

Auditing 543.20



Information Technology Division

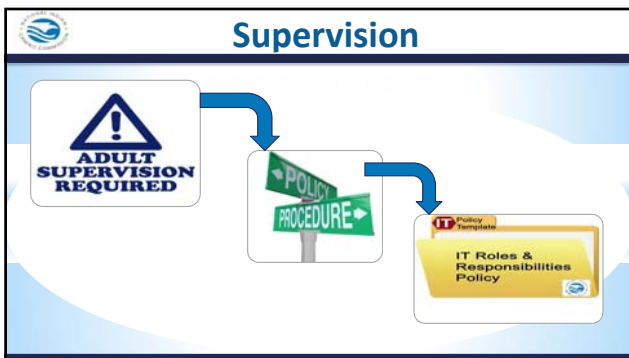
What to Expect

- 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

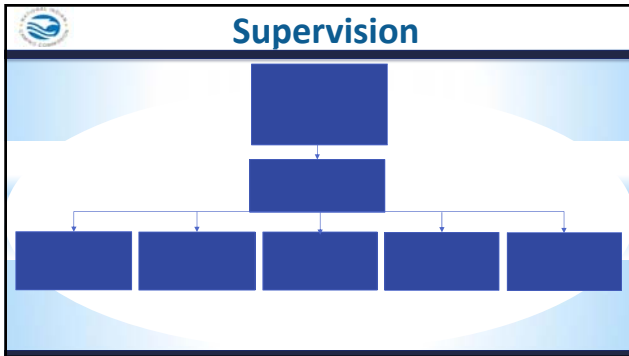
- Software Downloads - CFR543.20k
- Verifying Downloads - CFR543.20l
- Installation and/or modifications - CFR543.20g
- Incident monitoring and reporting - CFR543.20i





Exercise 1 - Handout #1

On Handout #1 - fill in the supervision hierarchy from top to bottom.
(Note: you have more job titles than spaces)



Class II Gaming Systems Logical and Physical Controls

Importance of:


- Tribal Internal Controls or (TICS)
- System of Internal Controls or (SICS)

A Venn diagram with four overlapping circles labeled "Threat", "Asset", "Vulnerability", and "Risk". A hand is shown pointing to the intersection of "Threat" and "Asset".

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

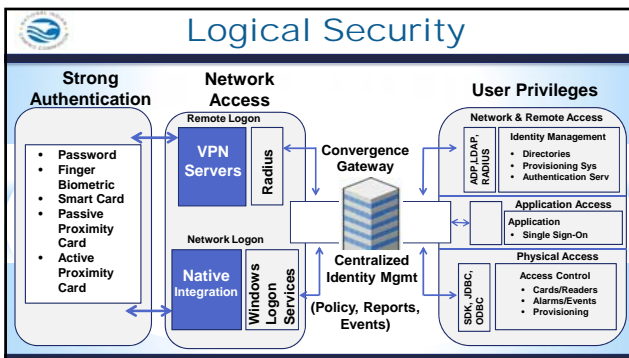
Ask Yourself

3. What group or who is recording and why?

4. Should that person be in the area?




4



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

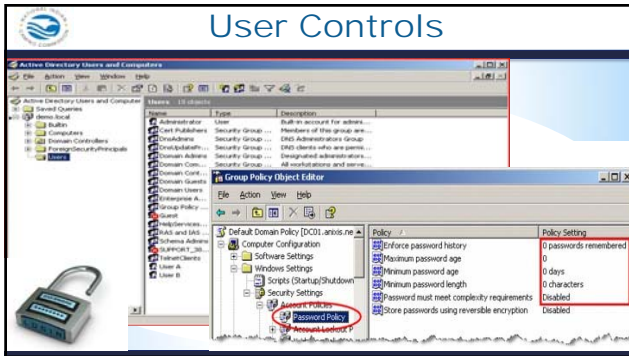
 Exercise #2 - Handout 2



Handout 2

 INSTRUCTIONS

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



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

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

00000000000000000000 UNCOMMON (NON-GIBBERISH) SINGLE WORD Troub4dor & 3 CAPS? COMMON SUBSTITUTIONS NUMERALS PUNCTUATION <small>(Why don't you try a password like 'Tr0ub4dor&3' to see how it fares?)</small>	~26 BITS OF ENTROPY 2 ²⁶ = 3 DAYS AT 1000 GUESSES/SEC. (Assuming you can guess a new password every 10 seconds and you have a 1000-guess-per-second limit.) DIFFICULTY TO GUESS: EASY
correct horse battery staple FOUR RANDOM COMMON WORDS	~41 BITS OF ENTROPY 2 ⁴¹ = 530 YEARS AT 1000 GUESSES/SEC. DIFFICULTY TO GUESS: HARD

Source: <https://kkcd.com/936/>



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	VendorName 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	VendorName 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	VendorName 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

A slide titled "Ask Yourself" with a question about remote access processes. It includes a small icon of a globe and laptops at the bottom right.

 **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

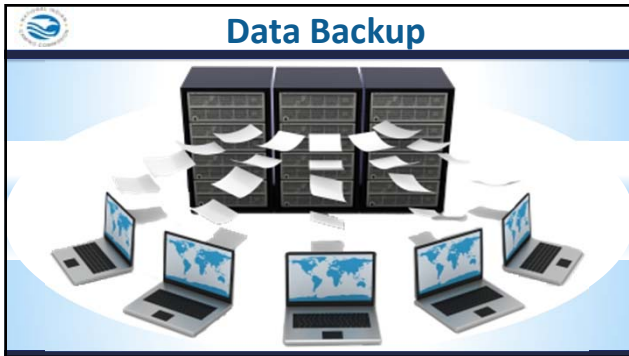
 **Exercise 3 – Handout #3**

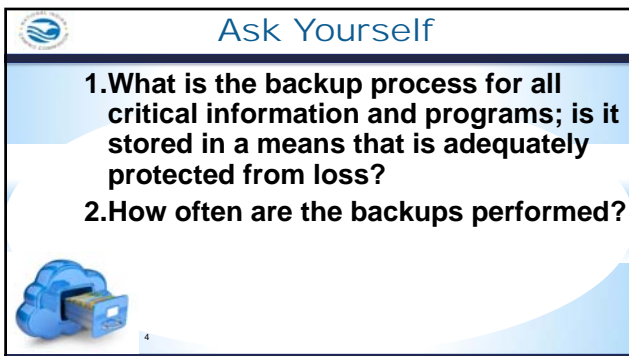
Handout 3

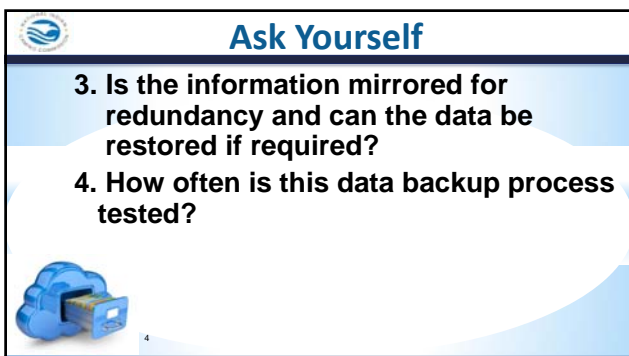


 **INSTRUCTIONS**

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.







 **Software Downloads**



 **Verifying Downloads**

Verified By




YOU!


 **Installations &/or Modifications**

<p>Casino Management System</p> 	<p>Surveillance</p> 
<p>Hotel Shops</p> 	<p>Hospitality</p> 


 **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

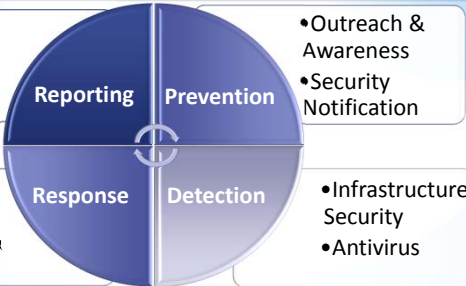
 **Ask Yourself**

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




3


 **Incident Monitoring & Reporting**




- Tracking & Referral
- Trending & Analysis
- Forensic Analysis
- Mitigation & Remediation
- Outreach & Awareness
- Security Notification
- 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



Knowledge Review - IT-109 Auditing to 543.20
When survey is active, respond at PollEv.com/nigc

0 surveys done
0.0 surveys underway

Start the presentation to get the content, follow the content until the end of the slide or PollEv's message

