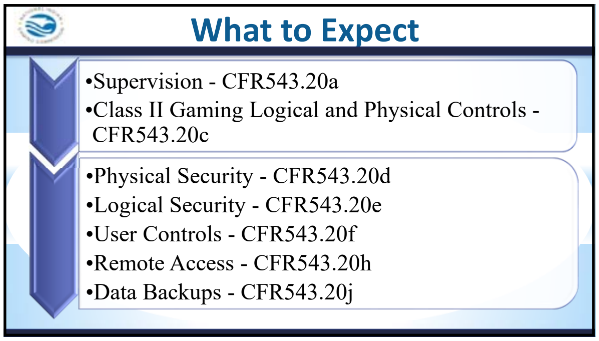
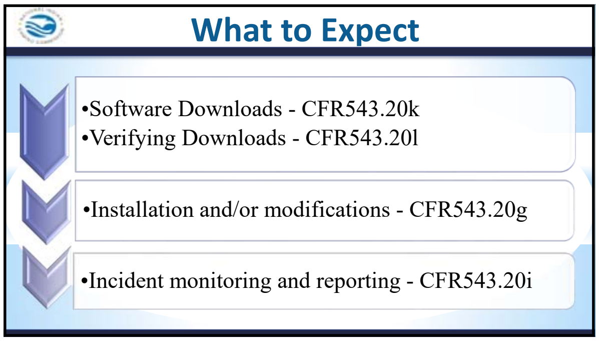
Auditing 543.20

Information Technology Division



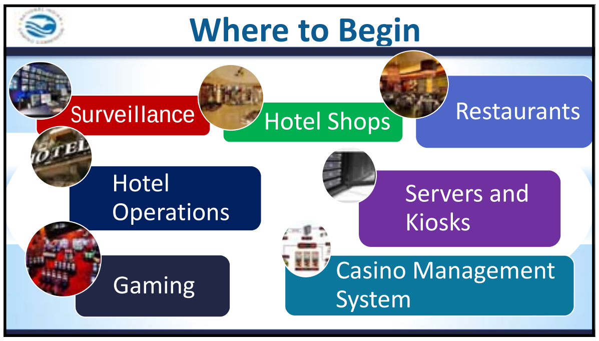
What to Expect

- •Supervision - CFR543.20a
- •Class II Gaming Logical and Physical Controls - CFR543.20c
- •Physical Security - CFR543.20d
- •Logical Security - CFR543.20e
- •User Controls - CFR543.20f
- •Remote Access - CFR543.20h
- •Data Backups - CFR543.20j



What to Expect

- •Software Downloads - CFR543.20k
- •Verifying Downloads - CFR543.20l
- •Installation and/or modifications - CFR543.20g
- •Incident monitoring and reporting - CFR543.20i



Where to Begin

Surveillance

Hotel Shops

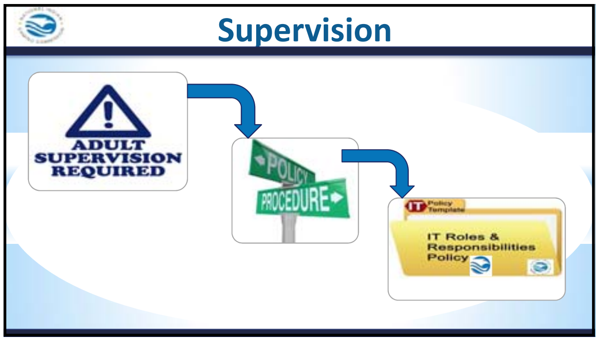
Restaurants

Hotel Operations

Servers and Kiosks

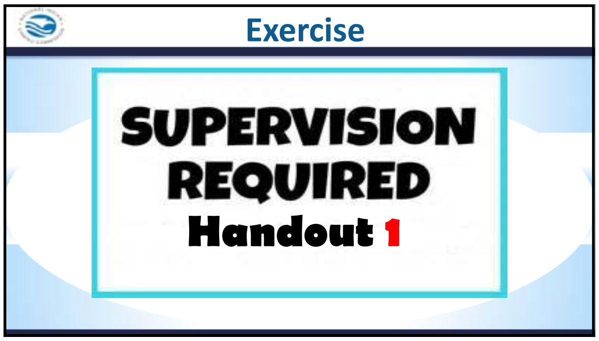
Gaming

Casino Management System



Supervision

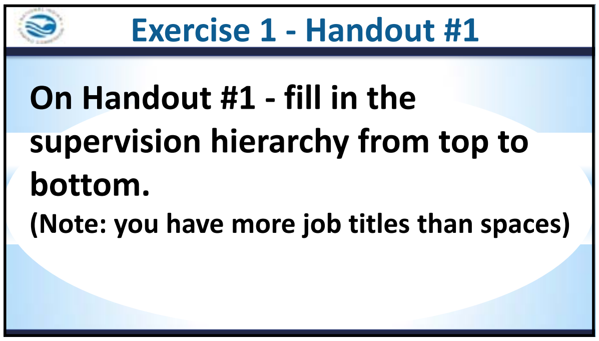
ADULT SUPERVISION REQUIRED
POLICY
PROCEDURE
IT Policy Template
IT Roles & Responsibilities Policy



Exercise

SUPERVISION REQUIRED

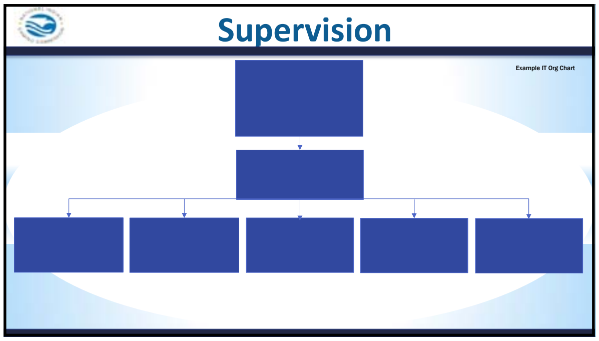
Handout 1



Exercise 1 - Handout #1

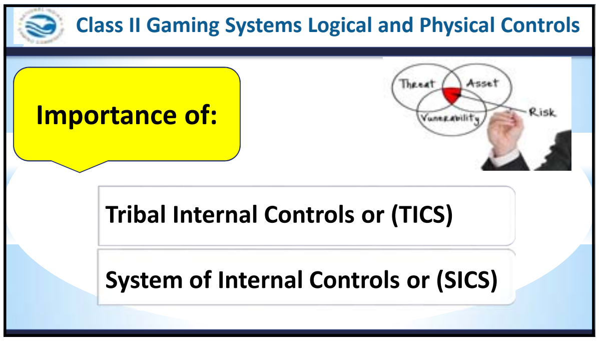
On Handout #1 - fill in the supervision hierarchy from top to bottom.

(Note: you have more job titles than spaces)



Supervision

Example IT Org Chart

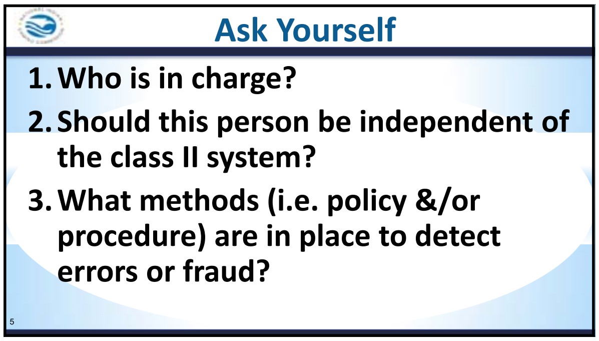


Class II Gaming Systems Logical and Physical Controls

Importance of:

Tribal Internal Controls or (TICS)

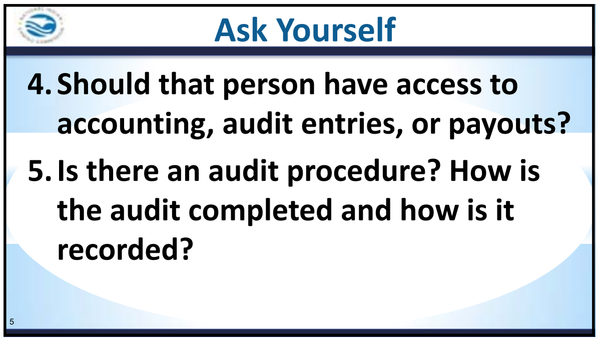
System of Internal Controls or (SICS)



Ask Yourself

1. Who is in charge?
2. Should this person be independent of the class II system?
3. What methods (i.e. policy &/or procedure) are in place to detect errors or fraud?

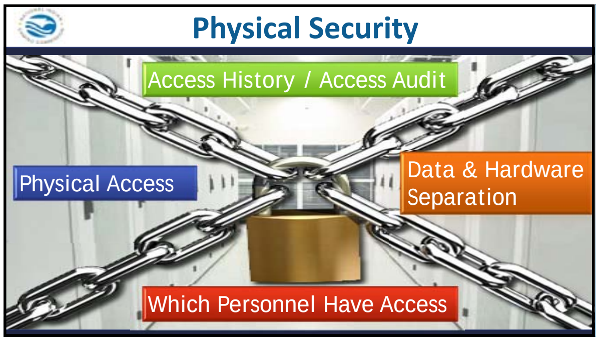
5



Ask Yourself

4. Should that person have access to accounting, audit entries, or payouts?
5. Is there an audit procedure? How is the audit completed and how is it recorded?

5



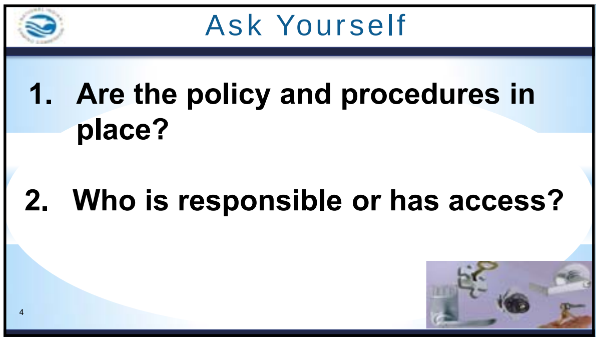
Physical Security

Access History / Access Audit

Physical Access

Data & Hardware Separation

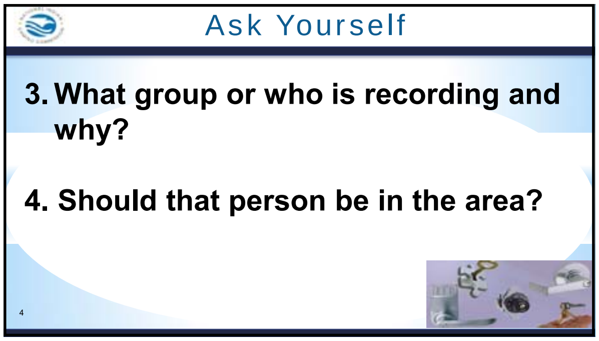
Which Personnel Have Access



Ask Yourself

1. Are the policy and procedures in place?
2. Who is responsible or has access?

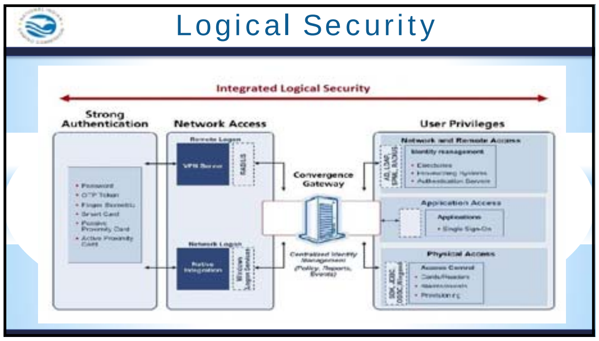
4



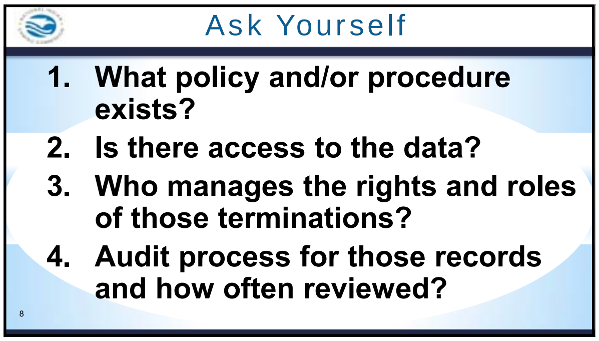
Ask Yourself

3. What group or who is recording and why?
4. Should that person be in the area?

4



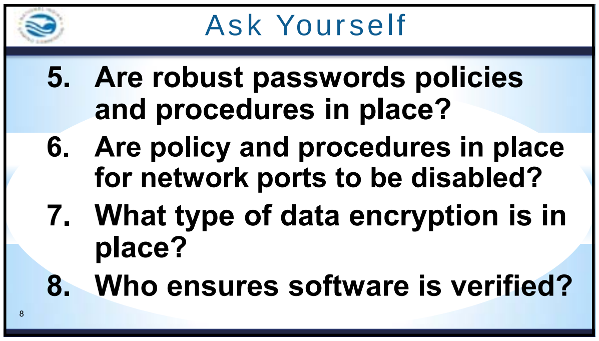
Logical Security



Ask Yourself

1. What policy and/or procedure exists?
2. Is there access to the data?
3. Who manages the rights and roles of those terminations?
4. Audit process for those records and how often reviewed?

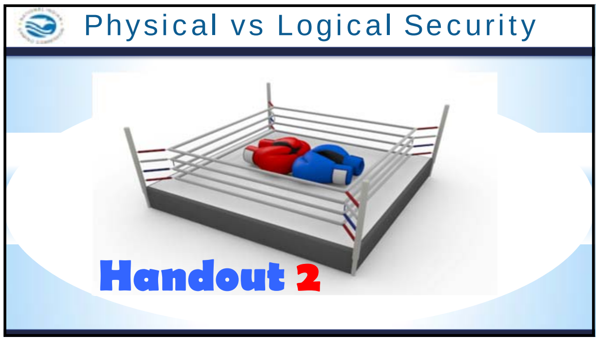
8



Ask Yourself

5. Are robust passwords policies and procedures in place?
6. Are policy and procedures in place for network ports to be disabled?
7. What type of data encryption is in place?
8. Who ensures software is verified?

8



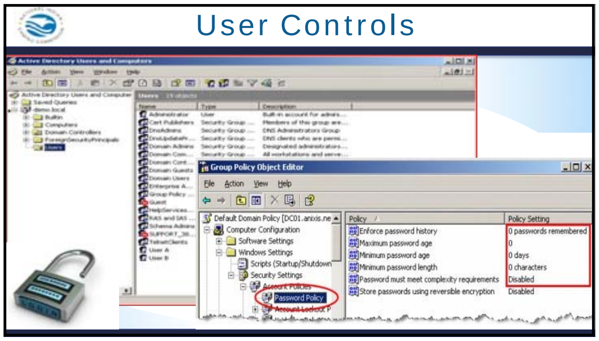
Physical vs Logical Security

Handout 2

INSTRUCTIONS

Using all the terms at the bottom of the handout. Place the terms in the correct column.

User Controls



Active Directory Users and Computers

- Active Directory Users and Computer
  - Saved Queries
  - demo.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Users

Users 19 objects

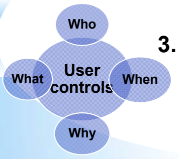
Name	Type	Description
Administrator	User	Built-in account for admin...
Cert Publishers	Security Group ...	Members of this group are...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Com...	Security Group ...	All workstations and serve...
Domain Cont...		
Domain Guests		
Domain Users		
Enterprise A...		
Group Policy ...		
Guest		
HelpServices...		
RAS and IAS ...		
Schema Admins		
SUPPORT_38...		
TelnetClients		
User A		
User B		

Group Policy Object Editor

- Default Domain Policy [DC01.anixis.ne
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Scripts (Startup/Shutdown
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout P

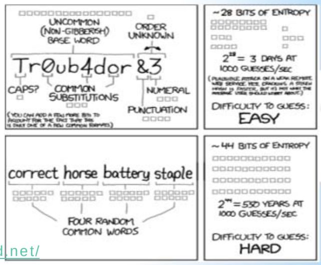
Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Ask Yourself



1. **Who is assigned to control, update or modify system functions?**
2. **Are there roles and responsibilities for controls and are they approved by the TGRA?**
3. **Are user controls recorded with Who, When, Why and What was completed?**

Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD

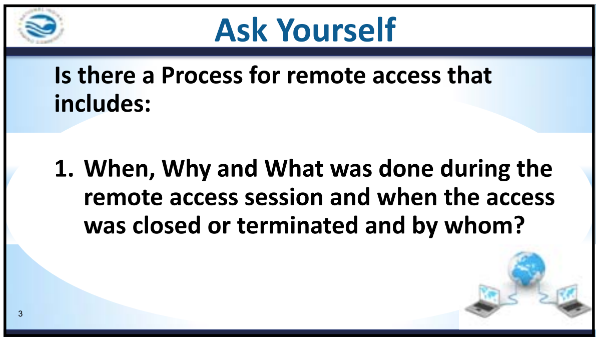
Online password strength checking site:
http://howsecureismypassword.net/

Remote Access

Remote Access

Monthly Logon/Logoff Report

Login	Logout	Group	Computer	Port	Remote IP	Username	Logon Type	Duration
Wed 2017-24-01 03:23:43PM	Wed 2017-24-01 04:25:44PM	Casino Name	DB Server	4025	10.70.158.129	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s
Thur 2017-24-01 03:23:43PM	Thur 2017-24-01 04:25:44PM	Casino Name	DB Server	4076	10.70.158.145	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s
Tue 2017-24-01 03:23:43PM	Tue 2017-24-01 04:25:44PM	Casino Name	DB Server	5284	10.70.158.121	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s

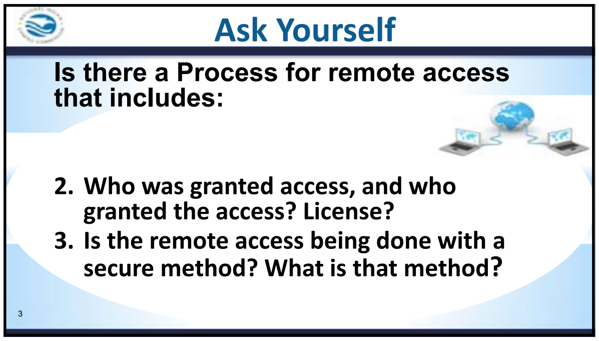


Ask Yourself

Is there a Process for remote access that includes:

1. When, Why and What was done during the remote access session and when the access was closed or terminated and by whom?

3



Ask Yourself

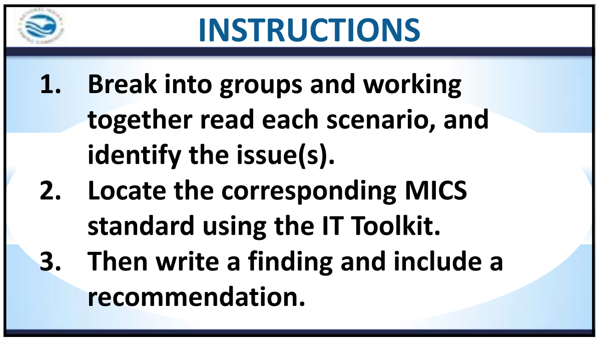
Is there a Process for remote access that includes:

2. Who was granted access, and who granted the access? License?
3. Is the remote access being done with a secure method? What is that method?

3

Exercise 3 – Handout #3

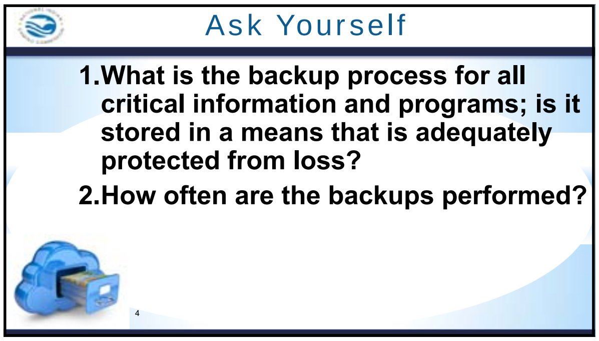
Handout 3



INSTRUCTIONS

1. Break into groups and working together read each scenario, and identify the issue(s).
2. Locate the corresponding MICS standard using the IT Toolkit.
3. Then write a finding and include a recommendation.

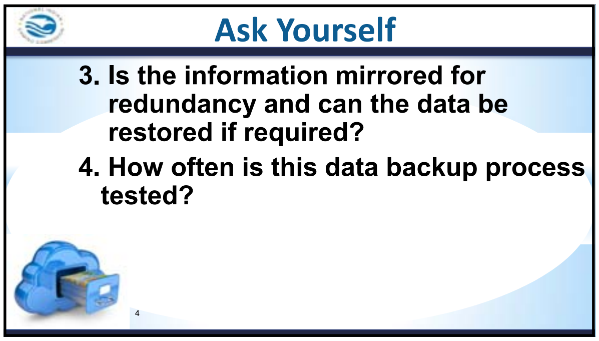
Data Backup



Ask Yourself

1. What is the backup process for all critical information and programs; is it stored in a means that is adequately protected from loss?
2. How often are the backups performed?

4

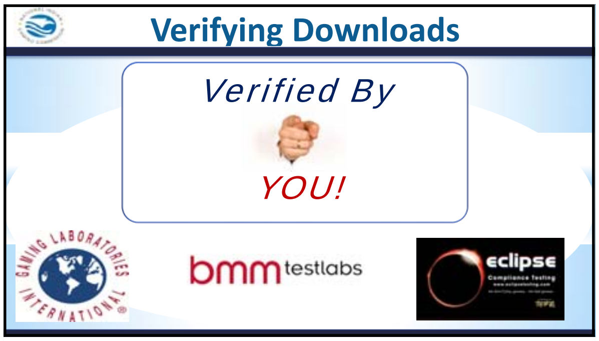


Ask Yourself

3. Is the information mirrored for redundancy and can the data be restored if required?
4. How often is this data backup process tested?

4

Software Downloads



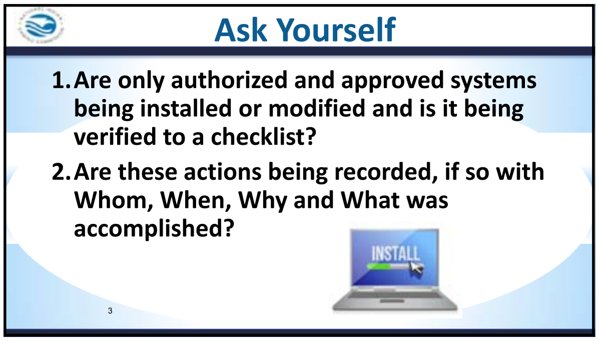
Verifying Downloads

Verified By

YOU!

GAMING LABORATORIES INTERNATIONAL
bmm testlabs
eclipse
Compliance Testing

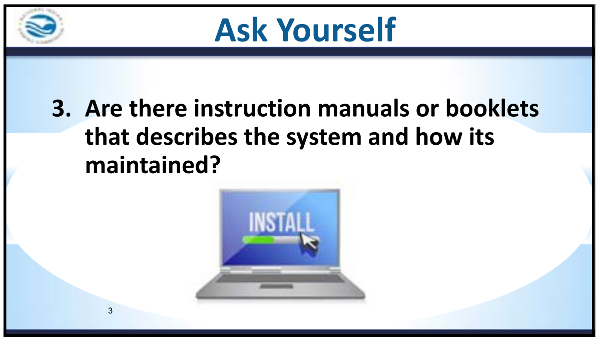
Installations &/or Modifications



Ask Yourself

1. Are only authorized and approved systems being installed or modified and is it being verified to a checklist?
2. Are these actions being recorded, if so with Whom, When, Why and What was accomplished?

3

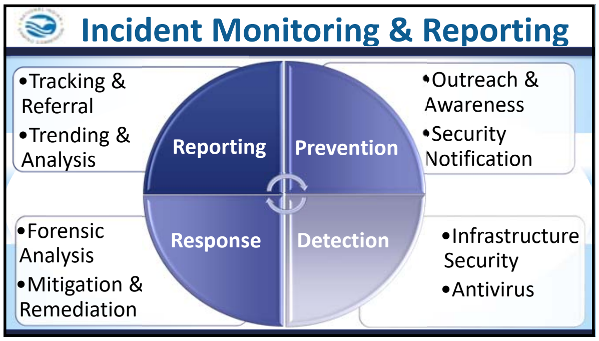


Ask Yourself

3. Are there instruction manuals or booklets that describes the system and how its maintained?

3

Incident Monitoring & Reporting



- Tracking & Referral
- Trending & Analysis

- Outreach & Awareness
- Security Notification

- Forensic Analysis
- Mitigation & Remediation

- Infrastructure Security
- Antivirus

Ask Yourself

1. What are the policies and/or procedures for responding to, monitoring, investigating and resolving all security incidents that is approved by the TGRA?
2. What time period has been established with the TGRA for supporting documentation to be supplied?

2

Questions

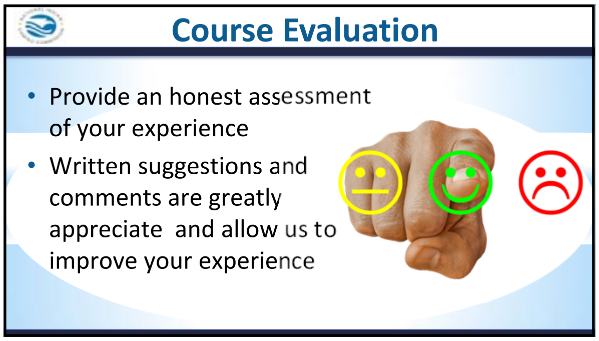
Tim Cotton
IT Auditor
timothy_cotton@nigc.gov

Jeran Cox
IT Auditor
jeran_cox@nigc.gov

Michael Curry
IT Auditor
michael_curry@nigc.gov

Sean Mason
IT Auditor
sean_mason@nigc.gov

Travis Waldo
Director, IT
travis_waldo@nigc.gov



Course Evaluation

- Provide an honest assessment of your experience
- Written suggestions and comments are greatly appreciate and allow us to improve your experience