NORTH CAROLINA
CYBERSECURITY
AWARENESS SYMPOSIUM

Being Cyber Smart for Continuity of Government

Debora Chance
CGCIO, CPM, CIA, CISA, CRISC
State IT Business Continuity & Disaster Recovery Specialist
FEMA Master Continuity Practitioner
Debora.Chance@nc.gov

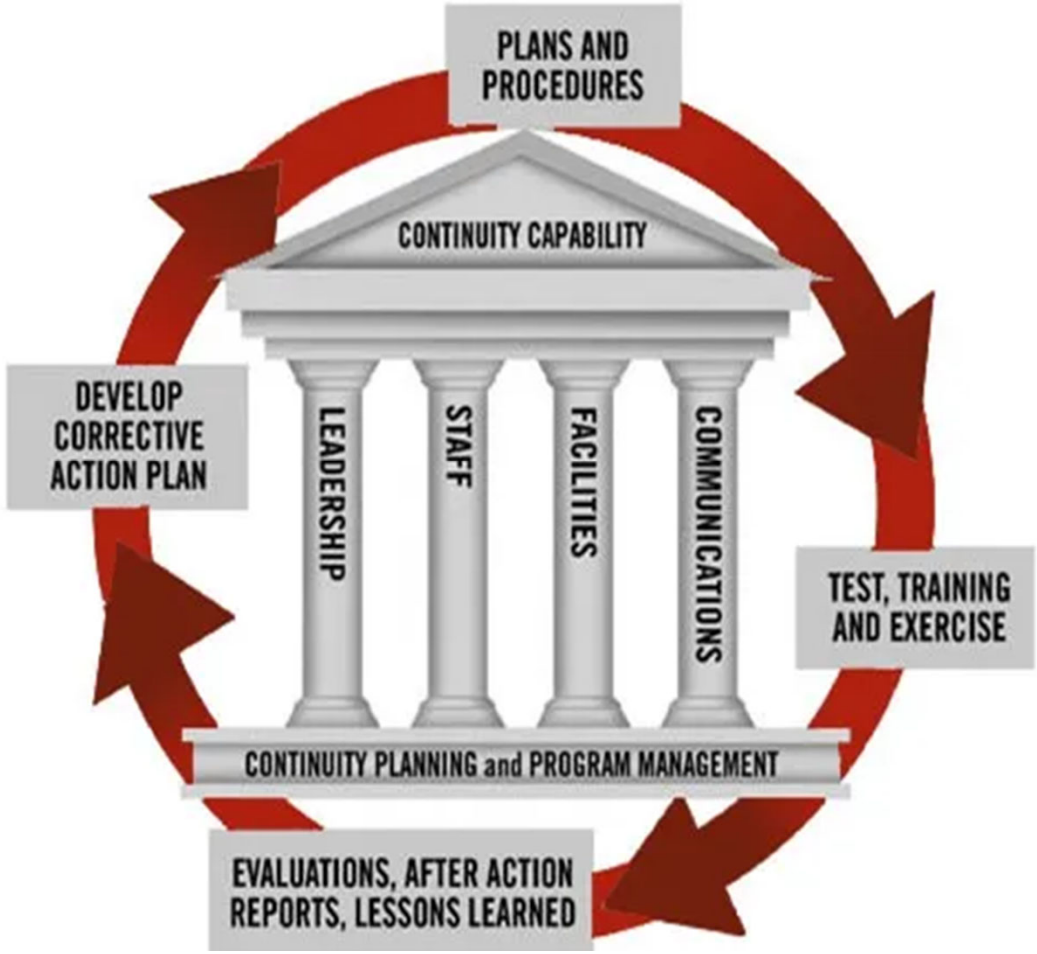
NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

What is Continuity of Government (COG)?

Being Cyber Smart for Continuity of Government

What is Continuity
of Operations (COOP)?



Being Cyber Smart for Continuity of Government

Relationship between COOP and COG

Continuity of Operations	Continuity of Government
Effort within individual organizations to continue essential functions.	Coordinated effort across governments and jurisdictions to continue national, state, local, tribal, and territorial essential functions.
Applies to all organizations within the whole community, including non-governmental organizations, faith- and community-based organizations, and the private sector.	Specific to the executive, legislative, and judicial branches of government (at all levels).
All events (fire, flood, hurricane, etc.)	Major or catastrophic disasters that could impact the entire nation, state, tribe, or jurisdiction and overwhelm a government's ability to respond unless it is prepared to deal with the situation. Events that threaten the institutional stability of SLTT governments effect the ability to achieve COG.

Being Cyber Smart for Continuity of Government

Polling Question 1

Were the essential services your organization provides adversely impacted by COVID-19?

- ❑Yes
- ❑No
- ❑Unsure

#BeCyberSmart
#CyberSecureNC

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

Polling Question 2

Did your organization modify its Business Continuity and/or COOP Plan because of COVID-19?

(select one answer)

- ❑Yes
- ❑No
- ❑Unsure

#BeCyberSmart
#CyberSecureNC

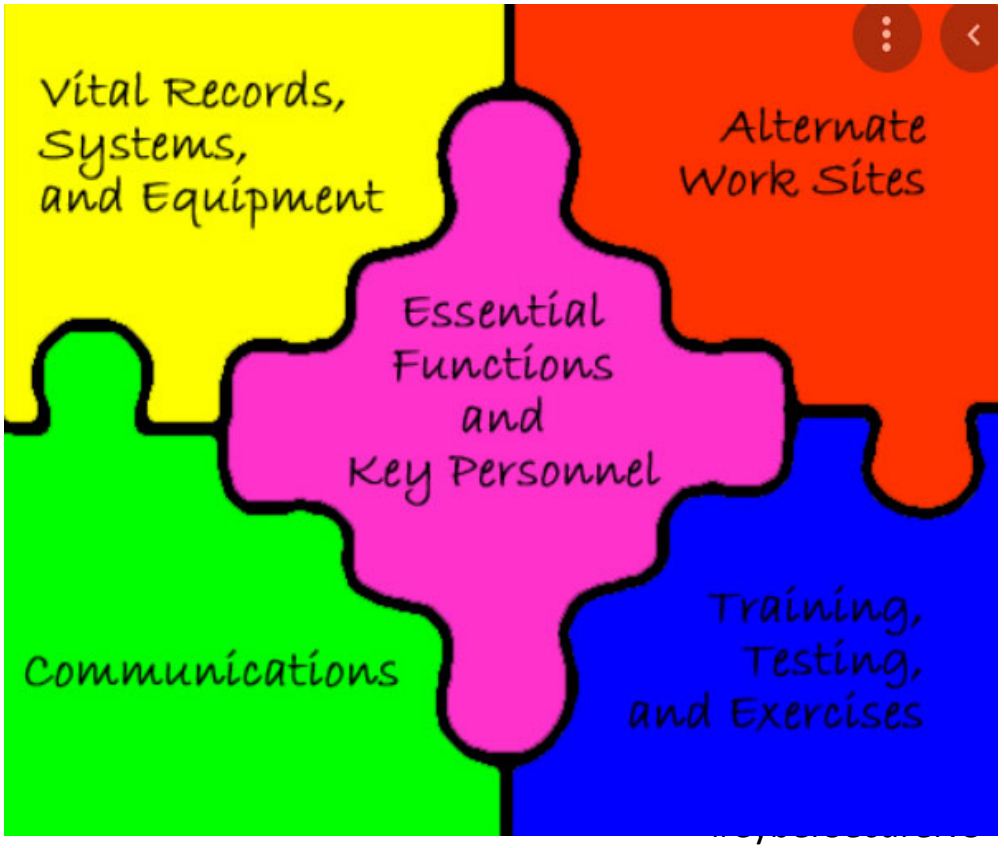
NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

A recent survey found that 82% of organizations have made changes to their business continuity plans since the onset of COVID-19, but 40% of organizations have not trained employees or tested their plans since updating them.

Ensuring your employees are prepared is the best way to reduce or eliminate threats and impacts to your business.

- ✓ **Define clear roles and responsibilities**
- ✓ **Train employees**
- ✓ **Test your plans!**



NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

Polling Question 3

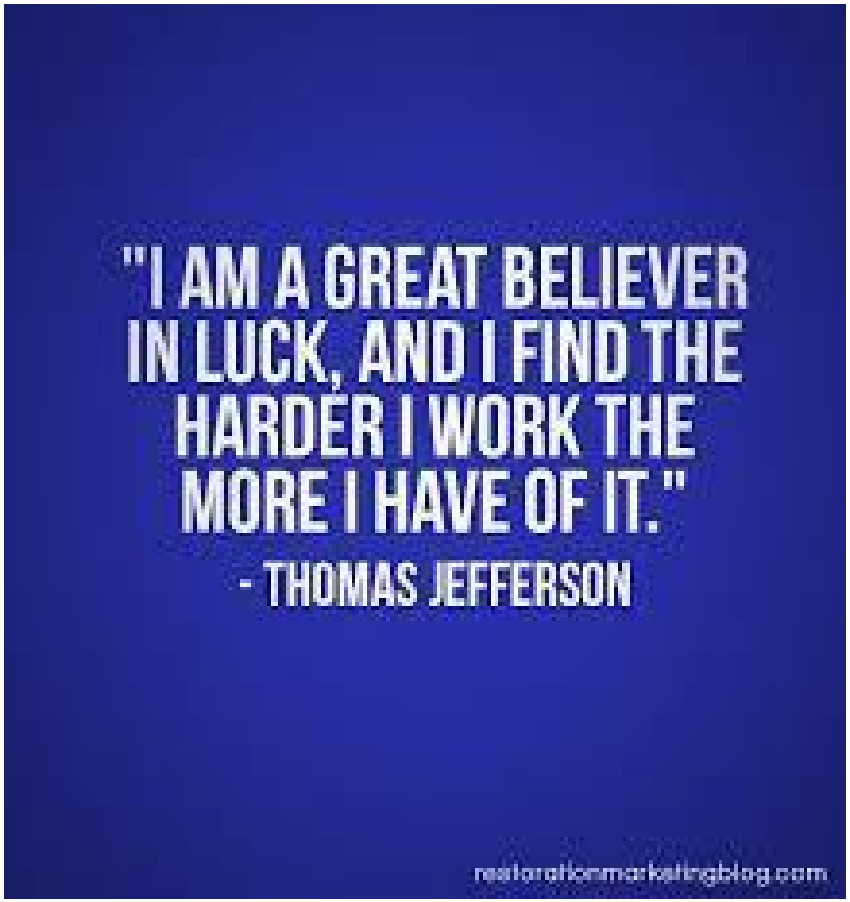
Regarding Continuity of Operations, has your organization: *(select all that apply)*

- ❑ Defined clear roles and responsibilities for key roles?
- ❑ Offered training for employees?
- ❑ Tested a plan in the last two years?
- ❑ Updated a plan based on test results and/or lessons learned?
- ❑ Retested a plan?

#BeCyberSmart
#CyberSecureNC

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government



#BeCyberSmart
#CyberSecureNC

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

You can avoid cyber risks by setting up the proper controls. The following are things you can do to protect yourself, your family, your property , and your business before a cyberattack occurs:

•Limit the personal information you share online. Change privacy settings and do not use location features.

•Keep software applications and operating systems up-to-date.

•Using a password manager, use upper and lowercase letters, numbers and special characters, as well as, two-factor authentication (two methods of verification).

•Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true or needs your personal information. Think before you click, and when in doubt, do NOT click. Do not provide personal information.

•Use encrypted (secure) Internet communications.

•Protect your home and/or business on a strong, using a secure Internet connection and Wi-Fi network.

#BeCyberSmart
#CyberSecureNC

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

- Protect your home and/or business on a strong, using a secure Internet connection and Wi-Fi network.
- Use a stronger authentication such as a personal identification number (PIN) or password that only you would know. Consider using a separate device that can receive a code or uses a biometric scan (e.g. fingerprint scanner or facial recognition).
- Check your account statements and credit reports regularly.
- Only share personal information on secure sites (e.g. “https://”). Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more secure connection.
- Use antivirus solutions, malware and firewalls to block threats.

#BeCyberSmart
#CyberSecureNC

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Being Cyber Smart for Continuity of Government

- Regularly back up your files in an encrypted file or encrypted file storage device.
- Protect your home network by changing the administrative and Wi-Fi passwords regularly. When configuring your router, use either the instruction manual or speak to your internet-cable provider, to setup the Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES) setting, which is the strongest encryption option.

#BeCyberSmart
#CyberSecureNC

Source:https://www.ready.gov/cybersecurity

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Continuity Planning Checklist

- Examine current state of organizational continuity program.
- Identify the organization's current and potential partnerships within the community, which are critical to developing and sustaining a culture of continuity.
- Identify existing coordinating structures in which organizational continuity planners should participate in to integrate continuity planning, operations, and responsibilities into emergency management, preparedness, and resilience efforts.
- Identify other inter- and intra-organizational continuity plans and programs (e.g., incident management, Occupant Emergency Plans, and Emergency Operations Plans, IT/Disaster Recovery Plans), which should be coordinated with to ensure synchronization across plans and programs.

Continuity Planning Checklist

- Create an overall continuity strategy that is agreed upon by elected officials or organizational leadership.
- Identify existing, applicable continuity regulations or requirements. In the absence of requirements, identify continuity guidance, and principles most applicable to the organization.
- Identify continuity program planning roles and responsibilities.
- Establish a continuity planning team to assist with planning including representatives from other organizational offices or departments.
- Develop a project plan, timelines, and milestones.
- Identify preliminary budgeting and resource requirements.
- Obtain the support of leadership and elected officials for the continuity program.

Continuity Planning Checklist

- Conduct a BPA to identify and document the activities and tasks that are performed within an organization, with an emphasis on the big picture (how the organization interacts with partners and stakeholders) and the operational details.
- Conduct a risk assessment to identify and analyze potential threats and hazards.
- Conduct a Business Impact Analysis (BIA) to identify and evaluate how the organization's threats and hazards may impact the organization's ability to perform its essential functions.
- Identify the organization's essential functions and essential supporting activities by determining what organizational functions are essential, taking into account statutory requirements and linkages to National Essential Functions and other essential functions in the community.
- Identify mitigation options to address the risks identified in the BIA (e.g., alternate operating facilities, telework policies, devolution procedures, mutual aid agreements).

Continuity Planning Checklist

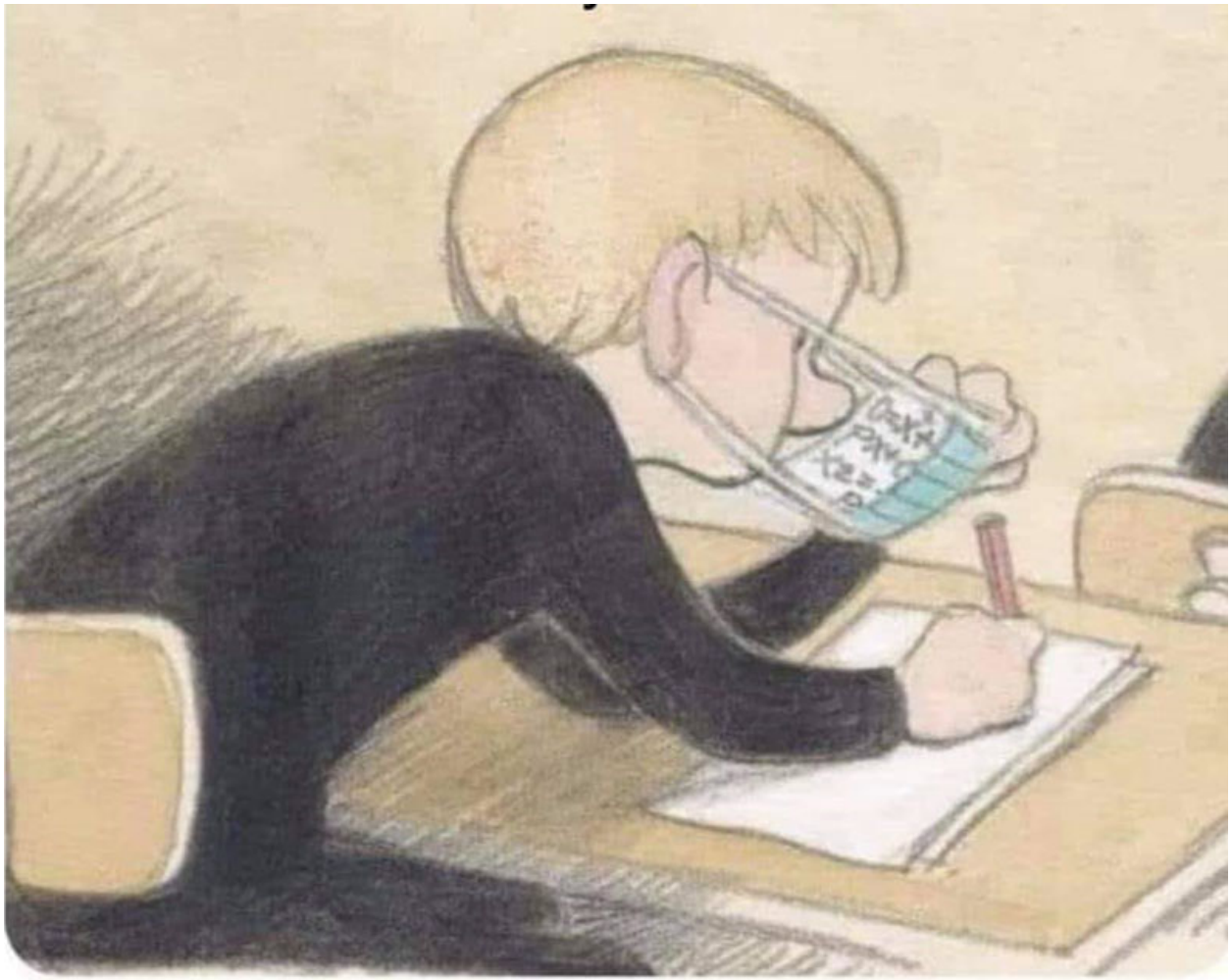
- Identify the organization's key elements (e.g., technology, people) and detail how those elements support the execution of essential functions.
- Draft a comprehensive plan that outlines the requirements and procedures needed to perform essential functions and establishes contingency plans in the event that key resources are not available.
- Establish a schedule for conducting regular test, training, and exercise events to assess and validate continuity plans, policies, procedures, and systems.
- Create a corrective action program to implement and track areas for improvement identified during tests, exercises, or real-world incidents.
- Develop continuity metrics and success criteria to evaluate and assess the organization's continuity plans and program against.

Continuity Planning Checklist

- Establish a schedule for conducting a review (using the continuity metrics and success criteria) and revision of the organization's continuity strategy, plan, and supporting documents and agreements such as Memorandums of Understanding and Memorandums of Agreement.
- Align and allocate resources (e.g., budget) to implement continuity activities before, during, and following a continuity activation.
- Develop a continuity multi-year strategic plan to provide for the development, maintenance, and review of continuity capabilities to ensure the program remains viable and successful to include test, training, and exercise activities, and plan reviews.

Source: FEMA.Gov

Always be prepared!



CYBERSECURITY AWARENESS MONTH

Do Your Part. #BeCyberSmart