IT Service Continuity Management

Business Impact Analysis Process Activity

VERSION: 1.2 REVISION DATE: 07/14/2016

Contents

Section 1. Introduction

1.1 Purpose

The UCSF Business Impact Analysis (BIA) is the process that identifies and evaluates the potential effects (ex. Financial, life/safety, regulatory, legal/contractual, reputational and so forth) of natural and man-made events or disasters on the IT services that support business operations.

1.2 Scope

In Scope:
The BIA of IT services supported by UCSF IT, Clinical Systems & Engineering and any non-IT-managed applications or services that are hosted in our UCSF Data Centers.

Out of Scope:
The BIA of Departments provided by the Campus and Med Center Emergency Management or IT services supported by internal department IT units.

1.3 Goals

The UCSF BIA process goals are:

- To identify the business recovery priority for all in scope IT services
  - Categorization of IT services by Tier
  - IT Service Restoration Order
- To align IT Service Continuity Management Annual Plan to Business requirements with cost justification
- To clearly define Customer expectations and IT expectations during a major disaster

Section 2. Roles and Responsibilities

2.1 BIA Requester

An IT Project Manager or Technical App/Svc Manager typically holds the BIA Requestor. During the BIA process the BIA Requester is responsible for:

- Completing the Business Impact Analysis Request Form
- Providing BIA interviewees list (ex. Subject Matter Experts, Contributors, IT Support contacts, etc.)
- This role is typically held by an IT Project Manager

2.2 Business Owner

The Business Owner is typically the main customer or a customer that can represent the needs of most consumers of an IT Application/Service

During the BIA process, the Business Owner is responsible for:

- Providing a description of department, vital business functions, IT services and impacts resulting from downtime
- Ensuring department downtime procedures are aligned to IT disaster recovery capabilities

2.3 Technical Application/Service Manager

The Technical Application/Service Manager (TAM) is responsible for all aspects related to the Application/Service, such as, System upgrades, Application/Service patching, maintenance, troubleshooting, disaster recovery solutions, etc.

During the BIA process, the Technical Application/Service Manager is responsible for:

- Providing all technical information related to Application or Service (ex. Infrastructure location, backup information, Number of Users, etc.)

2.4 Subject Matter Experts and Contributors

Subject Matter Experts and Contributors are responsible for providing:

- Any supplemental impact information from a Business Owner or Technical Application/Service Manager perspective.

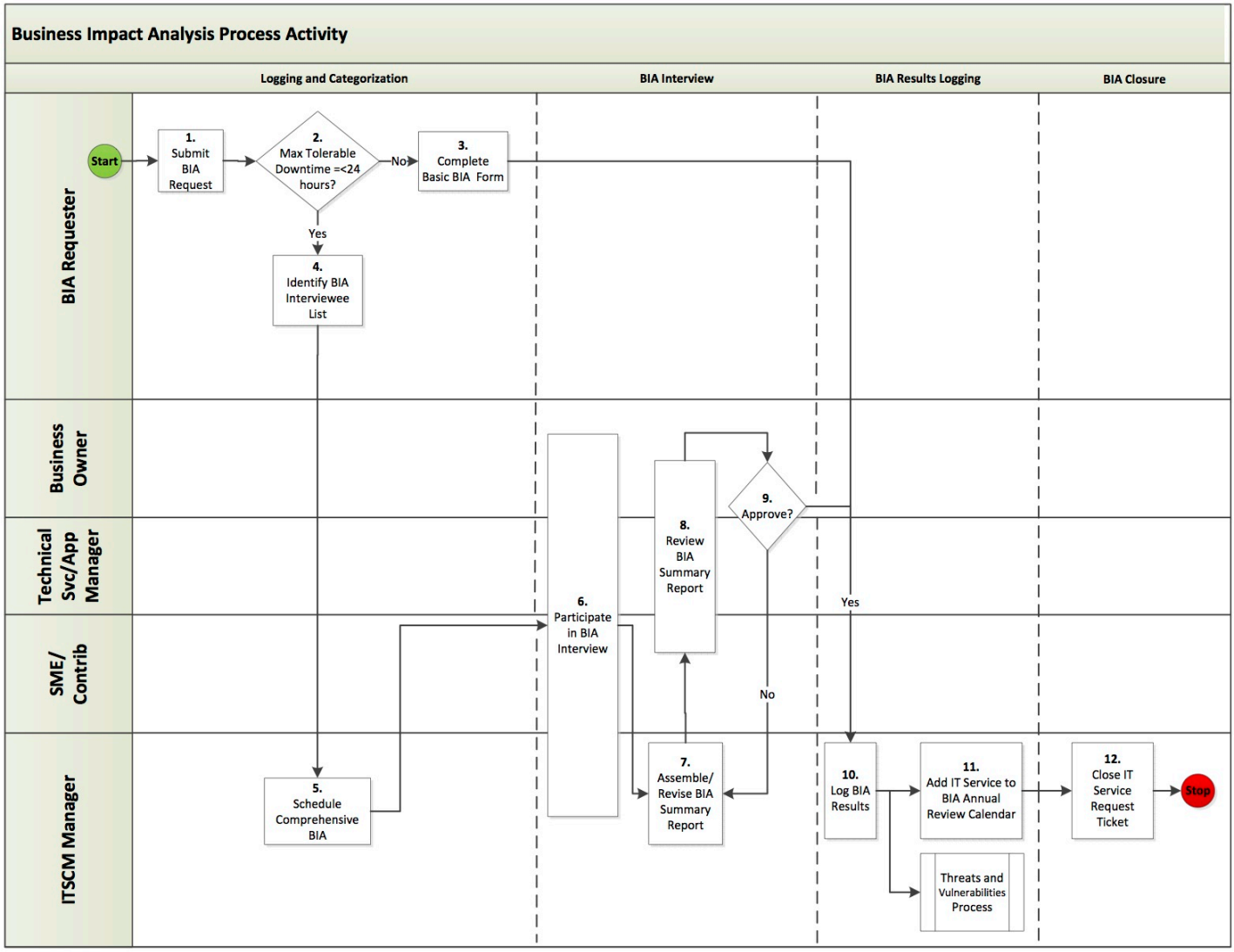
2.5 IT Service Continuity Manager

The IT Service Continuity (ITSCM) Manager is responsible for managing the IT Service Continuity Process. During the BIA Process, the ITSCM manager is responsible for:

- Conducting BIA interview and assembling BIA Summary Report
- Updating supporting IT systems with BIA information (ex. CMDB, DR Planning tool)

Section 3. Process Definition

3.1 Business Impact Analysis High-Level Process Map



3.2 RACI Chart

Step #	Business Impact Analysis Process	BIA Requester	Business Owner	Technical App/Service Manager	ITSCM Manager	SME/Contributors
Logging and Categorization						
1	Submit BIA Request	R		A	C	
2	Maximum Tolerable Downtime =<24 hours?	R, A	C		I	
3	Complete Basic BIA Form	R, A	C	C	I	
4	Identify BIA Interviewee List	R, A	C	C	I	C
5	Schedule Comprehensive BIA	C	C	C	R, A	C
BIA Interview						
6	Participate in BIA Interview		R	R	R, A	R
7	Assemble/Revise BIA Summary Report		C	C	R, A	C
8	Review BIA Summary Report		R	R	A	R
9	Approve?		R	R	A	I
BIA Results Logging						
10	Log BIA Results		I	I	R, A	I
11	Add IT Service to BIA Annual Review Calendar	I	I	I	R, A	I
	Threats and Vulnerabilities Process				R, A	
BIA Closure						
12	Close IT Service Request Ticket	I	I	I	R, A	I

Responsible - People who do the work, facilitate it and/or organize it

Accountable - The one who ensures that desired outcomes are reached and has yes/no decision making authority

Consulted - People who have critical expertise to contribute before a decision is made

Informed - People who are significantly affected by the activity/decision and must be informed to ensure successful implementation

3.3 Entry Criteria

- New IT Service or Application Managed by UCSF IT, Clinical Systems & Engineering or contracted service providers
- Major Change to existing IT Service or Business Function
- BIA is aged more than 12 months

3.4 Procedure

ID	Step	Responsibility
Business Impact Analysis Request Logging and Categorization Sub-Process		
1.	**Submit Business Impact Analysis Request form** Requester opens ServiceNow Request Item ticket or ServiceNow Request Item ticket is generated upon creating a new application CI record.	BIA Requester
2.	**Maximum Tolerable Downtime (MTD) =<24 hours?** Yes – go to step 4 / No – go to step 3	BIA Requester
3.	**Complete Basic BIA Form** Go to step 10; see Section 4.4 Basic BIA Questions. Basic BIA Form is completed, if: • IT Service or Application is not supported by UCSF IT, Clinical Systems or Engineering • IT Service or Application can be down longer than 24 hours, therefore, automatically a Tier 3 or Tier 4 service • IT Service or Application does not support a vital business function	BIA Requester
4.	**Identify BIA Interviewee List** Indicate Business Owner, Technical Service Manager, Subject Matter Experts and Contributors	BIA Requester
5.	**Schedule Comprehensive BIA**	ITSCM Manager
BIA Interview Sub-Process		
6.	**Participate in BIA Interview** See Section 4.5 Comprehensive BIA Questions.	• Business Owner • ITSCM Manager • Tech Svc Manager • SME(s)/Contributor(s)
7.	**Assemble/Revise BIA Summary Report**	ITSCM Manager
8.	**Review BIA Summary Report**	• Business Owner • Tech Svc Manager
9.	**Approve?** Yes – go to step 10 / No – go to step 7 If Approval Request is => 1 month, BIA is marked as approved.	• Business Owner • Tech Svc Manager
BIA Results Logging Sub-Process		
10.	**Log BIA Results** Record results in CMDB and DR Planning Tool.	ITSCM Manager
11.	**Add IT Service to BIA Annual Review Calendar**	ITSCM Manager
	Threats and Vulnerabilities Process	ITSCM Manager
BIA Closure Sub-Process		
12.	**Close IT Service Request Ticket**	ITSCM Manager

3.5 Exit Criteria

- IT Service Tiering, RTO, RPO, RTA Classification

Section 4. Appendices

4.1 Key Terms and Definitions

Common terms and vocabulary may have disparate meanings for different organizations, disciplines or individuals. It is essential early in a process implementation to agree on the common usage of terms. It is recommended where possible not to diverge from Best Practice unless necessary, as many other customers and suppliers may be also using the same terms if they are following best practice process frameworks. This brings unity in the areas of communication to help enhance, internal dialog, but also documentation, instructions, presentations reports and interaction with other external bodies.

These terms and definitions will be used throughout the process documentation, communications, training materials, tools and reports.

Business Continuity Management (BCM): The Business Process responsible for managing risks that could seriously impact the business. BCM safeguards the interests of key stakeholders, reputation, brand and value creating activities. The BCM Process involves reducing Risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. BCM sets the objectives, scope, and requirements for IT Service Continuity Management.

Business Impact Analysis (BIA): BIA is the activity in Business Continuity Management that identifies vital business functions and their dependencies. BIA defines the Recovery requirements for IT Services including Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.

Crisis Management: Crisis Management is the process responsible for managing the wider implications of Business Continuity. A Crisis Management team is responsible for strategic issues such as managing media relations and shareholder confidence and decides when to invoke Business Continuity Plans.

Downtime Procedure Viability (DPV): This is the maximum period of time a given business process can reasonably be maintained, when an IT service outage requires a business to utilize of downtime procedures.

Maximum Tolerable Downtime (MTD): This is the maximum period of time a given business process can be inoperative before major impacts occur.

Recovery: Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the IT Service can be made available to the Users.

Recovery Option: A strategy for responding to an interruption to Service. Commonly used strategies are Do Nothing, Manual Workaround, Reciprocal Arrangement, Gradual Recovery, Intermediate Recovery, Fast Recovery and Immediate Recovery. Recovery Options may make use of dedicated facilities or Third Party facilities shared by multiple businesses.

Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured in time that a business process can endure.

Recovery Time Objective (RTO): The targeted duration of time and service level within which a business process or supporting IT application must be restored after a major disaster in order to avoid unacceptable consequences associated with a break in business continuity.

Recovery Time Achievable (RTA): The proven period of time it takes to restore an application or service to acceptable service levels based on recovery testing or *actual* recovery from a major disaster or disruption.

Risk: A possible event that could cause harm or loss, or affect the ability to achieve objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the impact it would have if it occurred.

Scenario: The scenario is designed to add realism to the exercise by providing participants with situations that will inspire responses that help participants achieve exercise objectives. The scenario chosen should be crafted to adequately address the broad topic areas and specific objectives selected in the design phase. In addition, exercise developers should ensure the scenario does not stray outside the scope of the exercise. Exercise scenarios may be crafter to explore worst-case situations; however, it is often useful to develop scenarios that cause participants to respond to topical issues they are apt to encounter in the real world. For example, an exercise of an IT contingency plan for an organization that is prone to disruptions from natural disasters may consider a scenario involving a significant power outage caused by a hurricane. A narrative scenario is documented and typically distributed to participants via handouts or an oral presentation on the day of the exercise.[2]

Threat: A threat is anything that might exploit Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example, a fire is a Threat that could exploit the Vulnerability of flammable floor coverings.

Tiering: Application or IT service criticality will be categorized by the Requested Recovery Time Objective of the Business Owner and assigned a numeric Tier value.

Tier	Recovery Time Objective
1	6 hours or less
2	6 hours to 24 hours
3	24 hours to 1 week
4	1 week+

Vital Business Function (VBF): A UCSF business function or process, which is critical to the success of the business (ex. One of the Payroll Department's Vital Business Functions is 'Paying Employee Wages').

Vulnerability: A weakness that could be exploited by a Threat; for example, an open firewall port, a password that is never changed or a flammable carpet

4.2 Citations

[1]Info-Tech Research Group (Date: Unknown) *Disaster Recovery Plan Template, ITA – Premium: Strategy & Planning Tool*. Retrieved from **https://www.sfmsdc.org/pdfs/DisasterRecoveryPlanTemplate.docx**

[2]National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce (Date: September 2006) *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. Retrieved from **http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf**

4.3 BIA Request Form Instructions

To access the BIA Request Form, you must login to MyAccess and:

1. Go to URL: **http://help.ucsf.edu**
2. Select 'Consulting and Development'
3. Login with your MyAccess Account
4. Select 'Business Impact Analysis Request Form'
5. Complete all required fields and click the 'Order Now' button

4.4 BIA Request Form Fields/Questions

No	Field/Question	Values
1.	Requester Name	
2.	Requester Phone Number	
3.	Department Name	
4.	Manager for Notification	
5.	Requested For Name	
6.	What is the name of your Application or Service?	
7.	Please provide a brief description or overview of your application or service	
8.	How long has your application or service been in use at UCSF? If it is not in use, when will it be?	
9.	How long will you use your Application or Service?	• Less than 1 month • Less than 1 year • More than a year • Indefinitely • Don't Know
10.	What Vital Business Functions does your Application or Service support?	
11.	What is the impact to Vital Business Functions if your Application or Service was down or disrupted for 1 day? [1]	
12.	What IT organization supports your Application or Service?	• Our Internal IT Department • UCSF IT • Clinical Applications • Clinical Engineering • I don't know[1]
13.	What is your perceived criticality of this system?	• High, very critical • Medium, somewhat critical • Low, not critical
14.	Business Owner (main customer or user)	
15.	Technical Application or Service Manager	
16.	Subject Matter Expert(s)	
17.	Has a BIA been conducted before by UCSFIT? If yes, please attach a copy.	
18.	Please attach documents (ex. Architecture drawing, previous BIA, etc.)	

4.5 Basic BIA Questions for Customer

No	Field/Question	Values
1.	What is your Department Name?	
2.	What is a brief description of your department (or website URL)?	
3.	What business function does this application or system support?	
4.	Can this application or system be down longer than 24 hours? If no, please explain:	
5.	In the event this application or system is unavailable due to a major outage, how long are downtime procedures viable before major impacts occur?	
6.	If your application or system resides in a UCSF Data Center, data is backed up every 24 hours. Do you have any special needs that require more frequent backups? If yes, please explain:	
7.	Has a Business Impact Analysis (BIA) been conducted before? If yes, please attach a copy.	

4.6 Basic BIA Questions for Technical Application Manager

No	Field/Question	Values
1.	What is the Application Name?	
2.	What is the Organization (ex. Campus, Med Center, Enterprise - Both)?	
3.	Who is the Technical Application Manager?	
4.	Who is the Business Owner?	
5.	What is a description of the application or system?	
6.	What is the number of users?	
7.	What is the Server Hosting Arrangement?	
8.	Where is the infrastructure location?	
9.	Who is the Disaster Recovery Plan Manager?	
10.	What is the High Availability Status?	
11.	What is the current Disaster Recovery Strategy?	
12.	What is the Recovery Capability Status?	
13.	Who is the Backup Owner?	
14.	Where is the Data Backup location?	
15.	Has a Security Risk Assessment been completed in the last 12 months?	

4.7 Comprehensive BIA Questions for the Customer

Includes all above 'Basic BIA Questions for the Customer' and:

No	Field/Question	Values
Department General Information		
1.	Who are your departments' internal & external customers?	
2.	What are the peak operating periods of your department services?	
3.	What are the inputs to your department?	
4.	What are the outputs to your department?	
5.	What is the status of Existing Response and Recovery Plans?	• No Existing Emergency Action or Business Continuity Plan • Emergency Action Plan Completed

		• Business Continuity Plan Completed • Both Emergency Action and Business Continuity Plans Completed • Plans Completed-Aged More than 12 months
Business Department Functions		
1.	What is the function name?	
2.	What is a brief description of this function?	
3.	If this function was not available (ex. Major flu outbreak impacts staff), please describe the potential impacts to:	
4.	Financial?	
5.	Reputational?	
6.	Operational?	
7.	Regulatory/Legal/Contractual?	
8.	Environmental?	
9.	Patient Care?	
10.	What are the Patient Safety implications?	
11.	What are the Research implications?	
12.	What is the number of faculty that would be affected if this function were unavailable?	
13.	What is the number of patients that would be affected if this function were unavailable?	
14.	Identify the number of Postdoctoral Scholars.	
15.	What is the number of residents (physicians, dentists and pharmacists in training)?	
16.	What is the number of staff affected that would be affected by this function?	
17.	What is the number of students that would be affected by this function?	
18.	What are the potential regulatory implications (CMS/MMS/joint commission)?	
19.	What are the productivity/organizational implications?	• Multiple users in a high volume area affected • Multiple users in a low volume area affected • Limited user groups in a high volume area affected • Limited users in a low volume area affected
20.	What is the total potential revenue loss, if this function was unavailable for one day?	• Greater than $5M • Between $1M and $5M • Less than $250K • No financial implications
21.	If this function became unavailable due to a disaster, when would it need to be restored to avoid harmful impacts (Recovery Time Objective = RTO)?	• < 1 hour • < 4 hours • < 12 hours • < 1 day • < 2 days • < 3 days • < 4 days • < 1 week • < 2 weeks • < 3 weeks

		• < 4 weeks • >4 weeks
22.	If you have an agreement that guarantees this function will be restored (Committed RTO), what is the timeframe?	• < 1 hour • < 4 hours • < 12 hours • < 1 day • < 2 days • < 3 days • < 4 days • < 1 week • < 2 weeks • < 3 weeks • < 4 weeks • >4 weeks
23.	If you answered yes to the above question and have tested this agreement, when were you able to restore this function (Proven RTO)?	• < 1 hour • < 4 hours • < 12 hours • < 1 day • < 2 days • < 3 days • < 4 days • < 1 week • < 2 weeks • < 3 weeks • < 4 weeks • >4 weeks
Business Department Application Dependencies		
1.	What is the Application Name?	
2.	Are there any application alias names?	
3.	Identify the functions (from above) using this application.	
4.	Describe how your department uses this application.	
5.	Who is the IT point of contact that supports this application?	
6.	What is the total number of end users?	
7.	Identify the total number of internal department users?	
8.	What is the status of the manual workarounds?	• Periodic testing of approved procedures and staff training • Infrequent testing of approved procedures and staff training • Leadership approval of documented procedures and staff training • No procedures documented
9.	What is the location of the manual workaround procedures?	
10.	Identify the length of time manual workarounds remain viable?	• < 1 hour • < 4 hours • < 12 hours • < 1 day • < 2 days • < 3 days • < 4 days • < 1 week • < 2 weeks • < 3 weeks

		• < 4 weeks • >4 weeks
11.	Identify the upstream application and data dependencies.	
12.	Identify the downstream application and data dependencies.	
13.	What are the manual workarounds?	
14.	What is the requested RTO (Recovery Time Objective)?	• < 1 hour • < 4 hours • < 12 hours • < 1 day • < 2 days • < 3 days • < 4 days • < 1 week • < 2 weeks • < 3 weeks • < 4 weeks • >4 weeks
15.	Explain the justification for the requested RTO?	
16.	What is the data loss tolerance or Recovery Point Objective (RPO)?	• < 1 hour • < 4 hours • < 12 hours • < 1 day • < 2 days • < 3 days • < 4 days • < 1 week • < 2 weeks • < 3 weeks • < 4 weeks • >4 weeks
17.	Explain the justification for the requested RPO.	
18.	What is the impact rating?	4: Catastrophic A loss of this resource affects safety/patient care or a loss would most likely result in a significant inability to meet customer needs, or other substantial operational, financial (greater than $5M) or reputation issues. 3: Major A loss of this resource would likely lead to a high degree of customer dissatisfaction. The loss may result other major operational, financial ($1M - $5M) or reputation issues. 2: Moderate A loss of this resource would likely cause some customer dissatisfaction, including

		potentially delays in product or service obligations. Financial implications between ($250K and $1M) 1: Minor A loss of this resource would only likely result in slight customer annoyance or service deterioration, potentially requiring process rework. Financial implications of $250K or less.
19.	Explain your rationale for selecting this Impact rating.	
20.	Any additional comments.	
Business Department Interdependencies		
1.	What is the name of the interdependency?	
2.	What functions, from above, use this interdependency?	
3.	Please provide a description of the interdependency.	
4.	Please provide a description of the manual work around (current or potential) for this interdependency.	
5.	What is the requested Recovery Time Objective (RTO)?	
6.	What is the justification for this RTO?	
7.	What are the impacts of downtime?	
Business Department Recovery Staff Requirements		
1.	What is the Recovery Staff Role name?	
2.	How many individuals comprise this role during normal non-disaster periods?	
3.	How many individuals can work from home?	
4.	Provide the number of people in this role needed for recovery **1 to 23 hours after** a disruption.	
5.	**< 1 day** after a disruption?	
6.	**< 2 days** after a disruption	
7.	**< 4 days** after a disruption	
8.	**< 5 days** after a disruption	
9.	**< 2 weeks** after a disruption	
10.	**< 3 weeks** after a disruption	
11.	**< 4 weeks** after a disruption	
Business Department Recovery Resource Requirements		
1.	What is the name of the recovery resource needed?	
2.	What is quantity of this resource used under normal conditions?	
3.	Provide the quantity needed for recovery **1 to 23 hours after** a disruption.	
4.	**< 1 day** after a disruption?	
5.	**< 2 days** after a disruption	
6.	**< 4 days** after a disruption	
7.	**< 5 days** after a disruption	
8.	**< 2 weeks** after a disruption	
9.	**< 3 weeks** after a disruption	
10.	**< 4 weeks** after a disruption	

4.8 Comprehensive BIA Questions for the TAM

Includes all above 'Basic BIA Questions for the Technical Application Manager' and:

Technical Application Questions		
No	**Field/Question**	**Values**
1.	What is the name of the application?	
2.	What are key tags or keywords for this application?	
3.	What organization does this application serve?	- Medical Center - Campus - Enterprise (Campus and Medical Center) - Other
4.	Who is the Technical Application Manager for this application?	
5.	Who is the Business Owner of this application?	
6.	Please provide a brief description of this application:	
7.	What is the total number of users who access this application?	
8.	What is the number of IT personnel supporting or administering this application?	
9.	What is the server hosting arrangement of this application:	- A third party vendor hosts the servers (SAAS) - Central IT hosts the servers - Hosted internally by UCSF department (not Central IT) - UC Irvine hosts the servers - UCOP hosts this application (not on mainframe) - UCOP hosts this application on the mainframe
10.	Identify the location where this infrastructure is hosted.	- UCSF Data Center (please specify which one) - Software As A Service (SAAS) - UCOP - UC Irvine - Multiple Locations - Unknown/Unspecified
11.	Lowest requested RTO (Recovery Time Objective). This field is auto-populated from the Business Impact Analysis section.	
12.	What is the committed RTO? (List in hours, days or weeks)	
13.	What is the proven RTO? (List in hours, days or weeks)	
14.	Lowest requested RPO (Recovery Point Objective). This field is auto-populated from the Business Impact Analysis section.	
15.	What is the committed RPO? (List in hours, days or weeks)	

16.	What is the proven RTO? (List in hours, days or weeks)	
17.	What is the data change rate?	
18.	What is the maximum acceptable network latency in milliseconds (ms)? To view an explanation of network latency, **click here**.	
19.	What is the current disaster recovery strategy?	
20.	What is the current status of this application's disaster recovery plan?	- Periodic testing of approved procedures and staff training - Infrequent testing of approved procedures and staff training - Leadership approval of documented procedures and staff training - Procedures documented - No procedures documented
21.	Who is the disaster recovery plan manager?	
22.	What is the recovery capability status?	- Unknown - Meets Requirements - Risks Accepted - In Process / Mitigation - Obsolete / End of Life
23.	Identify the date of the last disaster recovery test for this application	
24.	Where is the Disaster Recovery (DR) site?	- No DR site - UC San Diego - UC Davis - Other - Unknown
25.	What is the type of disaster recovery test performed last?	- Failover Test - Functional Tabletop - No DR test
26.	Where is data for this application backed up?	- Offsite backup (separation greater than 75 miles) - Offsite backup (separation is less than 75 miles) - No offsite backups - Unknown
27.	Identify who is responsible for backing up data for this application?	- UCSF - UCOP - UC Irvine - Unknown - Other
28.	What is the last known date on which backup data was tested for accuracy?	
29.	Who validated data during the last known backup test?	
30.	What are the application dependencies?	
31.	What is the virtualization state?	- Physical or Mixed infrastructure that can not be virtualized

		- Physical or Mixed infrastructure that can be virtualized - Virtual infrastructure - Unknown
32.	List the minimum required infrastructure to operate this application after a major disaster and loss of your production environment.	
33.	What is the likelihood rating of an impactful loss of this resource?	1. Possible: An impactful loss of this resource occurs rarely (every five to ten or more years) 2. Likely: An impactful loss of this resource occurs periodically (every 2-5 years) 3. Probable: An impactful loss of this resource occurs at least biennially (every two years) 4. Certain: An impactful loss of this resource inevitably occurs multiple times annually
34.	Please describe any controls that would limit the likelihood of a risk.	
35.	Explain any unique threats that could lead to the loss of this item.	
36.	How often should the technical application questions (in this table) be reviewed?	
37.	Please provide any attachments (ex. System Architecture Drawing).	
38.	What are all the required operating systems for this applications infrastructure?	
39.	Has a security risk been completed in the last 12 months?	- Yes, a security risk assessment has been completed in the last 12 months - No, a security risk assessment has not been completed in the last 12 months

4.9 Document Version Control

Document Name	Business Impact Analysis Process		
Process Owner	Francine Sneddon		
Version Number	**Issue Date**	**Prepared By**	**Reason for Change**
1.0	03/01/2016	Francine Sneddon	
1.1	03/30/2016	Francine Sneddon	• Changed Role Name to Business Owner Name • Expanded Roles & Responsibilities Description
1.2	07/14/2016	Francine Sneddon	• Revised Basic BIA and Comprehensive BIA questions

4.10 Reviewers

Name	Role
Rebecca Nguyen	IT Service Continuity Management Process Owner
Francine Sneddon	IT Service Continuity Management Process Manager
Don Francis	IT Solutions Engineering Manager
Sherman Chin	IT Database Administration Manager
Chris Miller	IT Infrastructure Engineering Manager
Kevin Barney	IT Data Center Facilities and Service Assets and Configuration Management Manager
Mo Bagadi	IT Clinical Infrastructure Manager
Sunny Bang	IT Clinical Applications Manager
Ramana Sastry	IT Clinical Engineering Manager
Paul Jimenez	IT Clinical Engineering Manager
Erik Wieland	IT Campus Applications Manager
John Robinson	IT Data Center Operations Manager
Brett Moraga	IT Project Management Office Manager
Nilesh Shah	IT Clinical Systems Project Management Office Manager
Nelson Lee (S&P)	IT Information Security Manager
Irene Brezman	IT Clinical Applications Manager
Lisa Pelletier	Emergency Management – Campus
Marjorie Smallwood	Emergency Management – Medical Center