First Things First:

The Business Impact Analysis Approach to Meeting Your Mission

ANTHONY HARRIS

Introduction

You know:

- What functions and services your facility performs
- Why your facility performs those functions and services
- Who depends on those functions and services
- When and how to restore those functions and services

Are you 100% sure about that?

Objectives

During this presentation, we will explore:

- What a business impact analysis (BIA) is
- What goes into a BIA and what comes out
- Why performing a BIA gives you the analyzed guidance to restore functions efficiently and reliably
- How performing a BIA helps identify gaps and barriers to performing functions
- Identifying the IT systems that support critical functions so they can be restored in the right order after an outage
- Understanding dependencies with other departments, agencies, and third parties that affect performing IHS functions
- How BIAs are a key component in complying with security controls

“Before the BIA” Exercise Scenario

Scenario

You work in Sandy’s Total Health Clinic.

- List your primary functions – what you do
- List the major systems that support each – what you need

Pick an Event (Scenario)

- Heat dome
  - Causes all of the roads and bridges to crack and buckle impeding clinic access by staff and clients
  - Overtaxes the power grid. You lose power and your generator fails (or you don’t have a generator).
- Lightning strike
  - Causes significant fire damage to the clinical, administrative, and server areas.
  - Several IT staff members are severely injured
- Cyberattack
  - Targeted disinformation sent to clients and patients
  - IT systems are hijacked and inoperable. Patient records, lab records, scheduling, etc. are either locked, corrupted, or exfiltrated.
- Influenza outbreak
  - Increased patient load but reduced clinical staffing
  - Shortage of medications and other supplies

Implement Recovery (Scenario)

- Which functions are the most critical to meet the clinic's mission? How do you know?
- Which functions do you restore first? Why?
- How much time do you have to restore functions? Any repercussions if you don't?
- You restore less critical functions later? Does that affect other clinics, labs, or vendors?
- Which systems do you restore first?
- How much time do you have to restore systems?
- What if your data restore is unavailable or fails?
- After the clinic has returned to operational, what do you say during the after action review (hotwash) about the recovery's efficiency?

Moments You're Glad You Built a BIA

You Need to Recover From Disruptive Events

Luck and hope are not recovery strategies.

Events that can derail meeting the mission:

- **Natural**: tornado, lightning strikes, floods, excessive heat or cold spells
  - Damage to buildings, power, environmentals, IT infrastructure, barrier to staff access to facility
- **Technological**: cyberattacks, remotely-initiated power outages, targeted disinformation
  - System unavailability, hijacked data, exfiltration, ransomware, compromised decision capability
- **Human made**: terrorist attack, infrastructure breach, hazmat spill
  - Damage to infrastructure, dangerous environment for habitation, fear of returning to work
- **Other**: pandemic, labor strike
  - Staff unavailability, loss of skills and knowledge, unhealthful working conditions

Careful planning reduces time and cost of response.

You Need to Plan For Recovery

Where do we start?

- **Planning documents**: identified and described in NIST standards and based on the BIA
  - COOP – planned devolved services
  - DRP – plan for facility recovery
  - ISCPs – plans to recover systems
  - Contracts and agreements – included everywhere
- **Restoring Functions**: all identified in the BIA
  - Which functions do we restore first and what do we need to do that?
  - Which functions need to be restored because another department depends on them?
  - Which functions can be performed differently until the facility is back up and running?
  - Which functions can wait?
- **Restoring Systems**: all prioritized in the BIA; recovery covered systems' ISCPs
  - Which systems must be restored first?
    - By function supported
    - By dependency on other systems
  - Which systems can wait?

BIAs remove the guesswork.

You need to plan for the future

Plan for:

- Future infrastructure procurement and implementation
- Weak points that impede continuity and recovery
  - Dependencies with other organizations, departments, vendors, public support organizations
  - Lack of defined agreements that level-set expectations and obligations
  - Adequate, appropriate staffing and skills

Streamline operations:

- Identify redundancy in functions and systems
- Identify where more support is needed

You need to develop COOP plans, DRPs, and ISCPs (based on the BIA).

Careful planning reduces time and cost of meeting your mission.

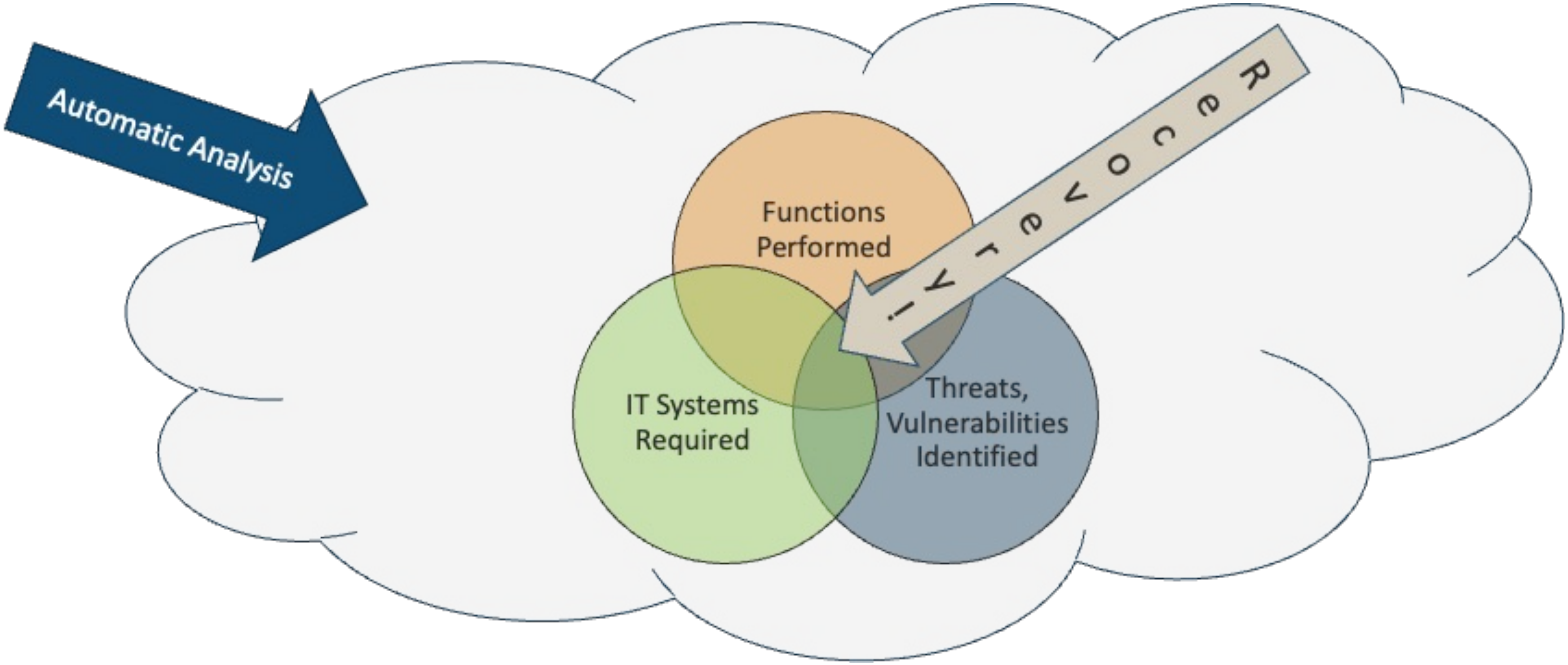
BIA – The Blueprint to Recovery

What’s a BIA?

The BIA is an analytical tool. It provides a structured process to:

- Capture the functions the facility performs and the mandates to do so
- Differentiate between critical and non-critical functions based on structured analysis of impacts of not performing certain functions and time frames
- Determine the priority to restore critical functions after an outage
- Identify dependencies between the functions and other departments and organizations
- Identify the IT systems that support performing those critical functions (and thus, the priority to restore those systems)
- Use the resulting analysis to develop DRPs and ISCPs.
- Develop real-world exercises that help train staff to respond effectively and update plans that provide substantive guidance to respond.

What’s in a BIA?



Functions

Functions are the services your facility provides.

- The functions the organization performs
- Reasons to perform functions (e.g., contract, compact, legislative mandate, organization mission)
- Impacts if each function is *not* performed
- Thresholds for how soon the functions must be restored
- Dependencies

Every function is important but not everything is critical.

Systems

Systems include the IT infrastructure and applications that support functions.

- IT infrastructure that supports each function
- Priority and timeframes to restore systems

Not all systems must be restored at the same time.

Threat Assessments

Threats and vulnerabilities are environmental conditions that can impact meeting the mission.

- Threats can include earthquakes, power outages, tsunami, or other events that may affect facilities in your geographic area.
- Identify the threats to your facility that merit analysis of impacts of an event.

Some outages are more predictable than others.

Structure for Capture and Analysis

The BIA tool's structure helps you capture critical information and prioritize the order to restore after an outage.

The BIA tool automates much of the data capture and analysis.

Results

When finalized, you can easily determine:

- Who and what is impacted if an event or outage occurs
- Priority and timeframes to restore functions
- A road to recovery based on analysis

What’s *not* in a BIA?

A BIA is not:

- A plan; it’s an analysis tool.
- An indictment of deficiencies; it’s a tool to capture information to address deficiencies and best practices
- A set of procedures; it provides fodder to capture procedures
- A final analysis; it is routinely reviewed and updated as the facility changes

Let’s Build a BIA

It’s Not as Hard as it Sounds

The BIA tool is based on using consistent data (e.g., “8 hrs” vs. “8 hours”) to support reliable analysis.

It includes lots of functionality to ensure

- Consistency in capturing data
- Accuracy in data analysis.

Prepare

Get the Right People.

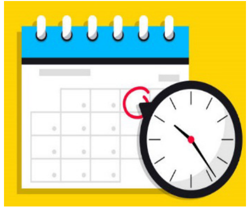
- Facility policy people / Management for support and buy-in
- People who perform functions
- People who know why the facility performs its functions
- IT folks
- DRCP for support and guidance

Get the Right Tools.

- BIA data collection sheets
- BIA tool – a spreadsheet that uses site-specific site data to perform the analysis
- Contracts, agreements, etc. or someone who knows about them
- A physical or virtual place to meet
- A place to store information, drafts, reviewed versions, and final versions, “parking lot” issues

Get the Time.

- Set a schedule with milestones
- Iterative process to capture the right information
- Time to review



Build

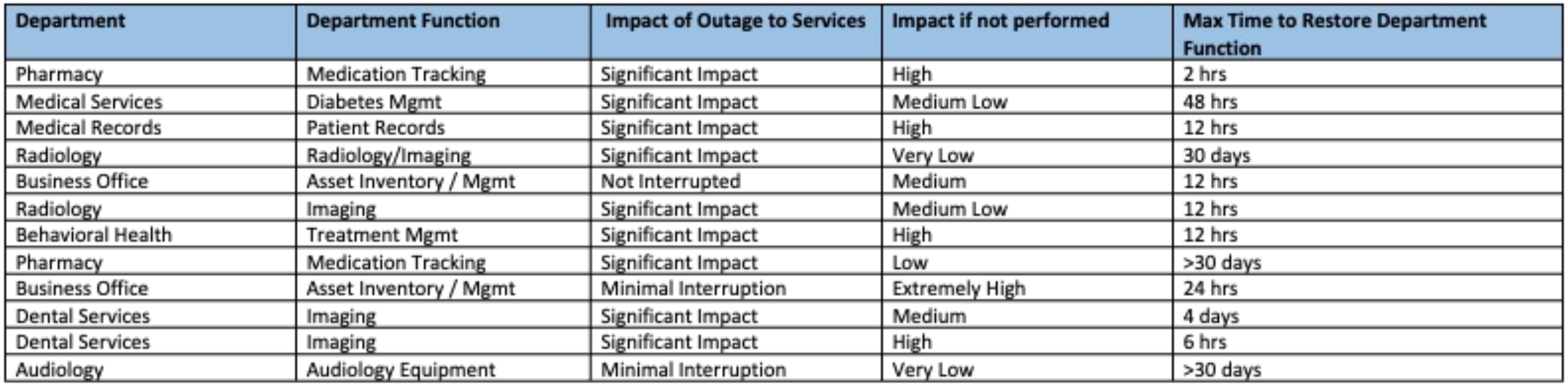
Capture the Fundamental Data with the BIA Data Collection Sheets.

- List of **Facility Departments** and their functions
- List the **IT system** details
- List the **Threats and hazards** to the facility

Capture Facility Departments

List facility departments and their functions.

- Impact if not performed
- Dependencies on other departments, vendors, etc.

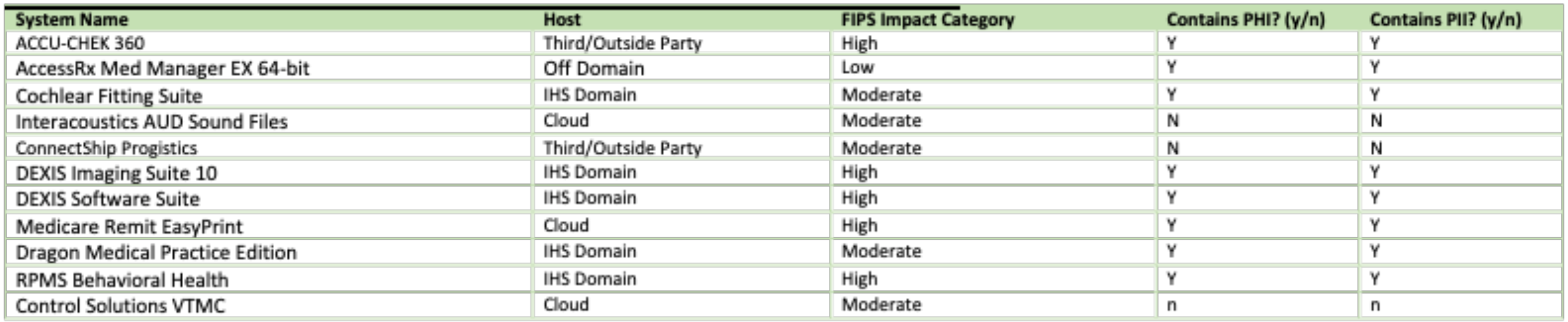


Department	Department Function	Impact of Outage to Services	Impact if not performed	Max Time to Restore Department Function
Pharmacy	Medication Tracking	Significant Impact	High	2 hrs
Medical Services	Diabetes Mgmt	Significant Impact	Medium Low	48 hrs
Medical Records	Patient Records	Significant Impact	High	12 hrs
Radiology	Radiology/Imaging	Significant Impact	Very Low	30 days
Business Office	Asset Inventory / Mgmt	Not Interrupted	Medium	12 hrs
Radiology	Imaging	Significant Impact	Medium Low	12 hrs
Behavioral Health	Treatment Mgmt	Significant Impact	High	12 hrs
Pharmacy	Medication Tracking	Significant Impact	Low	>30 days
Business Office	Asset Inventory / Mgmt	Minimal Interruption	Extremely High	24 hrs
Dental Services	Imaging	Significant Impact	Medium	4 days
Dental Services	Imaging	Significant Impact	High	6 hrs
Audiology	Audiology Equipment	Minimal Interruption	Very Low	>30 days

Capture IT System Details

List IT system details.

- DRCP can generate the basic systems list for you
- For each system, capture:
  - Type of IT application (e.g., custom, commercial off-the-shelf, etc.) and the host environment
  - Whether the IT application contains personally identifiable information (PII) or personal health information (PHI)

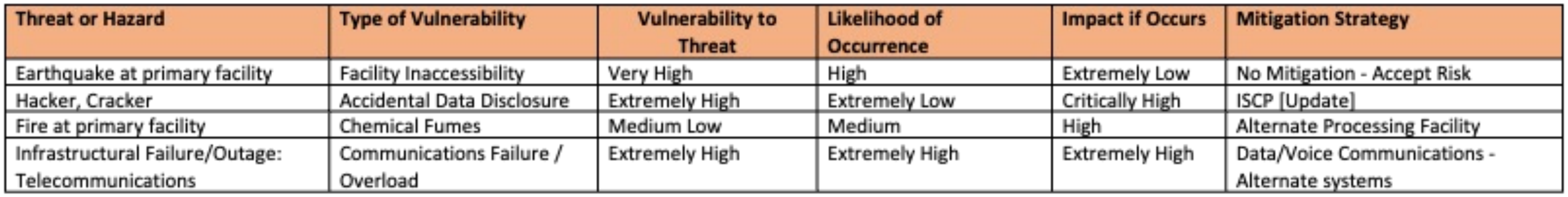


System Name	Host	FIPS Impact Category	Contains PHI? (y/n)	Contains PII? (y/n)
ACCU-CHEK 360	Third/Outside Party	High	Y	Y
AccessRx Med Manager EX 64-bit	Off Domain	Low	Y	Y
Cochlear Fitting Suite	IHS Domain	Moderate	Y	Y
Interacoustics AUD Sound Files	Cloud	Moderate	N	N
ConnectShip Progistics	Third/Outside Party	Moderate	N	N
DEXIS Imaging Suite 10	IHS Domain	High	Y	Y
DEXIS Software Suite	IHS Domain	High	Y	Y
Medicare Remit EasyPrint	Cloud	High	Y	Y
Dragon Medical Practice Edition	IHS Domain	Moderate	Y	Y
RPMS Behavioral Health	IHS Domain	High	Y	Y
Control Solutions VTMC	Cloud	Moderate	n	n

Capture Threats, Hazards, and Vulnerabilities

List threats, hazards, and vulnerabilities to the facility.

- Likelihood of occurrence
- Impacts if the hazard occurs
- Mitigation strategies



Threat or Hazard	Type of Vulnerability	Vulnerability to Threat	Likelihood of Occurrence	Impact if Occurs	Mitigation Strategy
Earthquake at primary facility	Facility Inaccessibility	Very High	High	Extremely Low	No Mitigation - Accept Risk
Hacker, Cracker	Accidental Data Disclosure	Extremely High	Extremely Low	Critically High	ISCP [Update]
Fire at primary facility	Chemical Fumes	Medium Low	Medium	High	Alternate Processing Facility
Infrastructural Failure/Outage: Telecommunications	Communications Failure / Overload	Extremely High	Extremely High	Extremely High	Data/Voice Communications - Alternate systems

Refine

Once the data sheets are finished:

- DRCP will pre-populate the BIA tool
- The BIA tool performs much of the preliminary analysis
- The BIA team captures the associations between functions, IT systems, and threats

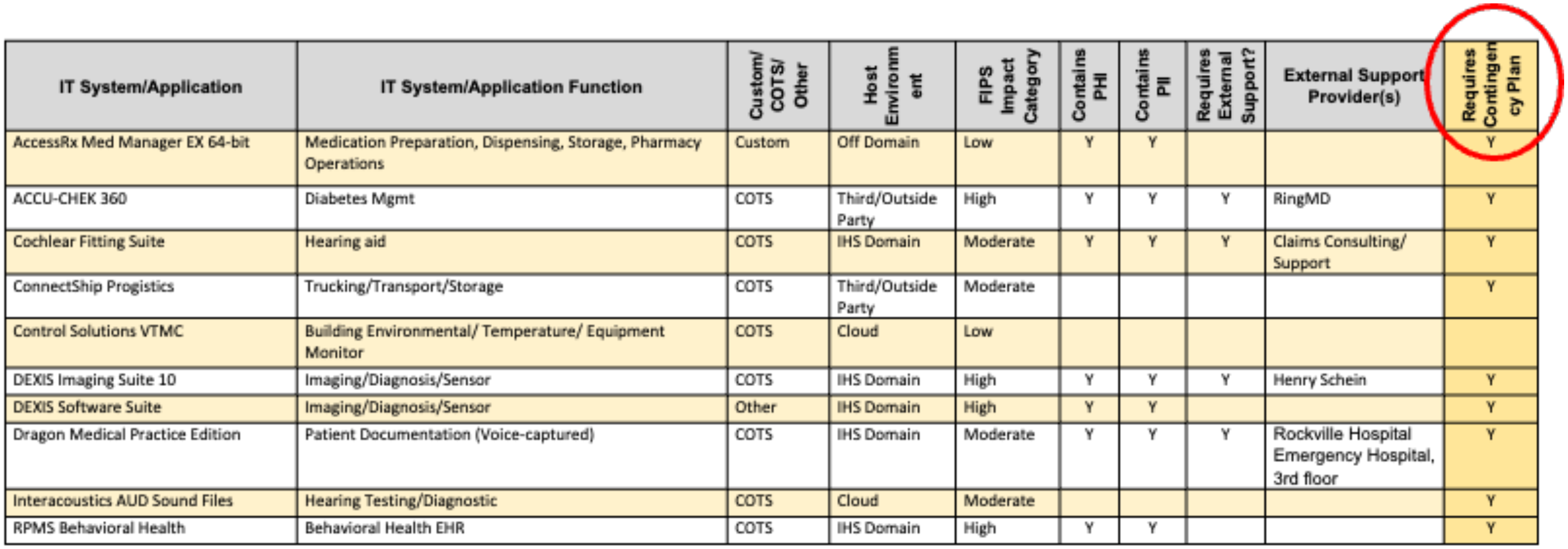
Rubber: meet road

- Building the BIA is an iterative process.
- Can start with functions, departments, or IT systems. You'll get to the same place.

Refine IT Systems Information

Capture the last of the IT system information.

- The BIA tool calculates which systems require ISCPs based on FIPS category, PHI, and PII

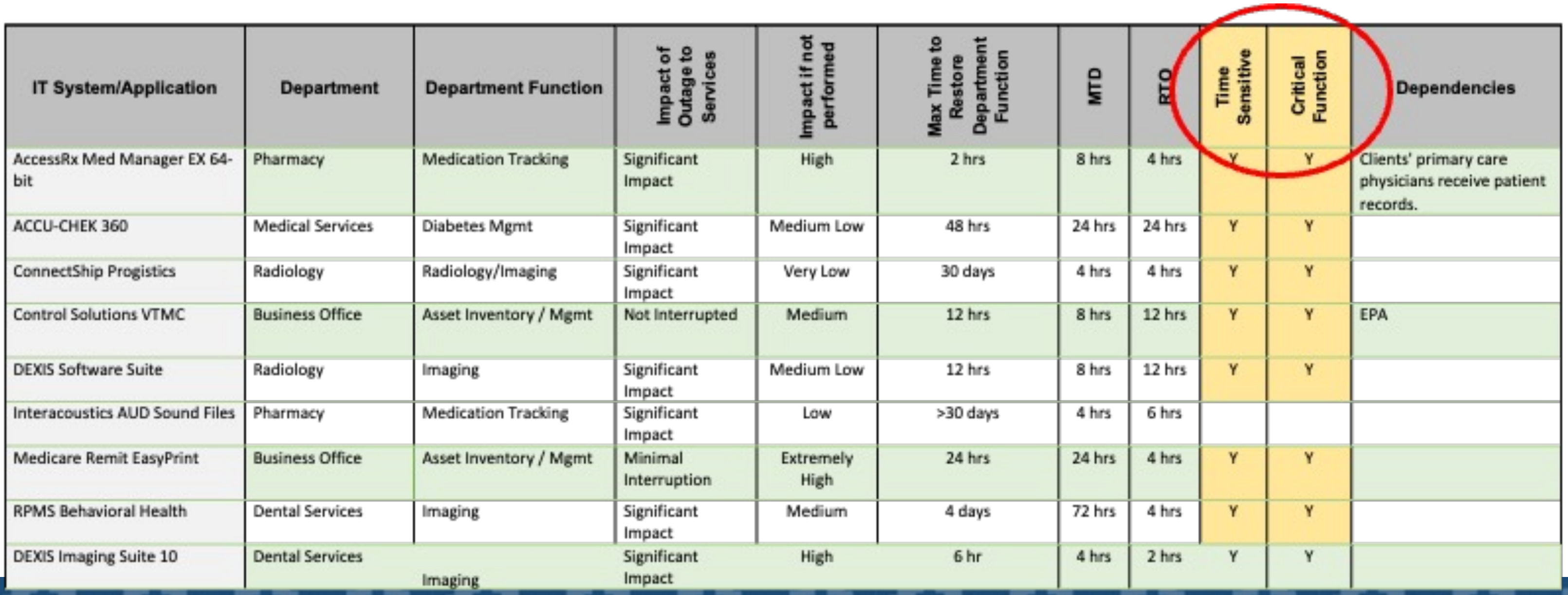


IT System/Application	IT System/Application Function	Custom/ COTS/ Other	Host Environment	FIPS Impact Category	Contains PHI	Contains PII	Requires External Support?	External Support Provider(s)	Requires Contingency Plan
AccessRx Med Manager EX 64-bit	Medication Preparation, Dispensing, Storage, Pharmacy Operations	Custom	Off Domain	Low	Y	Y			Y
ACCU-CHEK 360	Diabetes Mgmt	COTS	Third/Outside Party	High	Y	Y	Y	RingMD	Y
Cochlear Fitting Suite	Hearing aid	COTS	IHS Domain	Moderate	Y	Y	Y	Claims Consulting/ Support	Y
ConnectShip Progistics	Trucking/Transport/Storage	COTS	Third/Outside Party	Moderate					Y
Control Solutions VTMC	Building Environmental/ Temperature/ Equipment Monitor	COTS	Cloud	Low					
DEXIS Imaging Suite 10	Imaging/Diagnosis/Sensor	COTS	IHS Domain	High	Y	Y	Y	Henry Schein	Y
DEXIS Software Suite	Imaging/Diagnosis/Sensor	Other	IHS Domain	High	Y	Y			Y
Dragon Medical Practice Edition	Patient Documentation (Voice-captured)	COTS	IHS Domain	Moderate	Y	Y	Y	Rockville Hospital Emergency Hospital, 3rd floor	Y
Interacoustics AUD Sound Files	Hearing Testing/Diagnostic	COTS	Cloud	Moderate					Y
RPMS Behavioral Health	Behavioral Health EHR	COTS	IHS Domain	High	Y	Y			Y

Align IT Systems with Department Functions

Associate IT systems with department function.

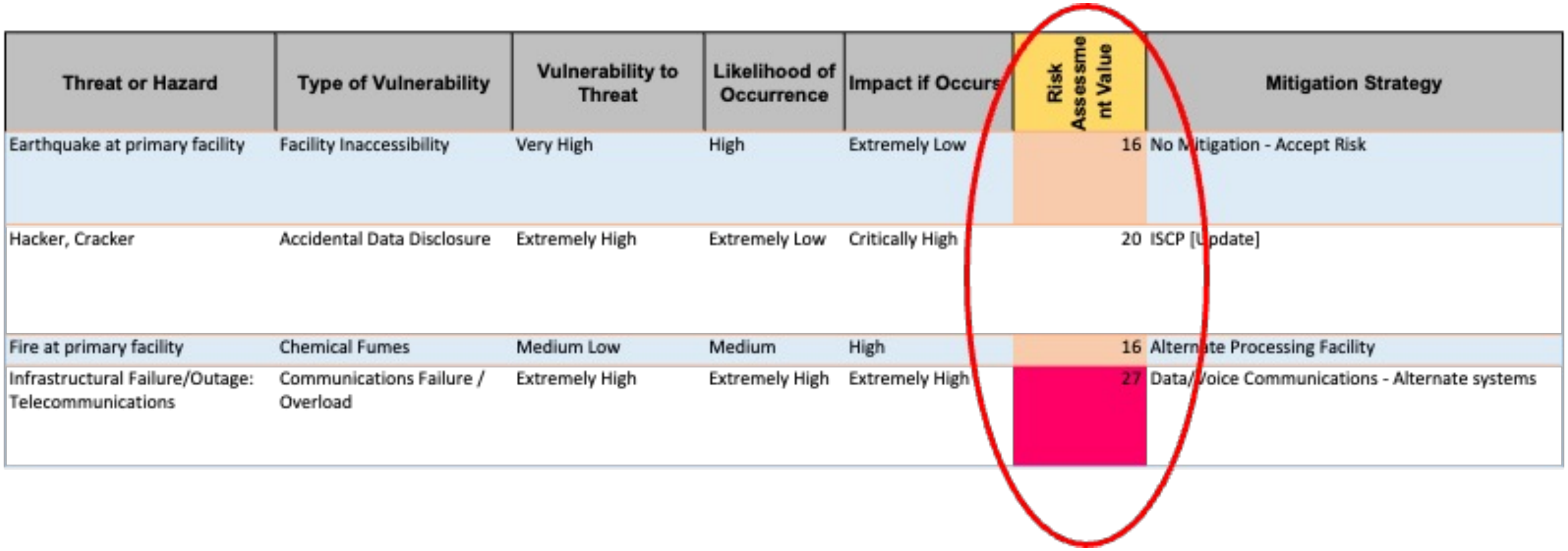
- A function and/or department can require more than one IT system
- The function determines RTO and MTD
- The BIA tool calculates the time sensitivity and criticality to restore the function



IT System/Application	Department	Department Function	Impact of Outage to Services	Impact if not performed	Max Time to Restore Department Function	MTD	RTO	Time Sensitive	Critical Function	Dependencies
AccessRx Med Manager EX 64-bit	Pharmacy	Medication Tracking	Significant Impact	High	2 hrs	8 hrs	4 hrs	Y	Y	Clients' primary care physicians receive patient records.
ACCU-CHEK 360	Medical Services	Diabetes Mgmt	Significant Impact	Medium Low	48 hrs	24 hrs	24 hrs	Y	Y	
ConnectShip Progistics	Radiology	Radiology/Imaging	Significant Impact	Very Low	30 days	4 hrs	4 hrs	Y	Y	
Control Solutions VTMC	Business Office	Asset Inventory / Mgmt	Not Interrupted	Medium	12 hrs	8 hrs	12 hrs	Y	Y	EPA
DEXIS Software Suite	Radiology	Imaging	Significant Impact	Medium Low	12 hrs	8 hrs	12 hrs	Y	Y	
Interacoustics AUD Sound Files	Pharmacy	Medication Tracking	Significant Impact	Low	>30 days	4 hrs	6 hrs			
Medicare Remit EasyPrint	Business Office	Asset Inventory / Mgmt	Minimal Interruption	Extremely High	24 hrs	24 hrs	4 hrs	Y	Y	
RPMS Behavioral Health	Dental Services	Imaging	Significant Impact	Medium	4 days	72 hrs	4 hrs	Y	Y	
DEXIS Imaging Suite 10	Dental Services	Imaging	Significant Impact	High	6 hr	4 hrs	2 hrs	Y	Y	

Determine Threat Impact

The BIA tool calculates risk impact based on threats and vulnerabilities.



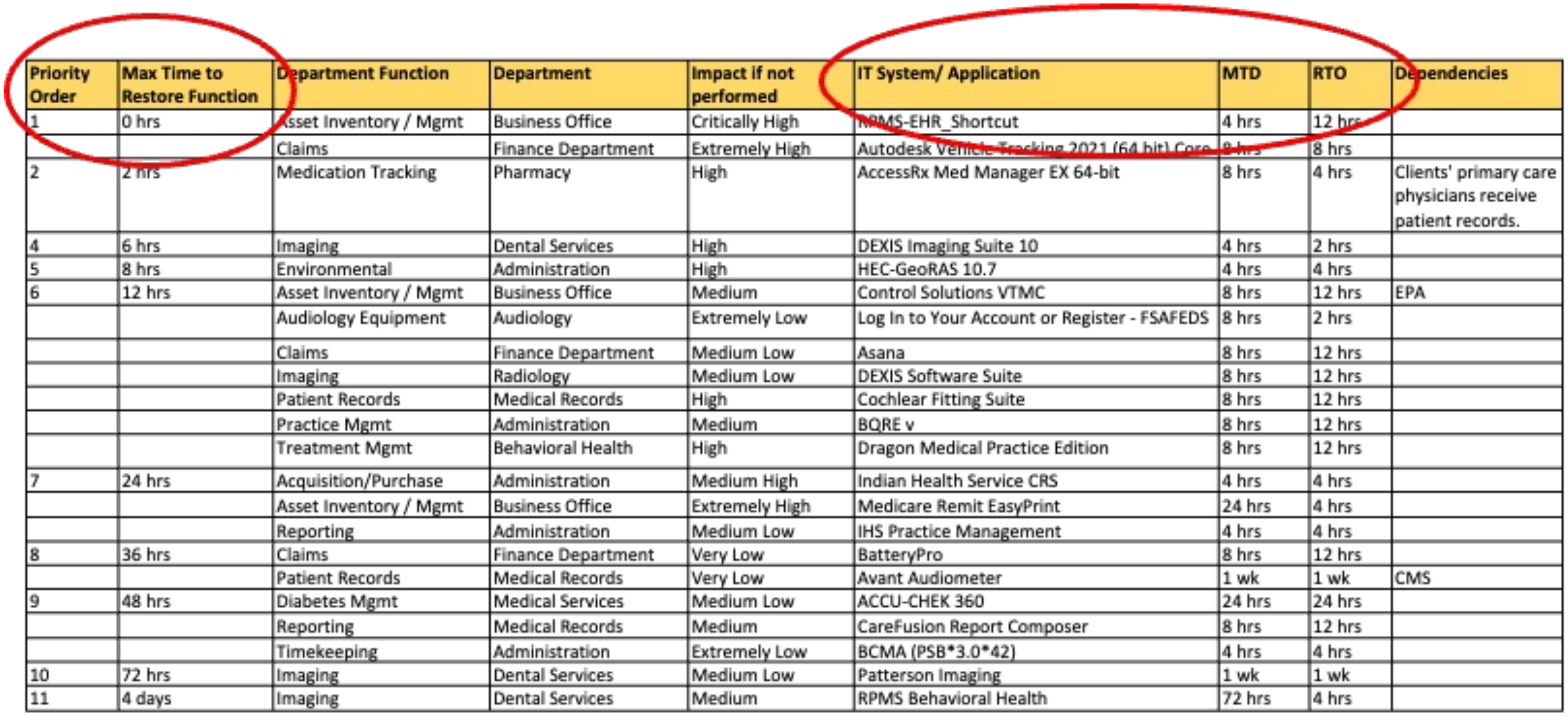
Threat or Hazard	Type of Vulnerability	Vulnerability to Threat	Likelihood of Occurrence	Impact if Occurs	Risk Assessment Value	Mitigation Strategy
Earthquake at primary facility	Facility Inaccessibility	Very High	High	Extremely Low	16	No Mitigation - Accept Risk
Hacker, Cracker	Accidental Data Disclosure	Extremely High	Extremely Low	Critically High	20	ISCP [Update]
Fire at primary facility	Chemical Fumes	Medium Low	Medium	High	16	Alternate Processing Facility
Infrastructural Failure/Outage: Telecommunications	Communications Failure / Overload	Extremely High	Extremely High	Extremely High	27	Data/Voice Communications - Alternate systems

Outputs

The BIA tool performs the final analysis and reports.

- The priority to restore functions and systems
- The departments and functions that rely on systems or applications
- Impact of an IT system or application outage on services
- Impact if the service is unavailable
- System maximum tolerable downtime (MTD) and recovery time objective (RTO)
- Whether a system requires an ISCP
- Threats to your facility, calculated risks to meeting your mission, and mitigation strategies

Recovery Report



Priority Order	Max Time to Restore Function	Department Function	Department	Impact if not performed	IT System/ Application	MTD	RTO	Dependencies
1	0 hrs	Asset Inventory / Mgmt	Business Office	Critically High	RPMS-EHR_Shortcut	4 hrs	12 hrs	
		Claims	Finance Department	Extremely High	Autodesk Vehicle Tracking 2021 (64 bit) Core	8 hrs	8 hrs	
2	2 hrs	Medication Tracking	Pharmacy	High	AccessRx Med Manager EX 64-bit	8 hrs	4 hrs	Clients' primary care physicians receive patient records.
4	6 hrs	Imaging	Dental Services	High	DEXIS Imaging Suite 10	4 hrs	2 hrs	
5	8 hrs	Environmental	Administration	High	HEC-GeoRAS 10.7	4 hrs	4 hrs	
6	12 hrs	Asset Inventory / Mgmt	Business Office	Medium	Control Solutions VTMC	8 hrs	12 hrs	EPA
		Audiology Equipment	Audiology	Extremely Low	Log In to Your Account or Register - FSAFEDS	8 hrs	2 hrs	
		Claims	Finance Department	Medium Low	Asana	8 hrs	12 hrs	
		Imaging	Radiology	Medium Low	DEXIS Software Suite	8 hrs	12 hrs	
		Patient Records	Medical Records	High	Cochlear Fitting Suite	8 hrs	12 hrs	
		Practice Mgmt	Administration	Medium	BQRE v	8 hrs	12 hrs	
		Treatment Mgmt	Behavioral Health	High	Dragon Medical Practice Edition	8 hrs	12 hrs	
7	24 hrs	Acquisition/Purchase	Administration	Medium High	Indian Health Service CRS	4 hrs	4 hrs	
		Asset Inventory / Mgmt	Business Office	Extremely High	Medicare Remit EasyPrint	24 hrs	4 hrs	
		Reporting	Administration	Medium Low	IHS Practice Management	4 hrs	4 hrs	
8	36 hrs	Claims	Finance Department	Very Low	BatteryPro	8 hrs	12 hrs	
		Patient Records	Medical Records	Very Low	Avant Audiometer	1 wk	1 wk	CMS
9	48 hrs	Diabetes Mgmt	Medical Services	Medium Low	ACCU-CHEK 360	24 hrs	24 hrs	
		Reporting	Medical Records	Medium	CareFusion Report Composer	8 hrs	12 hrs	
		Timekeeping	Administration	Extremely Low	BCMA (PSB*3.0*42)	4 hrs	4 hrs	
10	72 hrs	Imaging	Dental Services	Medium Low	Patterson Imaging	1 wk	1 wk	
11	4 days	Imaging	Dental Services	Medium	RPMS Behavioral Health	72 hrs	4 hrs	

Use

Put the outputs from the BIA tool work for you.

- Update
  - Continuity of Operations (COOP) plan
  - Disaster Recovery Plans (DRP)
  - Information System Contingency Plans (ISCP)
- Address or acknowledge any gaps identified
- Prove compliance with NIST 800-53r5 security controls

Collateral Benefits

Gap Analysis

- Identification – you didn’t know you needed support or supplies
- Contracts and agreements – you need to confirm expectations
- Access – you need to be able to access information or systems you don’t have access

Redundancy

- Multiple applications that support the same function or perform the same work
- Dependencies on different organizations for the same support

Conflicts

- Among function and IT restoration priority
- Between agreements
- Between expectations

Wrap Up

Let’s Review the Objectives

- What a BIA is
- What goes into a BIA and what comes out
- Why performing a BIA gives you the guidance to restore functions efficiently, reliably, and in the proper order based on functions’ *quantified* priority
- How performing a BIA helps identify gaps and barriers to performing functions
- Pinpointing the systems that are necessary to perform functions
- Understanding the dependencies with other departments, agencies, and third parties that affect performing function
- How BIAs are a key component in complying with NIST SP 800-53

Where Can I Get Help?

You're not alone.

- Disaster Recovery / Contingency Planning (DRCP) Team
- NIST SP 800-34, rev. 1: Contingency Planning Guide for Federal Information Systems, May 2010
- NIST SP 800-53, rev. 5: Security and Privacy Controls for Information Systems and Organizations, September 2020
- IHS Contingency Planning Handbook
- DIS SOP 20-03: Business Impact Analysis Standard Operating Procedure

Questions? Ready to get started?

INDIAN HEALTH SERVICE · PHS · 1955