ncmbc
CONNECTING BUSINESS AND MILITARY

NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP 4

www.cybernc.us

3 February 2021

CyberChat Series Description

- Objective: To help defense contractors develop a cybersecurity quality management system [QMS] program that is compliant with [DFARS 252.204-7021] – the new CMMC regulation – and protects national security.
- Technical advice regarding cybersecurity tools and providers will not be given by the NCMBC. The focus will be on developing a compliance roadmap using tools and information provided on www.cybernc.us.
- CyberChats are not to be used to sell products or services. IT/Cyber companies can sign up as a resource for defense/federal contractors. Note: the NCMBC does not vet these companies. https://www.ncmbc.us/matrices-resources/

Agenda – CyberChat Workshop #4

- Latest CMMC/cybersecurity updates
- Questions from last session
- Homework questions from CyberChats 1, 2 and 3- management/ownership buy-in, CUI or FCI, current contracts, draw a network diagram, begin an asset inventory, data-flow diagram, employee intro. to cybersecurity
- Quick review of CyberChats 1, 2 and 3
- Documentation
- Continuous Improvement
- Project status
- Homework

CMMC/Cyber Updates

Federal News Network – Cybersecurity Strategies in Government: Defense and Homeland. Interviews with US Army Cyber Command, DHS, DIA, Fortinet, Verizon and Illumio

Key takeaways:

- Cybersecurity is everyone’s responsibility – we must all be “cyber patriots”
  - Gets back to employees understanding their roles and responsibilities, buying into the change in culture, tapping into patriotism – understanding the threat to our country, being appropriately trained
- Cybersecurity must be embedded into every function/department
  - Requires a change in company culture and a change in individual mindset – why “tone at the top” is critical

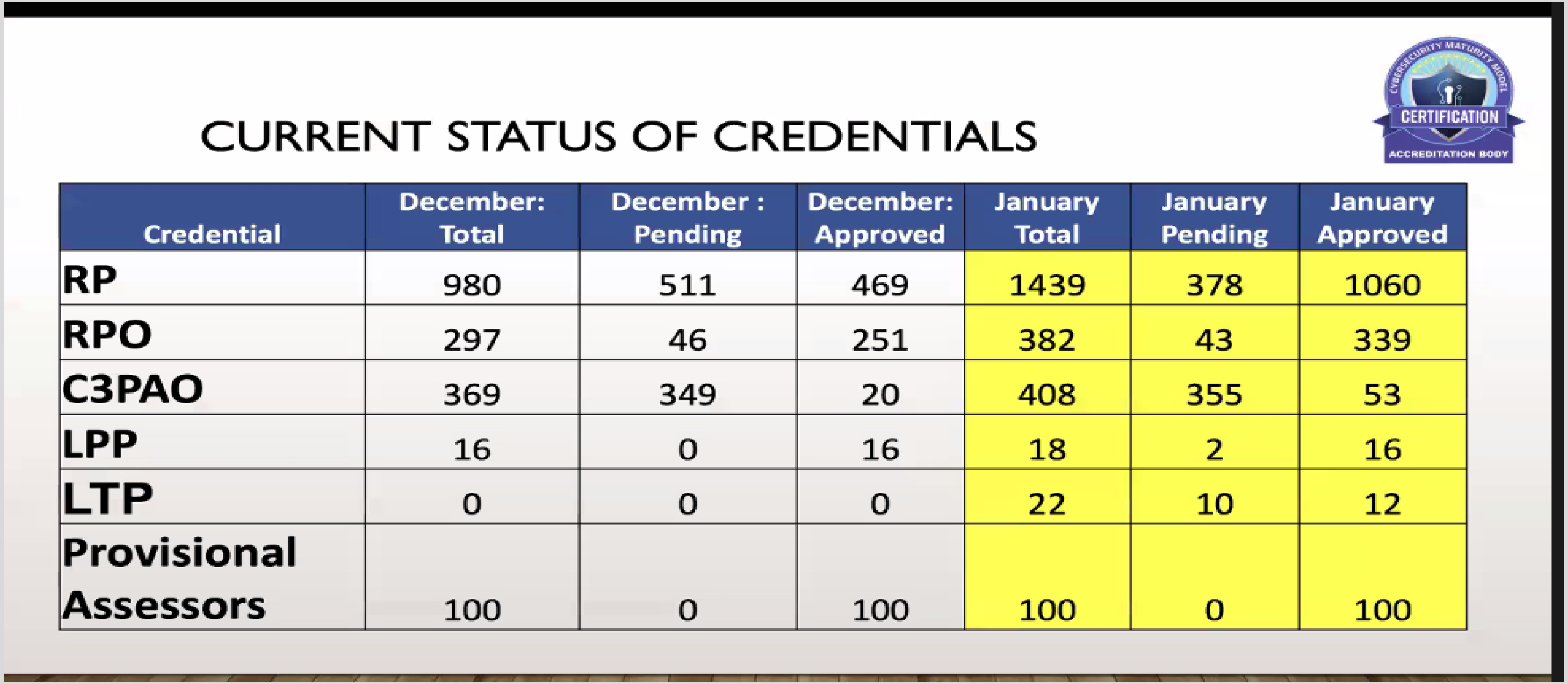
CMMC/Cyber Updates

- Cybersecurity is a **business risk –** it is not a problem for the IT/Cyber department to solve
    - Cybersecurity must be as foundational as cost, schedule, performance or any other criteria used to inform decisions – can't slap cybersecurity on at the end
    - Must include supply chain risk management
    - Don't want to be the weak link in the supply chain – brings vulnerability to everyone
- Must have a zero-trust architecture in place and develop a zero-trust mindset
    - All users – even those inside the network – must be authenticated, authorized, and validated before being granted access to applications and data
- Must manage your IT assets – if you don't know what you own, you can't protect it.

CMMC/Cyber Updates

All the issues can be mitigated by developing a cybersecurity quality management system that can mature, AND incorporates the appropriate controls/practices in the DoD cybersecurity regulations – what the CyberChat series is designed to help NC companies accomplish.

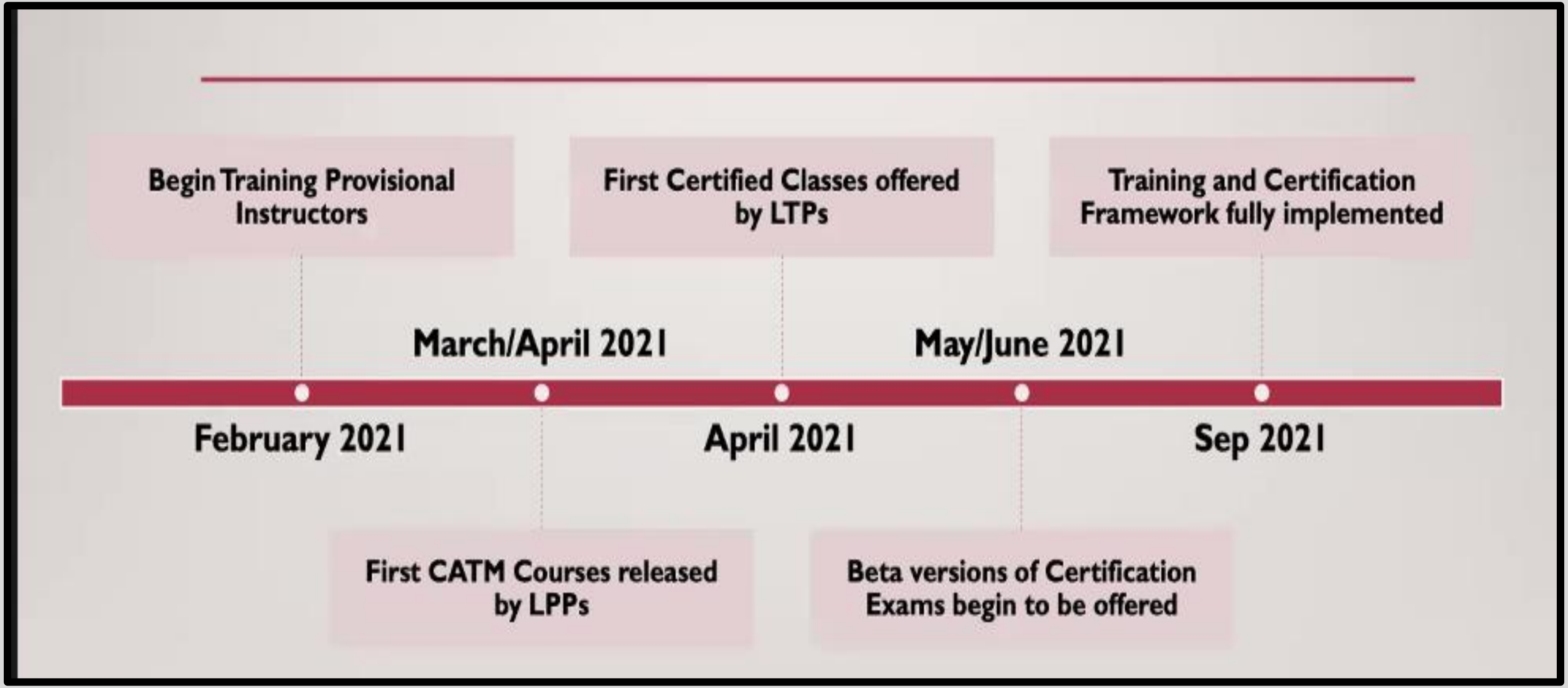
Notes from CMMC-AB Town Hall



CURRENT STATUS OF CREDENTIALS

Credential	December: Total	December : Pending	December: Approved	January Total	January Pending	January Approved
RP	980	511	469	1439	378	1060
RPO	297	46	251	382	43	339
C3PAO	369	349	20	408	355	53
LPP	16	0	16	18	2	16
LTP	0	0	0	22	10	12
Provisional Assessors	100	0	100	100	0	100

Notes from CMMC-AB Town Hall



February 2021

Begin Training Provisional Instructors

March/April 2021

First CATM Courses released by LPPs

April 2021

First Certified Classes offered by LTPs

May/June 2021

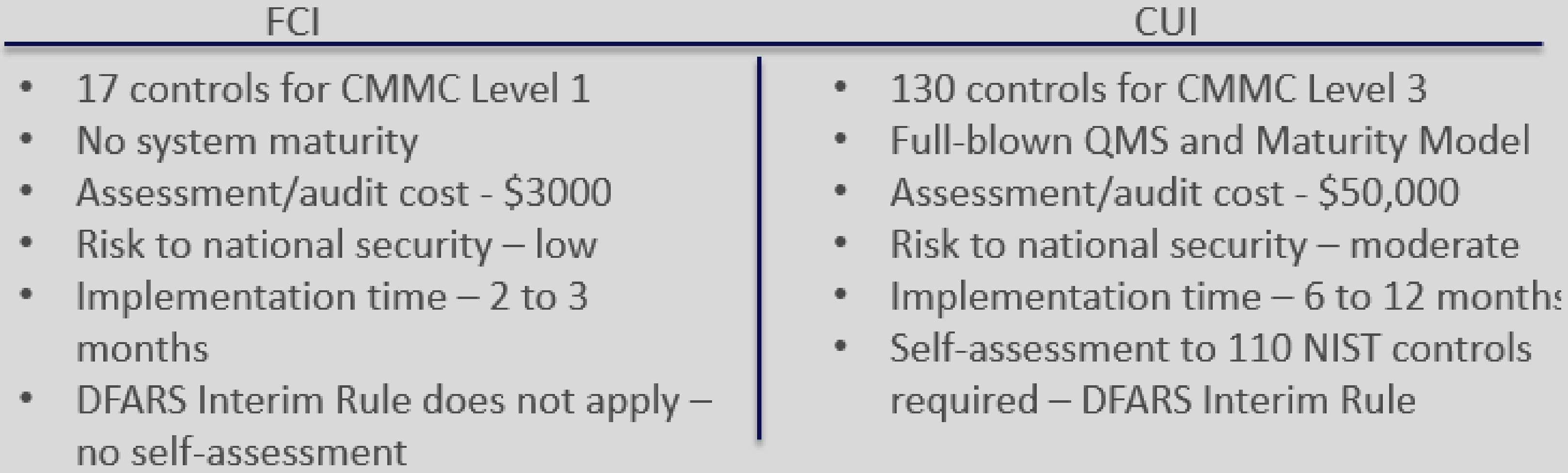
Beta versions of Certification Exams begin to be offered

Sep 2021

Training and Certification Framework fully implemented

CyberChat #1 Review - Data

- Data – cybersecurity regulations are data-driven
  - ✓ FCI – Federal Contract Information = CMMC Level 1
  - ✓ CUI – Controlled Unclassified Information = DFARS 252.204-7012/7019, then CMMC Level 3



FCI

- 17 controls for CMMC Level 1
- No system maturity
- Assessment/audit cost - $3000
- Risk to national security – low
- Implementation time – 2 to 3 months
- DFARS Interim Rule does not apply – no self-assessment

CUI

- 130 controls for CMMC Level 3
- Full-blown QMS and Maturity Model
- Assessment/audit cost - $50,000
- Risk to national security – moderate
- Implementation time – 6 to 12 months
- Self-assessment to 110 NIST controls required – DFARS Interim Rule

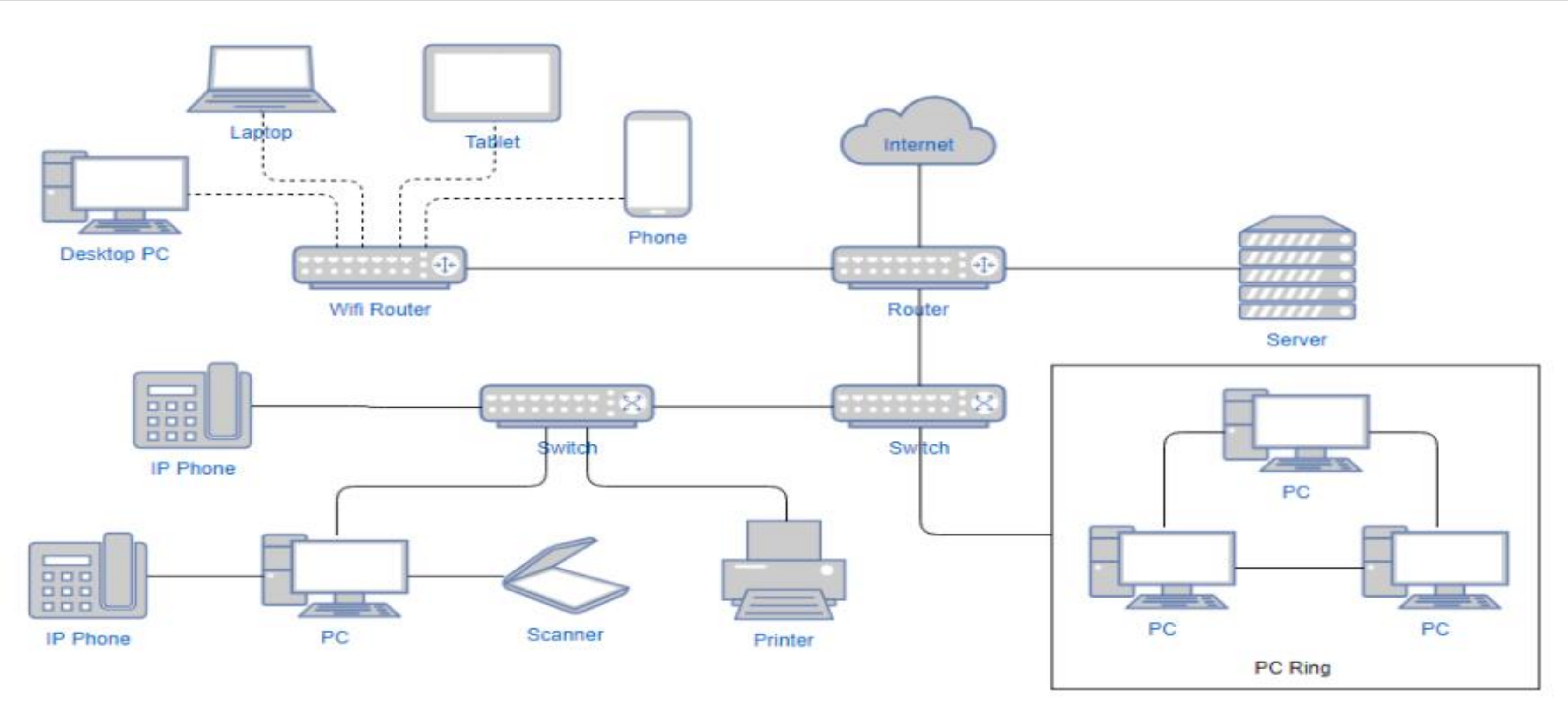
CyberChat #2 Review – Employee Training

- Why do employees need to understand your cybersecurity compliance project?
  - ➢ The majority of cyberattacks target people; e.g., business email compromise [impersonating trusted people] and email account compromise [compromise a victim’s email account and send convincing emails using their credentials]
  - ➢ Employees are your first line of defense against those attacks, so you need their buy-in that the company culture surrounding cybersecurity is changing
  - ➢ They need to understand the project and what might be required of them, including their responsibility for continuous improvement
  - ➢ Prepare them for technical training

CyberChat #2 Review – Employee Training

- Training should cover:
    - ➢ Why changes in cybersecurity culture are needed [can use slides from CyberChat #1 or any other cybernc.us presentation]
        - ✓ Protect national security
        - ✓ DoD regulations
        - ✓ Protect company
    - ➢ Project details
        - ✓ Assess current state – data, IT assets, network, data flow, gap analysis, risk analysis
        - ✓ Implementation phase – filling gaps in controls/practices, establishing policies and procedures, employee technical training
        - ✓ Assessment
        - ✓ Continuous improvement

CyberChat #2 Review - Network Diagram



CyberChat #2 Review - Asset Inventory

- Cloud storage
- Contracts with 3rd party technology suppliers
- Desktop computers
- Digital cameras
- Fax machines
- Scanners
- Keyboards
- Laptops
- Monitors
- Mouse
- Printers
- Routers
- Switches
- Servers
- Smartphones
- Software applications
- Software licenses
- Tablets
- Internet of Things [IoT]
- Cables

Documentation

- As you work through setting up your cybersecurity quality management system, it is a good idea to begin documenting the process.
  - Meetings/work sessions should be documented with attendees, dates, action items – who they are assigned to and due date.
  - Track action items to completion
  - If you want to keep everything in one place, use the CMMC Level 1 in a Box Guide. Tabs can be added to record meetings, actions, etc.
  - Documenting the process will help keep you organized, and the documents can be used as audit “artifacts” – documents that provide proof that you are doing what you said you are doing.

If an activity isn’t documented, it didn’t happen.

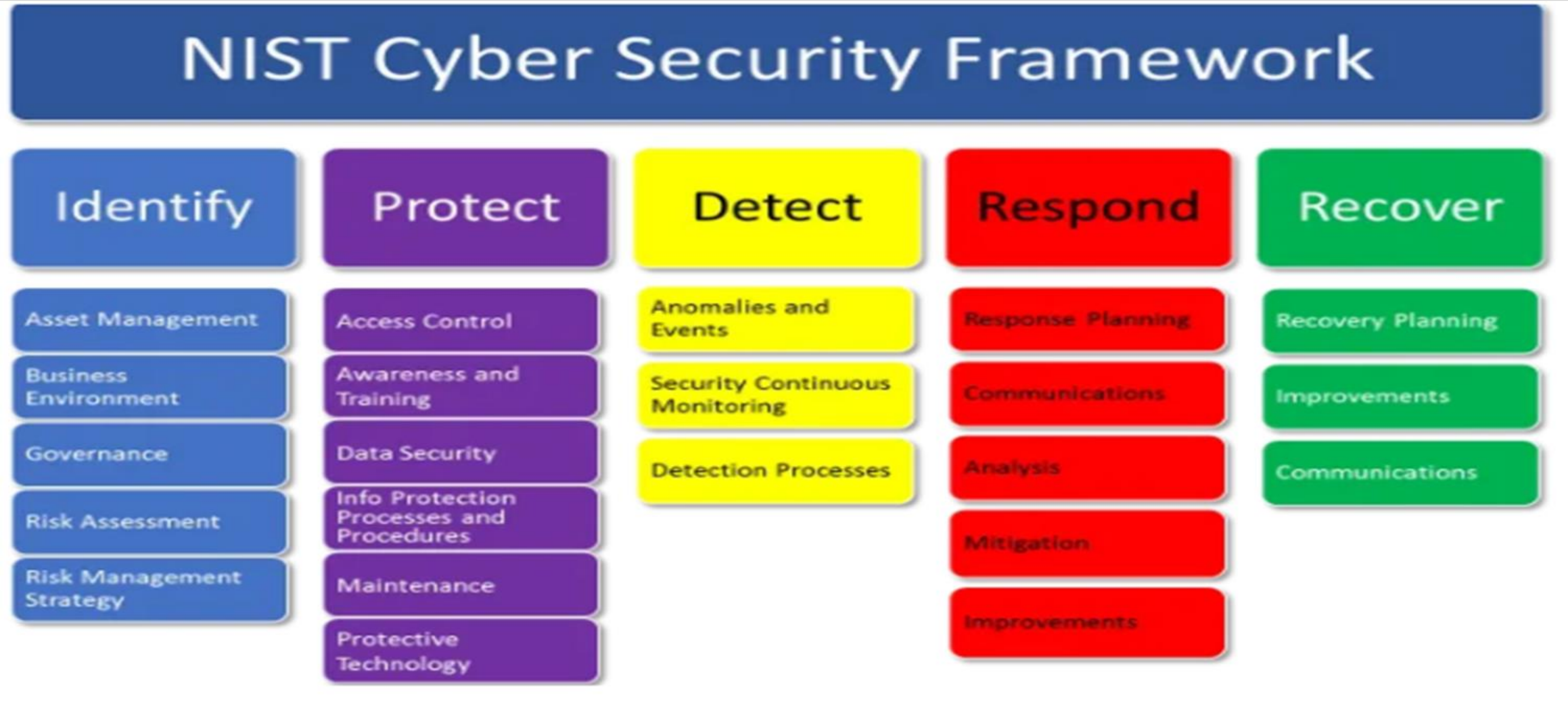
Continuous Improvement

Models

- PDCA – Plan, Do, Check, Act
- Lean
- Six Sigma
- Total Quality Management

“If you can’t measure it, you can’t improve it” – Peter Drucker, Father of Management Thinking

Continuous Improvement



NIST Cyber Security Framework

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

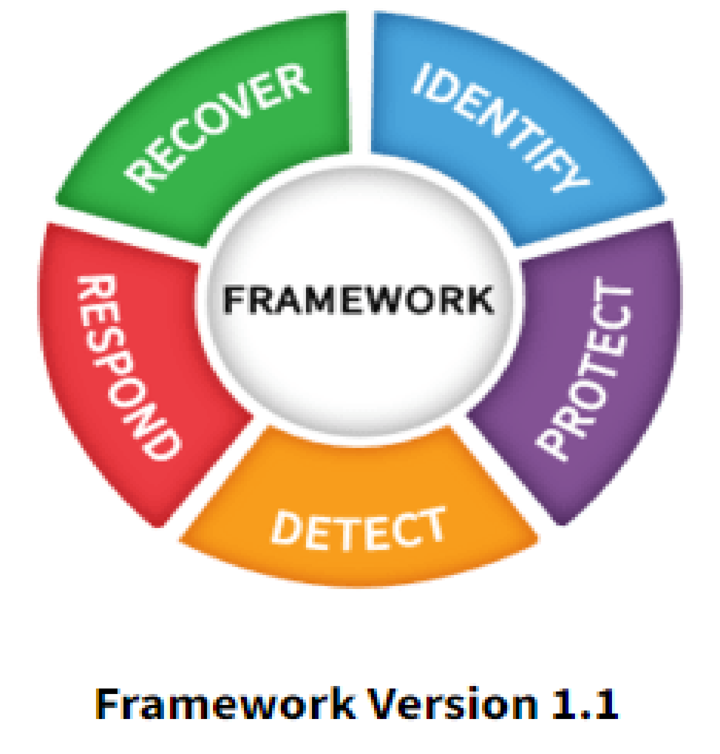
Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

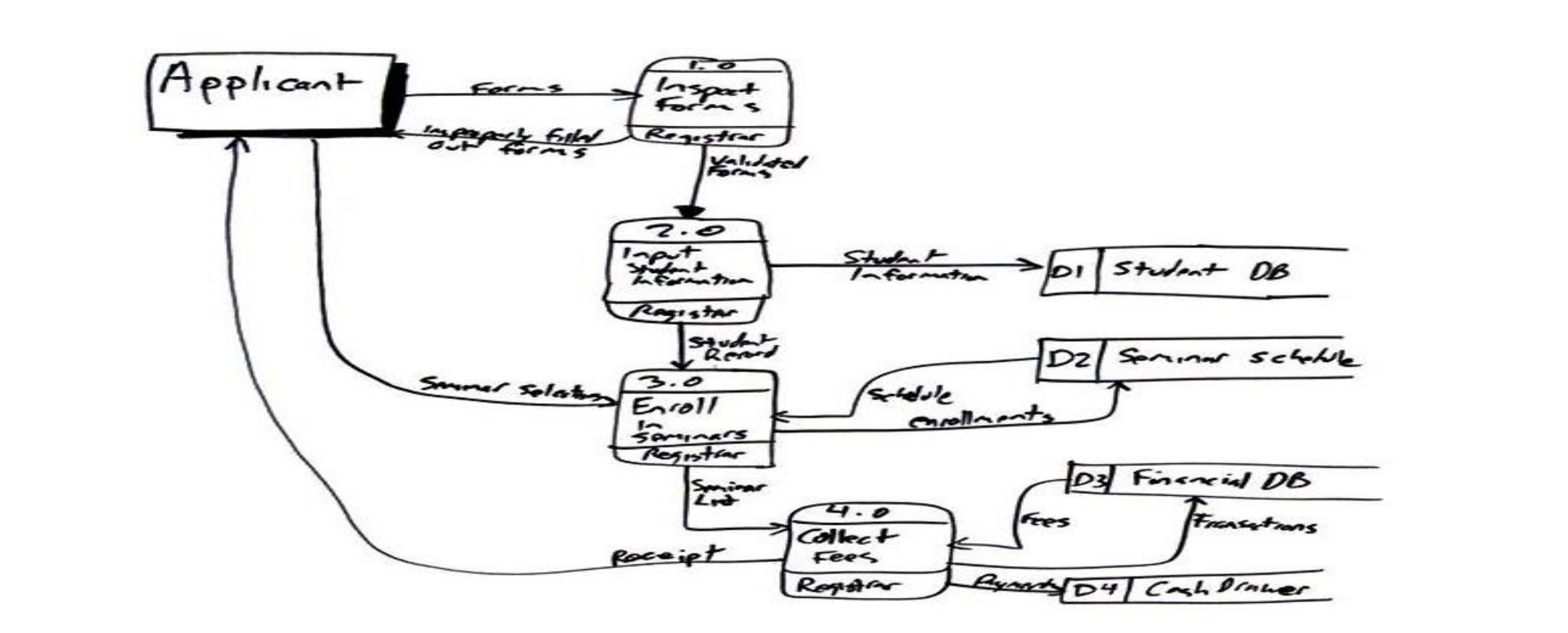
Continuous Improvement



Data Flow Diagram

- Diagram the flow of **DoD data** in your network – from when the data “enters” your network until it flows out of your network. The information may come from the contracting officer, your prime, etc. and may be flowed down to your subs/suppliers.
- No need for a formal diagram. The goal is to know how and where the data flows, is stored, transmitted, etc. and who is handling the data and who has access to the data.
- This exercise is critical to determining to performing a risk analysis and determining “scope”

Data Flow Diagram



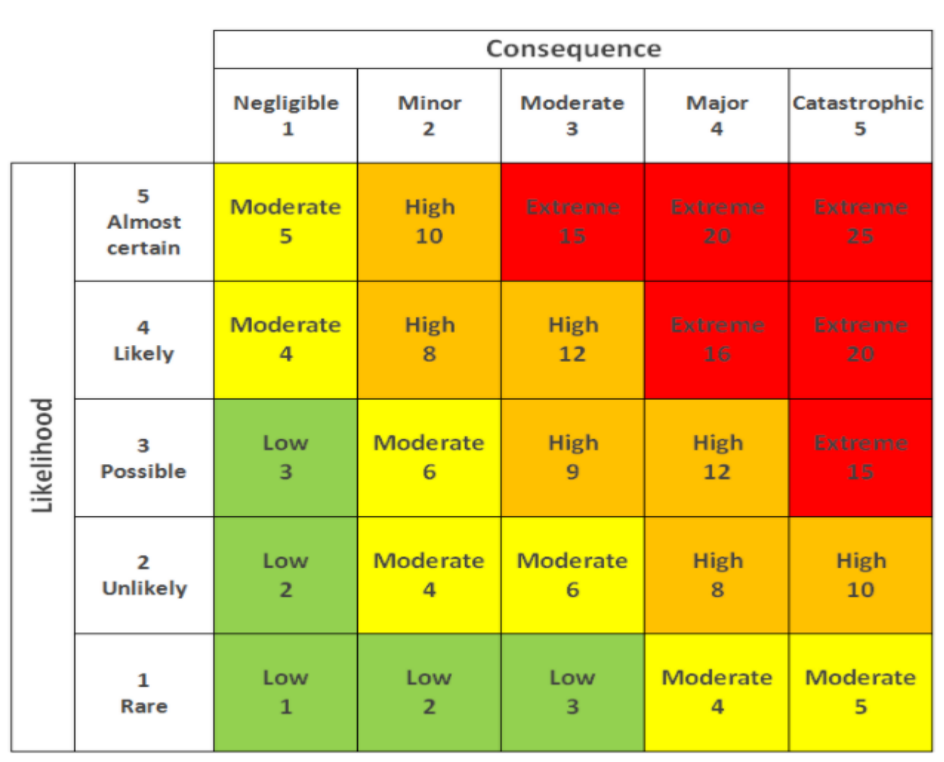
Cybersecurity Risks

Cybersecurity risk is defined as risk to organizational operations, resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT.

In order to perform a risk assessment/analysis we will use our network diagram, data flow diagram, asset inventory and results of employee interactions to help determine our current risk level.

Cybersecurity Risk Assessment

- Need to define your level of risk by considering the likelihood of an event happening and the severity of the consequences (impact to your business) of the resulting consequences.
- ***Need to put time and money into high probability/high impact issues.***



		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Cybersecurity Risks

People Risks

- Ransomware – a form of malware that attempts to encrypt your data then extort a ransom to release an unlock code. Typically delivered via email.
- Phishing – an attempt to gain sensitive information while posing as a trustworthy contact. Typically delivered via email. Spear phishing is a highly targeted attempt to gain information.
- Data leakage via mobile devices – because they are relatively cheap almost everyone has them, making them a target for data thieves.
- Hacking – gaining access to network from outside an organization
- Insider threats – malicious or inadvertent

Cybersecurity Risks

Physical Risks

- Use the House analogy – how can someone physically gain access to my company and therefore my network?
  - ✓ Do I know who has physical access and are they authorized to be there?
  - ✓ Once inside, are there other levels of security to prevent them from unauthorized access?
  - ✓ Is after-hours access controlled?

It is critical that you document and analyze all cybersecurity risks in order to develop a mitigation strategy. Need to put time and money into high probability/high impact issues.

Cybersecurity Risks

Mitigation strategies (controls/practices)

- Staff awareness/training
- Malware/virus protection
- Software updates
- Data backups
- Spam filters
- Use encryption software when using portable storage devices
- Network firewalls
- Least privilege access
- Control the use of portable storage devices – such as flash drives
- Strong, complex passwords/phrases

Policies/procedures (documentation) to back up these controls/practices

Supply Chain Cyber Risk

Requires thorough vetting process of both sides of the supply chain

- Check DUNS
- Review SAM profile
- Check website
- Check references
- Check for negative reviews
- Ask questions
  - What controls are in place to protect the network and data
  - Is the company in working toward compliance with DFARS/CMMC cybersecurity regulations

Cybersecurity Compliance Project Status

- Current State
  - ✓ Review contracts for cybersecurity DFARS clauses
  - ✓ Data – FCI or CUI
  - ✓ Upper management/ownership buy-in
  - ✓ Initial employee training – project introduction
  - ✓ Network Diagram
  - ✓ Asset inventory
  - ✓ Data flow diagram – for DoD data
  - ✓ Risk assessment
  - ○ Gap analysis

Homework – CyberChat #4

1. Perform a cybersecurity risk assessment/analysis (be sure to include supply chain risks)

Remember to document your work!

ncmbc
CONNECTING BUSINESS AND MILITARY

NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP 4

www.cybernc.us

3 February 2021