Business Continuity and Disaster Recovery Standard

Introduction

The Oklahoma Office of Management & Enterprise Services Information Services prescribes to a standardized strategy and tactical procedures that responds to the State of Oklahoma's requirement for rapid recovery of critical services after a disaster and continuity of operations during that event. Oklahoma state agencies, partners, vendors, suppliers and other third parties in conjunction with, as a service of, as a request from and/or as a participating member in OMES's business continuity and disaster recovery process reduce the impact of various disasters to the IT and business services provided by the State of Oklahoma's agencies. BCDR is integral in OMES's vision and fulfilling its mission to Oklahomans.

BCDR ensures our organization delivers the State of Oklahoma and its agencies' IT services with minimal disruption even in the event of a disaster. BCDR allows OMES IS to assess the requirements, risks and impacts to state agencies, streamlining the decisions impacting the State of Oklahoma's IT systems and solutions in the absence of a normal decision-making environment. This ensures that the state delivers essential public services to its citizens in the most efficient manner and with minimal disruption during a disaster.

Purpose

This document establishes the requirement for Oklahoma State agencies and third parties contracting, supporting, managing and/or installing IT services and systems with, on behalf of, in partnership with and/or under the authority of Oklahoma State agencies do so in compliance with OMES IS policies, standards and procedures. Details regarding OMES IS policies, standards and procedures can be found in the State of Oklahoma Policy, Procedures and Guidelines website.

Definitions

Third party – Any contractor, service provider, consultant or any other individual and/or organization external to state government providing services on behalf of, for or as an agent of state government.

Disaster recovery – The process of responding to an interruption in services by implementing the disaster recovery plan to restore the agency's critical business technology functions. This includes the tasks and activities designed to return the agency to an acceptable operational level.

Disaster recovery planning – The technological aspect of contingency planning. It is the advanced planning and preparations necessary to minimize loss and ensure continuity of the critical technology functions of the agency in the event of disaster.

Disaster recovery plan (DRP) – The document that defines the resources, actions, tasks and data required to manage the business technology recovery process in the event of a business interruption. The plan is designed to restore the technologies required to support critical business processes within clearly stated disaster recovery goals.

Business continuity planning – A process that identifies potential impacts that threaten the business operations of our agency. The deliverables from this process provide a framework for building resilience, with the goal of mitigating risk by planning an effective response that safeguards the interests of the agency.

Business continuity plan (BCP) – The document that includes written practices and procedures to mitigate interruptions to “business activities and business processes” from the effects of major business failures resulting from natural or manufactured disasters. The BCP focuses on sustaining an organization’s business functions during and after a disruption.

Business impact analysis (BIA) – The process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery and recovery time objectives and recovery point objectives. These recovery requirements are then used to develop strategies, solutions and plans documented in a BCP and a DRP.

Standard

The disaster recovery plan addresses the recovery of all technology processes required to support critical business functions. It is one of two major components of contingency planning. The second component is the business continuity plan, which is separate from the disaster recovery plan; it addresses the continuation of critical business operations with or without the availability of the Lincoln Data Center.

OMES IS shall prepare, implement, test and maintain a comprehensive disaster recovery plan and supporting documentation that, in the event of a disaster, facilitates the rapid recovery of critical OMES IS resources, services and operations. The DRP will be used, in conjunction with the agency-specific business continuity plan documentation, and any other documents deemed critical to the recovery effort.

The BCDR solutions utilized by the State of Oklahoma are documented in the enterprise reference architecture.

Additionally, the following applies to BCDR:

- All state agencies and third parties must participate in OMES IS BCDR strategy and processes.
- All state agencies shall conduct a BIA and produce a BCP based on the results.
- All third parties that provide connectivity to State of Oklahoma services and systems shall provide redundant connections to the main data center and disaster recovery center.
- OMES IS recommends each agency utilizes a person trained in business continuity planning to create and maintain their BIA and BCP.
- The BCP should be updated every six months, annually at a minimum, and the revised copy shall be provided to OMES IS. A BIA should be conducted every three years, five years at a minimum, to account for changes in the agency’s business.
- All state agencies shall provide OMES IS a copy of their BCP for review by the OMES IS BCDR team and to be used in disaster recovery planning for their agency.
- All third parties providing IT services to the State of Oklahoma shall provide a BCP and DRP to OMES IS related to the systems and services utilized by the state. The plans will be reviewed by the OMES IS BCDR team for incorporation into the state’s BCDR planning.
- Third parties shall provide updated BCPs and DRPs upon request by OMES IS.

- All third parties shall participate in disaster recovery planning and exercises related to State of Oklahoma services and systems and shall provide documentation on any exercises performed related to the recovery of the state's systems and services.
- Communications and submissions related to business continuity and disaster recovery shall be sent to bcdr@omes.ok.gov.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References
- Policy, Standards & Publications (oklahoma.gov).
- Enterprise Reference Architecture.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 01/18/2022	**Review cycle:** Annual
Last revised: 06/15/2023	**Last reviewed:** 07/09/2024
Approved by: Joe McIntosh, Chief Information Officer	