

UNIFIED BUSINESS IMPACT ANALYSIS

Completion Guide

A practical reference for completing the SFA dynamic BIA form

BUSINESS CONTINUITY | OPERATIONAL RESILIENCE | IT RECOVERY ALIGNMENT

Purpose

This guide provides concise, section-by-section instructions for completing the University's Unified Business Impact Analysis (BIA) dynamic form. It is intended to be used with SFA business continuity training and the resources available on the SFA Business Continuity webpage.

KEY POINT

Complete one BIA per essential process or function: The BIA is not completed once for an entire division unless the division has only one essential function. Each essential process or function should be assessed separately.

How the BIA supports continuity and technology recovery



Before you begin

- Identify the specific essential process or function being assessed.
- Consult personnel who understand the process, technology, vendors, records, and operational requirements.
- Use realistic recovery requirements based on consequences to the University - not preference or convenience.
- Save progress as needed and submit the completed form electronically for review.

Office of Emergency Management | 936-468-1667 | jeremy.pickett@sfasu.edu

1

Department and Process Overview

Identify the function, its owner, and its relationship to the University COOP.

What to enter

Dynamic Form Field	What to Include	Completion Tip
Department / Division	The formal name of the department, division, college, office, or operational unit responsible for the function.	Use the same organizational name used in the BCP.
Process or Function Name	A clear, action-oriented name for the essential activity being assessed.	Name the business function, not only the software used.
Associated COOP Essential Function #	Select the University COOP essential function most closely supported by the process.	Choose the best fit; OEM can help validate alignment.
Process Owner	The position or individual accountable for ensuring the function is performed and recovered.	Use a role/title when possible to reduce impact of personnel turnover.
System or Application ID	The primary system or application supporting the function, when applicable.	List the official application or system name; leave blank only if none applies.
BEST PRACTICE	Write the function as an activity: Examples include "Process student financial aid disbursements," "Provide emergency communications," or "Maintain payroll operations." Avoid entries such as "Banner" or "email" unless the technology itself is the function.	

COMMON PITFALL

Do not combine unrelated functions: Functions with different impacts, recovery timelines, owners, or technology dependencies should be assessed on separate BIA forms.

2

Impact Assessment

Describe what happens to SFA if the function cannot be performed.

Focus on the consequence of disruption - not the cause.

The dynamic form asks for a combined narrative describing operational, financial, legal, and reputational impacts. Include the impacts that are reasonably foreseeable and explain how they increase over time.

Operational	Financial	Legal / Compliance	Reputational
Service delays, loss of capability, backlogs, missed deadlines, impacts to students or research.	Lost revenue, added labor, penalties, emergency purchases, contractual costs, or delayed payments.	Regulatory violations, reporting failures, records obligations, accreditation, contract, or policy impacts.	Loss of trust, negative attention, stakeholder concern, donor or partner impacts, or harm to institutional credibility.
BEST PRACTICE	Use time-based language: Explain what happens during the first several hours, after one day, and after several days when impacts materially worsen.		

3

Recovery Requirements

Establish realistic time and data recovery needs for each essential function.

Maximum Tolerable Downtime (MTD)

Meaning: The longest period the function can be unavailable before consequences become unacceptable to the University.

< 4 hours	4-24 hours	1-3 days	4-7 days	> 7 days
Failure rapidly threatens safety, critical operations, or immediate institutional obligations.	The function must be restored the same operational day.	Short disruption is manageable, but impacts become unacceptable within several days.	The function can be deferred temporarily with controlled impacts.	The function is non-critical or can be deferred for more than one week.

Recovery Time Objective (RTO)

Meaning: The target timeframe for restoring the function after a disruption. The RTO should normally be shorter than the MTD to provide a practical recovery buffer.

Recovery Point Objective (RPO)

Meaning: The maximum tolerable amount of data loss, expressed as time. Example: an RPO of four hours means the function may need access to data no more than four hours old.

MTD	RTO	RPO
When disruption becomes unacceptable	When the function should be restored	How much recent data can be lost

Priority Classification

Mission Critical Immediate restoration is required.	Essential Restore within 24-72 hours.	Important Restore within one week.	Deferrable Can remain unavailable for more than one week.
BEST PRACTICE	Base recovery objectives on institutional impact: Recovery requirements help establish cross-University priorities. They should reflect the operational need, while recognizing that final technology recovery sequencing will be validated with Information Technology Services and the CISO.		

COMMON PITFALL	Do not mark every function as Mission Critical: Overstating priority reduces the value of the BIA and makes it harder to distinguish what must be restored first during a widespread disruption.
----------------	--

Quick consistency check

- Is the RTO shorter than or equal to the MTD?
- Does the RPO reflect the frequency and importance of data changes?
- Does the priority classification match the selected MTD and described impacts?
- Could the recovery requirement be defended to University leadership during a major incident?

4

Dependencies and Resources

Identify what the function needs in order to operate and recover.

List the resources that are necessary to perform the function under normal conditions and during recovery. Include internal and external dependencies. Be specific enough that the BCP can develop practical continuity strategies.

PEOPLE Minimum staffing, specialized knowledge, alternates, decision authority, cross-trained personnel.	FACILITIES Primary workspace, alternate locations, labs, classrooms, storage, secure areas.	TECHNOLOGY Applications, systems, network access, devices, telecommunications, authentication.
DATA & RECORDS Vital records, databases, files, forms, retention requirements, backup or access needs.	VENDORS & PARTNERS Cloud providers, suppliers, contractors, banks, government agencies, partner institutions.	EQUIPMENT & UTILITIES Specialized equipment, vehicles, power, water, environmental controls, fuel, supplies.

BEST PRACTICE

Identify single points of failure: Note when only one individual, vendor, system, location, or specialized resource can support the function. These items should become priorities for continuity strategies and cross-training.

COMMON PITFALL

Do not list only IT systems: Technology is important, but most functions also depend on people, authority, facilities, records, communications, vendors, and physical resources.

5

Historical Disruptions / Lessons Learned

Use actual experience to test assumptions and strengthen recovery planning.

Describe previous incidents, outages, exercises, near misses, or recurring disruptions that revealed vulnerabilities or effective workarounds. The purpose is not to assign blame; it is to preserve operational knowledge.

WHAT HAPPENED Briefly identify the event and how the function was affected.	WHAT WORKED / FAILED Record successful workarounds, bottlenecks, communication gaps, or missing resources.	WHAT CHANGED Explain any corrective action, new capability, cross-training, vendor change, or planning assumption.
---	--	--

Examples that may inform this section

- Technology outages, cyber incidents, or extended loss of application access.
- Severe weather, utility failure, facility closure, flooding, or transportation disruption.
- Pandemic conditions, staffing shortages, vendor failure, supply chain disruption, or loss of key personnel.
- Exercises, audits, after-action reports, or prior use of manual workarounds.

KEY POINT

No prior disruption is acceptable: When there is no relevant history, state that clearly and document the most credible planning assumptions or exercise observations available.

6

Best Practices and Common Pitfalls

Use these checks before submitting the dynamic form.

BEST PRACTICES

- Complete one BIA for each essential process or function.
- Use measurable, time-based impacts and realistic recovery requirements.
- Consult process owners, technical staff, and subject matter experts.
- Identify upstream and downstream dependencies, including third parties.
- Document manual workarounds and minimum resource requirements.
- Use consistent names for functions, systems, and organizational units.

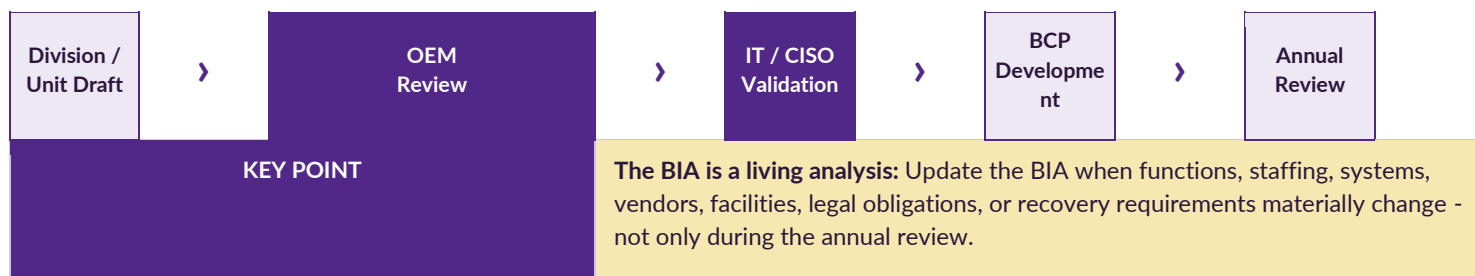
COMMON PITFALLS

- Assessing an entire division as one function.
- Naming software instead of describing the business process.
- Marking every function Mission Critical or selecting an unrealistic RTO.
- Leaving technology, vendor, staffing, or facility dependencies blank.
- Describing the cause of disruption without describing the consequence.
- Copying another unit's BIA without validating local operations.

Quality review questions

1	Would someone outside the department understand what the function does and why it matters?
2	Are the consequences specific enough to explain when disruption becomes unacceptable?
3	Are MTD, RTO, RPO, and priority classification internally consistent?
4	Have all critical people, technology, facilities, records, vendors, and resources been identified?
5	Does the BIA provide enough information to develop actionable continuity strategies in the BCP?

Review and integration workflow



7

Submission and Quick Reference

Finalize, sign, and submit the dynamic form for review.

Submission steps

1	Review	Confirm all required fields are complete and recovery values are consistent.
2	Save Progress	Use the dynamic form's Save Progress option when additional coordination is needed.
3	Sign	Complete the electronic signature and date fields.
4	Submit	Select Submit Form to route the completed BIA for review.
5	Respond	Address any clarification requests from OEM or IT and retain supporting information for BCP development.

Quick reference: key terms

Term	Plain-language meaning
Essential Function	A critical activity that must continue or resume within a defined timeframe to support the University's mission.
MTD	The point at which continued disruption becomes unacceptable.
RTO	The target time for restoring the function.
RPO	The maximum acceptable amount of data loss measured in time.
Dependency	A person, system, facility, vendor, record, resource, or service required to perform the function.
Priority Classification	The relative urgency assigned to recovery of the function.

Need assistance?

SFA OFFICE OF EMERGENCY MANAGEMENT

Questions, section review, COOP alignment, or assistance establishing recovery requirements

936-468-1667 | jeremy.pickett@sfasu.edu

KEY POINT

Use with the SFA continuity program resources: This guide supplements the BIA/BCP training, dynamic forms, and information available on the SFA Business Continuity webpage.