Business Continuity Plans and Procedures

Table of Contents

Business Continuity Plans and Procedures

**062 Instructor: In this particular lecture, what we want to cover is business continuity planning and procedures that are related to it.

Business Continuity Management

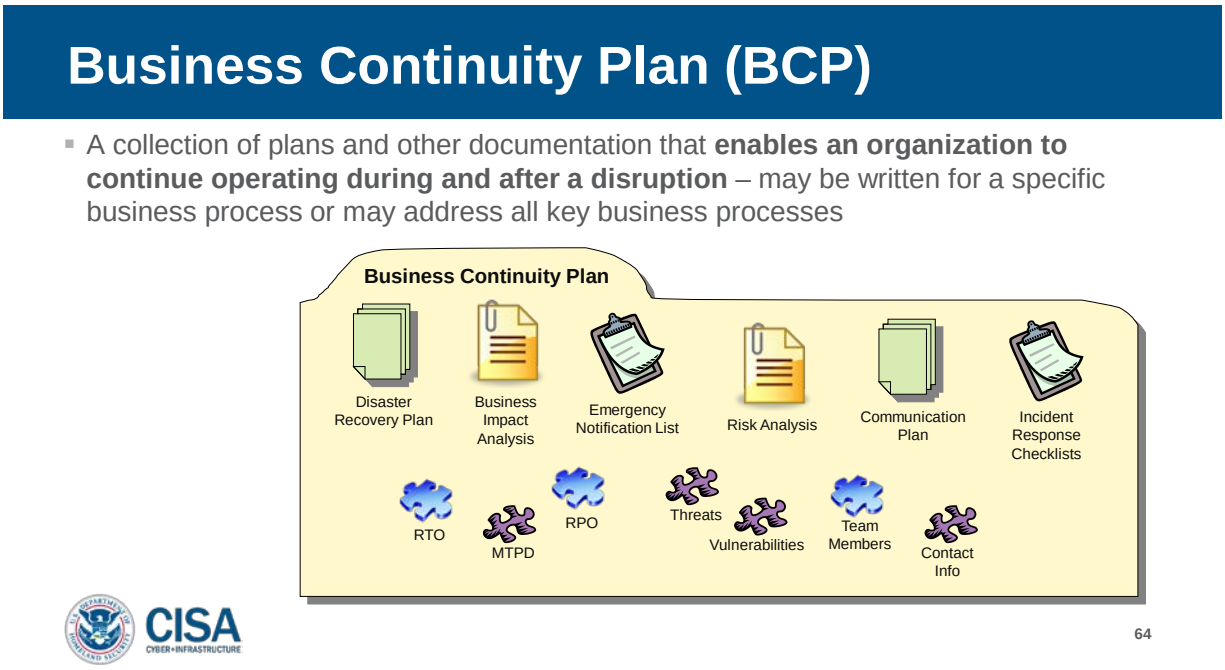
- **Business Continuity Planning (BCP)**
- Identification, selection, implementation, testing, and updating of processes and specific actions necessary to prudently protect critical business processes from the effects of major system and network disruptions

- **Disaster Recovery Planning**
- Ensure the timely restoration of business operations if significant disruption occurs
  - Part of BCP

CISA CYBER+INFRASTRUCTURE

63

**063 Now, you've got to understand that there's different terms that are used here, and we want to be clear what exactly we're doing. Business continuity planning is actually going through an entire arc of events that includes identifying risks, selecting proper controls, implementing those controls, testing them, making sure that the processes and policies that you have in place work. This can contrast to disaster recovery planning, which may focus on a specific scenario or event. Remember that the disaster recovery plan is actually part and parcel, or a piece to that overall business continuity plan.

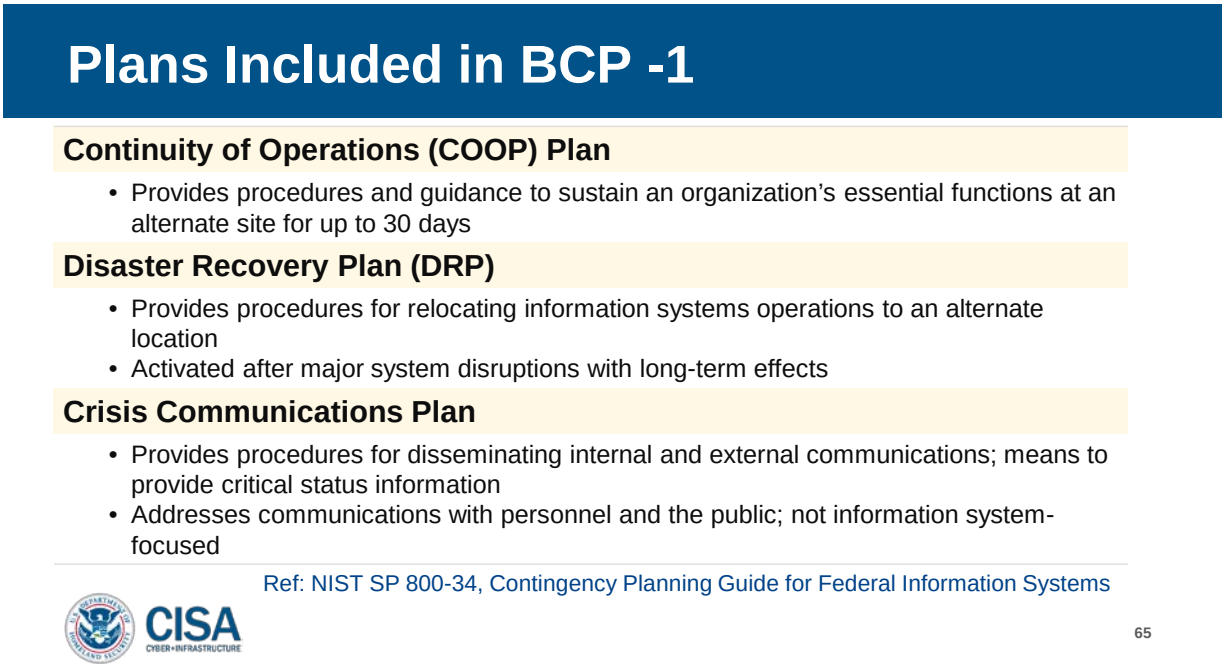


**064 Speaking of pieces, there are lots of them. All these pieces play a critical element in enabling your organization to operate once it's had that dark day where a risk has come to realization.

Now, like I said, the disaster recovery plan is clearly going to be a part of that. You may have additional analysis where you're assessing assets to understand what the impacts could be. You may have lists of people who need to be contacted in terms of emergency notification. You may include your package with your risk register and the analysis related to it, so you understand how to prioritize your actions. You're going to want to have a communication plan, so people know how to reach out to others. And you may even have checklists for your

immediate responders so that they know what to do when that risk is finally realized. All these pieces need to add up and come together into a cogent plan that's easy to understand and implement.

Plans Included in BCP -1



**065 Harder than it sounds. So, that said, let's talk about the sub plans that may be in here. We could also have a continuity of operations plan as part of this, also called a COOP. Now, typically, what this is is procedures and maybe some additional guidance that it tells you how to keep your organization running for like thirty, maybe sixty days following a major incident. Typically, it's thirty days. And by the way, it also may not actually occur at the original site where the incident has taken place. It may have a continuity of operation plan that will

extend to another site, a hot site, a warm site, etc.

You also need to have detailed procedures for actually finding where you're going to put your new system. So, if I have a bad incident, let's say a fire that burns down my facility altogether, and I make it out luckily with my data backups. A disaster recovery plan will help you know how to get to your alternate location and how to get stood back up again.

You should also have a crisis communications plan. Now, what you understand here is who you're going to call, when you're going to call, who's going to do it, and how. There's a lot that needs to go on there. And the trick to having a good crisis communication plan is keeping it updated. It's not just internal people in your organization who are coming and going that you need to know who to contact. It may be external as well. Exercise this plan often so it stays up to date.

Plans Included in BCP -2

Cyber Incident Response Plan

- Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse
- Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information

Information System Contingency Plan (ISCP)

- Provides procedures and capabilities for recovering an information system
- Addresses single information system recovery at the current or alternate location

Ref: NIST SP 800-34, Contingency Planning Guide for Federal Information Systems

CISA CYBER+INFRASTRUCTURE

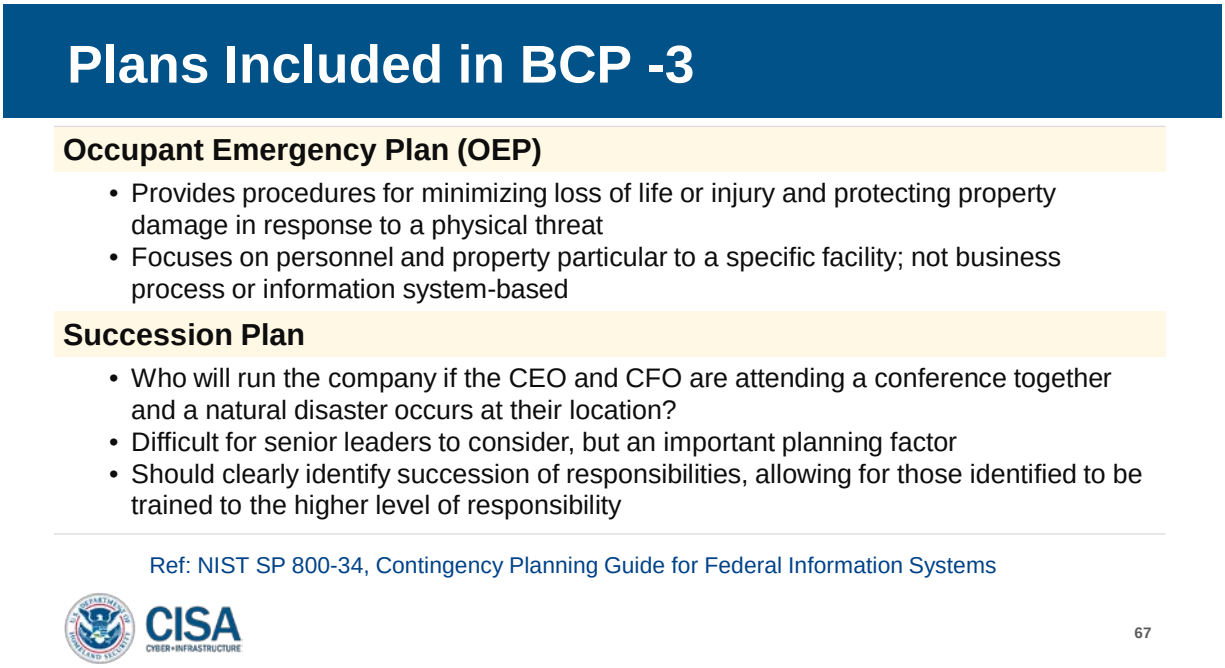
66

**066 You may have an incident response plan. Now, this may get into the nitty-gritty. You may have it scenario based so that way you know what your operators are doing specifically when they see a threat that becomes resident on your system. It's going to have some immediate actions and have some mitigation steps that need to take place such that that bad thing that has happened is contained and is properly responded to. It may even also provide some indication of how to do clean up and how to mitigate or limit the amount of impact you have on your organization.

You may also have a contingency plan for your information system. Now, this would be like a similar system, and it may have reduced functionality or capability, but you

need to know how to operate it altogether so that way you can keep your enterprise going. Note that that system may be resident at another site and not just where you're located.

Plans Included in BCP -3

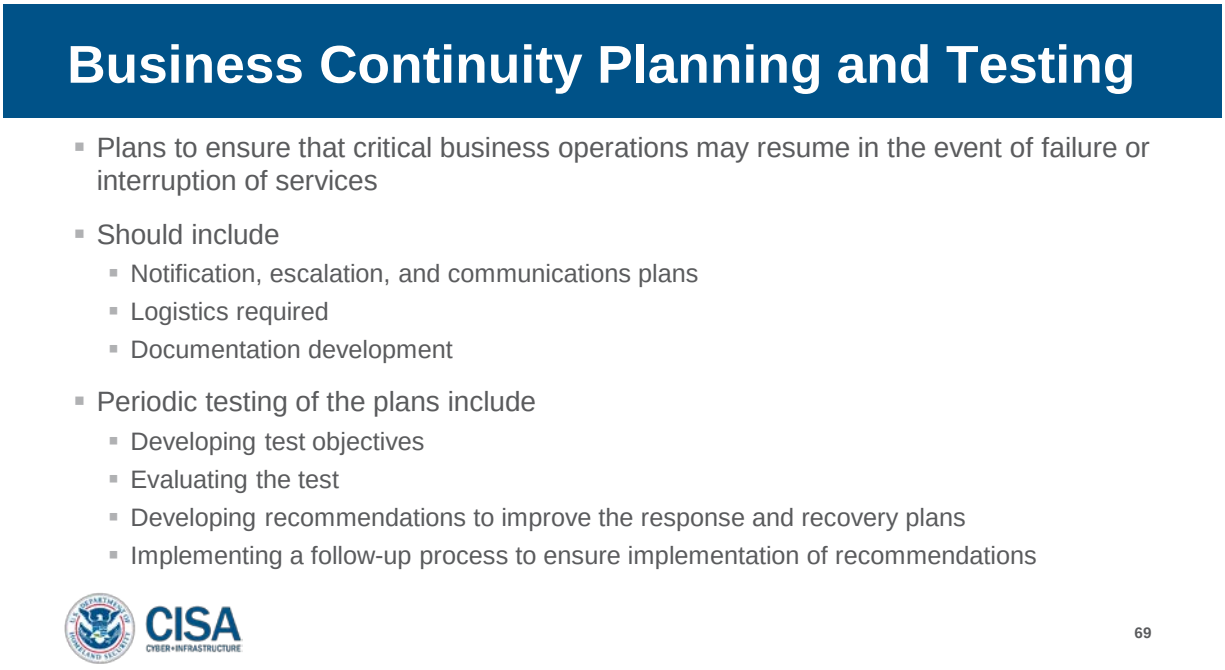


**067 You could also have something like an occupant emergency plan. This is really getting physical for an organization, and you're thinking about where people were physically located, especially in a large operating environment. Think about a manufacturing plant, one that maybe deals with chemicals or something that could be explosive. You have to understand where people are located so if that darkest day comes, and unfortunately there may be some casualties, you need to know who is located where so that way you can understand how to take

assessment of the damage that's there.

You may also want to consider a succession plan. So, let's go back to that incident I just talked about where unfortunately there were casualties in an organization. Suppose the entire C-suite was wiped out for whatever reason. Who would take their place? Who is making the critical decisions? Succession plans can get funny, too. If you think about it, if I have some executives who travel together, say my CEO and CFO, maybe I have as part of that plan that they're not allowed to travel on the same plane. It just makes good sense.

Business Continuity Planning and Testing



**069 Now, when you have these plans together, it's always a great idea to test them. And we've talked

about this time and again, this idea of if you have a plan, it really isn't going to do you any good unless people come together and actually walk through the plan and understand their own individual responsibilities and what they need to do. So, you want to think about who's being notified again. How are these incidents being escalated up in the organization in terms of communication? Who's being called and how? And what logistics are necessary to pull off this plan?

You're going to want to do this periodically. Remember, there are comers and goers in an organization. As people leave, you have new people come in. They may not know what they have to do. You're going to have a set of objectives, and you're going to test those objectives quite regularly. You're going to also look at recommendations that come out of your tests and make sure you implement those recommendations such that you can improve your response plans. Don't just let them sit on a shelf and collect dust.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098