# Frequently Asked Questions

## 1) Is University of Illinois *Ready* an Emergency Response Tool?

**University of Illinois *Ready*** does not produce an emergency response plan, often called an Emergency Operations Plan. These are campus-level plans, already in place at UIC, that focus on preserving life, health, and property. Continuity planning aims to keep the institution operating (doing what we normally do) by focusing on the mission.

## 2) Does University of Illinois *Ready* Produce Step-by-Step Recovery Plans?

**University of Illinois *Ready*** is designed on the premise that post-disaster conditions are so variable that step-by-step "recovery" plans are seldom useful. Experience shows that, when faced with crisis, leaders (1) analyze then (2) act. Only in certain situations do they "read the plan" before acting. **University of Illinois *Ready*** stores information that might aid a leader's decision-process (such as a prioritized list of critical functions), or aid implementation (such as contact information to reach vendors). But the tool's primary thrust is to identify and track action items that, if completed in advance of disaster, will position the department and the campus to more easily keep operating.

For example, an HR department might create an action item to "maintain a stock of paper forms to conduct personnel actions during periods of system failure". If it follows through and completes that action item, it will be positioned to continue doing hiring, layoff, pay actions, etc. during times of crisis, using workaround processes despite the loss of its IT system. HR leaders probably don't need help deciding WHEN to invoke these processes or WHICH processes to invoke - that will depend on the circumstances - but they MUST have the paper forms available to make the alternate processes possible.

There certainly are some departments and situations where step-by-step instructions, decision trees, and other aids are essential or at least useful, and **University of Illinois *Ready*** offers the capability to upload these as attached documents - but the **University of Illinois *Ready*** questionnaire does not walk the user through their creation.

## 3) Does University of Illinois *Ready* Do Risk Assessment?

Risk assessment is typically done at the institution level, and **University of Illinois *Ready*** is a departmentally-focused tool. However, in August 2010 UIC conducted a robust and comprehensive risk assessment process at the campus level which assessed the operation, utility, and physical risks; analyzed risks by unit, department, and location; reviewed risk mitigation strategies for risks that can be mitigated; and developed risk reduction strategies for risks that cannot be fully mitigated. Overall, the results of the assessment have been very useful to the **University of Illinois *Ready*** campus community. (The more one knows of the relative risks, the more effectively one can focus and prioritize.) However, the absence of an institutional risk assessment is not a show-stopper. **University of Illinois *Ready*** is an all-hazards tool, designed to prepare the institution to face any type of risk.

## 4) How Does This Relate to Disaster Recovery Planning?

Disaster Recovery planning, commonly called DR, is a specialized subset of continuity planning. Its aim is to position the IT organization to rapidly recover from disruptions to its applications, infrastructure, and other services (or better, to continue without disruption).

The campus IT Division can benefit from using the **University of Illinois *Ready*** tool in the same fashion as other campus departments; but the tool does not walk the IT Division through the steps needed to create the various elements of the "DR plan" (prioritized lists of applications & servers, detailed information about data center operations, detailed startup/recovery procedures that can require hundreds of pages). Other tools are available for DR planning

### 5) Who should do continuity planning?

All administrative units, support units, colleges, schools, departments, research units, and other units that conduct teaching, research, public service, or patient care should have a continuity plan. Other units that provide essential support or infrastructure to these units should also do continuity planning. These two definitions encompass virtually every unit of the campus.

### 6) Should we appoint a departmental continuity coordinator?

Yes: typically a staff member who has access to your senior management. The role is part project manager, part group facilitator. It is a temporary, part-time assignment for the duration of the planning project, but the coordinator often continues informally as the departmental expert and contact person for continuity issues.

### 7) How long does it take to create a continuity plan?

Most of the time will be "white space" waiting for meetings to happen and people to come to agreements on priorities and action items. The number of actual staff hours required is surprising small, because **University of Illinois *Ready*** uses a "fill in the blanks" process. Virtually no time is spent learning how to do a continuity plan -- simply fill in the blanks and your plan is done.

### 8) How detailed & complete does our plan need to be?

Your continuity plan can never be "complete" because you can't know what disaster you're planning for. The **University of Illinois *Ready*** tool will prompt you for the appropriate level of detail, and most of those details will be things that your group easily knows or can figure out.

### 9) What assumptions can we make about what the campus will do for us after a disaster?

**Access to buildings**. If campus officials have reason to suspect that a building is hazardous to enter, they will immediately close the building and call in trained inspectors. In the worst case, the inspection process alone could take weeks, with hazmat cleanup and repairs taking much longer. You may be unable to enter your building for an extended period of time.

**Computing infrastructure**. Restoration of our many centrally supported ACCC or AITS applications are a high priority after any disruption. This includes email, internet, banner, payroll, and many other applications, as well as the physical campus data network. Much money and effort continues to be spent on hardening our IT systems to minimize damage and aid quick recovery. Definite predictions, of course, are not possible. Within your unit, you should be taking steps to backup data and make plans for recovering your own servers and applications.

**Communication protocol**. General communications with students, faculty, staff and the public will be handled by the Office of Public Affairs, and will be tightly managed so that messages are consistent. As your unit resumes functioning, communications of an operational nature will be your responsibility.

**Contacting your staff**. This will be a departmental responsibility. Each school or department should keep its own emergency contact lists.

**Care of staff**. Many staff issues arise during disaster recovery: pay, temporary leave, temporary alterations of assignment, safety, benefits, layoffs, work-at-home, stress, and family issues. You should assume that central Human Resources will be available with guidance and mechanisms to assist departments in these complex areas. Conversely, departments should seek guidance from central HR when uncertain how to act in these matters-both before a disaster and after it.

**Temporary staffing**. Mechanisms will be available (operated by central HR) for hiring temporary staff and for redeploying existing staff. Available staff who are less critical to your operation may be redeployed elsewhere.

**Course scheduling and classroom assignment**. In emergency conditions, courses will be accordingly prioritized by department chairs in collaboration with the Office of the Provost and Vice Chancellor for Academic Affairs. Departmentally controlled classrooms may revert to the Chancellor's control.

### 10) What help and money can we expect from state and federal governments?

Outside assistance for disaster recovery can be expected from both state and federal governments, but it is impossible to say before any disaster exactly what form it will take. It is important to know that the federal government never ADVANCES funds to institutions like ours for disaster recovery. Reimbursement is the path, and it is always a long one. UIC will be eligible for reimbursement for many repair and reconstruction costs, but it will take years of negotiating with the state and federal governments. Many real losses may not be reimbursed. So the more capable we are, individually and collectively, of taking care of ourselves, the better off we will be.

### 11) How can we craft a plan to handle unknown circumstances?

The methodology that we employ for continuity planning mostly avoids discussion of particular major adverse events that could interrupt our mission. All such adverse events (fire, pandemic, human sabotage, etc.) will affect our functioning in similar ways: they will temporarily prevent us from using some of the resources to which we have become accustomed.

These resources include:

- space (our classrooms, labs and offices);
- people (our staff);
- equipment (computers, networks, other equipment);
- information (libraries, data);
- funds (our income stream).

Our planning focuses on:

- identifying the resources that are critical;
- safeguarding critical resources against loss (e.g., backup of systems & data, bracing of equipment, safe storage of research items);
- actions that will lessen the impact of losses (e.g., pre-arrangements with UIUS and UIS campuses for mutual aid);
- replacing resources quickly (e.g., contracts with vendors);
- performing critical functions without some of those resources (e.g., teaching via distance learning technology);
- providing our people with the information they will need, post-disaster, to get the campus back in action.

At best, a continuity plan is not a step-by-step cookbook, but rather a jumping-off point for ingenuity.

## 12) What is OpenVPN?

The Virtual Private Network (VPN) client/gateway is used to encrypt data destined for UIC while it travels over the Internet. ACCC has installed a VPN gateway for use of UIC faculty, staff and students that need secure access to resources at UIC over a non-UIC Internet connection.

While connected to the VPN gateway, the client software works with the operating system to determine when you are accessing an Internet location that the client should protect. When you are accessing such a location, the VPN client encrypts the data and sends it to ACCC's VPN gateway. As your information is flowing across the Internet to reach UIC, it is securely encrypted and is only decrypted once it reaches the VPN gateway.

For example, if you are at home and have started the VPN client to connect to the gateway (this is technically referred to as a tunnel) and use your Web browser to visit www.uic.edu, the portions of the connection that are encrypted are:

- The Web browser request to browse www.uic.edu until it reaches the VPN gateway.
- The Web page results from www.uic.edu after they are passed through the VPN gateway.

The web browser request from the VPN gateway to www.uic.edu and the reply from www.uic.edu to the VPN gateway would not be encrypted.