kuali

A Thorough Guide to

Continuity Planning in Higher Education

Table of Contents

Chapter One:
Identifying Risks

Continuity planning is not about stopping bad things from happening. Rather, it is the knowledge that your organization will face unexpected risks, and taking the correct steps to prepare for those risks.

Continuity planning is all about building a culture of resilience. That is, the “ability to recover from or adjust easily to misfortune or change.” When your organization is resilient, it is better able to continue beyond any kind of adversity it could face.

Identifying and Mitigating Risks

When it comes to higher education, the risks are more diverse than those commonly faced by businesses and other organizations. Where most businesses are concerned with continuing business functions that affect the bottom line, there are often significantly more moving parts in institutions of higher education. Not only do you have to figure out how to minimize impact on instruction, but you also have to have plans in place for continuing education, protecting both employees and students, and saving important research initiatives.

> **Resilience**
>
> **re·sil·ience | \ ri-’zil-yən(t)s**
>
> 1. the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress
> 2. an ability to recover from or adjust easily to misfortune or change
>
> Merriam-Webster

Potential Risks

A significant part of preparing for future adversity is making oneself aware of the various risks that an institution could face. By considering all possibilities, and the various threats and effects associated with each one, it becomes easier to take the necessary steps to prepare. Risks differ by institution based on the region or location of the campus, whether it is a research institution, and many other considerations. Here are some examples:

Hazardous chemical spill

- Damage to facilities/equipment
- Temporary building closure
- Evacuation
- Threat to human safety

Plumbing issues/water leaks

- Damage to facilities/equipment
- Temporary building closure
- Potential loss of data
- Threat to human safety

Cybersecurity threats

- Effects on communication
- Security threat
- Threat to finances
- Potential loss of data

Power outage

- Effects on communication
- Security threat
- Potential loss of data

Infectious disease outbreak

- Temporary campus closure
- Evacuation
- Threat to human safety

Natural disaster (fire, hurricane, tornado, flood, etc.)

- Temporary building/campus closure
- Damage to facilities/equipment
- Evacuation
- Threat to human safety
- Potential loss of data

Closing due to inclement weather

- Temporary campus closure

Active shooter

- Evacuation
- Threat to human safety

Suspicious mail

- Evacuation
- Threat to human safety

One of the main principles of emergency planning is that you simply cannot predict every catastrophic event. If you try to, you run the risk of bogging down your preparation with endless “what if” scenarios.

Resource

A Guide to Continuity Planning Basics: Analyzing the Criticality of Functions and Applications

However while considering the aforementioned risks, and the effects that are associated with each of them, you are able to use those as starting points for identifying and protecting essential functions. In doing so, you are then able to take steps towards mitigating certain risks, and their effects, and in some cases eliminate them altogether.

Solution

Kuali Ready helps you to prepare for all emergency situations through simple question-based forms, robust reporting, and a unified dashboard to manage everything.

Chapter Two:
Mitigating or Eliminating Risks

Now that you have considered some of the potential risks facing your institution, you may be feeling as though you are looking in a million different directions at once, unsure where to start and which risks to deal with first.

The good news is that you do not have to address every risk in isolation. As mentioned before, it is impossible to identify every single risk that you may face in the near or distant future. However, we are now able to look at the potential risks listed in chapter one, and establish patterns in how they will affect operations.

Chapter Two: Mitigating or Eliminating Risks

Using the Kuali Ready methodology, we are able to simplify the problem through sorting the effects of various risks into four important elements:

1. **Loss of essential employee(s)**
2. **Loss of a normal work location**
3. **Loss of critical applications**
4. **Loss of unique resource e.g. specialized equipment**

Doesn't that seem more manageable? Now that we are aware of the four main effects that most disasters will have, we can take a sample event, and determine which effects they will have.

Example Event: The Burst Pipe

Let's walk through one example of a potential event and how you would go about addressing it in your continuity plan.

Element One: Essential Employees

While you might not initially think of something as seemingly harmless as a burst pipe or water leak as being dangerous, there are potential threats to human safety when that water is mixed with technology. As such, considerations in this area are:

- Does the building have an evacuation plan?
- Are students, faculty, and staff all aware of the dangers of such things as standing water, and the need to avoid it? Are they familiar with the protocol of a building evacuation?
- Do you have plans in place for work to continue should any essential personnel be harmed and thus away from work for any period of time?

Element Two: Normal Work Location

This kind of event can shut down anything from a single room to an entire building. Questions to address are:

- What plans are in place to move everyday functions from the normal work location to an alternate location?
- Are there provisions for both short term continuity (immediate relocation of operations) and long term continuity (will the short term solution still work if the building is shut down for weeks or months)?

Element Three: Critical Functions and Applications

Having already identified critical functions and applications, as mentioned in chapter one, you can now assess how they could be affected by this specific type of event. This is the area where most continuity plans are focused — those daily functions that contribute to the institution's main service offerings — the hint is in the word "critical." They typically include things such as instruction, research, residential, food service, and business functions. Questions to consider:

- Are there provisions in place for continuing instruction, even with the loss of elements one or two?
- Is all research secure and backed up regularly?
- If the building affected provides food service, are there other places or plans in place to provide food for those who rely on it? For example, students with meal plans for one provider that is now closed.
- Are there plans in place for new living arrangements, should on-campus housing be affected?
- Should there be a power outage or something that affects regular communication channels, are there plans in place for a different way to communicate?

Element Four: Unique Resources

When an organization has unique resources such as specialized equipment, damage to or loss of them can be a huge blow. These kinds of unique resources may be specialized lab equipment and musical instruments. As such, here are things to consider in this area:

- Is this kind of situation covered in an insurance policy?
- How long will it take to replace unique resources and what will the impact be on instruction and research?
- Do we have an alternate vendor for this resource in the event our vendor can not provide the resource?
- What will the costs be if these resources are damaged or lost permanently, and how can you minimize that cost?
- How will we function without the resource?

Resource

Building Organizational Resilience in Higher Education

Building Resilience

No two crises occur in the exact same way, with the exact same effects. That is why building up a culture of organizational resilience should always be the main priority. When you have worked to protect every essential resource and function with a plan to recover after any situation, you contribute to the overall resilience of your organization, and can truly be prepared for anything

Solution

Kuali Ready provides a dashboard to collect relevant information from each department and store it in one secure place.

Chapter Three:
Getting Buy-In from Leadership

When building a continuity program, it is critically important that you have leadership support for completing and funding the different continuity activities that will ultimately create a more resilient and recoverable institution.

In this chapter, we will look at the main steps toward doing just that.

Chapter Three: Getting Buy-In from Leadership

After the events of 2020, few people need convincing that continuity planning is valuable. However, you will still need to present your plan to executives to ensure the continuity program has support. The goal is to get buy-in from the entire institution. If leadership supports the program, it will be much easier to get others to participate.

1. Demonstrate the "why"

The first step in obtaining support for building a continuity program is identifying what executives wish to protect. What is the mission of your institution? Is it teaching? Is it research? Document the services that are being provided.

Action Items

- Document the 'mission' of the institution and include the services provided. These generally are revenue-bearing activities such as instruction, research, clinical, retail, food service, and so on.
- Ask leadership why it is important, to them individually, for these to be protected.
- Use the Kuali Higher Ed Continuity Planning Self-Assessment to demonstrate areas in your organization where attention is needed.

Did you know?

In 2019, New York City-based Monroe College was hit with a ransomware attack, in which hackers demanded $2 million in bitcoin.

New York Daily News

2. Discuss specific risks that the institution faces

After you have completed the action items in step one, which demonstrate the why, you will then need to illustrate how a continuity program will help the institution — before, during, and after an event. You will do this through collecting solid data that will illustrate the benefits in a specific way.

Action Items

- Provide data on the benefits of continuity planning.
- Outline potential risks identified in your risk assessment. Include data on the likelihood and impact of any of these occurring, as well as associated costs of not performing the mission-critical services.

- Emphasize that preparing for adverse events will increase recoverability of the institution, and thus reduce the costs of downtime.
- Include the return on investment (ROI) data associated with preventing the aforementioned costs.
- Consider ways in which it will protect the institution's brand or image, and how that can also have monetary value.
- Include the less tangible — but no less important — benefit of providing peace of mind to employees and students.

3. Present a plan

Once you've collected the data and formulated your plan, present it to the executives for approval and support. A good place to begin is with the division leaders at the VP level. A VP of Finance is especially interested in reducing risks to the financial stability of the institution, but other division leaders are interested in protecting the services provided by their individual division as well. For example, the Provost has an explicit interest in ensuring that instruction is protected and can continue following an adverse event. Presenting to a group of executives is not only efficient but generally proves to be the most effective way to gain leadership buy-in. With the proper preparation, your chances of getting the needed support will be greater.

Action Items

- Provide a plan that is simple and cost effective. The plan should include a roadmap from the current to the future state of resilience.
- Include the high-level gaps that may reduce the institution's ability to recover from any of the potential risks.
- Include specific objectives — for each one, identify how much funding and resources you will need, as well as other support.
- Show the benefits with specific examples and projections for ROI.
- When presenting the plan, be clear of what your 'asks' are at each stage of the roadmap. Do you need extra staff (will an intern be sufficient during the early stages); will you be much more efficient if you incorporate a Continuity Planning tool, such as Kuali Ready; what level of top-down support do you need to ensure all levels of the organization participates?

- Following the plan presentation, be sure to gain a commitment. Otherwise, agree to discuss the need for continuity planning further, until you have a full understanding of how leadership wants to move forward.

Resource

You can find a number of successful case studies at Kuali.co/resources under the “Ready” tab.

4. Reiterate the importance of executive-level involvement

Executive involvement should not be limited to just funding and approval; continuous executive involvement will benefit the continuity efforts greatly. This is especially true at the beginning of the process, as cooperation is needed from multiple personnel across multiple departments, but the benefits extend into future reporting and program adjustments.

Keeping executives informed will not only help to keep their interest and support throughout the continuity lifecycle, but will also be helpful when extra funding is needed. The next chapter will go into this in more detail.

Chapter Four:
The All-Hands Approach

Building a robust continuity program requires participation from all levels throughout the institution; this is no more evident than when you are building a continuity program for higher education.

Because institutions of higher education are so multi-faceted, a complete plan requires involvement that stretches not only from the top down, but across various departments — each of which comes with its own unique ecosystem of people to consider and risks to manage.

Considerations Across Departments

When writing continuity plans no one person can build a plan alone. Input from others is not only helpful, but necessary. Because no one person, or even team, is familiar with all aspects of the institution, it is imperative that all departments and personnel at all levels participate in the continuity planning activities. Therefore, when identifying risks there needs to be input from IT, Facilities, Public Safety, HR, and many other departments. You will need a department head to lead the efforts for each department plan, and perhaps even a specialist or division leader who can help identify the various critical functions, resources, and other considerations they would require for a recovery effort.

Because knowledge that is needed for the program lifecycle is spread across the institution, it is important to involve staff and faculty from the start. But because people are busy and may not initially see the importance of continuity planning, you'll want to be creative in soliciting their participation. Here are some ways to build resilience and recoverability, as a culture, across your campus(es).

- Conduct business continuity campaigns
  - Email and poster campaigns, with slogans such as 'BC is Coming to the University" and "How Prepared is your Department?"
  - BCP 101 "Lunch and Learns" to educate those who are not familiar with continuity planning
- Gamification
  - Make it fun with creative games and other ways to encourage competition
- Use advocates
  - Find continuity "champions" and reward them, encouraging more people to talk about its value
- Start at the top — work with execs to gain support
  - Provide frequent updates
  - Provide meaningful metrics i.e. how resilient/recoverable are we?
  - Use real-life examples every chance you get e.g. wildfires and power outages
- Be a consultant, not a salesperson

- Educate yourself before you begin. Here are some great resources to get you started: www.DRJ.com, www.continuityinsights.com, www.thebci.org
- Be able to articulate why we are doing BC

- Practice what you preach
  - Complete the individual projects for your department first and lead by example

Solution

Kuali Ready connects people virtually to efficiently utilize everyone's expertise, and includes a database of all of the institution's applications, buildings, and other elements that may be needed for various different department plans to make things easier for each department head.

Executive Reporting

As you build your continuity program it is important to regularly report the status of your program and the progress that you have made. This is imperative for several reasons:

- Ensures continuous program support
- Portrays a point-in-time picture of resiliency
- Identifies areas of non-participation
- Gains buy-in for upcoming projects
- Provides data for board reporting
- Provides a status of ROI and helps to secure additional funding, as needed

So, as you assess your institution's resiliency — whether that be through the Kuali Self Assessment tool or other means — you will need help from people across every department, as well as leadership.

Program Maintenance

Simply building a continuity plan does not make an institution, or even a department resilient or recoverable. Continuity is simply not something you can throw together and forget about. Each element of the program should be reviewed and updated at some frequency. Here are some guidelines:

Risk Assessment

Update every three years or as hazards present themselves. Several years ago, we could not have imagined an event that would destroy the World Trade Center and cause a ripple effect across the United States. We had to rethink our continuity processes. And even though the world has dealt with epidemics and pandemics throughout history, did we ever consider in our planning that one could impact the entire world to the point of shut down, for many months? What we know and plan for today will not be the same in the future; we must keep thinking forward.

Impact Analysis

Update every three years or as you encounter changes to institutional processes. The impact analysis provides criticality data for functions and the applications used to carry out those functions. As your institutional offerings change and technology advances, the functions and tools you use change and advance as well. It is important to keep the data — especially as it relates to technology — current so that when you face an adverse event, first recovery efforts can focus on the most critical functions. While the data should be updated as changes occur, best practices suggest a complete impact analysis refresh every three years.

Continuity Plans

Critical 1 and 2 plans, your most critical plans, should be updated every six months, while critical 3, plans of lesser priority, and deferrable plans should be updated on an annual basis. Changes in higher ed occur constantly: departmental functions change, stop, or sometimes transfer to another department or division; people retire or change roles; applications or other resources are replaced or retired. To be most recoverable, in addition to the recommendations above, significant changes to information in the plan must be updated as the change occurs. Updates should reflect changes to:

- Functions
- Supporting applications
- Staff
- Resources
- Unique equipment or transportation needs
- Communication methods and techniques

Chapter Five:
Continuity Training and Testing

All of your continuity efforts and the projects you complete will not ensure people will know what to do when faced with an emergency event, or that executives, staff, and faculty can work together, as a team, to recover the institution as quickly as possible.

The concept of continuity management, the importance of continuity planning, and what to do if an emergency presents itself must be very familiar and practiced.

Chapter Five: Continuity Training and Testing

Training

Training can occur in several ways, but you'll want to be sure it fits the 'audience.' Training for executives works best when presented with specific examples of events that have occurred and the cost of those events to the institution. Training for faculty will look different than training for operations or business staff, and very specific training should occur for the Incident Management and Communications teams.

However, the overall message is the same: emergencies happen. Preplanning by mitigating or minimizing risks, identifying required equipment and other resources, and where any particular group, department, or team will recover all help with minimizing the impact and easing the stress during the recovery effort. Training can occur through lunch and learns, presentations, or even one-on-ones, but it is a critical piece in building the culture of resilience across the institution.

Exercising the Plans

When a general level of continuity understanding and knowledge exists, conducting exercises will take your program to the next level. There are many types of exercises from simple, quick, and high level, such as a tabletop exercise, to an all-inclusive end-to-end exercise. These exercises help to validate your program and progress. They allow you to better determine appropriate timelines, what extra training is required, and reduce the chance of panic should an adverse event occur. The most important exercise outcome is to further train on how to respond to an adverse event, regardless of the role one holds. Here are just a few examples of exercises you should consider in your program roadmap.

Plan Review/Tabletop Test (TTX)

This involves a small group of key team members, with at least the department's recovery team. Participants walk through every detail of their continuity plan, responding to how they would react to a specific situation, such as an unavailable work location or the absence of an essential staff member. The main goal is to familiarize participants with the continuity plan and their role during an event. This exercise also helps to identify gaps in the plan.

Structured Walkthrough

This has more of a role-playing aspect to it, with a chosen hypothetical (but realistic) event. Every member of the team walks through their role in management and recovery, step-by-step. This type of exercise is especially effective for executive staff.

Data Center Recovery

A data center recovery exercise is designed to simulate the loss of a critical application or server, or on a more advanced level, the entire data center or network. Initially these should be conducted with only the data center staff; then a more advanced exercise will include end users, who will use workarounds while the application or network is unavailable. When the service is recovered, they will test the application availability, and ultimately the data integrity.

Emergency Communication

There are two types of communication that occur during an emergency event, and both should be tested regularly. The first, and most critical is the executive communication that provides updates to the internal and external community. There have been many cases where poor, inaccurate, or untimely communication has severely damaged an organization's reputation, cost millions of dollars in damages, and in some cases put organizations out of business completely. The exercise is a walkthrough of all the following crucial elements for communicating effectively:

- Who your communication recipients are e.g. media, board, local community, students/parents
- The message you will communicate — it is best to draft examples in advance to customize when needed for each specific event
- The method of communication e.g. website, texts, media updates
- How often you will provide updates — initially in a big event this should be daily, if not more often, but can be reduced over time and as the event settles
- Who will provide the communication, dependent on all of the above

The second type of communications take place internally between staff members, either within a department or across the institution. Here, different methods of communication should be tested to familiarize staff with the tools you will use. For instance, if your office phone and cell phones are unavailable you may resort to online or virtual methods, such as Zoom or MS team meetings. Not everyone can adjust to using alternative methods quickly, so conducting an exercise using them will help to acclimate staff to these new tools.

End-to-End

This large scale, all-inclusive exercise is a full simulation of a real-life event. Multiple departments, generally the most critical, work together to recover. During an end-to-end exercise data center applications are assumed to be unavailable so that workarounds can be practiced. Participants will work through the recovery effort as they would in a true event, using alternative methods of communication and even relocating to their alternate work location. This exercise is the most effective and involves activating the Incident Management Team and sending emergency communication but requires months of planning. It is for the most mature programs.

In the early stages of your program, you should start small. Begin with the Plan Review/Tabletop exercise, which is conducted at the department level. As your program matures, and at least on an annual basis, progress to an exercise that incorporates another element of recovery. For instance, in year two combine a tabletop exercise with emergency communication, or perhaps include all departments in a division to work through the tabletop together. Advancing in this way builds on the knowledge, exercise-over-exercise, and discovers gaps within interdependencies. All exercises should have a common set of goals:

- Familiarize participants with their roles in recovery activities
- Exercise application and function workarounds where available
- Identify gaps in alternate recovery methods and resources
- Practice methods of emergency communication
- Discover and reduce risk
- Document gaps in the plan interdependencies that will affect or delay the recovery

As mentioned, exercises provide training, knowledge, and status of recoverability. No matter the exercise, people and planning are involved, but the benefits are great. To reap full benefits, all exercises should include a test script and results document; gaps should be addressed, and plans updated. For every exercise that is completed, the institutional level of resilience and recoverability will be advanced, thus increasing the maturity level of your overall program.

Chapter Six:

Communicating During An Adverse Event

One of the biggest continuity challenges faced by any institution is communication. Specifically, continuing communication during an adverse event.

Regardless of the event in question, there is a good chance that communication will be affected. But even if it is not, you still need to be able to communicate with a number of different groups, for a number of different purposes. As such, in preparing for an event, you need a solid plan for who you need to communicate with, what needs to be communicated, and how you will communicate.

Who?

The simple answer to this question is: everyone. There is important information that must be communicated to people both within and outside the institution. This will include some or all of the following:

- Students
- Faculty
- Staff
- Local emergency management authorities
- Local emergency responders
- Vendors
- Families of affected persons
- Surrounding local residents
- News/media

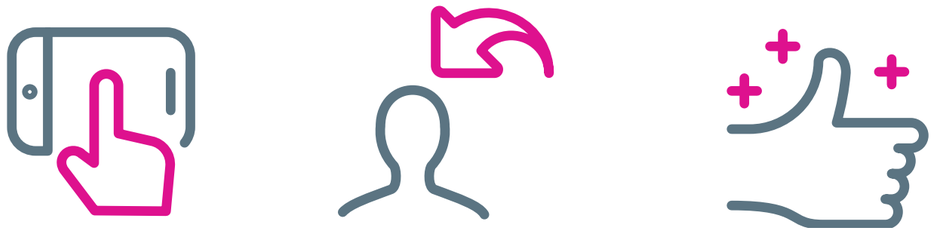
That may seem like a long list, but the exact list of people — especially those outside of the organization — who need to be informed about certain events will often depend on the nature of the event itself. They will also require different levels of information.

What?

Different groups of people will require different information. In order to help you figure out what kinds of information needs to be relayed to each group of people, we have broken it into two categories of communication:

Informational Updates

This will typically be one-way communication that is intended to provide key updates to relevant parties. For example, students, faculty, and staff all need to be updated as the event progresses, and are provided information on what they can and cannot do at each phase of the event. As mentioned in the previous section, this may also extend to other relevant persons such as vendors, nearby residents, and media. Furthermore, you may need to provide updates to family and others about the safety of individuals on campus.



Continuity Communications

Essential personnel may require a different level of information, as their roles are likely to be more involved. Members of your continuity team and other essential personnel will need to be able to communicate with each other throughout the crisis in order to organize response efforts, as well as implement various phases of the continuity plans.

How?

When building out plans for communication during an adverse event, remember that regular communication methods may be unavailable. As such, it is considered good practice to have multiple forms of communication available and practiced. For example, you may plan a text or phone chain for your team and other key personnel, but in some emergency situations, power losses or traffic surges may jam cell towers or overload providers.

For general updates, email blasts, automatic notifications, and social media are common options. In these situations, relevant employees should already be trained on best practices for tone and voice, and plans should be put in place to reach those who are outside of this scope.

As mentioned, communication internally with key team members is also essential. This will require more comprehensive communication tactics than something like social media and, again, backup plans for when primary communication methods are unavailable. This will be key for implementing different stages of the emergency response and continuity plan, as well as organizing any adjustments that may be required.

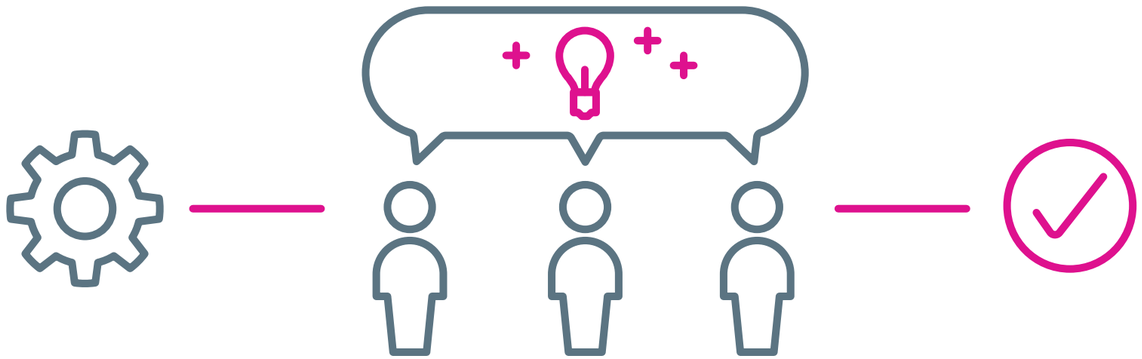
Solution

Continuity planning software is only as useful as it is easy to use and accessible during an event. Kuali Ready is cloud-based and requires minimal training, allowing users to access it during or after an emergency from any internet-connected device.

Chapter Seven:
The Incident Management Team

An Incident Management Team, or IMT, is a group of individuals who provide direction, support, and much of the decision-making during an event.

Primarily the team includes representation from each of the divisions. The IMT oversees the recovery, and therefore must be kept updated on the progress of individual areas throughout the institution at each stage of recovery. In larger, wide-spread events, such as the COVID-19 pandemic, this team may be broken down into multiple teams, each with their own set of responsibilities.



Functions

Because the IMT is the eyes and ears of the recovery, they are responsible for reporting up to senior executives, such as the President, Provost, Board of Directors, and any external regulating bodies, as required. Each member's specific role will differ based on their area of expertise, and the facilitator of the team will change based on the specific event. But generally, the team's overall responsibilities will include the following:

- Assessing incidents to determine the appropriate response
- Coordinating with essential personnel
- Directing communication efforts
- Ensuring correct response implementation
- Monitoring response across departments
- Assisting with securing resources during the event
- Providing funding where necessary
- Making critical decisions to aid in a safe and efficient recovery process
- Keeping informed on event data external to the institution to provide effective communication to the institution's community
- Secure contractors to subsidize staff if necessary

Team Members

The exact roles in your IMT will depend on the size and specific needs of your institution and the impact of the event, but as mentioned, it is important that your team has senior representation from each division of the institution; at the very least the team should include the following:

Incident Response Manager

Generally called the incident commander (IC), this person is responsible for

coordinating response and recovery efforts. Because adverse events differ, the person filling this role is completely dependent on the event. For instance, if the event is a data center outage, the IC will most likely be the Chief Technology Officer (CTO) or someone assigned by the CTO. If the event is a fire in a building, the IC may be the Continuity Manager, Facilities Manager, or the Campus Safety Manager. If the event is an active shooter on campus, the IC may be the Chief Security Officer. But in any event, all team members bring something to the table. You can see how, in the example of the active shooter, Security, Public Safety, Risk, HR, and Legal all have very important roles during the recovery.

Chief Technology Officer (or other assigned technical leader)

Since a crucial aspect of continuity planning is protecting and recovering technology, both hardware and software, you will need someone with strong IT knowledge to coordinate these efforts. They will also likely have a team of their own.

Continuity Manager

The Continuity Manager generally has the most knowledge of all data contained in the Enterprise Continuity Plan, and will be able to answer specific questions related to individual departments quickly. The Continuity Manager is often the liaison between the IMT and the senior executives and the Board of Directors, providing frequent updates. They will also facilitate any IMT conference calls for virtual meetings. The Continuity Manager will also be mainly responsible for communicating with first responders.

Director of Security

Security is a major concern in most emergency situations, but even if it is something as simple as evacuating a building, you will need someone to direct these efforts.

Public Relations Coordinator

As discussed in chapter six, it may be necessary to talk to the media as part of a coordinated response to an event. For such situations — or even simply when drafting emails and social media posts — a public relations expert should be part of the team.

Director of Human Resources (or other assignee)

Your director of human resources, or someone who fills a similar role in your institution, should also be involved in any incident management team.

Unit Response Directors

Other senior representation will be dependent on the event or situation. As the event plays out the required representation may change.

To subsidize your IMT, continuity managers, public safety, and security personnel should build relationships with external partners such as local authorities, first responders, healthcare personnel, and so on. Local authorities can educate you on laws and regulations you'll need to be sure are covered in your program. First responders should be familiar with your campus layout, and also have a campus map and floor plans for each of the buildings. (Inviting first responders to participate in your emergency drills provides extreme value.) Healthcare personnel can assist with an overflow of health emergencies, and also provide data during events such as a pandemic.

Like all aspects of your continuity program, your IMT should be fully trained in the practice or continuity management, and should also regularly practice their roles during recovery through an organized exercise.

Chapter Eight:
Pulling It All Together

So far we have discussed various aspects of the process of preparing your organization for an adverse event, but now it is time to talk about the actual act of pulling it all together.

This chapter will walk you through the main steps of putting together your Enterprise Continuity of Operations Plan, or ECOOP. This is sometimes also known as the Enterprise Business Continuity Plan (EBCP).

What is an Enterprise Continuity Plan?

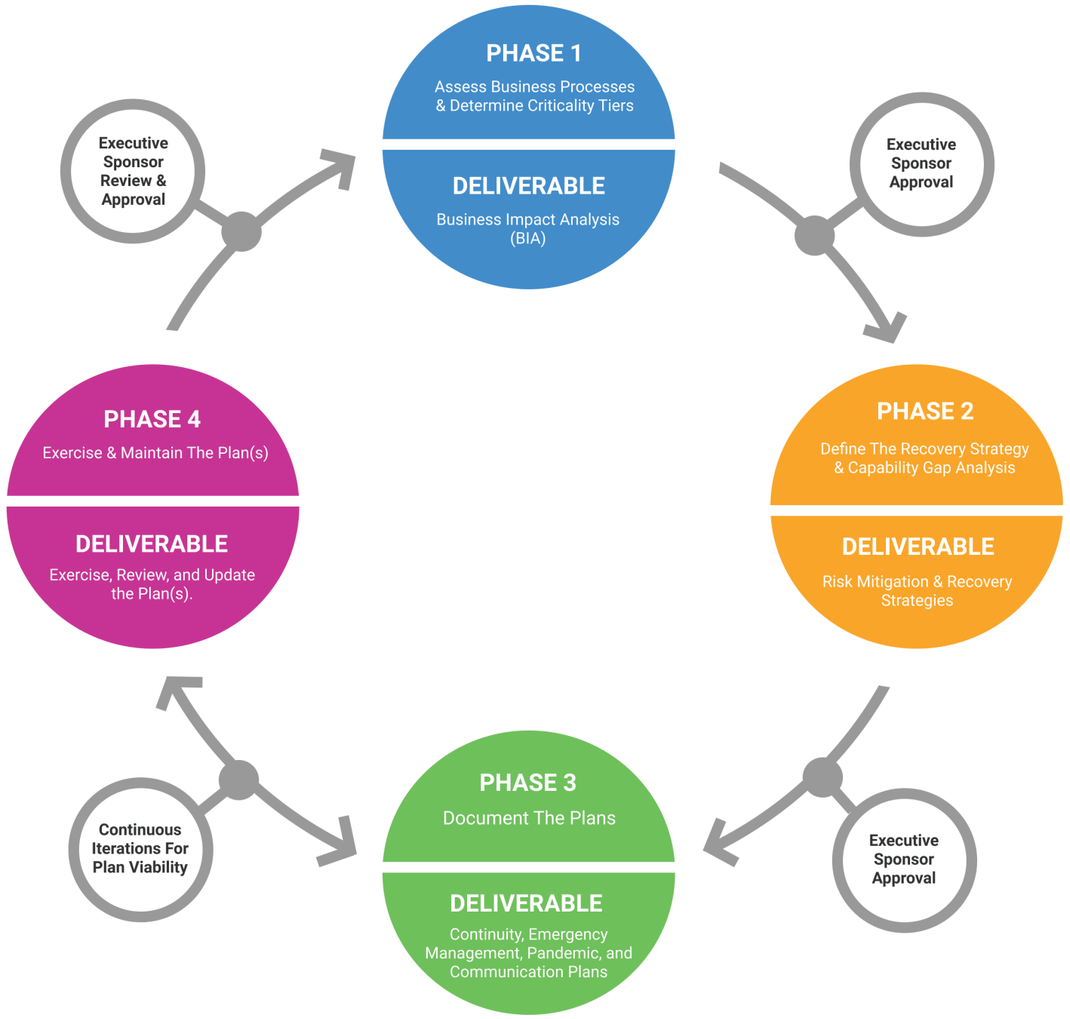
An Enterprise Continuity of Operations Plan, or ECOOP, is exactly what it sounds like: an organization's plan for continuing operations during and after emergency situations. While many institutions already have some form of existing Emergency Operations Plan, or EOP, that plan is typically more focused on disaster response; conversely, an ECOOP is the plan that will help facilitate continuity in the manner that we have been discussing throughout this ebook.

Resource

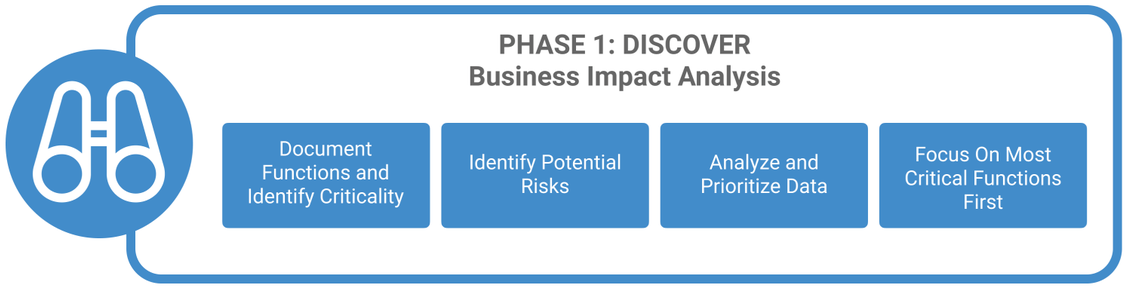
Webinar: What is an Enterprise Continuity of Operations Plan, and Why does my Institution Need One

The Process

Each chapter of this ebook goes into various stages of this process in greater depth, but to help you to better visualize the task ahead of you, we have detailed the steps of a typical process for compiling an ECOOP for higher education below. The first two phases



will typically take place on a departmental level, as each unit builds out their own continuity plan. After this, the ECOOP will require organizing these plans, pulling it all together in one place.

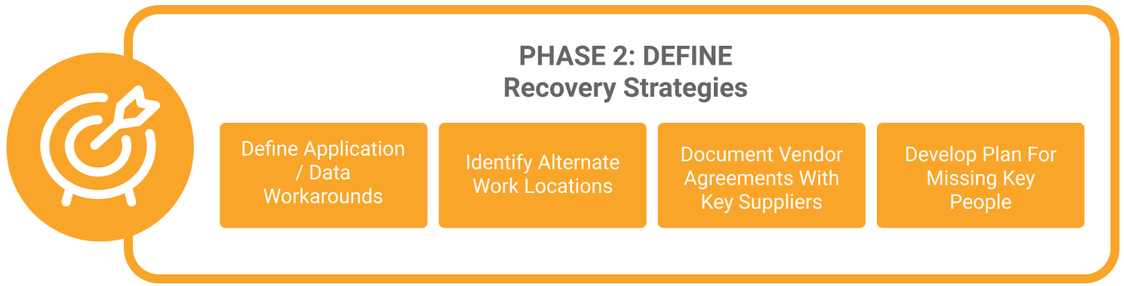


Phase One: Business Impact Analysis

This is the initial data collection phase, and will take place on a department level. Each department head or assigned continuity manager will need to assess their unit's functions to determine how critical they are. This stage will require a lot of aid from others, as discussed in chapter four, and there may even already be some form of initial unit plans in place for various departments.

Key Tasks

- Identify the functions for each department or business unit.
- Identify the applications that support those functions
- Assess the criticality of functions for each department
- Assess the criticality of supporting applications
- Compile the data collected from all departments
- Prioritize functions and applications by most essential, and establish a recovery hierarchy for both
- Identify potential risks the functions or applications are subject to for the top levels of criticality (based on the risk appetite of the university)
- Perform a gap analysis for most critical functions and applications vs. the risks



Phase Two: Risk Management

Now that you know which functions are the most critical, you can start the process of eliminating, mitigating, or accepting risks. In order to do this, you will have to

put strategies in place for mitigating, or recovering from, the loss of the four main elements detailed in chapter two:

1. Loss of essential employee(s)
2. Loss of a normal work location
3. Loss of critical applications
4. Loss of unique resource

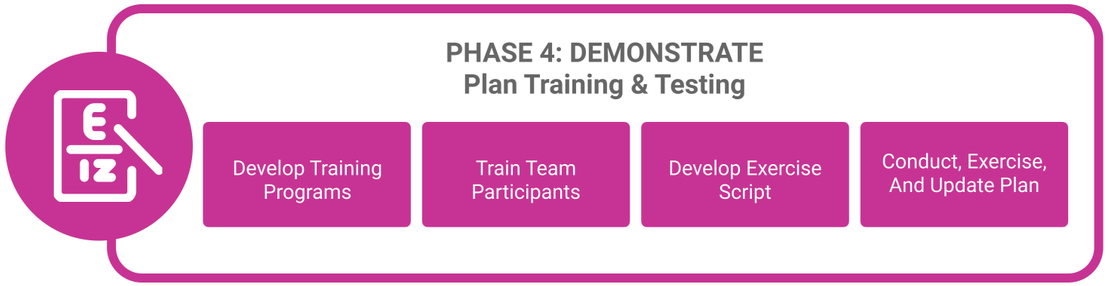
Phase Three: Compile the ECOOP

Now it is time to collect all of the information gathered in the first two phases and create your full plan for continuity, the ECOOP. This is primarily the job of the continuity manager, and will be updated and tweaked as necessary. As you collect the information together, you may begin to see gaps and places where extra information is required. This is where you will need to reach out to relevant parties to get the answers you need and take steps required to ensure that you have included all critical buildings, alternate buildings, essential personnel, resources, and so on. This unified continuity document serves a number of purposes:

- Illustrates the recoverability of your institution to leadership, prior to an event
- Outlines all aspects of the program, including details for recovery, where people will go, what resources are needed and so on
- Serves as a primary reference point for continuity in the face of adverse events
- May highlight any gaps in current continuity efforts that need to be addressed

Solution

Kuali Ready's easy-to-use software allows you to crowdsource the process of compiling your ECOOP. You can use simple, question-based forms to get the answers you need from department leaders, with progress reports along the way.



Phase Four: Training & Testing

As detailed in chapter five, testing is an essential part of the ECOOP process. In order to be successful, your plan will need to be tested and tweaked as necessary. Furthermore, rigorous training should be commenced to ensure that your entire team and all essential personnel are aware of their role and responsibilities in the plan. This typically takes place on the executive level, or else in individual units for each department's own continuity plan.

Resource

Continuity Program Methodology for Higher Education

Chapter Nine:
Post-Event Activities

Continuity planning has an ongoing lifecycle. It is not a matter of if; there will always be the prospect of another event occurring.

Following an adverse event, if you document what you have learned, work to close the gaps you have discovered, and update the continuity plans accordingly, you will be better prepared for the next event.

Post Incident Reports

The most important activity of post-event practices is documenting the Post Incident Report (PIR). The purpose of this report is to provide an overview of the event and can be used to:

- Provide an event evaluation for executives, the Board of Directors, and external regulating bodies
- Assist in the evaluation of the overall response and effectiveness of your continuity program
- Identify lessons learned to create a gap analysis and roadmap for improvements
- Provide data to support additional funding where necessary
- Apply for insurance claims or government funding, where applicable

The PIR should include:

- A thorough description of the event
- A timeline of events and response activities
- What continuity plans were activated, if not all, and the date and time the activation occurred
- Issues that hindered or delayed the recovery
- Costs associated with the recovery effort
- Negative effects on staff/faculty/students
- Any specific discoveries of equipment, applications, etc., that required emergency procurement
- A listing of lessons learned with detail
- Improvements that will be made (with an ETA) to improve recoverability

Chapter Nine: Post-Event Activities

Because it will be difficult to remember the enormous amount of information that is needed to draft the PIR, it is important to keep accurate records throughout the event. This should be done at the department level throughout the institution. The following information should be captured:

- Emergency expenses
- Any required overtime
- Staff that had to be subsidized
- Recovery timeline with specific activities (positive and negative)
- On-the-fly decisions that went against policy
- Critical functions that missed the recovery time, and the cause for the delay
- Impacts to dependencies, and to internal and external customers

While this information is tracked independently at the department level, it should be collected and compiled by the IMT or IC following the close of the event, or at a point that makes sense during an extended event.

Implementing New Processes (addressing lessons learned)

In continuity jargon, a real event is the best exercise and you should always turn a live event into a learning opportunity. With that, debrief sessions should be held at the department and division level, as well as within the IMT, to ensure everything was captured, and to discuss what changes can be made to:

1. Improve recoverability
2. Mature the continuity program

Every lesson learned or issue that delayed recovery should be scrutinized for resolution. Continuity plans should be updated, policy changes discussed and considered, and processes written for items that were confusing during the event. Prioritize the post-event activities to address these and build a roadmap with resolutions to closure, estimated times for completion, responsible party, and any required funding. This will provide a tracking document that can be shared and tracked. Resolutions that require funding will need to go to executive management for approval or alternate solutions.

Kuali Ready Simplifies Continuity in Higher Education

That’s a lot of information to get started with — and no one gets that more than us! That’s why we aim to simplify the process of continuity planning in higher education.

At Kuali, we understand that continuity planning software must address both business and academic needs. We also understand that those who are placed in charge of continuity efforts are often overwhelmed by the amount of work required — on top of their regular responsibilities. That is why we developed a product to help you more efficiently accomplish your continuity planning responsibilities, leaving everyone more time for teaching, researching, and keeping the lights on.

Adaptable

Because every institution is unique, Kuali Ready is easily adaptable to your specific needs.

All-Hands Approach

Getting the answers and information you need to compile your plans is easy with simple, question-based surveys.

Data and Reporting

Kuali Ready provides structured data collection and meaningful reports within the software, as well as key insights and plan management, all in one place.

Easy to Use and Cloud-Based

Uniform elements within the software help everyone to use it with minimal planning and training. And, as accessibility during an event is essential, all of our software is cloud-based and can be accessed from any internet-connected device.

REQUEST A FREE TRIAL