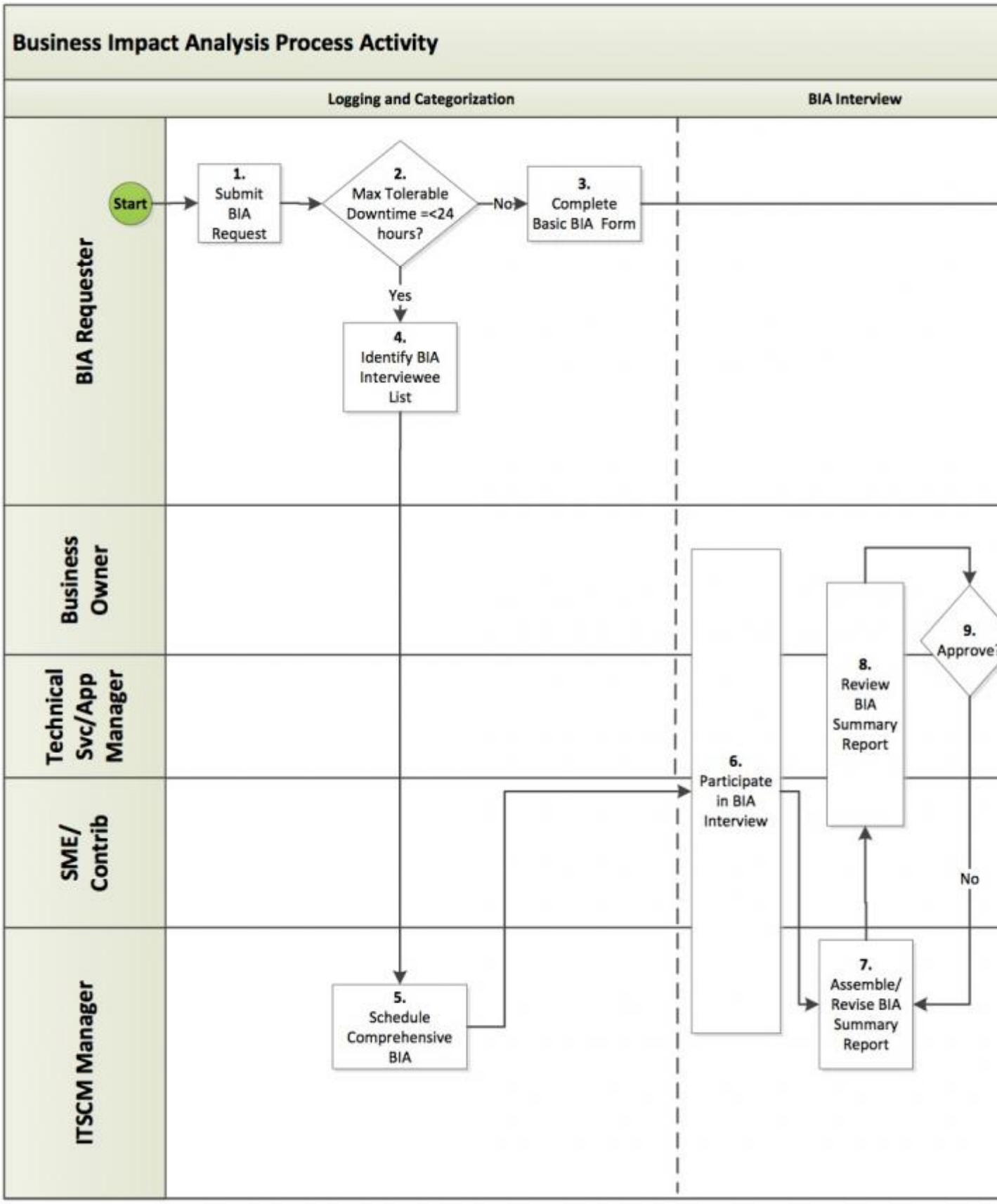
Business Impact Analysis (BIA)

The UCSF Business Impact Analysis (BIA) process identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputational and so forth) of natural and man-made events or disasters on business operations. The information is quantified and analyzed and reported to executives to meet regulatory diligence, compliance requirements, and as an input to disaster recovery solution planning. This is a broad brush approach to seeing the risk at a high level.



Documentation

Business Impact Analysis Process [1]

Frequently Asked Questions (FAQs):

- What is a BIA?
- BIA versus Risk Assessment
- How do I know if a Business Impact Analysis (BIA) is required?
- What should I expect during the BIA Process?
- Who should attend the BIA interview?
- What are the types of BIA?
- What type of BIA will I need?
- What are the BIA Interview questions?
- What is the information in the BIA used for?
- What are the application Tiers?
- When will I see the BIA results?
- How do I access my BIA Summary Report?
- How often will BIAs be reviewed?

What is a BIA?

A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuance plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, UCSF may be able to continue more or less normally if one of the cafes on campus has to close, but would come to a complete halt if the information systems crash.

As part of a disaster recovery plan, a BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, staff and data, and so on. A BIA report quantifies the importance of business components and may suggest appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts in areas such as safety, finances, marketing, business reputation, legal compliance and quality assurance and in this case IT resiliency. Where possible, impact is expressed monetarily for purposes of comparison. For example, UCSF may spend three times as much on recruiting potential students, faculty and staff in the wake of a disaster to rebuild customer confidence. The BIA should assess a disaster?s impact over time and help to establish recovery strategies, priorities, and requirements for resources and time.

BIA versus Risk Assessment

Business impact analysis and risk assessment are two important steps in a business continuity plan. A BIA often takes place prior to a risk assessment. In particular UC San Francisco?s IT Business Continuity Team will focus its BIA efforts on the effects or consequences of the interruption to critical IT business functions and attempts to quantify the

financial and non-financial costs associated with a disaster. The business impact assessment looks at the parts of the organization that are most crucial. A BIA can serve as a starting point for a disaster recovery strategy and examine recovery time objectives (RTOs) and recovery point objectives (RPOs), and resources and materials needed for business continuance.
A risk assessment identifies potential hazards such as a hurricane, earthquake, fire, supplier failure, utility outage, IT or network availability or cyber-attack and evaluates areas of vulnerability should the hazard occurs. Assets put at risk include people, property, supply chain, information technology, business reputation and contract obligations. Points of weakness that make an asset more prone to harm are reviewed. A mitigation strategy may be developed to reduce the probability that a hazard will have a significant impact.

During the risk assessment phase, the BIA findings may be examined against various hazard scenarios, and potential disruptions may be prioritized based on the hazard?s probability and the likelihood of adverse impact to business operations. A BIA may be used to justify investments in prevention and mitigation, as well as disaster recovery strategies.
UCSF has a department that manages continuity for the campus (Office of Emergency Management ? OEM) who are conducting separate BIAs and risk assessments for the business side of our campus. You may be in contact with OEM regarding the UCReady project or wish to contact OEM for more information. The IT Business Continuity Team specializes in IT resiliency and thus a BIA conducted by IT Business Continuity will focus on IT assets owned or managed by the interviewee.

How do I know if a Business Impact Analysis (BIA) is required?

To determine if a BIA is required, please complete the Business Impact Analysis Request Form (must have MyAccess Account):

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

What is should I expect during the BIA process?

A BIA is generally a multi-phase process that includes the following steps (with possible follow-up interviews):
? Gathering information via both survey and in-person interviews
? Evaluating the collected information
? Preparing a report to document the findings
? Presenting the results to the interviewee
? Potentially saving the information in UCSF's BIA repository, BC Catalyst

The information gathered may include participation by the functional owner of the data or system/application, subject matter experts and technical IT managers. A description of the principle activities that the business units perform, subjective rankings of the importance of specific processes, names or organizations that depend on the processes for normal operations, estimates of the quantitative impact associated with a specific business function and the non-financial impact of the loss of the function, critical information systems and their

users, the staff members needed to recover important systems, and the time and steps required for a business unit to recover to a normal working state may be parts of the information gathered during an IT BIA.

Questions to explore during the discovery phase include interdependencies between systems, business processes and departments, the significance of the risk of points of failure, responsibilities associated with service-level agreements, staff and space that may be required at a recovery site, special supplies or communication equipment needed, and cash management and liquidity necessary for recovery.

A BIA for information technology might start with the identification of applications supporting essential business functions, interdependencies between existing systems, possible failure points, and costs associated with the system failure. The analysis phase examines the risks and prioritizes uptime requirements and RTO and RPO.

When information gathering is complete, the review phase begins in consultation with business leaders who can validate the findings. UC San Francisco has implemented a utility, BC Catalyst, that will store the information gathered in the BIA and will be used to track changes to the systems and applications that were identified as time-sensitive/critical. An annual review of the BIA in Catalyst ensures that the information is kept up to date and changes to the BIA can be tracked and made available for senior management and planning purposes.

The goals of the BIA analysis (and by storing in Catalyst) are to determine the most crucial business functions and systems, the staff and technology resources needed for operations to run optimally, and the time frame within which the functions need to be recovered for the organization to restore operations as close as possible to a normal working state.

Who should attend the BIA interview?

The Business Impact Analysis interview attendees should include:

- Business Owner or Customer representative: An individual that understands the key business processes an application or system supports and impacts of downtime.
- Technical Application Manager: An individual responsible for the support of the application or system life cycle, including: maintenance, upgrades, development, etc.
- Subject Matter Experts (SMEs): An individual(s) that can provide application or system expertise from a business or technical perspective.

What are the types of BIAs?

There are two types of BIAs:

1. Comprehensive BIA: A Comprehensive BIA is conducted for all critical applications or systems that must be restored within 24 hours following a disaster.

2. Basic BIA: A Basic BIA is an abbreviated version of the Comprehensive BIA and is conducted for less critical applications or systems.

What type of BIA will I need?

A Basic BIA will be required if:

- The application or system can be restored later than 24 hours after a catastrophic disaster.

A Comprehensive BIA will be required if:

- The application or system must be restored within 24 hours after a catastrophic disaster.

What are the BIA Interview questions?

Basic BIA Questions for the Customer:

- What is your Department Name?
- What is a brief description of your department (or website URL)?
- What business function does this application or system support?
- Can this application or system be down longer than 24 hours? If no, please explain:
- In the event this application or system is unavailable due to a major outage, how long are downtime procedures viable before major impacts occur?
- 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:
- Has a Business Impact Analysis (BIA) been conducted before? If yes, please attach a copy.

Basic BIA Questions for the Technical Application Manager:

- What is the Application Name?
- What is the Organization (ex. Campus, Med Center, Enterprise - Both)?
- Who is the Technical Application Manager?
- Who is the Business Owner?
- What is a description of the application or system?
- What are the number of users?
- What is the Server Hosting Arrangement?
- Where is the infrastructure location?
- Who is the Disaster Recovery Plan Manager?
- Is the application built with High Availability? If no, can it be?
- What is the current Disaster Recovery Strategy?
- What is the Recovery Capability Status?

- Who is the Backup Owner?
- Where is the Data Backup location?
- Has a Security Risk Assessment been completed in the last 12 months?

Comprehensive BIA Questions for the Customer:

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

- Who are your customers (internal or external)?
- What are your peak operating periods?
- What are the inputs and outputs to your department?
- Do you have existing response and recovery plans?
- What functions does your department support?
    - What is the function description?
    - What is the function impacts if unavailable (ex. Financial, Operational, Regulatory, Productivity, etc)?
    - Who is impacted if this function is unavailable (ex. Students, Patients, Scholars, etc)?
    - What is the function's RTO?
- What are your department's Application Dependencies?
    - What is the application description?
    - What is the application's RTO?
    - What is the justification for this RTO?
    - What are the manual workarounds?
    - What is the status of manual workarounds?
    - How long are manual workarounds viable?
    - What is your data loss tolerance?
    - What is the justification for this data loss tolerance?
    - What is the impact rating?
    - Who is your IT point of contact?
    - What are the upstream application/data dependencies?
- What are any interdependencies or unique relationships this department relies upon?
- What are the Recovery Staffing Requirements?
- What are the Resource Requirements?
- What are the Risks?

Comprehensive BIA Questions for the Technical Application Manager:

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

- What is the number of IT Personnel that support this application?
- What is the status of the Disaster Recovery Plan?
- Where is the Disaster Recovery site?
- When was the Disaster Recovery Test?
- What type of test was conducted?
- When was the last time backup data was validated?
- Who validated the backup data?

- What is the required infrastructure (ok to attach drawing)?
- What operating systems are required?
- Are all servers virtualized?
- What are the application dependencies?
- Are there any known risks or threats (ex. Vendor does not allow current security patches)?
- What is the Likelihood Rating of a failure of this application?
- What are Likelihood controls in place to prevent a failure?
- Do you have any documentation (ex. Architecture Drawings)?

What is the information in the BIA used for?

The information in the BIA is used to classify IT systems based upon criticality. Based upon the Business Owner's requested Recovery Time Objective (RTO) and the viability of downtime procedures or manual workarounds, a criticality Tier is assigned. Standard disaster recovery solutions are developed based upon an application's tiering and a data backup schedule is created based upon the Business Owner's Recovery Point Objective (RPO). Following a major disaster, IT will also use the RTO to define the restoration order of critical IT services.

What are the application Tiers?

RTO	Tier Name	Tier Definition	DR Strategy	Short Technology Description
Up to 15 minutes	0	Core technology infrastructure that requires multiple data centers to be able to serve production without manual intervention.	Geographically clustered (Active-Active)	Real time data replication between data centers (Active Directory, DNS, DHCP).
Up to 6 hours	1	Systems are critical to patient health and safety for immediate clinical decision making or patient diagnostic and documentation. Failure to function for even a short period of time could have a severe impact on patient treatment. Manual downtime procedures are planned, but cannot be sustained for a long period of time.	Hot/Warm Standby	Dedicated DR environment at alternate data center. Servers are racked, configured, tested, and ready to use at alternate data center. Asynchronous replication of business data and system states to available hardware.

RTO	Tier Name	Tier Definition	DR Strategy	Short Technology Description
Up to 24 hours	2	Systems are required in order to perform critical business operations, but can allow for manual processes for up to 1 day as a reasonable workaround.	Warm Standby	Servers are provisioned and configured at alternate site. Replicated snapshots throughout day to available hardware.
Up to 5 days	3	Systems are necessary to UC Health, but short-term interruption or unavailability of 3 to 5 days is acceptable.	Cold Standby	Hardware and servers are reserved or allocated at an alternate data center. Backup restoration to hardware with horizontal scaling and ship on-demand hardware.
Up to 30 days	4	The functions affected do not jeopardize health, safety or security of patients, faculty, students or employees and manual procedures could be used until system is available.	ATOD (At Time of Disaster)	Quick ship agreements may be possible with preferred vendors for delivery at time of disaster. No hardware in place at alternate site.

When will I see the BIA results?

BIA results will be provided within 1 business week following a BIA interview.

How do I access my BIA Summary Report?

1. Login to Catalyst by clicking the following URL: https://ucsf.bccatalyst.com [3]
2. Once you log on, you will navigate to the homepage where any documents assigned to you will be visible.
3. Click on the appropriate Business Impact Analysis (BIA) title to access the summary report. Within the summary report, you can click on any blue title to make updates, or revisions.

The summary report is broken down into several sections:

- Overview: provides a brief summary of the application/service(s) being analyzed
- Function: describes the business functions supported by the application(s) being analyzed
    - Recovery Time Objective or RTO denotes the time following a disruptive incident in which an activity must be resumed or application recovered.
    - If you need to update/change an RTO, or have major revisions to our conclusions,

please provide a brief email to Bernie Conlu (Bernie.Conlu@ucsf.edu [4]) in order to provide awareness of modification.

- Applications: detailed analysis of the application/service(s) being analyzed.
  - Recovery Time Objective or RTO denotes the time following a disruptive incident in which an activity must be resumed or application recovered.
- We took into account available manual workarounds, business requirements, and impacts of downtime when assigning RTOs
- If you need to update/change an RTO, or have major revisions to our conclusions, please provide a brief email to:
  - Bernie Conlu (Bernie.Conlu@ucsf.edu? [4]) in order to provide awareness of modification.
- Interdependencies: documents other internal departments or teams required to perform the business function(s) in the summary report
- Recovery requirements: captures the IT personnel who support, deliver, and maintain the application/service(s) being analyzed

How often will BIAs be reviewed?

BIAs will be reviewed annually or when a major change to the business impact or system/application is identified.

Information Technology
UCSF Main Site

Links
[1] https://itsm.ucsf.edu/sites/itsm.ucsf.edu/files/ITSCM_BIA_Process.pdf
[2] https://ucsf.service-now.com/ess/home.do
[3] https://ucsf.bccatalyst.com
[4] mailto:Bernie.Conlu@ucsf.edu