ECM CPO Glossary of Acronyms / Terms – *03/06/2006*

ECM CPO and LDRPS Acronyms / Terms

Acronym / Term	Translation	Detail
ECM CPO	Enterprise Continuity Management Central Program Office	OSU's office for university-wide continuity management planning
Continuity Management		The processes, procedures, activities, and decisions employed to ensure that an organization can continue to function through an operational interruption.*
LDRPS	Living Disaster Recovery Planning System	The Software BCP / DR planning tool used by the ECM CPO.
Phase I		The creation / population of contact data and response tasks to allow for an immediate response to an incident. Output = SEM plan.
Phase II		The identification of critical business processes and thorough plan(s) to support the continuity of these processes in the event of an incident. Done in conjunction with a BIA. Output = BCP plan -- or -- DR plan.
Phase III		Current = 1. The identification and documentation of all assets required to support the critical business processes (at least at a minimal level of functionality). 2. An assessment of risks and identification of possible mitigation strategies. Output = Asset reports and Risk Analysis (RA) Future = Examines the relationship and interdependencies between many plans and processes, including a university-wide analysis for recovery time objectives (RTOs) and single points of failure. Output = Enterprise-wide reports and action items
"Phase IV"		The discussion, creation, and execution of an exercise or exercises to evaluate the plan and identify weaknesses for augmentation.
Ongoing Maintenance Phase		After the initial creation of all necessary plans, the department updates and maintains the plans indefinitely. The ECM CPO will be available for consultations and exercises.
SEM (plan)	Site Emergency Management (plan)	The first plan you will develop in LDRPS. It focuses on your department's / unit's immediate response to an incident.
BCP (plan)	Business Continuity Planning (plan)	The second plan(s) you will develop in LDRPS. It focuses on maintaining your department's critical processes in the event of an incident.
DR (plan)	Disaster Recovery (plan)	Plans(s) focused on IT recovery of data following an incident.

* Source: All Hands Community – Glossary Of Terms and Definitions Second Edition: http://all-hands.net/pn//modules/Downloads/store_folder/REM/Glossaries/ahc_glossary.pdf

Plan Roles		• **Plan Owner:** Person(s) ultimately responsible for the authorization of the content of the plan. • **Plan Manager:** Primary person(s) responsible for the creation and on-going maintenance of the plan. • **Alternate Plan Manager:** Alternate person(s) responsible for the creation and on-going maintenance of the plan. • **Auditor:** Person authorized to review all plans. • **Reviewer:** Person authorized to review certain plans.
Internal Key Contact		Individual (named) staff and faculty within OSU (inside and outside of your department) who may need to be notified by your department in case of an incident.
External Key Contact		Organizations and agencies inside or outside of OSU who may need to be notified or who may be required to provide assistance in case of an incident. These organizations typically are not paid directly by you for their services. Examples: Essential services (police, fire, hospitals), government agencies, customers, OSU Services (OSU Physical Facilities, OSU EHS, UNITS).
Vendor		Organizations or companies who provide services for a fee. Examples: IBM, DELL, GUDENKAUF, AEP.
EOC	Emergency Operations Center	The location where the department's decision-makers will meet and work to address the incident. Also known as Emergency Command Center (ECC).

General Acronyms / Terms

Incident		Usually a minor event or condition that is a result of a human error, technical failure, or environmental condition. An incident or event typically interrupts normal activities. Note incidents may or may not lead to accidents, events, or disasters.*
BCP	Business Continuity Planning	A BCP defines and ranks key business functions according to vulnerability and risk, assigns priorities to those functions, and defines procedures to continue priority functions to ensure [business] continuation… in the event of a disaster. A responsive BCP depends on an adequate Business Impact Analysis (BIA) and Risk Assessment (RA). Computer systems and data recovery [are…] a subordinate but important part of a BCP. A BCP includes safeguards for personnel and families, business assets and reputation, customers/clients/citizens, vendors, communications and access to critical resources. It involves training, periodic exercises, post-exercise reviews, and plan updates with special attention to media relations.*
DR	Disaster Recovery	Plan(s) to recover Information Technology (IT) data following an incident.
BIA	Business Impact Analysis	A process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives.†

† Source: Disaster Recovery Journal & Disaster Recovery Institute International *Business Continuity Glossary*: http://www.drii.org/associations/1311/files/glossary.pdf

RA	Risk Analysis	Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.†
RTO	Recovery Time Objective	The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. Similar term: Maximum Allowable Downtime.†
RPO	Recovery Point Objective	The point in time to which systems and data must be recovered after an outage. (e.g., end of previous day's processing). RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered.
ICS	Incident Command System	A management system designed to integrate resources from numerous organizations into a single response structure using common terminology and processes. The National Incident Management System (NIMS) establishes ICS as a standard organization with incident management activities organized in five functions: command, operations, planning, logistics, and finance/administration, for management of all major incidents.*
Cold Site		An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold-sites have many variations…*
Hot Site		An alternative data and office center equipped with IT, telecommunications and office systems ready to house companies or agencies, private or public, whose facilities are affected… Hot sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication)… Similar terms: Backup Site; Recovery Site; Recovery Center, Alternate Processing Site.*
Warm Site		An alternate processing site which is only partially equipped, as compared to hot site which is fully equipped.* May have physical, IT, and/or telecommunications systems, but will not be pre-configured for the needs of the customer (affected organization).

LDRPS Unique Identifier Conventions

Unique Identifier	Example	Convention
Task ID	NWKDAMHVC00010	Prefix/Team/Task/No. = 14 chars
External Key Contact ID	CSNWKPD0000010	"CS"/Name/No. = 14 chars
Vendor ID	VENSTRHL000010	"VEN"/Name/No. = 14 chars