado	Storm classified by the National Weather Service as a tornado
Tsunami	Storm classified by the National Weather Service as a tsunami
Volcano	Eruption of a volcano near a VA facility
Winter Weather Hazards	Winter weather (e.g., cold, snow, ice) that impacts the normal, safe operation of the VA

TECHNICAL/ENVIRONMENTAL	
Biological Release	Release of a biological toxin at or near the facility (may also be categorized under Human)
Component Failure	Computer or systems component failures that require replacement
Dam Failure	Failure of a dam leading to significant threat of water and debris damage to the facility, suppliers, or VA staff homes
Dust/Debris	Dust or debris within a facility with access to systems and components
HAZMAT Release Spill	Release or spill of hazardous chemicals or materials at or near a facility
HVAC Failure	Failure of the heating, ventilation or cooling systems within a facility (e.g., temperature below 68 degrees, above 74 degrees, or rapid changes in temperature)
Indoor Humidity	Humidity inside of the facility above normal operating conditions (e.g., relative humidity below 40% (temperature between 68-74 degrees) or above 50% (temperature between 68-74 degrees)
Power Failure	Failure of the external power supplying the facility (e.g., brownout, blackout, voltage dip/spike)
System Misconfigur-ation	System hardware, software, or parameters not configured properly
System Penetration	Actions by software to gain unauthorized access to a system
Vibration	Vibration of VA facilities or systems, not classified as a earthquake
Water Damage	Water within a VA facility that is not contained in the feed or drain lines

HUMAN	
Burglary/ Break In	Unauthorized access to the facility with the intent to steal
Civil Unrest	Actions by the civilian population that cause people to feel unsafe to be outside their homes
Hacker, Cracker	Use of a computer system without proper authorization with the intent to cause harm or theft
Human Health Emergency	Actions that cause the health of VA staff, contractors, or suppliers to be degraded as to make them unavailable (e.g. Flu, pandemic, Meningitis)
Malicious Code	Malicious computer software that interferes with normal computer functions
Password Privacy Negligence	Users, systems, or software not following VA standards for password privacy
Personnel Unavailable	Actions that cause staff to be unavailable to work
Sabotage	Purposeful acts by non-VA staff to destroy VA facilities or capabilities
System Intrusion, Break-Ins	Unauthorized access to the system by a human
System Tampering	Malicious actions to modify the normal configuration of a system
Terrorist	Actions by outside parties against the U.S. with the intent to cause fear in the population
User Negligence	Unintentional acts by authorized VA system users that cause harm to the VA
User Sabotage	Intentional acts by VA authorized users of VA systems to destroy VA facilities or capabilities

(e) Also include input from groups located at the site being assessed, including, but not limited to, emergency management and facilities personnel. Further tailor the list by adding any site specific threats provided in the interview that have not been previously identified.

(f) Evaluation of Threat Capacity to Inflict Harm to IS Infrastructure. A threat must have the ability to render all or part of the site's IS infrastructure ineffective. For example, hurricanes are a staple threat to Florida and Gulf Coast states, having demonstrated a consistent capability to harm IS services in those geographical areas. However, hurricanes do not generally have the capability to move far enough inland to affect the upper Midwest and are thus not considered a significant threat to that geographic area.

(g) In addition to having the *capability* to harm IS services; human threats must have the *intent* to do so. Intent is determined largely through inference and historical precedent. Infer intent through a set of questions regarding the threat.

1. Does the threat have a current or projected need for the IS service in question?

2. Does the threat seek to deny use of the IS service?

3. Has the threat demonstrated an interest by targeting the IS service?

4. To what degree is the threat motivated to use its capability?

5. Has the threat previously attacked the specific IS service at the specific site in question?

(h) *Note: If a human threat has the capacity to harm IS infrastructure but lacks the intent, there is no threat. The reverse also is true. If the threat possesses the intent, but not the capacity, no threat exists.*

(i) Having considered all issues pertaining to the evaluation of threat capacity to harm IS infrastructure, note the capacity descriptions on the X, or horizontal, axis of Table 4 (Catastrophic, Major, Moderate, Minor, Insignificant). These characterizations are defined in Table 5.

Table 5: The Capacity of the Threat to Inflict Harm

Threat X Axis: Capacity of the Threat to Inflict Harm
Catastrophic: Documented knowledge exists of the threat's capability and intent* to render all or part of the IS infrastructure unavailable for a lengthy or undetermined period.
Major: Documented knowledge exists of the threat's capability and intent* to render all or part of the IS infrastructure unavailable for a protracted period.
Moderate: Some evidence of the threat's capability or intent* to briefly disrupt the IS infrastructure.
Minor: Little or no credible evidence of the threat's capability or intent* to disrupt the IS infrastructure exists.
Insignificant: No evidence of the threat's capability or intent* to disrupt the IS infrastructure exists.

* Except for natural and some environmental threats

(j) Since the hypothetical site in this example is located in central Florida and the identified threat is “Hurricane,” it is common knowledge that the threat catastrophically impacts the full panoply of IS infrastructure. Thus, the capacity of the threat to inflict harm on the IS infrastructure is .9, Catastrophic.

(k) Evaluation of Threat Likelihood. Note the likelihood descriptions on the Y, or vertical, axis of Table 6 (Certain, Likely, Possible, Unlikely, and Rare). See Table 6 for Threat Likelihood descriptions.

Table 6: Threat Likelihood Descriptions

Threat Y Axis: Likelihood the Threat Will Inflict Harm
Certain: The threat has harmed the IS infrastructure and/or similar assets frequently in the past, including the recent past.
Likely: The threat has harmed the same or similar IS infrastructure often in the past, including the recent past.
Possible: The threat has harmed the IS infrastructure in the past.
Unlikely: The threat has infrequently harmed the IS infrastructure.
Rare: The threat has only sporadically harmed the IS infrastructure and not in the recent past.

(l) Likelihood is a relative term subject to the best judgment of the assessor, using historical data and institutional knowledge to weight the decision. A high frequency of threat-related incidents can indicate an increased likelihood that a similar incident may take place in the future, especially if capability and intent[1] are high. For example, if a hurricane has impacted IS infrastructure one or more times in the past, the probability it will do so again is higher than if it had never done so, especially where no other circumstances have changed (i.e., additional mitigation strategies have not been applied). ***Note, however, that lack of threat action in the past is the least reliable predictor of future threat action.***

(m) Since the hypothetical site is located in central Florida and the identified threat is “Hurricane”, the likelihood of that threat impacting IS infrastructure is considered to be within the Certain range. Starting with the selected threat capacity point (cell) on the X or horizontal axis, move upward on the Y or vertical axis to determine the likelihood of threat occurrence as shown in the table. Determine a resting point on the Y axis that best describes the likelihood of occurrence of the threat. Determine a resting point (cell) on the Y or vertical axis by selecting a point (cell) from within the chosen category description (within the range). For example within the category of “Possible” the selection could range from “low-possible” to “high-possible”.

(n) Assignment of Threat Value and Threat Description. The intersection of the capacity and likelihood axes is the value assigned to the threat. Threat values have descriptors, as shown in Table 7. In the example, the threat is rated at .9 with a threat description of Critical. *Note: Assignment of a numerical value within a level is not scientific. It is based on the informed assessment of Emergency Management, Facilities, and IT personnel in evaluating the relative position of all threats within a given level.*

[1] *Where applicable.*

Table 7: Threat [Assessment] and Numerical Values

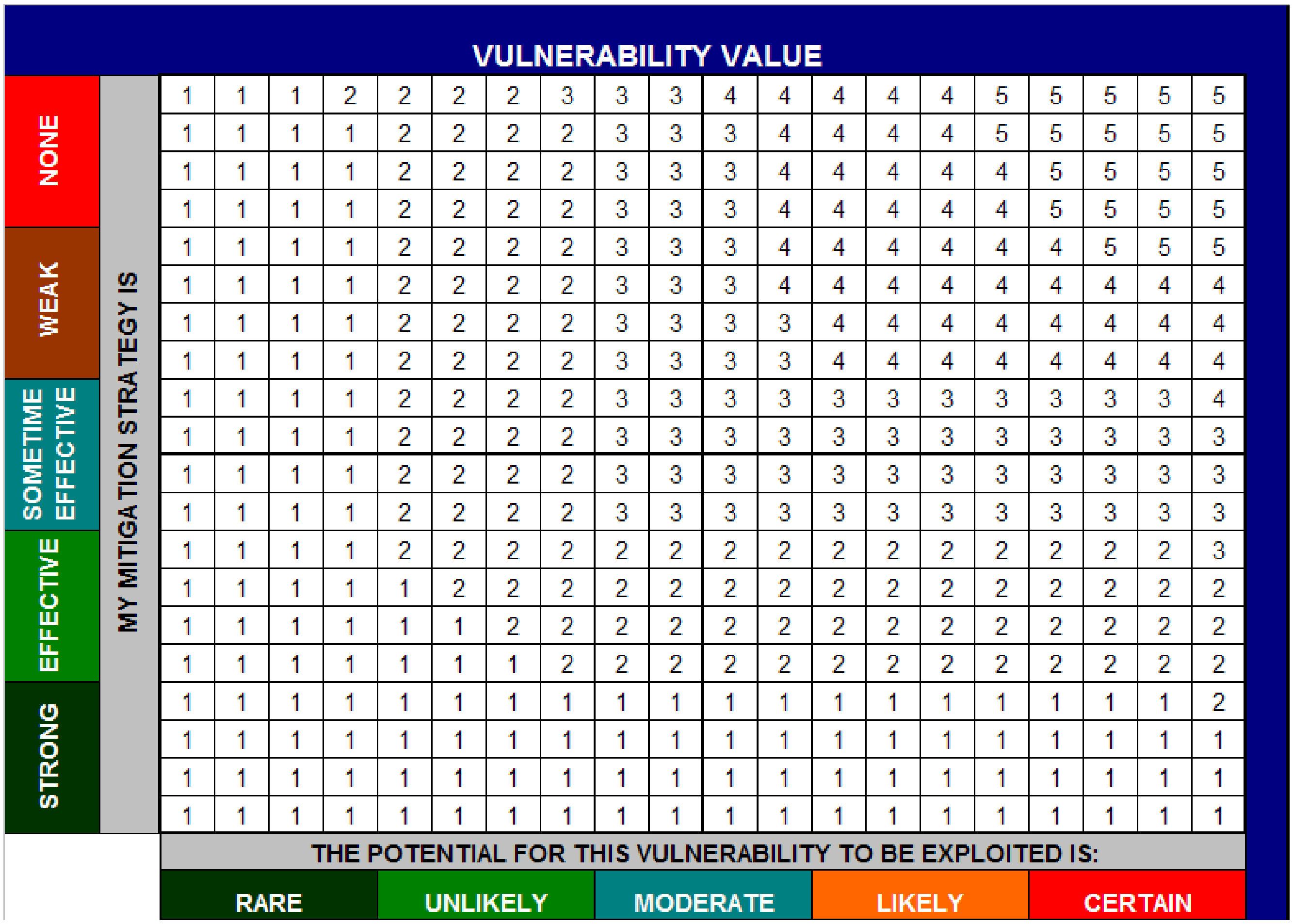
Threat [Assessment]	Numerical Value (TV)
Critical: The threat has the capability and intent* to harm the IS infrastructure. The same or similar IS services have been harmed in the past and are subject to the threat on a frequently recurring basis.	**0.64 < TV**
High: Documented knowledge exists of the threat's capability and intent* to render all or part of the IS infrastructure unavailable for a protracted period. The threat has harmed the same or similar IS infrastructure often in the past, including the recent past.	**0.36 < TV <= 0.64**
Moderate: Some evidence of the threat's capability or intent* to briefly disrupt the IS infrastructure. The threat has harmed the IS infrastructure in the past.	**0.16 < TV <= 0.36**
Minor: Little or no credible evidence of the threat's capability or intent* to disrupt the IS infrastructure exists. The threat has infrequently harmed the IS infrastructure.	**0.04 < TV <= 0.16**
Insignificant: No evidence of the threat's capability or intent* to disrupt the IS infrastructure exists. The threat has only sporadically harmed the IS infrastructure and not in the recent past.	**TV <= 0.04**

* Except for natural and some environmental threats

(o) Threats identified as **Critical** and **High** will be used in ISCPA, Step 4. Thus, in this example, only Hurricane and Component Failure move forward to Step 4.

(4) **ITCPA Step 4:** Vulnerability Assessment. The purpose of this step is to identify flaws or weaknesses in system procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach, violation of the system's security policy, interruption/loss of service, or other undesired events. Vulnerability assessments evaluate planned strategies and countermeasures that potentially avert or diminish the harm to IS services. Data gathered in the threat assessment (ISCPA Step 3) is necessary to the vulnerability assessment performed in this step. Vulnerability assessment guidance continues the facility location example given in ISCPA steps 1-3. Refer to Figure 4 and Table 8 for illustration of Step 4 instructions.

Figure 4: Vulnerability Values



VULNERABILITY VALUE

MY MITIGATION STRATEGY IS																				
NONE	1	1	1	2	2	2	2	3	3	3	4	4	4	4	4	5	5	5	5	5
	1	1	1	1	2	2	2	2	3	3	3	4	4	4	4	5	5	5	5	5
	1	1	1	1	2	2	2	2	3	3	3	4	4	4	4	4	5	5	5	5
	1	1	1	1	2	2	2	2	3	3	3	4	4	4	4	4	5	5	5	5
WEAK	1	1	1	1	2	2	2	2	3	3	3	4	4	4	4	4	4	5	5	5
	1	1	1	1	2	2	2	2	3	3	3	4	4	4	4	4	4	4	4	4
	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	4	4	4	4
	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	4	4	4	4
SOMETIME EFFECTIVE	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
EFFECTIVE	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3
	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2
STRONG	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
THE POTENTIAL FOR THIS VULNERABILITY TO BE EXPLOITED IS:	RARE				UNLIKELY				MODERATE				LIKELY				CERTAIN			

(a) This is an x-y chart. First, moving along the x-axis is a range of vulnerability values from rare to certain with results in a low potential vulnerability value of 1. Second, along the y-axis is a range of mitigation strategy values from strong to none with results in a strong mitigation value of 1 to a weak mitigation value of 5.

Table 8: IS Services Vulnerability Values (Data Notional)

IS Service	Threat	Vulnerability	Mitigation Strategy	Vulnerability Value
PBX	Hurricane	Location of PBX room in basement	Water sensors and sump pump	4
PBX	Component Failure	Aging infrastructure	Accelerated technology refresh schedule	3
LAN	Hurricane	Server room has large unprotected windows	Mylar window coatings to prevent shattering and flying glass	4
LAN	Component Failure	Heat buildup in server room	Improved server room HVAC	1

(a) Step 4 is comprised of the following sub-steps:

1. Match IS Services to Threats

2. Identify of IS Service Vulnerability(ies) to Threats

3. Describe Current Mitigation Strategies against All Vulnerabilities

4. Evaluate Potential for the Exploitation of a Vulnerability by a Threat

5. Evaluate the Strength of Mitigation Strategies Applied to Specific Threats

6. Assignment of Vulnerability Value and Description

(b) Match IS Services to Threats. Fill in the threat column with a single threat identified in Step 2. Fill in the IS service column with all IS services that have the potential to be affected by the threat. In this case, the featured IS service is PBX.

(c) Identify IS Service Vulnerability(ies) to Threats. Describe all known vulnerabilities of each IT service to the threat, Vulnerabilities may include, but are not limited to:

1. Faulty/Outdated Hardware Failure (All: Servers, Computers, Communications Equipment; etc.)
2. Faulty/Outdated Software
3. Location of the IS Service
4. Faulty IS Processes/Procedures
5. No/Inadequate IS Contingency Plan (ISCP)/ ISCP Not Tested
6. Faulty Maintenance (All: Hardware and Software)
7. Lack of/Inadequate Surge Protection
8. No/Inadequate Backup Power

(d) Describe Current Mitigation Strategies Against All Vulnerabilities. Most known IT [IS] vulnerabilities have one or more mitigation strategies in place. Identify all mitigation strategies against each individual vulnerability, as shown in Figure 4. Use a separate line for each mitigation strategy. Mitigation strategies may include, but are not limited to:

1. Current ISCP
2. Tested ISCP
3. IS Devolution Plan
4. Training/Cross Training
5. Improved Testing/Exercises
6. Service Level Agreement
7. Improved Equipment Protection Measures

8. Improved Equipment Protection Measures

9. Stronger Physical Security Protocols

10. Stronger Cyber Security Software

11. Current Hardware

12. Current Software

13. Alternate Communications

14. Backup Power

15. On-Hand Replacement Hardware

16. Surge Protection

17. Improved Fire Suppression System

18. Alternate Operating Facility

(e) Evaluate Potential for the Exploitation of a Vulnerability by a Threat. In the absence of mitigation strategies, capable threats will exploit vulnerabilities. Note the exploitation potential descriptions on the X, or horizontal, axis of Table 9a (Certain, Likely, Moderate, Unlikely, Rare), defined in Table 9.

Table 9: Vulnerability X Axis: Potential for this Vulnerability to be Exploited

Vulnerability X Axis: Potential for this Vulnerability to be Exploited
Certain: The weakness has been exploited frequently in the past and has multiple threats that can exploit it.
Likely: The weakness is known, has been exploited in the past and has multiple threats that can exploit it.
Moderate: The weakness is known, has never been exploited at the VA, but has outside and has multiple threats that could exploit it.
Unlikely: The weakness is known, has never been exploited, but has limited threats that could exploit it.
Rare: The weakness is one of a kind, has never been exploited and has only a single threat that can exploit it.

(f) Since the hypothetical site is located in central Florida, the identified threat is “Hurricane”. The PBX room is vulnerable to storm surge and resultant flooding because it is below sea level. Thus, it is likely the vulnerability will be exploited by the threat. Within the Likely designation, a very high level is appropriate.

(g) Evaluate the Strength of Mitigation Strategies Applied to Specific Threats. Mitigation strategies are unlikely to eliminate a vulnerability. Those that have failed or been shown to be inadequate in the past are, without improvement or additional strategies, likely to fail or be inadequate again. Having considered all issues pertaining to the evaluation of the strength of the mitigation strategy relevant to the specific vulnerability, refer to Table 10. Note the strength descriptions on the Y, or vertical, axis of the table (Strong, Effective, Sometimes Ineffective, Weak, None), defined in Table 10.

Table 10: Vulnerability Y Axis: My Mitigation Strategy Is

Vulnerability Y Axis: My Mitigation Strategy Is
Strong: Multiple layers of tested, integrated capabilities are in place to prevent harm and limit harm when prevention fails.
Effective: Multiple layers of tested capabilities are in place to prevent harm to the IS service and limit harm when prevention fails.
Sometimes Effective: Capabilities are in place that have been shown to limit or prevent harm only sporadically or have never been tested.
Weak: Minimal capabilities are in place to prevent harm.
None: Limited or no capabilities are in place either to prevent or limit harm.

(h) The identified mitigation strategy (water sensors combined with a sump pump) is known to have allowed a damaging degree of flooding in Category 2 and above hurricanes in the past and is therefore considered weak.

(i) Starting at the selected exploitation value, move vertically until the Weak category is reached.

(j) Assign Vulnerability Value and Description to All Vulnerabilities. Transcribe the numerical value identified in the previous step into the Vulnerability Value column in the cell adjacent to the relevant vulnerability, along with the Vulnerability Description shown in Table 11.

Note: Assignment of a numerical value within a level is not scientific. It is based on the informed assessment of Emergency Management and IT personnel in evaluating the relative position of all vulnerabilities within a given level.

Table 11: Vulnerability [Assessment] and Values

Vulnerability [Assessment]	Numerical Value
Insignificant: The vulnerability is unlikely to harm IS infrastructure.	**1**
Minor: The vulnerability has been exploited infrequently but has the potential to harm the IS infrastructure.	**2**
Moderate: The vulnerability has been exploited in the past.	**3**
High: The vulnerability has been exploited often in the past, including the recent past.	**4**
Critical: The vulnerability has been exploited frequently in the past, including the recent past.	**5**

(5) Generate the Critical Exposure Report. The purpose of this action is to calculate the Exposure values for all Service/Business Lines. These Exposure values are used to correlate, rank, and prioritize the IS services and IS components supporting the Service/Business Lines to determine which require ISCPs and DRPs. Since ISCPs and DRPs must be written for IS services having a High critical exposure ranking (and included in SMART), this report facilitates the identification of those particular IS components and IS services. Use the following formula to calculate Exposure Values: **Threat x Vulnerability x Impact = Critical Exposure.**

Table 12: IS Exposure Table

Critical Exposure	*Values*
High	**6.00-greater**
Moderate	**3–5.99**
Low	**0–2.99**

(a) In the example (Table 12) utilizing the data gathered in Steps 1 through 4 of the ISCPA process, the formula and solution for PBX exposure to hurricanes is: **Threat (.9) x Vulnerability (5) x Impact (4) = Critical Exposure 18.00 (High; see Table 13).**

(b) Use the numerical values generated in previous ISCPA steps to generate the IS Exposure Report, as shown in Table 13. IS services ranked High will progress to STAGE 2: Development of Contingency Plans.

Table 13: IS Critical Exposure Report

IS Service	Impact	Threat	TV	Vulnerability	Vulnerability Value	Highest Exposure	Exposure
PBX	5	Hurricane	.9	Location of PBX room in basement	4	18	High
	5	Component Failure	.6	Aging infrastructure	3	9	Moderate
LAN	5	Hurricane	.9	Server room has large unprotected windows	4	18	High
	5	Component Failure	.9	Heat buildup in server room	1	4.5	Moderate

d. **STAGE 2: Development of IS Contingency Plans.** Having now determined the Exposure Values for all Service/Business Lines, preparations can be made for appropriate ISCPs and DRPs. Office of Management and Budget Circular A-130, Appendix III, requires the development and maintenance of continuity of support plans. This Handbook includes IS contingency planning as a subset of continuity of support planning.

(1) Using the information elicited during the Stage 1 ISCPA, OI&T system owners must develop ISCPs and DRPs for general support systems and major applications considering IS services having a High critical exposure ranking, as identified in the Critical Exposure Report.

(2) ITCPs ISCPs must include the impact data developed in ISCPA Step 1, Business Impact Analysis (BIA); the IS components identified in ISCPA Step 2; response to threats to and vulnerabilities of IS services identified in Steps 3 and 4; and must comply with NIST SP 800-34 Rev 1 and NIST SP 800-53.

(3) ISCP and DRP templates developed by OI&T Office of Business Continuity and available in the Web Portal/Office of Business Continuity page should be used to complete this stage, since these templates are NIST compliant, auditable, and include extensive, detailed instructions and references.

e. STAGE **3: Post ISCP and DRP plans to the Security Management and Reporting Tool (SMART), if the plan addresses a system that exists in SMART. If the plan does not address a system in SMART, please follow local site documentation procedures.** To upload completed and reviewed plans in SMART, click on *Certification and Accreditation*" link; select *System*; select *Artifacts* tab and upload the plan.

f. **STAGE 4: Train, Test, and Exercise ISCPs and DRPs.** System or facility owners will train personnel in their contingency roles and responsibilities with respect to Moderate and High impact information systems and provide refresher training at least annually. Testing should validate plans, develop and maintain procedural understanding and technical skills, and develop a body of lessons learned to revise plans for operability in real world circumstances. All ISCPs and DRPs will be tested annually and when major organizational, operational, procedural, or technical changes (i.e., changes to OS, server upgrades; etc.) are made. When applicable, automated mechanisms will be employed to thoroughly and effectively test the contingency plan. When feasible, a full recovery and reconstitution of the information systems will be used as part of ISCP and DRP testing.

(1) Tests will have (a) specific objective(s), such as validating responses to the loss of specific IS services; validating data backup protocols; exercising implementation of manual business procedures; etc. There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing increases as the impact of the loss of the IS service increases. ISCPs and DRPs must be tested in the facilities specified in the respective plan. If the plan specifies use of an alternate facility(ies), the test must be conducted at the alternate site.

(2) ISCP/DRP tests will be documented by the system or facility owners and results reported in writing to the Regional CIO, Site Director, Site CIO, Facilities Director, and Emergency Management Director, with a copy uploaded to SMART. When applicable, automated mechanisms will be employed to thoroughly and effectively test the contingency

plan. When feasible, a full recovery and reconstitution of the information systems will be used as part of ISCP testing.

g. **STAGE 5: Post Training, Testing, and Exercise Results to the SMART Data Base.** For audit and reference, post testing dates and results in SMART. To do so, select *Systems* link and system name; select *Capital Planning* tab; select “date contingency plan was tested” field and insert *Date* and *Submit*.

Acronyms

Abbreviation / Acronym	Description
BIA	Business Impact Analysis
CBP	Critical Business Process
CIO	Chief Information Officer
DRP	Disaster Recovery Plan
FISMA	Federal Information Security Management Act
ISO	Information Security Officer
IS	Information System
ISCP	Information System Contingency Planning
ISCPA	Information System Contingency Planning Assessment
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
OS	Operating System
RTO	Recovery Time Objective
SMART	Security Management and Reporting Tool
SP	Special Publication
TV	Threat Value
VA	Department of Veterans Affairs
VACO	Department of Veterans Affairs Central Office

Definitions

IT Contingency Planning Definitions	
Business Continuity Planning	The process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change.
Business Impact	Result or effect of an event, i.e., the magnitude of harm that could be caused by a threat's exercise of a vulnerability.
Business Impact Analysis	Process of identifying the critical business functions within the business and determining the impact of not performing those business functions.
Business/Service Line	Logical element or segment of a VA organization representing a specific business function and a definite place on the organizational chart under the domain of a manager. Also called department or division.
Critical Business Process	A collection of interrelated tasks which accomplish a particular goal. MEFs are comprised of CBPs. Functional Areas perform CBPs in support of VA's responsibilities under the National Response Framework.
Continuity of Operations (COOP) Plan	A continuity of operations plan provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The Federal government and its supporting agencies traditionally use this term to describe activities otherwise known as disaster recovery, business continuity, business resumption, or contingency planning.
Contingency Plan **(Including IS Contingency Plan)**	Alternative strategy that identifies the plan to be undertaken to prevent or reduce the negative impact of a disaster. Includes the continuity of operations plan, the pandemic influenza plan, comprehensive emergency management plan, disaster recovery plan, information technology contingency plans, and similar plans.
Critical Exposure	The cumulative criticality of an IS service as it is affected by its relative importance in maintaining a critical business process, the threats arrayed against it, and its vulnerabilities to those threats, as expressed in the formula: Threat x Vulnerability x Impact (TxVxI).
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities that deny access to the normal facility for an extended period. It is an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency and may refer to ISCP plans to restore required IT components.

IT Contingency Planning Definitions	
Federal Information Processing Standards (FIPS)	Publicly announced standards developed by the Federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community.
Federal Information Security Management Act (FISMA) of 2002	Enacted in 2002, FISMA (44 U.S.C. §§ 3541-49) requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
General Support System (GSS)	An interconnected information resource under the same direct management control that shares common functionality. It usually includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Impact of No Service	A description of the effects on the operations or system if no service is provided by the vendor.
Information Technology Contingency Planning Assessment (ISCPA)	A document which consolidates the results of a business impact assessment and threat and vulnerabilities assessments to facilitate the preparation of information technology contingency plans and the related training, testing, and exercises.
IT Service	Any technology that supports information technology resources.
Major Application (MA)	An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.
Maximum Tolerable Downtime	The maximum allowable time a process or component can be down following a disruptive event.
Mitigation Strategy	An action taken or a physical entity used principally to reduce or eliminate one or more vulnerabilities. Mitigation strategies also may affect the threat (intent and/or capability).

IT Contingency Planning Definitions	
National Institute of Standards and Technology (NIST)	NIST is a non-regulatory Federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Policies	Policies are high-level guiding principles that set the overall requirements of the program and helps Executive Management set the direction around logical, physical and managerial practices to support the Contingency Planning Program. Policies are set at a high level and do not contain specific department, technology, vendor related, etc. specifications, and therefore should not change frequently.
Recovery Time Objective	The time available to recover disrupted systems and resources (systems recovery time). It is typically one segment of the total MTD. For example, if a critical business process has a three-day MTD, the RTO might be one day (Day 1).This is the time you will have to get systems back up and running. The remaining two days will be used for entering data or transactions collected manually/on paper during the outage.
Threat	A threat has (1) intent and capability targeted at the intentional exploitation of a vulnerability and 2) has a history of having done so. A threat may also be a technical or manmade situation that may accidentally trigger a vulnerability. This type of threat also will have a history of having triggered vulnerabilities in the past.
Vulnerability	A flaw or weakness in system procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach, violation of the system's security policy, interruption/loss of IS Service, or other undesired events.
Workaround	A process that can be used to avoid risk for a period of time but is not a permanent solution or mitigation of a risk.