Auditing 543.20

NIGC Information Technology Division

National Indian Gaming Commission

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

- 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

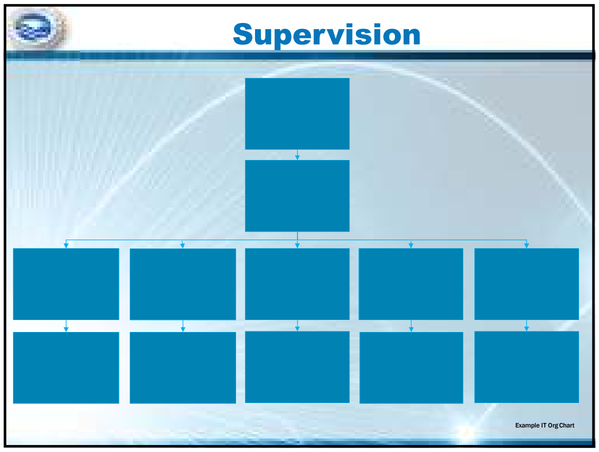
Supervision

ADULT
SUPERVISION
REQUIRED
POLICY
PROCEDURE
IT
IT Roles &
Responsibilities
Policy

Supervision

SUPERVISION REQUIRED

Handout 1



Supervision

Example IT Org Chart

Class II Gaming Systems Logical and Physical Controls

Importance Of :

Tribal Internal Controls or (TICS)

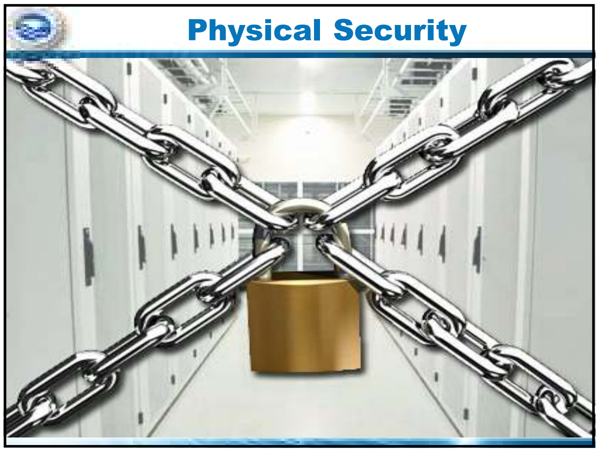
System of Internal Controls or (SICS)

Threat
Asset
Vulnerability
Risk

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) is in place to detect errors or fraud?
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?

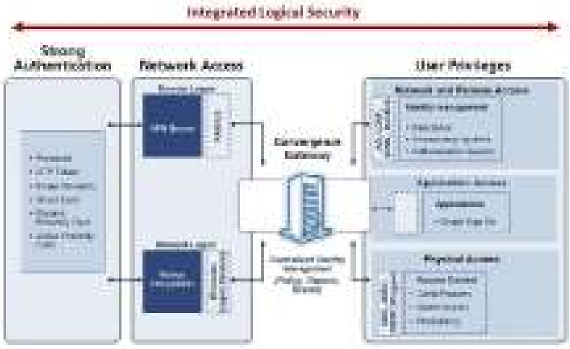
Physical Security



Ask Yourself

1. Are there policy and procedures in place for Physical Security?
2. Who is responsible or have access to IT with, keys, cards, fobs?
3. What group or who is recording those that access the area and why?
4. Should that person be in the area and are the credentials of non- employee/venders checked before access is granted?

Logical Security

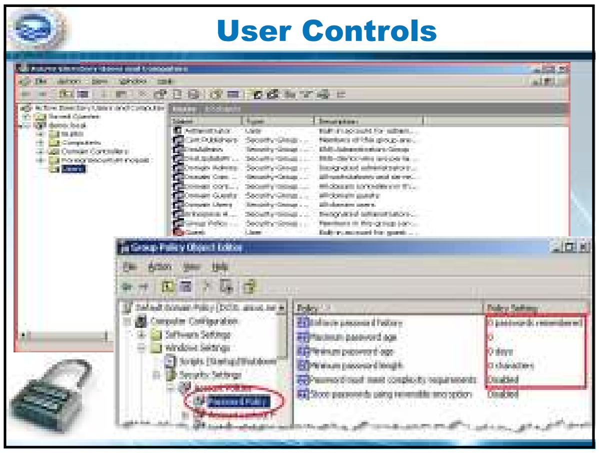


Ask Yourself

1. What policy and/or procedure exist for storage or recovery of media?
2. Is there access to the data, where is it logged, how often and by whom?
3. When an employee is terminated/leaves, who manages the rights and roles of those terminations? Also are there date restrictions?
4. What is the audit process for those records and how often are they reviewed?
5. Are robust passwords policies and procedures in place and what timeframe is set for them to be changed?
6. Are there policy and procedures in place for network ports on and off the floor to be disabled when not in use?
7. What type of data encryption is in place, if any?
8. Who ensures software is verified from the vendor(s)?

Physical vs Logical Security

User Controls

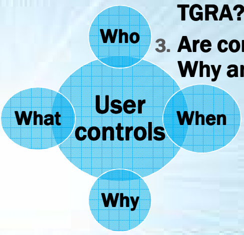

Group Policy Object Editor

- Default Domain Policy [DC01.abcut.loc
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Password Policy

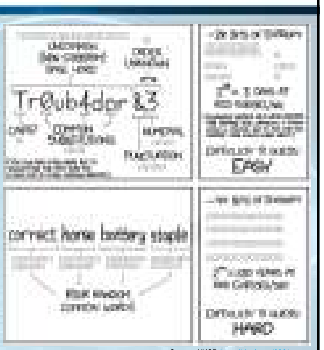
Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Ask Yourself

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



Passwords


Tr0ub4dor &3
Difficulty to guess: EASY
correct horse battery staple
Difficulty to guess: HARD

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

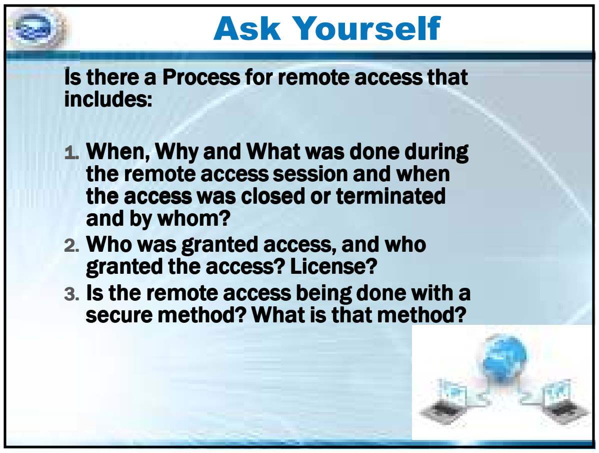
Source: XKCD https://xkcd.com/936/

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
Mon 2017-24-01 03:23:43PM	Mon 2017-24-01 04:25:44PM	Casino Name	DB Server	3845	10.70.158.102	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s



Ask Yourself

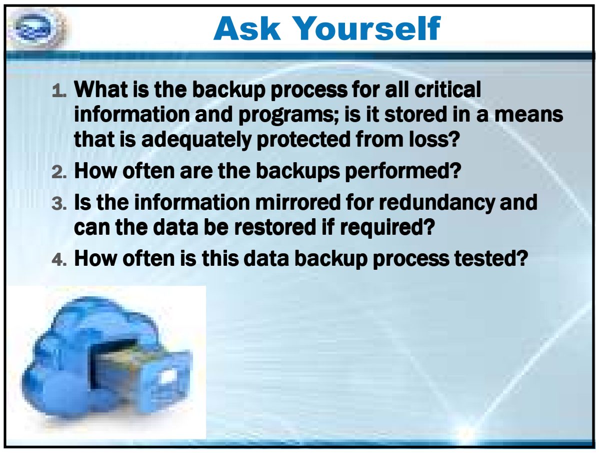
Is there a Process for remote access that includes:

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

Remote Access - Exercise

Handout 4

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

Software Downloads

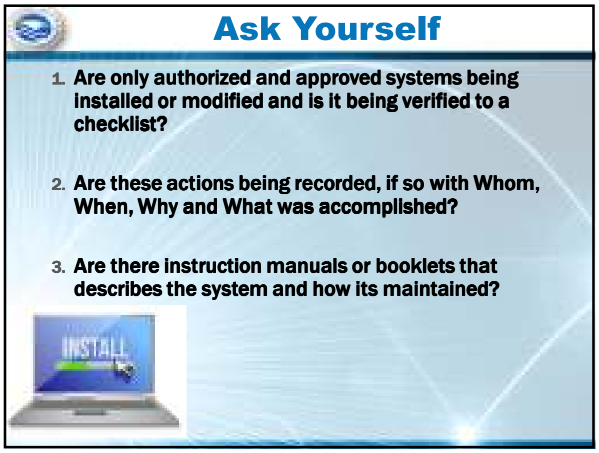
Verifying Downloads

Verified By

YOU!

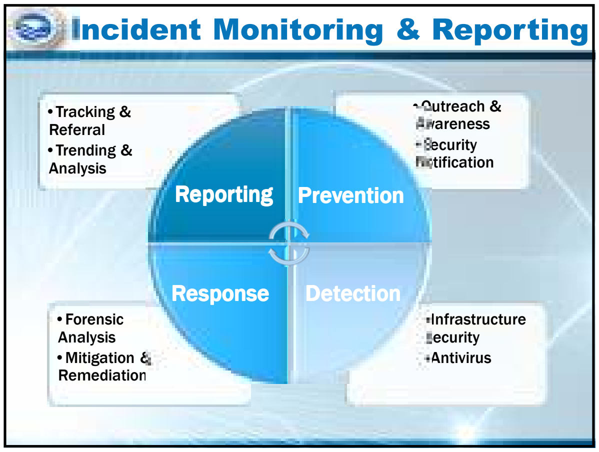
GAMING LABORATORIES INTERNATIONAL
bmm testlabs
eclipse

Installation &/or Modifications

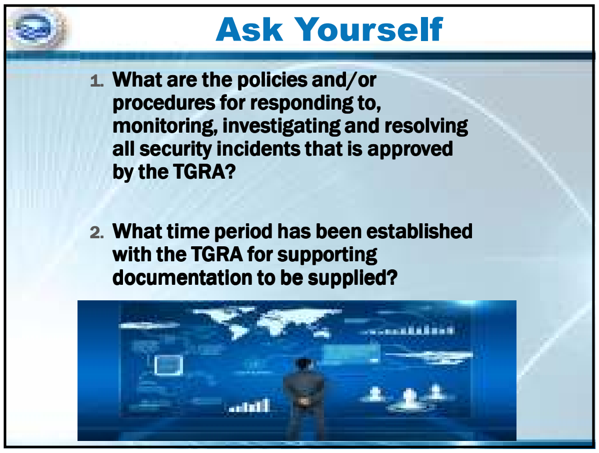


Ask Yourself

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



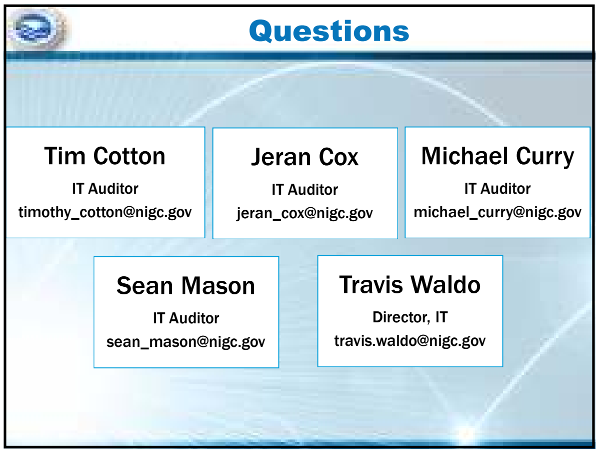
Incident Monitoring & Reporting



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?



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	