

CONTINUITY PLANNING GLOSSARY

Reference Guide

Plain-language definitions for SFA business continuity planning

BUSINESS CONTINUITY | OPERATIONAL RESILIENCE | COOP | IT RECOVERY ALIGNMENT

Purpose

This glossary provides consistent, plain-language definitions for terms used throughout the SFA Continuity of Operations (COOP), Business Continuity Plan (BCP), Business Impact Analysis (BIA), emergency management, information technology recovery, and continuity training programs.

KEY POINT

Use these terms consistently in BIAs, BCPs, annual reviews, exercises, and discussions with division leadership, the Office of Emergency Management, Information Technology Services, and the CISO.

How to use this glossary

- Use the glossary while completing the dynamic BIA and BCP forms.
- Apply the definitions when reviewing recovery priorities, dependencies, and continuity strategies.
- Contact the Office of Emergency Management when a term does not clearly fit a department-specific process.
- Use role titles and official system names consistently across all continuity documents.

How continuity terms connect

Essential
Function



BIA



BCP



COOP



Recovery

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

A–B**Core Planning Terms**

Alphabetical reference terms used throughout the SFA continuity program.

Term	Plain-language definition
Activation	The formal decision to begin using a continuity plan because normal operations are disrupted or are likely to be disrupted.
Alternate Facility	A location other than the normal worksite from which essential functions can be performed.
Alternate Personnel	Individuals designated and prepared to perform the duties of primary personnel when those personnel are unavailable.
Annual Review	The documented yearly evaluation of a BIA, BCP, contact list, recovery strategy, and supporting information to confirm that they remain current and workable.
Business Continuity	The capability to continue or restore essential functions during and after a disruption.
Business Continuity Management System (BCMS)	A structured system used to manage continuity plans, BIAs, reviews, exercises, assignments, approvals, and reporting.
Business Continuity Plan (BCP)	A department- or division-level plan that explains how essential functions will continue or be restored when normal operations are disrupted.
Business Impact Analysis (BIA)	A structured analysis used to identify essential functions, evaluate the consequences of disruption, determine recovery priorities, and document dependencies and resource requirements.
Business Process	A coordinated set of activities performed to deliver a service, meet an obligation, or support the University mission.

C-D**Governance, Technology, and Dependencies**

Alphabetical reference terms used throughout the SFA continuity program.

Term	Plain-language definition
Chief Information Security Officer (CISO)	The University official responsible for information security leadership and for coordinating cybersecurity risk, incident response, and related recovery considerations.
Continuity of Operations Plan (COOP)	The University-level framework for sustaining or restoring essential institutional functions, leadership, decision-making, communications, and supporting capabilities during a disruption.
Continuity Program Owner	The person or office responsible for administering, coordinating, and maintaining the continuity planning program.
Continuity Representative	A designated division or unit representative who coordinates BIA and BCP development, annual review, training, exercises, and updates.
Corrective Action	A specific improvement assigned after an exercise, incident, review, audit, or identified planning gap.
Critical Application	A technology application required to support an essential function within its established recovery timeframe.
Critical Resource	A person, facility, system, record, vendor, utility, supply, or item of equipment required to perform or recover an essential function.
Cyber Incident Response Plan (IRP)	The plan used to detect, assess, contain, respond to, and recover from cybersecurity incidents.
Dependency	A person, service, system, facility, vendor, record, utility, or resource that a function relies upon.
Disaster Recovery (DR)	The coordinated restoration of technology infrastructure, systems, applications, data, and related services following a disruption.
Downtime	The period during which a function, service, system, or facility is unavailable or cannot operate at an acceptable level.

E–I**Essential Functions, Impacts, and Incidents**

Alphabetical reference terms used throughout the SFA continuity program.

Term	Plain-language definition
Emergency Operations Plan (EOP)	The University plan that establishes the organizational structure and procedures for coordinating emergency response and recovery.
Essential Function	A University activity that must continue or resume within a defined timeframe to support safety, legal obligations, academic and research operations, financial stability, institutional governance, or other mission requirements.
Exercise	A discussion-based or operations-based activity used to validate plans, train personnel, identify gaps, and improve readiness.
Executive Sponsor	A senior leader who provides authority, direction, resources, and accountability for continuity planning within a division.
Impact	The operational, financial, legal, regulatory, safety, academic, research, or reputational consequence caused by disruption of a function.
Incident	An occurrence that disrupts or threatens normal operations and may require emergency response, continuity, cybersecurity, or recovery actions.
Interdependency	A reciprocal relationship in which two or more functions, departments, systems, or external organizations rely on one another.
Information Technology Recovery	The restoration of applications, infrastructure, networks, identity services, communications, and data needed to support University operations.

K-P**People, Priorities, and Program Roles**

Alphabetical reference terms used throughout the SFA continuity program.

Term	Plain-language definition
Key Personnel	Employees or positions with essential authority, specialized knowledge, access, credentials, or skills needed to perform or recover a function.
Manual Workaround	A temporary nonautomated method used to continue a function when normal systems or technology are unavailable.
Maximum Tolerable Downtime (MTD)	The longest period a function can remain disrupted before the consequences become unacceptable to the University.
Memorandum of Understanding (MOU)	A written agreement describing shared expectations, responsibilities, resources, or support between organizations.
Mission Critical	The highest recovery priority classification, indicating that immediate or near-immediate restoration is required because delay would create severe institutional consequences.
Operational Resilience	The ability to anticipate, withstand, adapt to, and recover from disruptions while continuing the University's most important services.
Plan Activation Authority	The position or official authorized to activate a BCP or initiate continuity procedures.
Plan Owner	The department, division, office, or designated leader responsible for maintaining and implementing a specific continuity plan.
Priority Classification	The relative urgency assigned to recovery of a function, commonly expressed as Mission Critical, Essential, Important, or Deferrable.
Process Owner	The position or individual accountable for the normal performance and recovery of a business process or essential function.

R-S**Recovery and Resilience**

Alphabetical reference terms used throughout the SFA continuity program.

Term	Plain-language definition
Recovery	The coordinated process of restoring functions, services, facilities, technology, staffing, and normal operations following a disruption.
Recovery Point Objective (RPO)	The maximum tolerable amount of data loss, measured in time. An RPO of four hours means the function may need access to data no more than four hours old.
Recovery Strategy	A planned method for continuing or restoring an essential function, such as telework, alternate facilities, manual workarounds, cross-training, vendor support, or technology recovery.
Recovery Time Objective (RTO)	The target timeframe within which a function, system, or service should be restored after a disruption.
Redundancy	An additional person, system, site, supplier, or capability maintained to reduce reliance on a single resource.
Risk	The potential for loss or harm based on the likelihood of an event and the severity of its consequences.
Single Point of Failure	A person, system, vendor, facility, or resource whose loss would prevent a function from continuing because no adequate alternative exists.
Succession	The predetermined transfer of leadership authority and responsibilities when primary officials are unavailable.
Subject Matter Expert (SME)	A person with specialized knowledge of a function, system, requirement, process, or operational dependency.

T-V**Technology, Training, and Supporting Resources**

Alphabetical reference terms used throughout the SFA continuity program.

Term	Plain-language definition
Technology Dependency	A system, application, network, device, communications service, authentication service, or data source required to perform an essential function.
Telework	The performance of job duties from an approved alternate location using available communications and technology.
Third-Party Vendor	An external company or service provider whose products, systems, supplies, expertise, or services support a University function.
Training	Instruction provided to ensure personnel understand continuity responsibilities, procedures, systems, and plan activation expectations.
Vital Records	Records or information required to continue essential functions, protect legal or financial rights, meet regulatory obligations, or support recovery.
Workaround	A temporary alternative method used to perform a function when the normal process, system, facility, or resource is unavailable.

QR

Quick Reference

Key distinctions that frequently cause confusion during BIA and BCP development.

Term	Plain-language definition
BIA vs. BCP	The BIA identifies what is essential, why it matters, and how quickly it must recover. The BCP documents how the department will continue or restore it.
MTD vs. RTO	MTD is the point at which disruption becomes unacceptable. RTO is the target time for restoration and should normally be shorter than or equal to the MTD.
RTO vs. RPO	RTO addresses time to restore a function or system. RPO addresses how much recent data may be lost.
Emergency Response vs. Continuity	Emergency response protects life, stabilizes the incident, and coordinates immediate actions. Continuity sustains or restores essential business functions.
Department Recovery vs. IT Recovery	Departments recover business processes and operational capability. IT restores technology services according to validated institutional priorities and technical dependencies.
Essential Function vs. Critical Application	An essential function is the business activity that must continue. A critical application is one technology resource that may support that function.

BEST PRACTICE

Write and discuss the business function first, then identify the people, systems, facilities, records, vendors, and other resources needed to support it.

COMMON PITFALL

Do not use “mission critical,” “essential,” “RTO,” or “MTD” interchangeably. Each term has a distinct purpose in continuity prioritization.

Need assistance?

SFA OFFICE OF EMERGENCY MANAGEMENT

Questions regarding terminology, COOP alignment, BIA/BCP development, or annual continuity reviews

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

Business Impact Analysis • Business Continuity Planning • Continuity of Operations