System Business Continuity Classification

	Criticality Levels				
	Core Infrastructure	**Critical**	**High**	**Medium**	**Low**
Business Continuity Procedures					
Information System Contingency Plan (ISCP)	Required	Required	Required	Not required	Not required
Business Impact Analysis (BIA)	Included in ISCP	Included in ISCP	Included in ISCP	Required	Not required, but suggested to complete
System Recovery Procedures (SRP)	Included in ISCP	Included in ISCP	Included in ISCP	Not required, but suggested to complete	Not required, but suggested to complete
Business Continuity Methods					
System Availability	High Availability	High Availability	High Availability	Recoverable	Reliable
Maximum Downtime	<2 hours	<4 hours	<24 hours	<72 hours	>72 hours
Data Recovery Strategy	Continuous backup	Continuous backup	Continuous backup	Incremental or differential between full backups	Incremental or differential between full backups
Testing					
Documentation Review	Semiannual	Semiannual	Annual	Biennial	Biennial
Walkthrough	Semiannual	Annual	Annual	Biennial	Biennial
Simulation	Annual	Annual	Biennial	Biennial	Not Required
Parallel	Not required, but suggested to complete annually	Not required, but suggested to complete annually	Not required, but suggested to complete biennially	Not required, but suggested to complete biennially	Not required
Interruption	Not required, but suggested to complete annually	Not required, but suggested to complete annually	Not required, but suggested to complete biennially	Not required	Not required

Criticality Levels

Criticality levels are determined by the service owner and are used to classify the criticalness of an IT system* to a business process. The level selected defines the necessary business continuity procedures, methods, and testing requirements.

- **Core Infrastructure:** IT systems that must be functioning and are considered core components, which will need to be operational before other dependent systems can perform as they are intended. Examples of core systems include, but are not limited to; electricity, the data network, network services such as DNS and DHCP, and various authentication systems such as Active Directory. Immediate recovery is required to prevent substantial interruption of University operations. Systems should have a maximum downtime of 2 hours or less.

- **Critical:** IT systems which are essential to support University business operations. Loss or failure of these systems will have an extreme impact on business operations. Systems should have a maximum downtime of 4 hours or less.

- **High**: IT systems which are crucial to support primary University business operations. Loss or failure of these systems will have a significant impact on business operations. Systems should have a maximum downtime of 24 hours or less.

- **Medium:** IT systems which are important to University business operations. Loss or failure of these systems will have a modest impact on business operations. Systems should have a maximum downtime of 72 hours or less.

- **Low:** IT systems which improve the effectiveness or efficiency of University operations. An extensive loss or failure of these systems will have a negligible impact on business operations.

**An IT system is a hardware or virtual computing environment that is installed or configured to provide, share, store, or process information for multiple users or, that communicates with other systems to transmit data or process transactions.*

Business Continuity Procedures

Three different services are offered to properly document and outline business continuity procedures. Each of these define different procedures and requirements necessary to properly restore an IT system.

- **Information System Contingency Plan (ISCP)**
  - An ISCP provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing procedures of a system.

- **Business Impact Analysis (BIA)***
  - The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system was unavailable.

- **System Recovery Procedures (SRP)***
  - System recovery procedures (SRP) provide general procedures for the recovery of a system from backup media or other sources.

*Included as a part of the ISCP.

Business Continuity Methods

Business Continuity Methods define the system availability and data recovery strategies.

System Availability:

- **Continuous Availability:** A system that is created with a goal of no scheduled or unscheduled downtime. Continuous availability systems can only be reliant upon other systems that are unremitting. Alternate facilities, not physically located within the same building, will be used to ensure that no local disruptions interfere with the system's continuous availability. Real time synchronization between the sites is used to route data to both the primary site and the alternate facility(ies). Continuously available systems consist of hardware and software designed to protect against component and system-level failures at any point in time, with an understanding that the system will always be active.

- **High Availability:** A system that can quickly recover from a failure by way of automation built into the system. There may be a small amount of downtime while one system switches over to another, but processing will continue. There should be a goal of no unscheduled outages or downtimes. High availability systems can only be reliant on unremitting

systems or other systems that have no lower availability than high. Alternate facilities, not physically located within the same building, will be used to ensure that no local disruptions interfere with the system's high availability. Near real time synchronization between the two sites is used to mirror the data environment of the original site. The alternate site will have hardware and system resource components; networking equipment with an active connection; and the resources needed to recover the business processes impacted by the system disruption.

- **Recoverable:** Redundant infrastructure components, such as web and file servers, which have data replication. The facility will have backups on hand, but they may not be current or could be incomplete. A full backup should be done first with either an incremental or differential backup completed on a set schedule. The system will recover by manual intervention which will cause some downtime as tolerable. An alternate facility (possibly smaller in scale) with the equipment and resources to recover the business functions affected by the occurrence of a disaster may be used.

- **Reliable:** Non-redundant components that have no protection or hot-swappable hardware. IT staff will restore them eventually after major failure, but the business does not depend on them. System will have backups, but they may not be current or could be incomplete. An alternate facility would not be needed in this instance.

Data Recovery Strategies:

- **Continuous backup:** Backup of computer data by automatically saving a copy of every change made to that data in real time or near real time. It allows for the data to be restored at any point in time. The data will be located in different physical locations to ensure data availability in the event of a disruption.

- **Full backup:** A backup in which all of a defined set of data objects are copied, regardless of whether they have been modified since the last backup.

- **Incremental backup:** An incremental backup stores all files that have changed since the last full, differential or incremental backup.

- **Differential backup:** A backup in which data objects modified since the last full backup or incremental backup are copied.

Testing and Exercises

The purpose of testing is to confirm the business continuity solution satisfies the organization's recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors.

- **Documentation Review:** Staff will individually review the plan for accuracy and completeness and ensure supporting documentation for critical systems is up to date. Business continuity documentation should be reviewed in conjunction with system changes and updated if necessary.

- **Walkthrough:** Staff walkthrough the plan as a group, discussing each step along the way.

- **Simulation:** Staff members perform a walkthrough in the context of a simulated disaster that includes periodic announcements of events as they occur. Staff do not actually perform any recovery steps.

- **Parallel:** Staff members perform actual recovery steps to move business processes to alternate locations. Staff build or activate recovery servers while primary servers are also still working. Primary everyday business processes should continue uninterrupted.

- **Interruption (complete rehearsal):** The business stops performing critical business processes, as though an actual disaster has occurred. Staff members carry out business operations according to the interim plan.

Minor issues identified in the initial testing phase may be documented and retested during the next test cycle. Significant complications, such as a lack of appropriate technologies needed to meet the maximum tolerable downtime or system recovery efforts, should be addressed and reexamined immediately.

References:

- *NIST 800-34 Contingency Planning Guide for IT Systems*
- *The BS 25999 series will include two standards, as follows:*
  - BS 25999-1:2006 Code of Practice for BCM
  - BS 25999-2:2006 A Specification for BCM.
- *NFOA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs*
- *ISO/IEC FDIS 27031: Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity*