Florida State University

Disaster Recovery & Business Continuity Planning Overview

October 24, 2017

Key Readiness Questions

- Has your department identified the business functions and infrastructure that are most critical to your operations?
  - This may include systems, data, applications, information, samples, research technologies, facilities, generators, UPS.
- What departmental assets, if any, need to be recovered or operational during a disaster?
- Do you have a documented plan to ensure that critical operations and assets are appropriately managed during a disaster?
  - Does your department practice its plan?

Florida Statutes

- Section 282.318 - Information Technology Security Act
  - Requires state agencies to develop a 3-year IT security plan defining security goals, objectives and costs including those related to disaster recovery.
  - "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission.
- Section 282.201(2)(c) – State Data Center
  - Requires the state data center to develop and implement a business continuity plan and a disaster recovery plan and annually conduct a live exercise of each plan.
- Section 252.365 – Emergency Coordination Officers; disaster-preparedness plans
  - Requires each executive department to select an emergency coordination officer to coordinate emergency preparedness issues, post-disaster response and recovery plans, disaster operations personnel rosters, and training.

The provisions above do not include state universities or boards of trustees.

FSU Official Policies

- 4-OP-H-5 Information Security Policy
  - Requires University Units to develop & maintain a written business continuity plan that provides information on recurring backup and recovery procedures for both natural and man-made disasters.
- 4-OP-H-10 Information Technology Disaster Recovery and Data Backup Policy
  - Requires Campus Units to develop & maintain a written business continuity plan for critical assets that provides information on recurring backup procedures and recovery procedures for both natural and man-made disasters.

What is a Disaster?

- The unplanned and significant displacement or interruption of normal business processes resulting from the failure or disruption of the assets, infrastructure or facilities such processes rely on.
- Common Disaster Types **Source: Healthcare Information and Management Systems (himss.org)**

Power outages	28%	Hurricanes	6%
Storm related	12%	Fires	6%
Flooding	10%	Software Error	5%
Hardware Error	8%	Power surge/spike	5%
Physical Attack	7%	Earthquake	5%

- Major Cybersecurity Incident

  Ex. Distributed Denial of Service, Ransomware or Other Malware, etc.

Terminology

- **Business Continuity (BC):** Addresses the academic, research and operational business activities of the University. This includes the procedures and information needed to keep critical functions running during a period of displacement or interruption to normal operations.
  - Business continuity planning often addresses a larger set of issues than DR planning.
  - **Recovery Point Objectives (RPO).** RPO are define the maximum time/period in which data is at risk of being lost due to a major incident.
- **Disaster Recovery (DR):** Activities to enable continued operation or recovery of technology or other infrastructure to an acceptable level of performance after a disaster occurs.
  - This includes the processes, policies, procedures, and infrastructure related to preparing for and implementing recovery or continued operation of vital technology after a disaster.
  - **Recovery Time Objectives (RTO).** RTO are defined as the duration of time within which a system or process must be restored to an acceptable level of service to avoid unacceptable consequences after a disruption has occurred.

DR-BC Cost Benefit Analysis

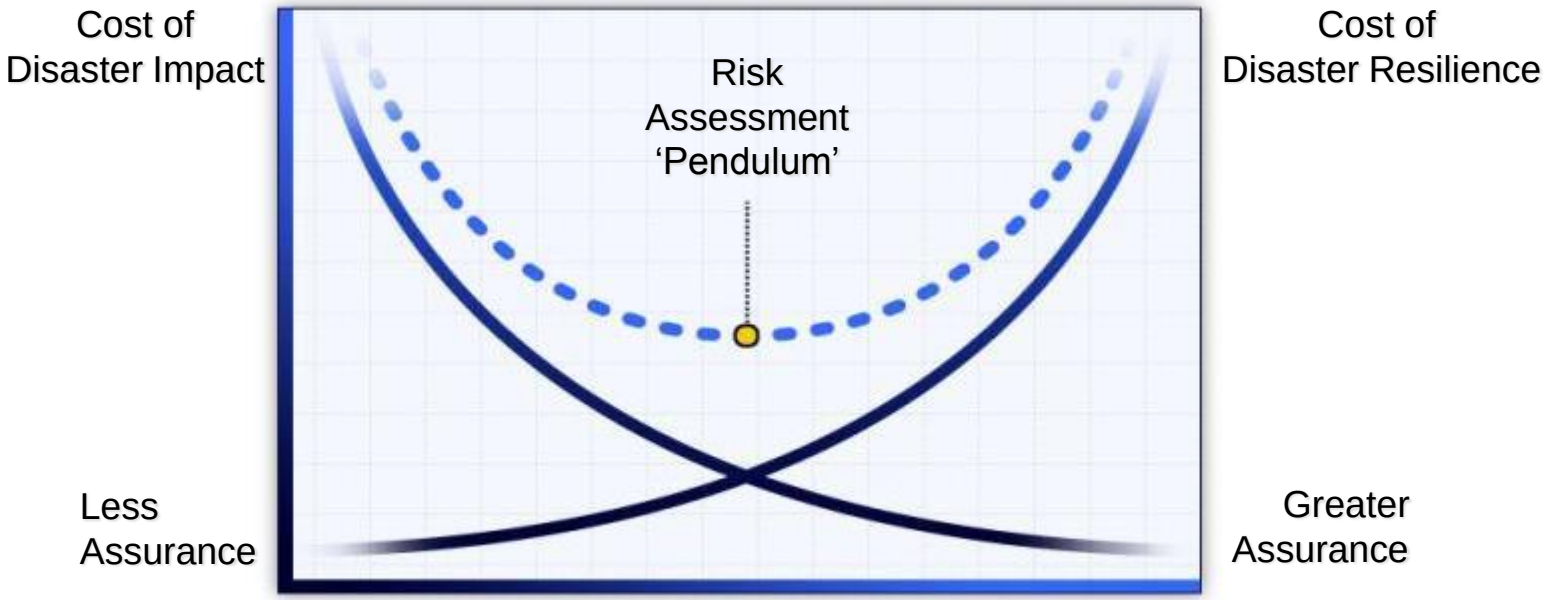


Chart adapted from CANHEIT 2012 Presentation

FSU Disaster Recovery Coordination

- University-wide DR-BC activities are coordinated under the direction of the FSU Emergency Management center. (FSU PD)
  - The University maintains a Comprehensive Emergency Management Plan (CEMP) which serves as the official emergency operations plan of the University. For additional information, refer to:
    - https://emergency.fsu.edu/cemp/tableofcontents
    - https://emergency.fsu.edu/cemp/hazardspecificannexes
- Enterprise Systems managed by ITS are addressed in the ITS continuity of operations plan.
  - Departments are responsible for Non-Enterprise Systems DR and business continuity.
- Emergency Management can assist on-campus units with scheduling short duration tabletop exercises or drills.

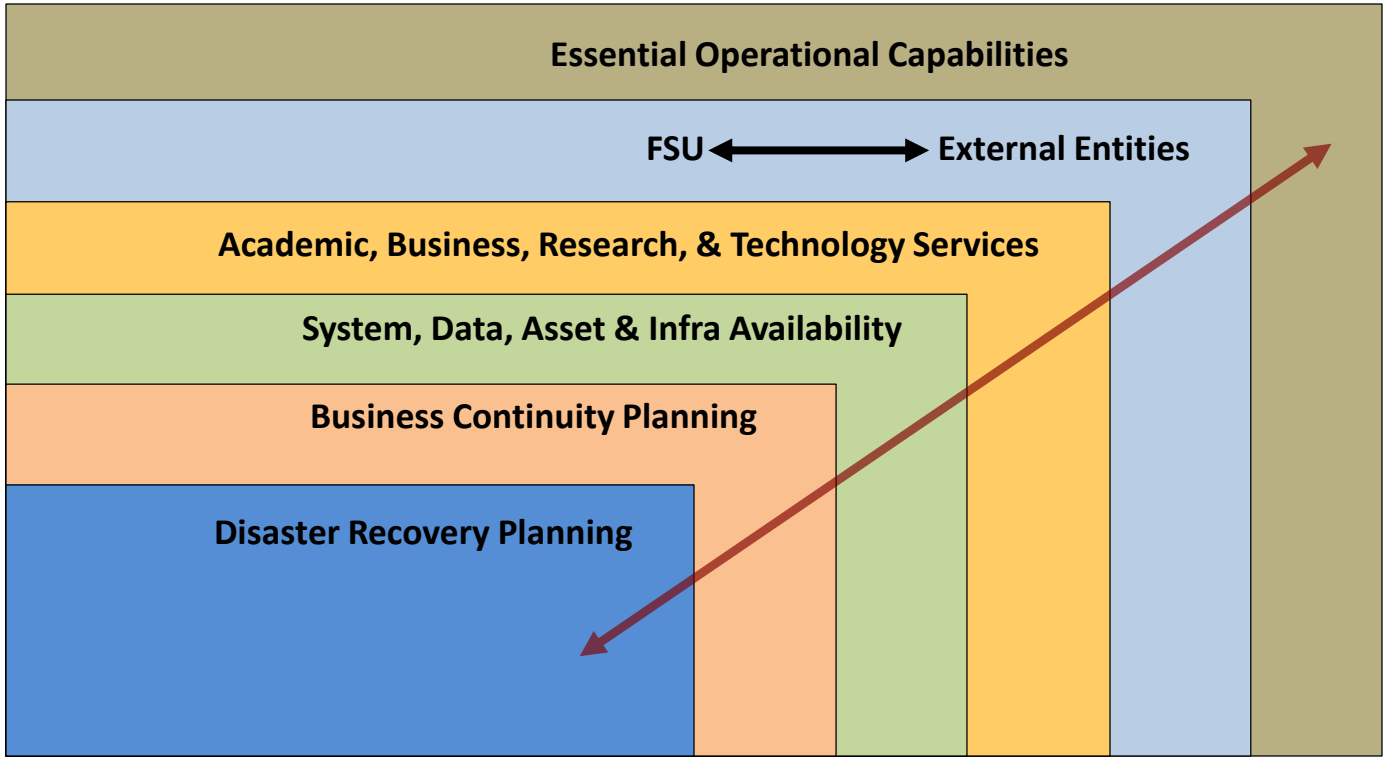
Departmental BC-DR Planning

- Form a planning team made up of business/academic and IT personnel. Identify the vital business processes that must remain operational.
- Identify & prioritize essential assets that need to be protected, recovered, or available in the event of a disaster.
  - Understand the impact of damaged facilities, assets and infrastructure, and system downtime on vital business functions.
  - Protect sensitive electronics and academic/research infrastructure. Determine whether extra insurance coverage is necessary.
- Determine system/asset Recovery Point & Recovery Time Objectives.
  - Understand who is responsible for preparation and recovery.
  - Include coordination, implementation, and communication tasks.
- The IT DR plan should be included as a component of the department's overall business continuity plan.
- Recommendation: Implement DR-BC planning as an ongoing lifecycle process rather than a one-time effort. Include required resources, risk assessment, plan development & update, testing, and maintenance.

How to Get Started

- Understand disaster-related risks to departmental infrastructure, facilities, and operations.
  - Shutdown non-essential systems to prep for an approaching disaster, e.g., a hurricane.
  - Understand whether facilities, or academic/research infrastructure must be protected during a disaster and what protections are required.
- Identify single points of failure that could affect department facilities, assets, and systems during a disaster.
- Plan for required backup power and perform preventive maintenance on generators, UPS, cooling systems, card key entry, etc.
  - Identify secure parking locations for department vehicles. Create checklists and schedules to ensure maintenance and prep tasks are completed.
- Develop a communications “call tree” for essential personnel required to take part in preparation, response or recovery.
  - Who is responsible for crisis communications? Will essential personnel be required to travel or work off-site? How will this be facilitated?
- Ensure that system backups are current, complete and available.

How to Get Started



Layered Planning Approach Helpful When Starting Out

Student, Faculty, and Staff Basics

- #1 Priority - Ensure Your Safety and Your Family's Safety!
  - Know evacuation routes and be alert for evacuation orders;
  - Monitor emergency.fsu.edu and alerts.fsu.edu; social media;
  - Install the SeminoleSAFE mobile app.
- Resident students follow the guidance of University Housing officials concerning evacuations or sheltering-in-place.
  - If leaving campus residence halls, advise University Housing of your plans.
- Off-campus students, faculty, and staff should prepare homes and apartments and protect personal belongings.
  - Inventory & photograph belongings; Secure potential windborne debris; ensure homeowner's or renter's insurance in place.
  - Raise electronics or other valuables off the floor; Shutdown sensitive equipment and computers if possible.
- Download the FSU Emergency Preparedness Guide
  - https://emergency.fsu.edu/sites/default/files/media/doc/FSUEmergencyPreparednessGuide1.pdf.

FEMA Online Training

FEMA provides comprehensive disaster recovery training materials, many of which are available at no cost. *A few of the core offerings are listed below.*

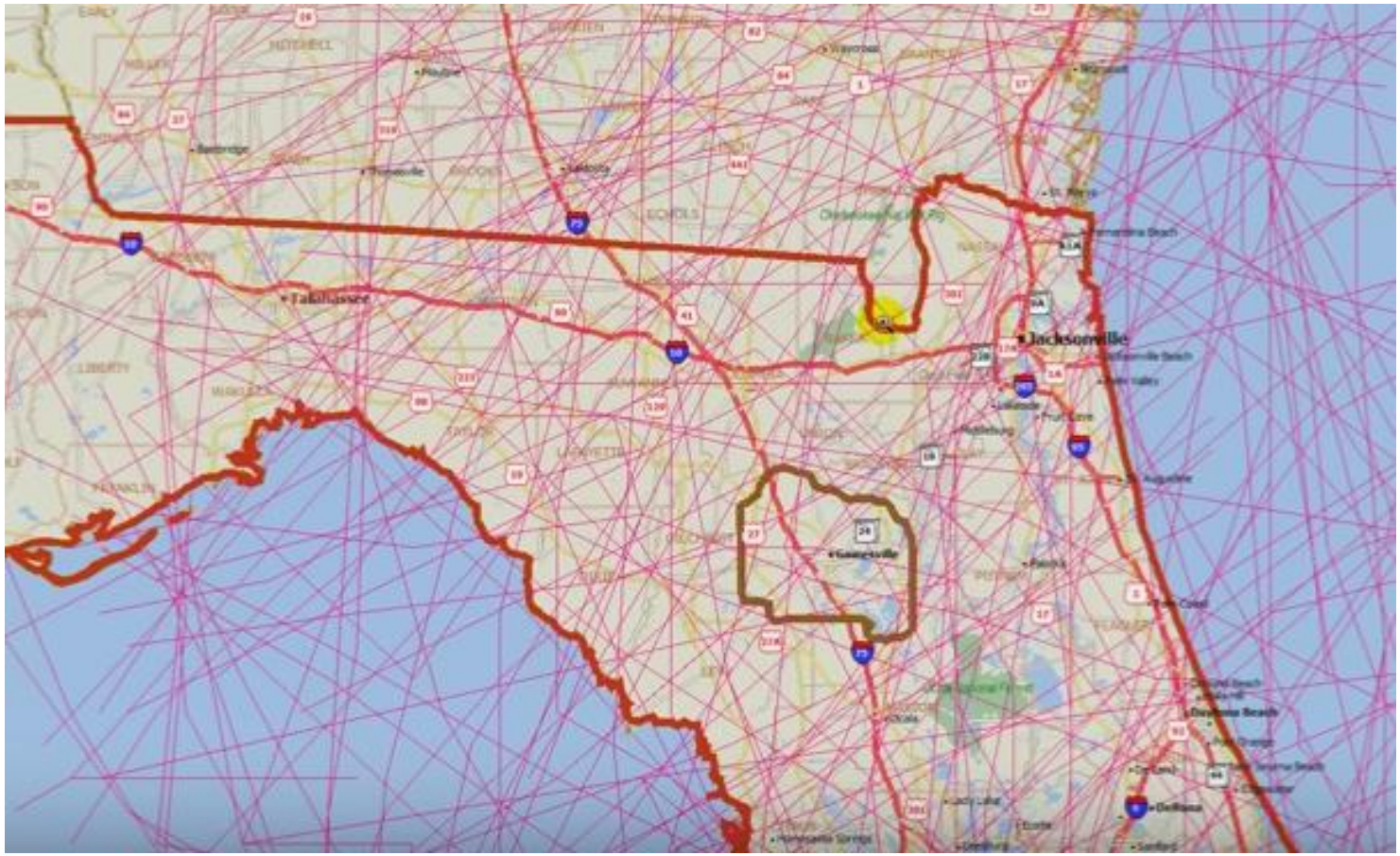
We recommend that Florida State University department BC & DR personnel complete the following online training courses as time allows.

- FEMA - Emergency Management Institute (EMI) Course | IS-700.A: National Incident Management System (NIMS) An Introduction
  https://training.fema.gov/is/courseoverview.aspx?code=IS-700.a
- FEMA - Emergency Management Institute (EMI) Course | IS-100.B: Introduction to Incident Command System, ICS-100
  https://training.fema.gov/is/courseoverview.aspx?code=IS-100.b
- FEMA – Continuity of Operations Awareness; Introduction to Continuity of Operations
  https://emilms.fema.gov/IS546.a/index.htm
  https://emilms.fema.gov/IS547A/index.htm

Next Steps

- Brief you Management on the need for an update DR-BC plan.
- Understand who is responsible for coordinating and implementing your department's disaster response.
- Develop business continuity and disaster recovery plans addressing departmental assets that need to be recovered or managed.
  - Practice Your Plan On At Least An Annual Basis!
- Understand the FSU CEMP and key university contacts responsible for disaster response.
- Complete the online FEMA training.

Hurricane Season June 1 – Nov 30th



Source: Thrall, Grant, Ph. D, Maptitude Software Map, http://www.caliper.com, June 2013.

Other Useful DR Resources

- Florida Division of Emergency Management
  - http://www.floridadisaster.org
  - http://www.floridadisaster.org/getaplan/family.aspx Get a Plan!
- NIST Computer Security Resource Center
  - http://csrc.nist.gov/publications/PubsSPs.html
- NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems
  - http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- NIST SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
  - http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

Contact Information

Joseph Brigham

ITS Disaster Recovery Program Coordinator

joseph.brigham@fsu.edu

(850)645-3601

Bill Hunkapiller

Director, Information Security and Privacy Office

bill.hunkapiller@fsu.edu

(850)645-0676