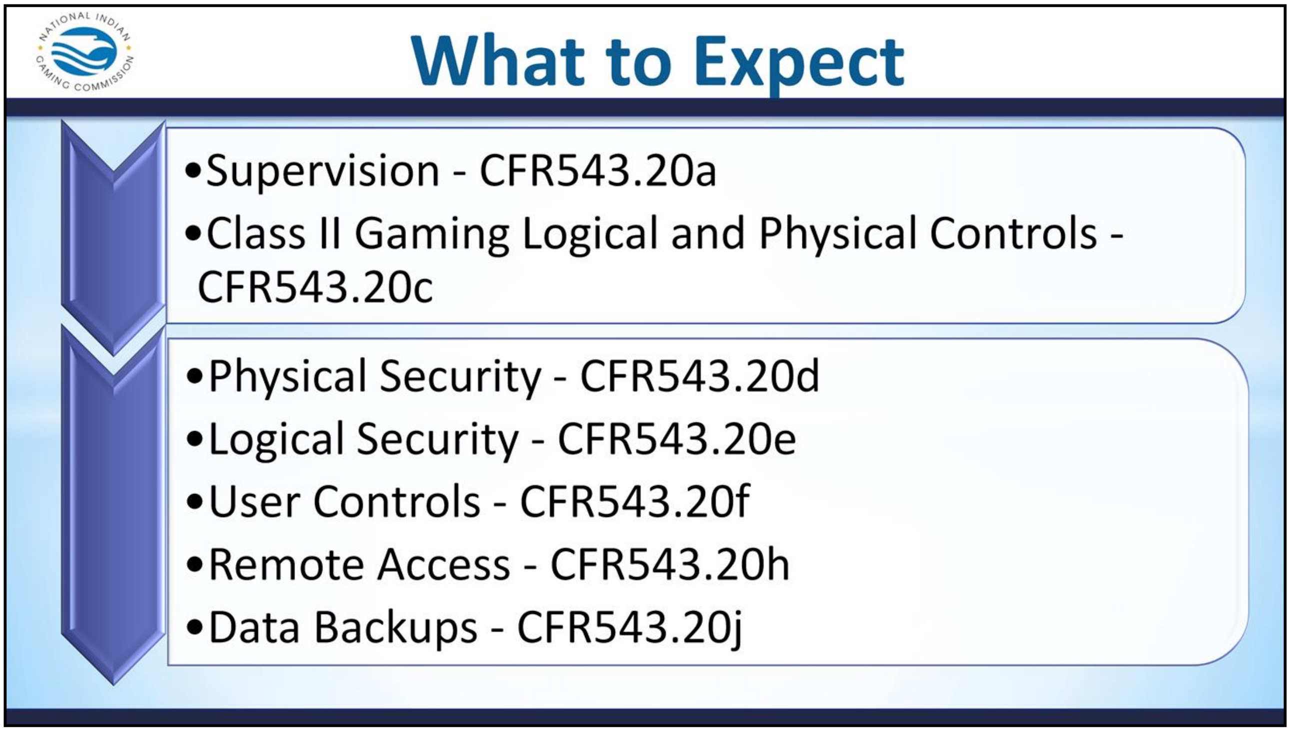
IT-109 Auditing 543.20

Information Technology Division

KEY POINTS

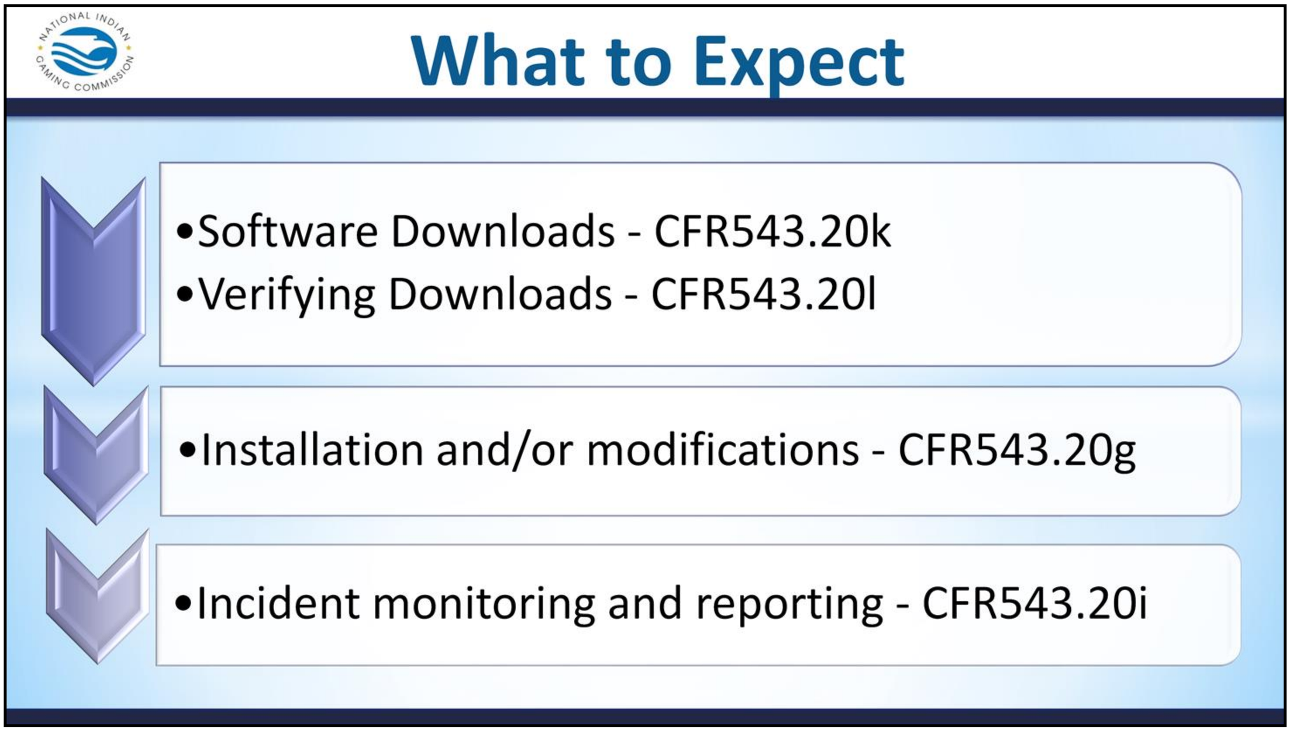


What to Expect

- 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

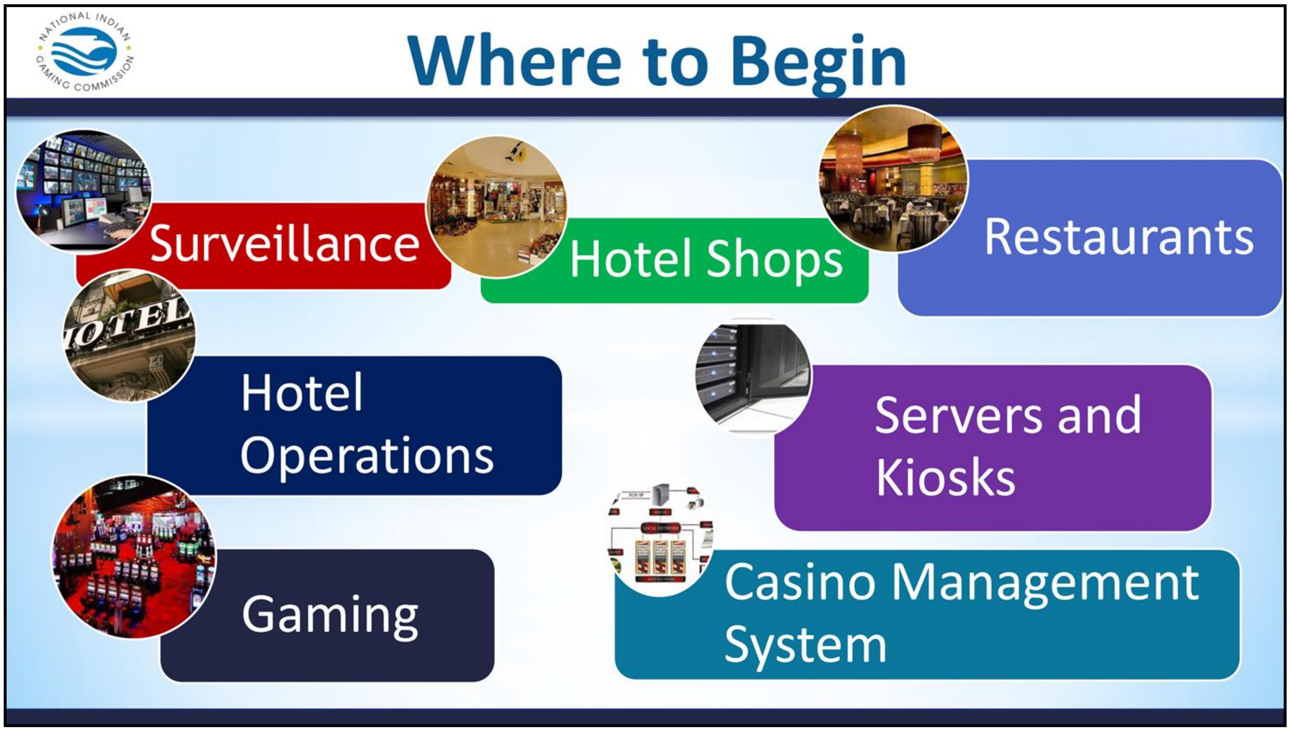
KEY POINTS



What to Expect

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

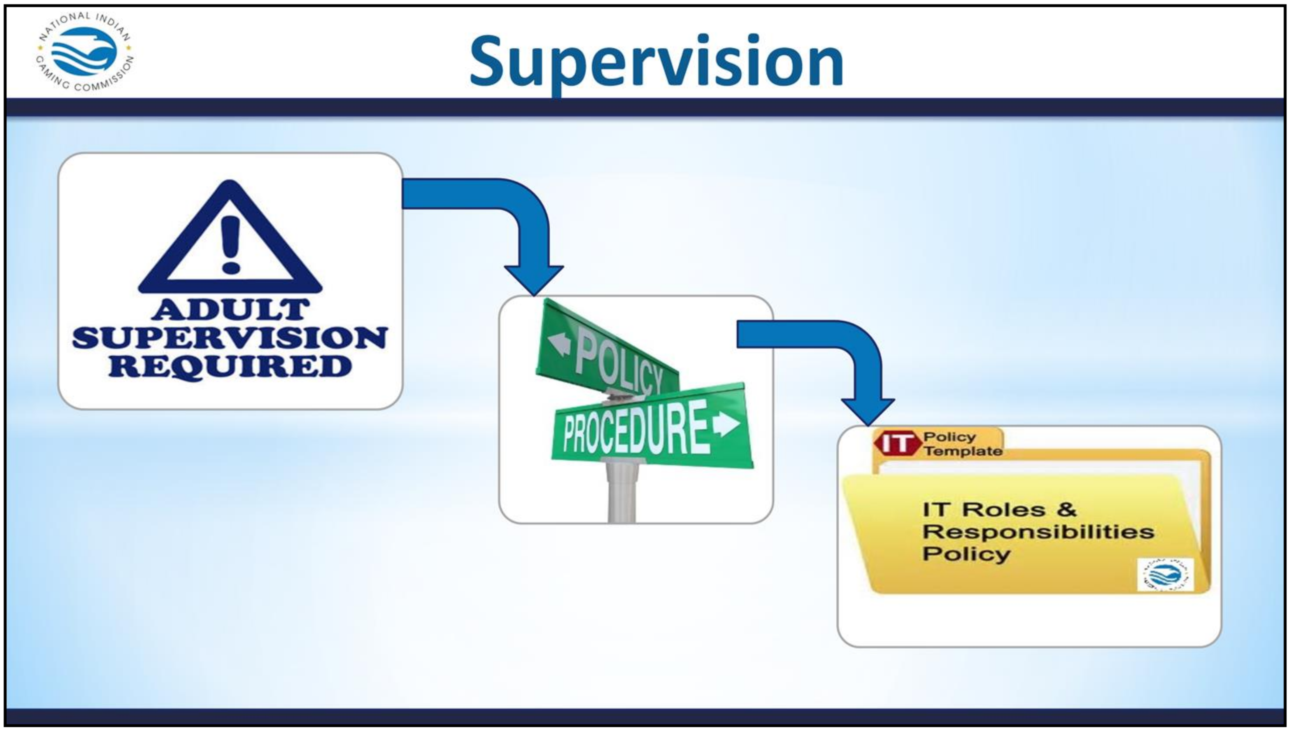
KEY POINTS



Where to Begin

- Surveillance
- Hotel Shops
- Restaurants
- Hotel Operations
- Servers and Kiosks
- Gaming
- Casino Management System

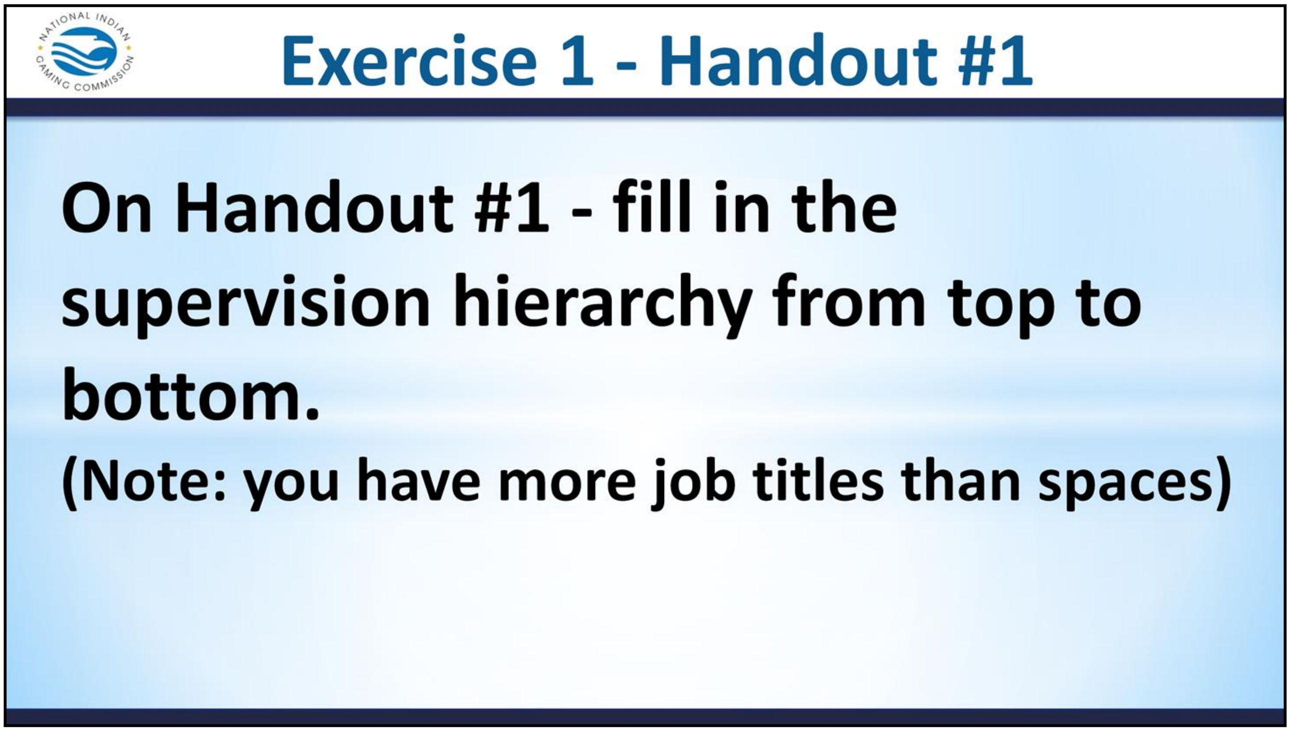
KEY POINTS



Supervision

KEY POINTS

- Supervision includes – the action or process of watching and directing what someone does or how something is done. IT supervision ensures you have:
  - Policy and Procedures
  - IT Roles and Responsibilities
- Common Policy and Procedures:
- IT Roles and Responsibilities

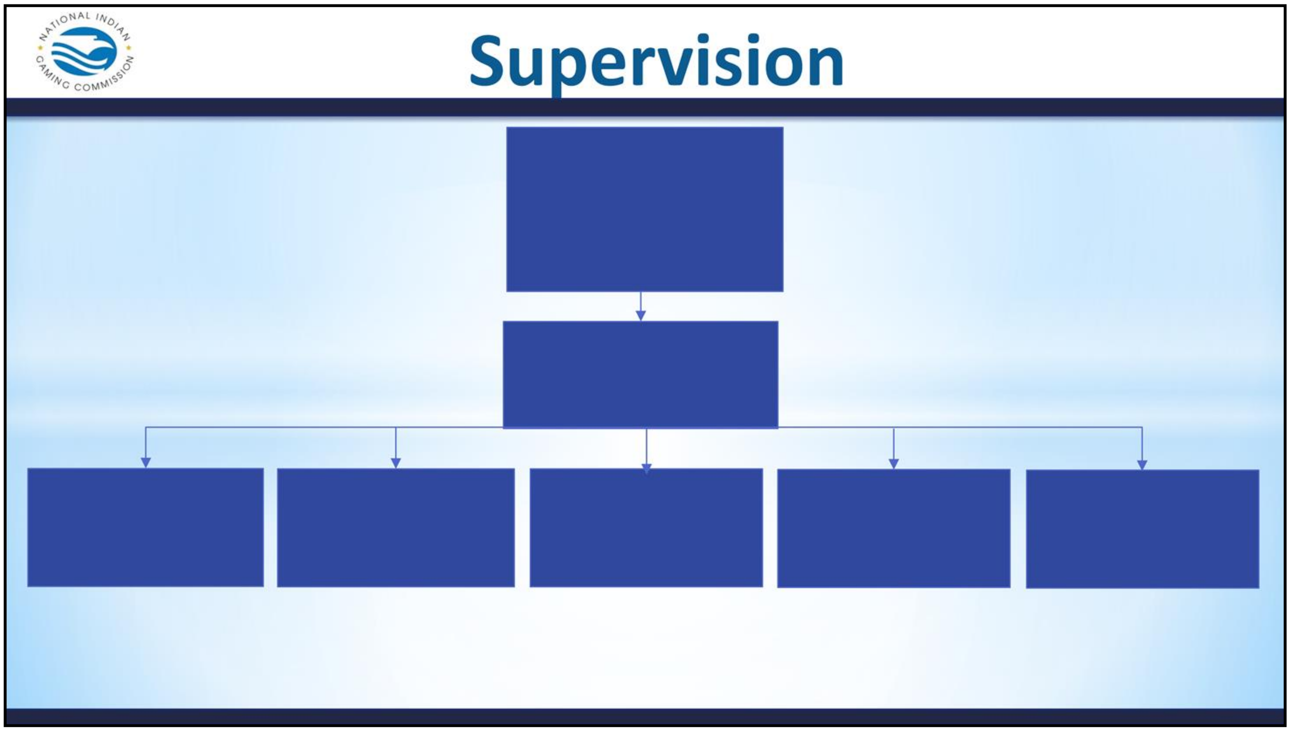


Exercise 1 - Handout #1

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

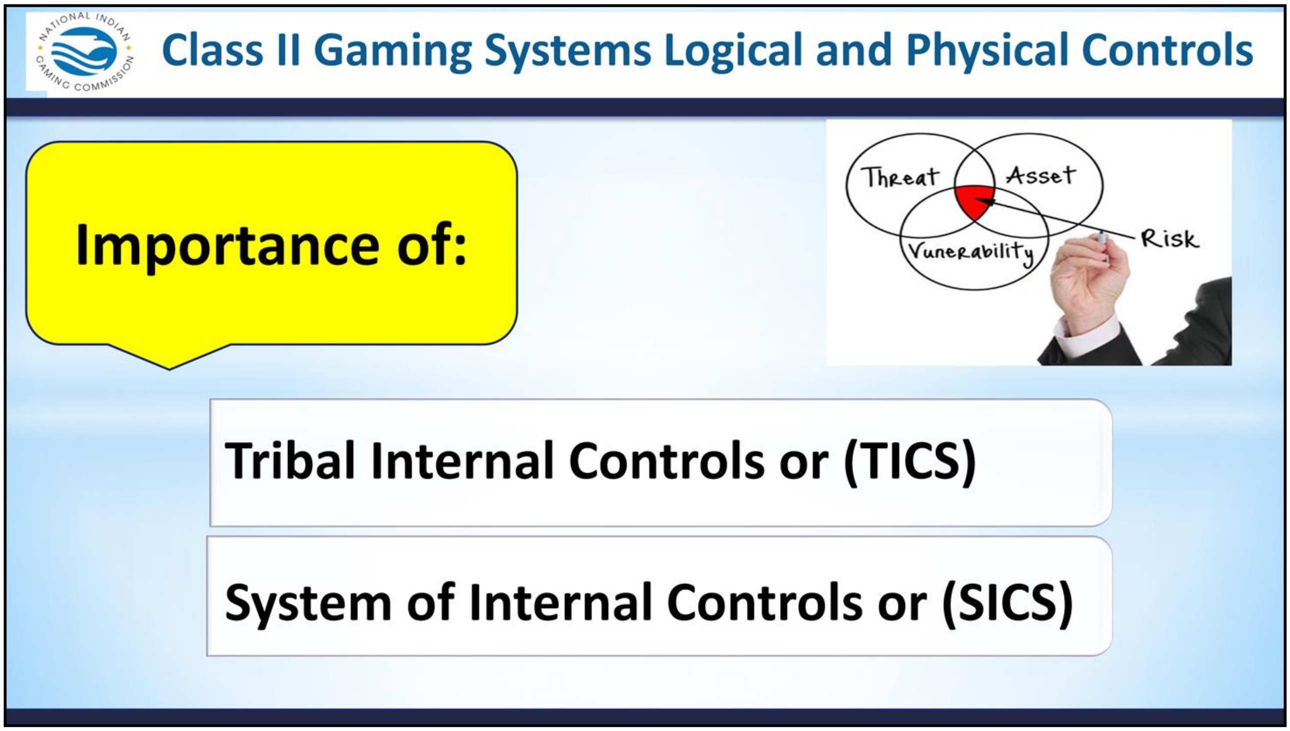
(Note: you have more job titles than spaces)

KEY POINTS



Supervision

KEY POINTS



Class II Gaming Systems Logical and Physical Controls

Importance of:

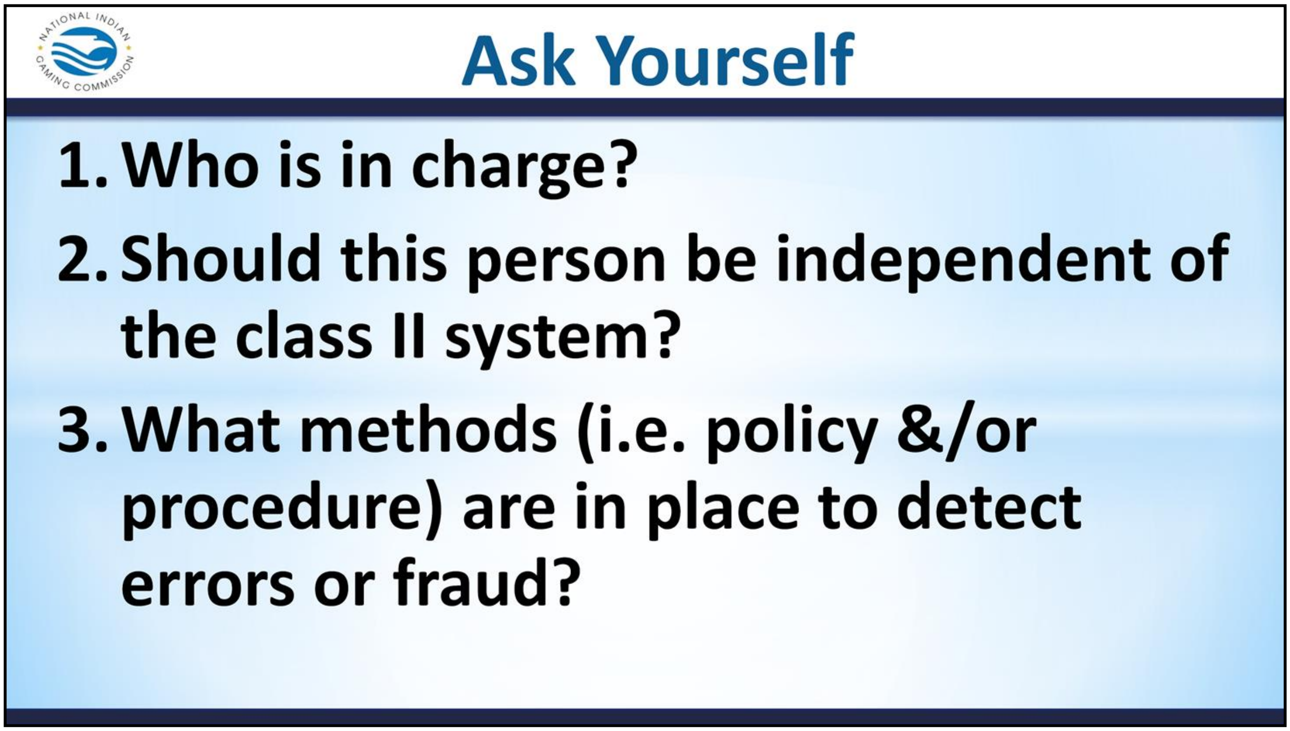
Tribal Internal Controls or (TICS)

System of Internal Controls or (SICS)

KEY POINTS

543.20 (c)(12) Are controls established and procedures implemented to ensure adequate: Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments? (Inquiry and review SICS)

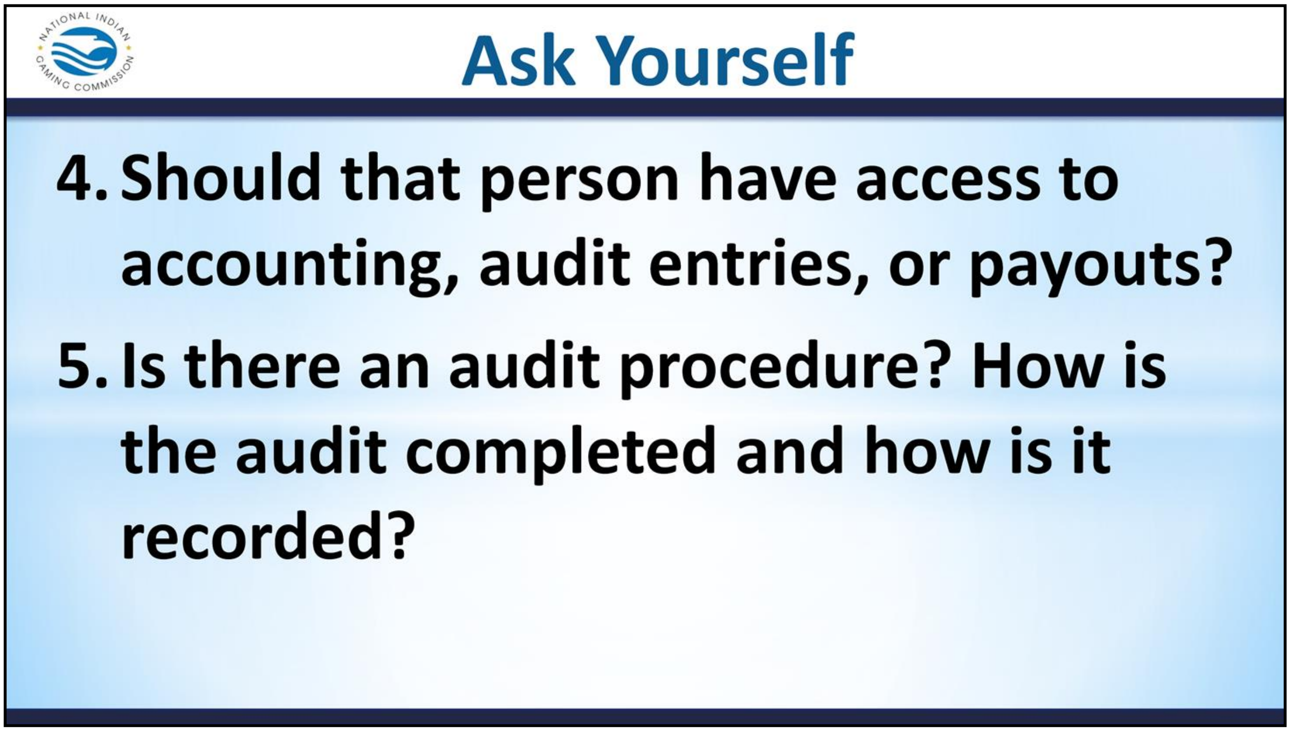
What are the differences between TICS and SICS?



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?

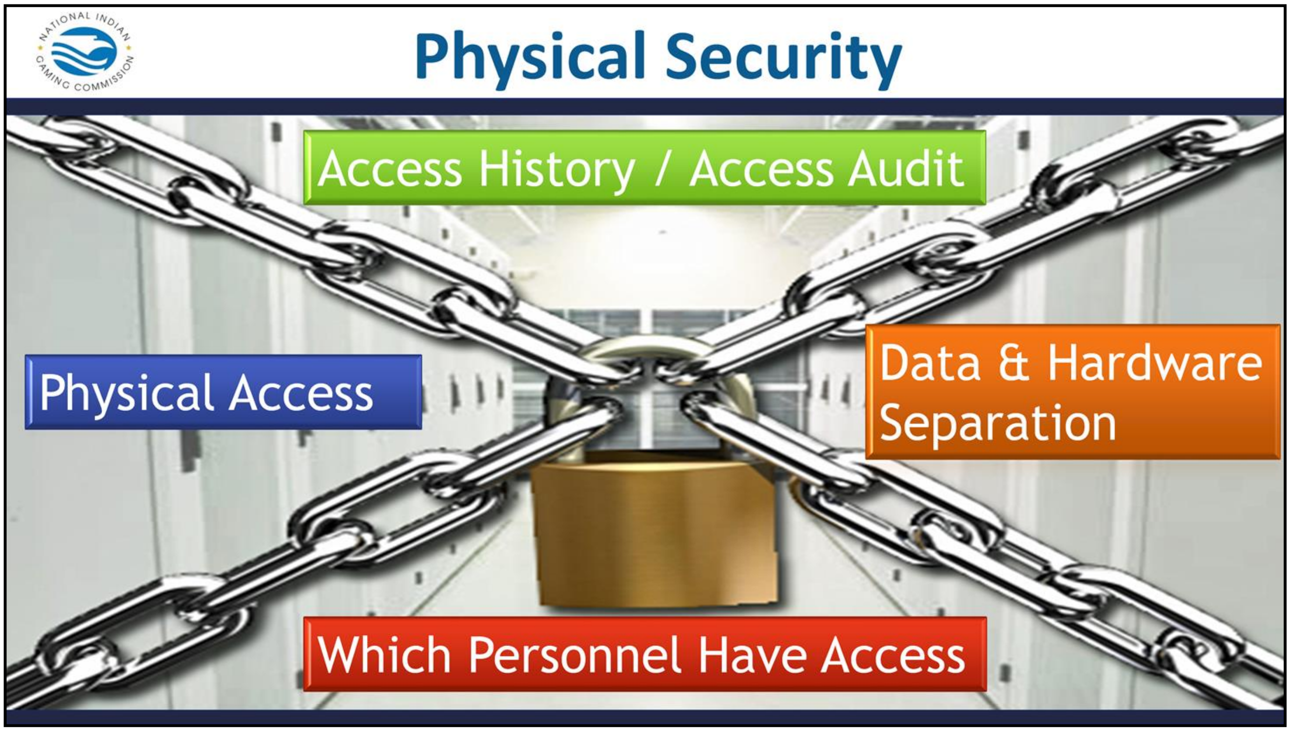
KEY POINTS



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?

KEY POINTS



Physical Security

Access History / Access Audit

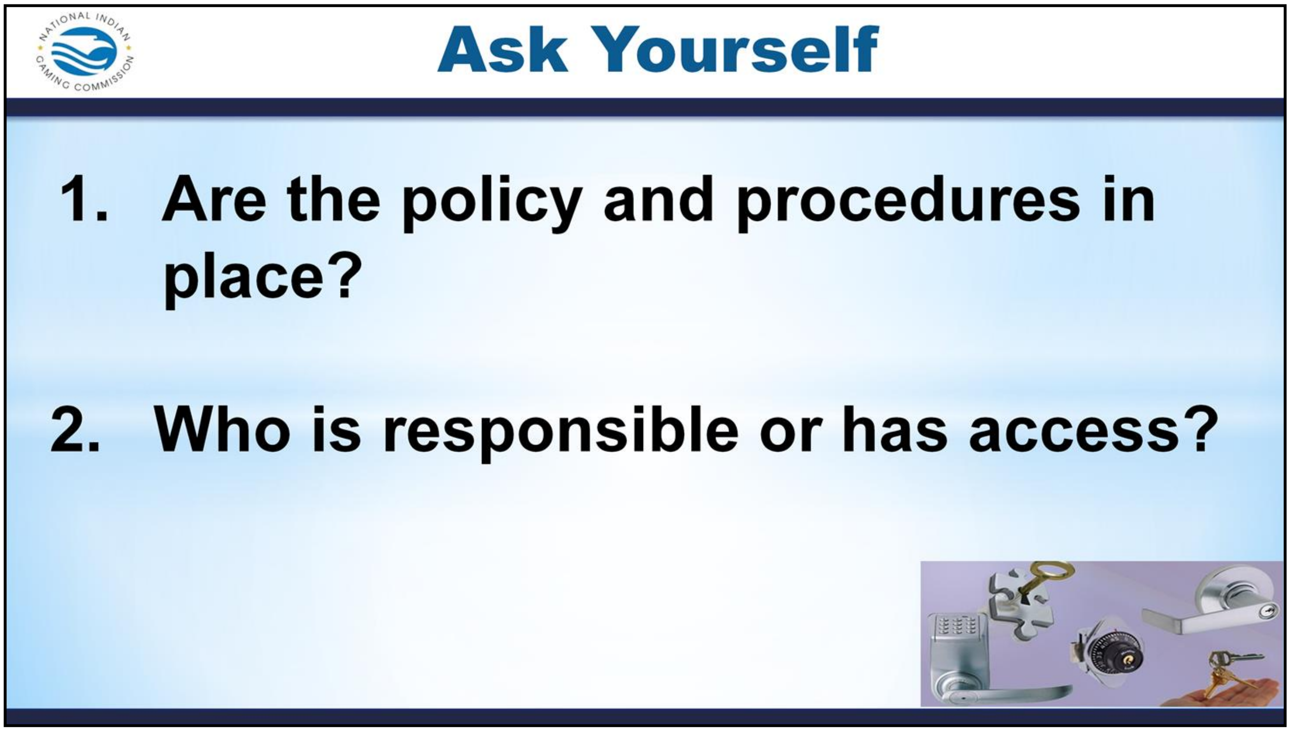
Physical Access

Data & Hardware Separation

Which Personnel Have Access

KEY POINTS

- *Look at physical access*.
- *Look at data and hardware separation.*
  - Are you housing different systems on the same server?
  - Is network equipment separated?
- *Look at which Personnel have access.*
  - Which IT people have access to what and when?
  - Which non-IT people have access to what and when?
- *Look at how often access history is audited and how often access privileges are audited?*
  - Depending on how access is logged, via a sign in sheet or via card key, how often is that log checked
  - How often are the access privileges of individuals audited?

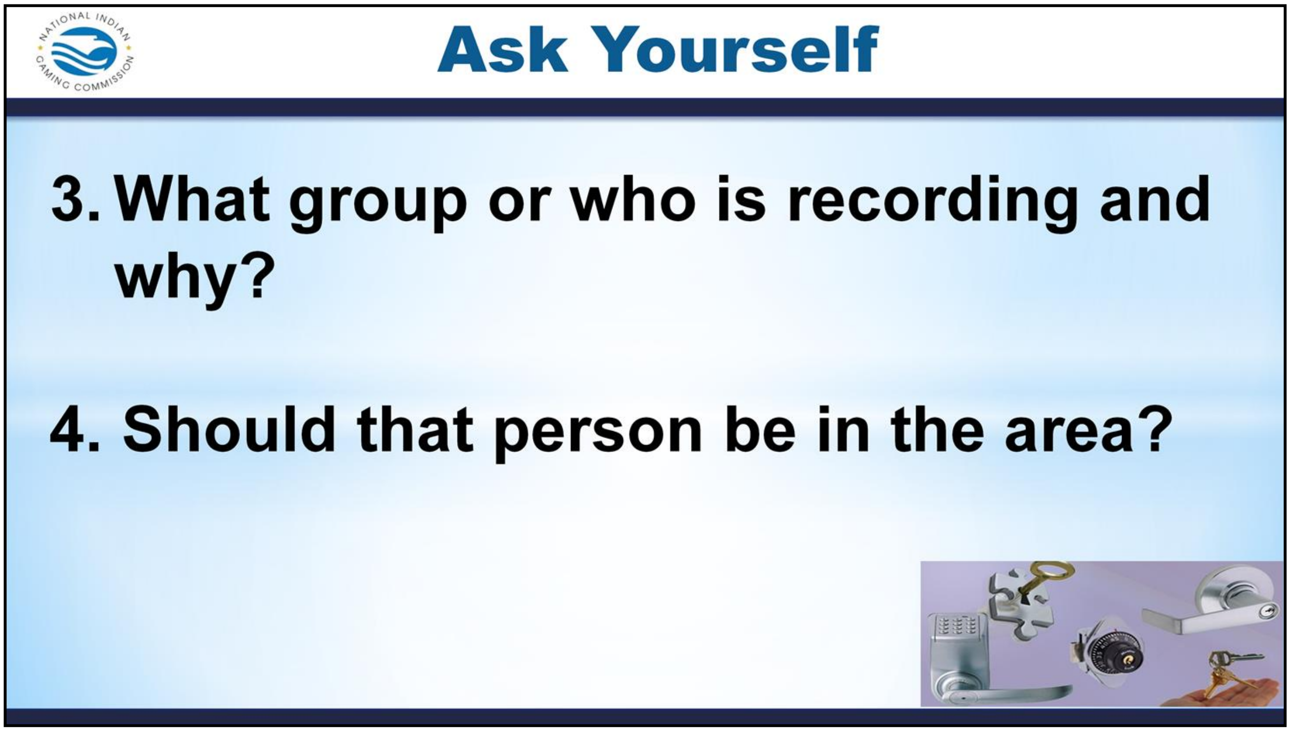


Ask Yourself

1. Are the policy and procedures in place?

2. Who is responsible or has access?

KEY POINTS

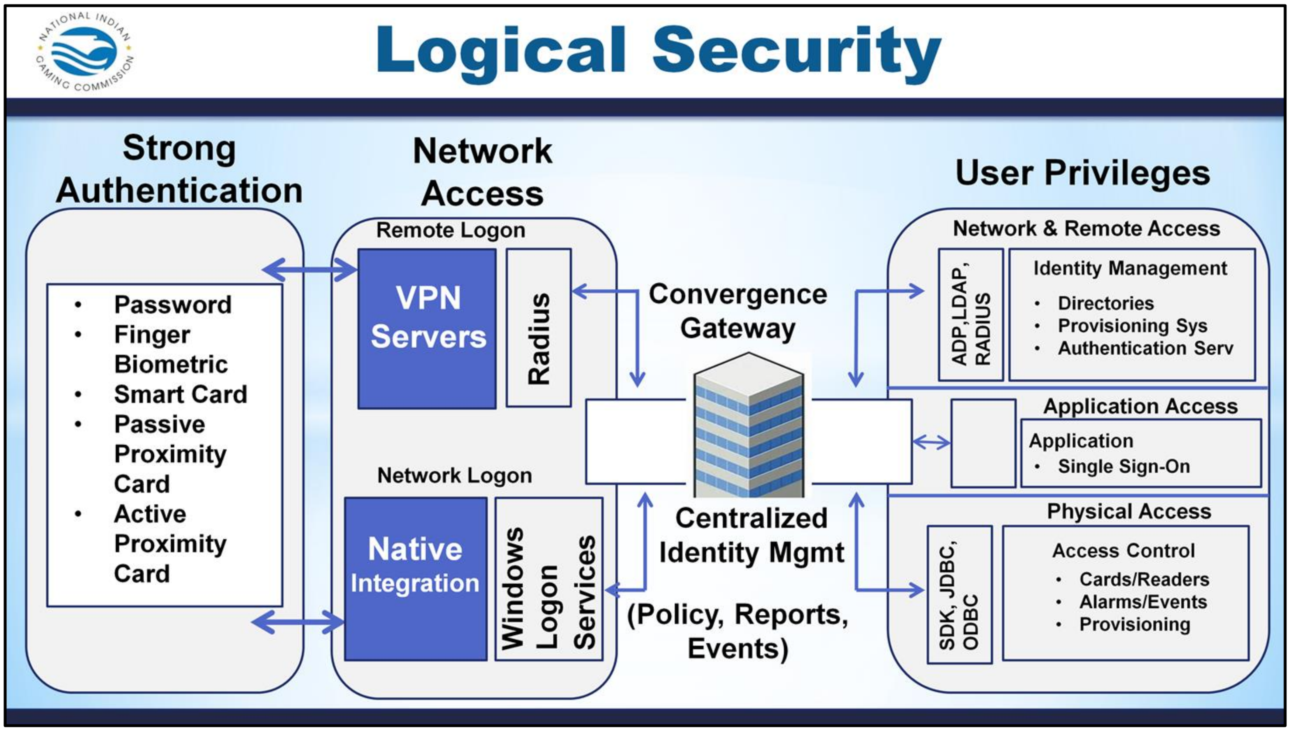


Ask Yourself

3. What group or who is recording and why?

4. Should that person be in the area?

KEY POINTS

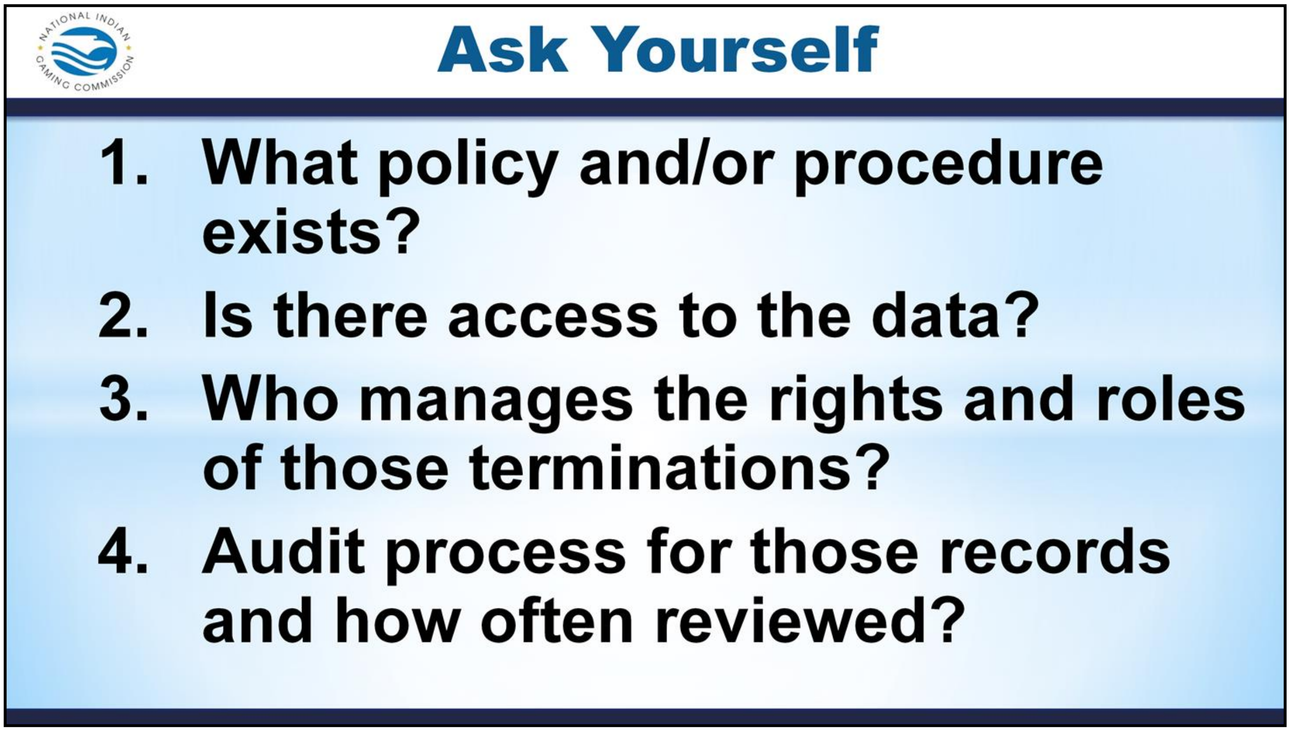


KEY POINTS
543.20 (e)(17) Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured: Systems' software and application programs? (Inquiry and review other – authorization lists)

> ***543.20 (e)(18)*** Are controls established and procedures
> implemented to protect all systems and to ensure that access to the following is restricted and secured:
> Data associated with Class II gaming? (Inquiry and review other – authorization lists)

- Look at SICS to protect all systems and ensure access is restricted

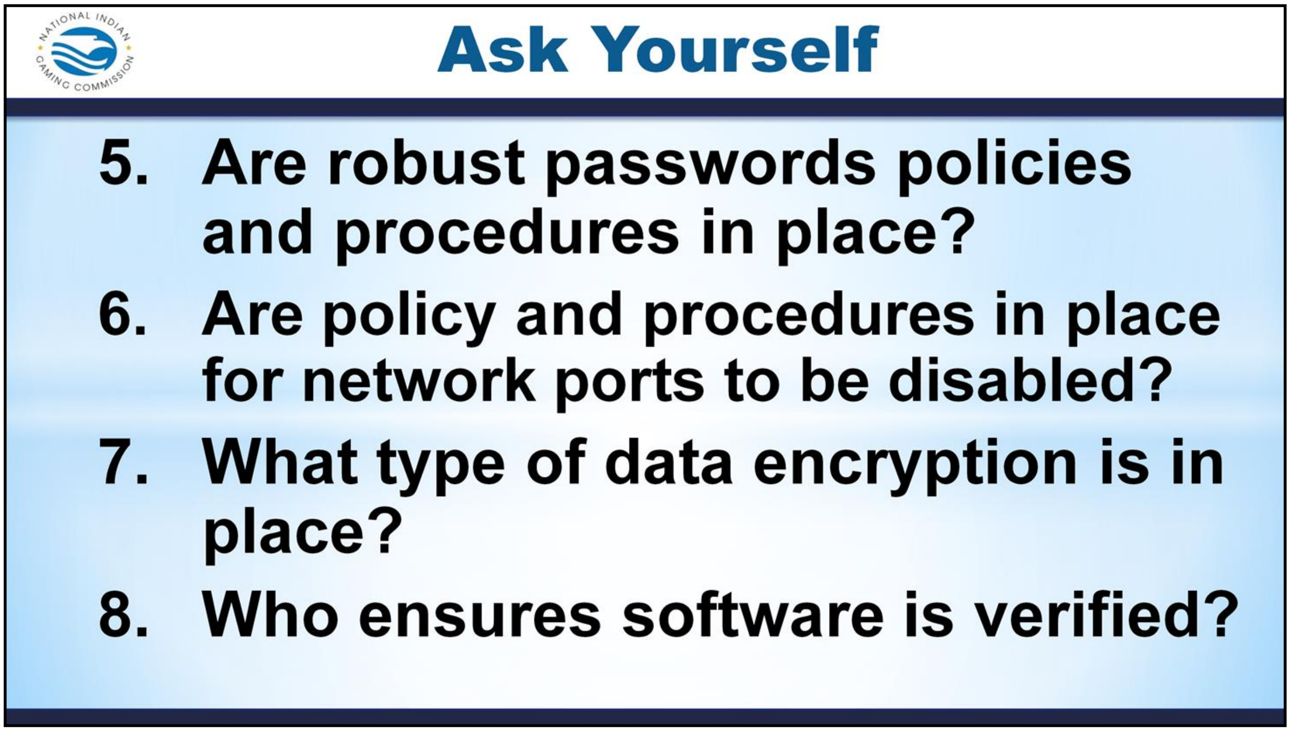
- Is there a process in place to grant or limit key access to various systems? (ie. Active Directory and Kerberos) –How are those utilized to give access to key servers, key folders, and key applications to users?
- Which IT personnel have access to each system? In a larger organization, you might have the floor operations support separate from the back-office operations support.
- Is the process of deciding who has access to what decided upon?
- Is the process of deciding access documented?



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?

KEY POINTS



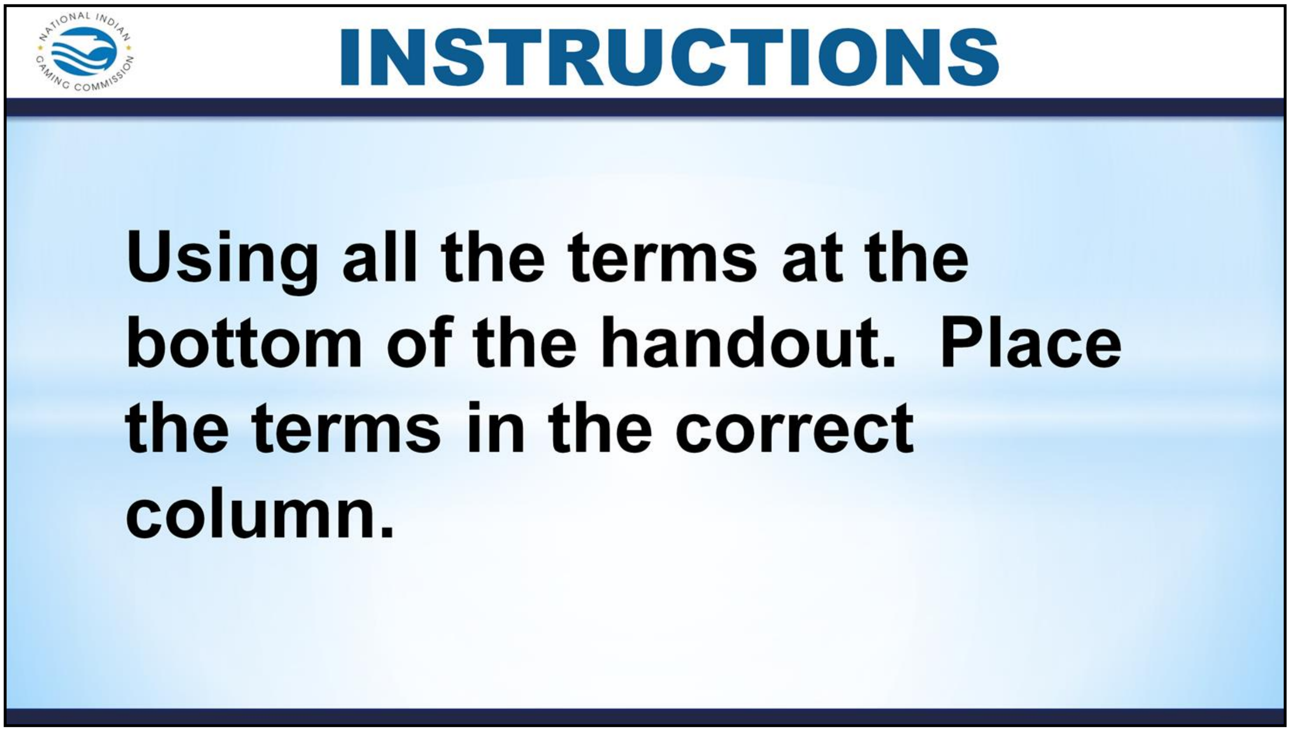
Ask Yourself

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?

KEY POINTS

Exercise #2 – Handout 2

KEY POINTS

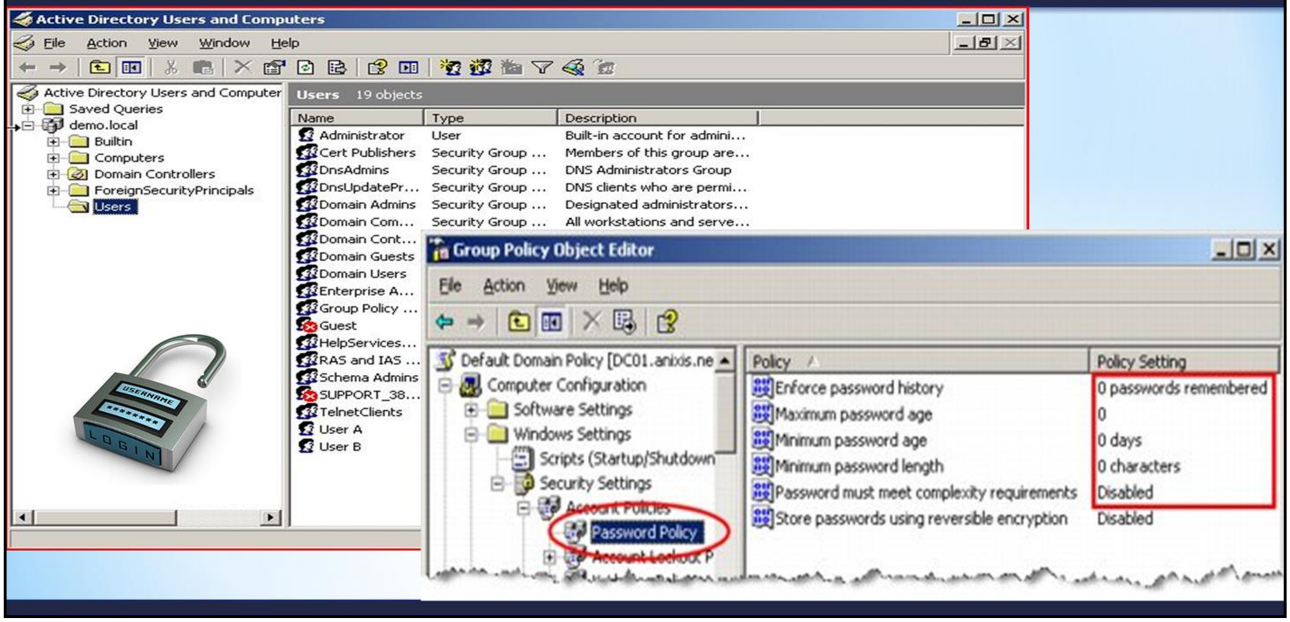


INSTRUCTIONS

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

KEY POINTS

User Controls



Active Directory Users and Computers

Users 19 objects

Name	Type	Description
Administrator	User	Built-in account for admini…
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

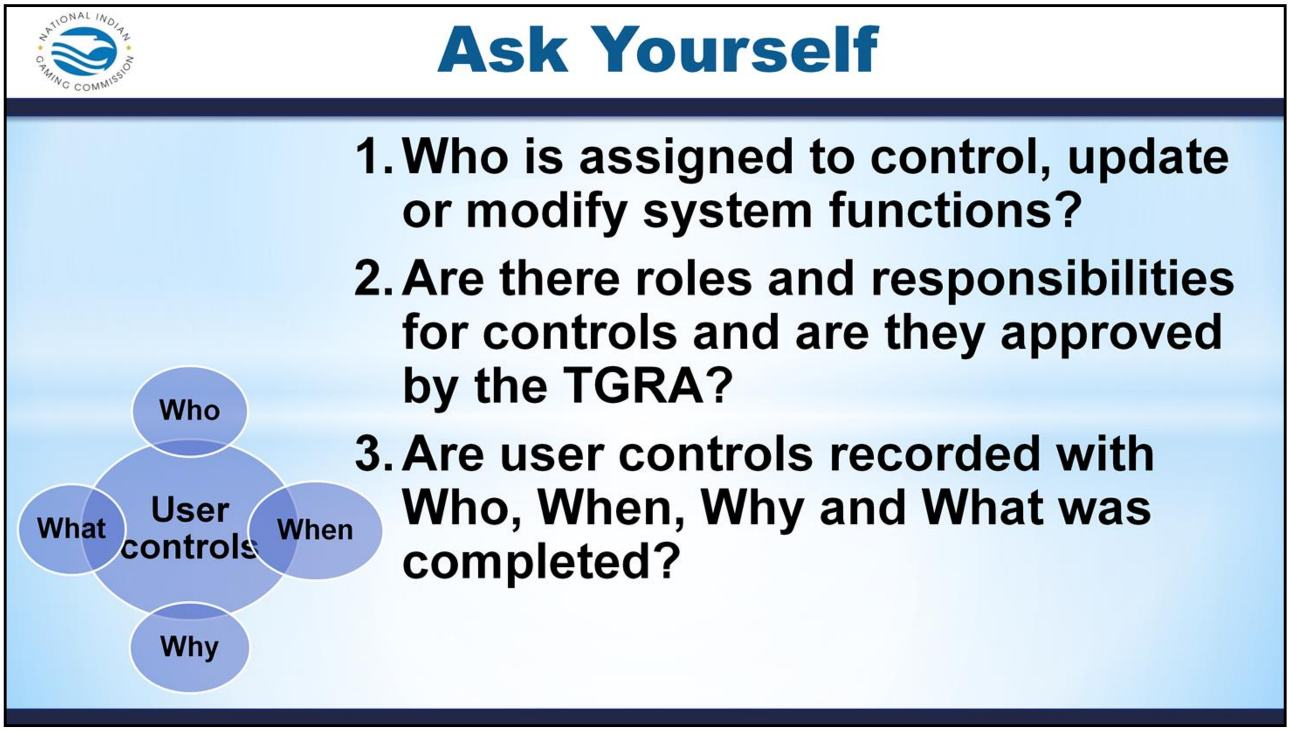
Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

KEY POINTS

543.20 (f)(24) Are systems, including application software, secured with passwords or other means for authorizing access? (Inquiry and perform log-in tests on network system(s) and each stand-alone system)

***543.20 (f)(32*)** Are lost or compromised access
credentials deactivated, secured or destroyed
within an established time period approved by the TGRA? State the time period
__________________. (Inquiry and review TGRA approval)

- *Look at SICS to make sure systems are protected with passwords or other means*
- *Look at SICS for lost and compromised access credentials* (ie. Terminated user policy, lost card policy)
- *Look at password complexity and reset period*

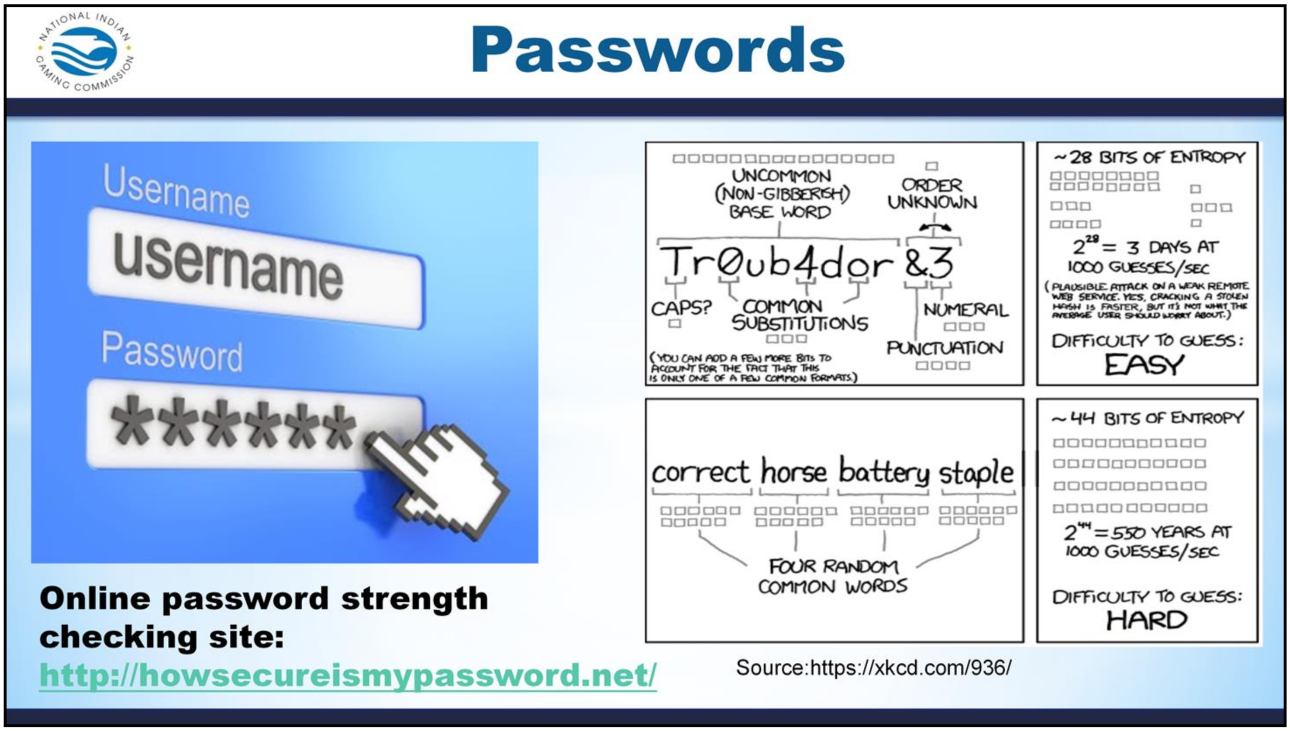


Ask Yourself

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?

Who
What
User controls
When
Why

KEY POINTS



Passwords

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

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

Username
username
Password
******
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

KEY POINTS

NIST standards for passwords updated in 2017: from 8 characters / 4 character types to short word phrases.

Remote Access

KEY POINTS

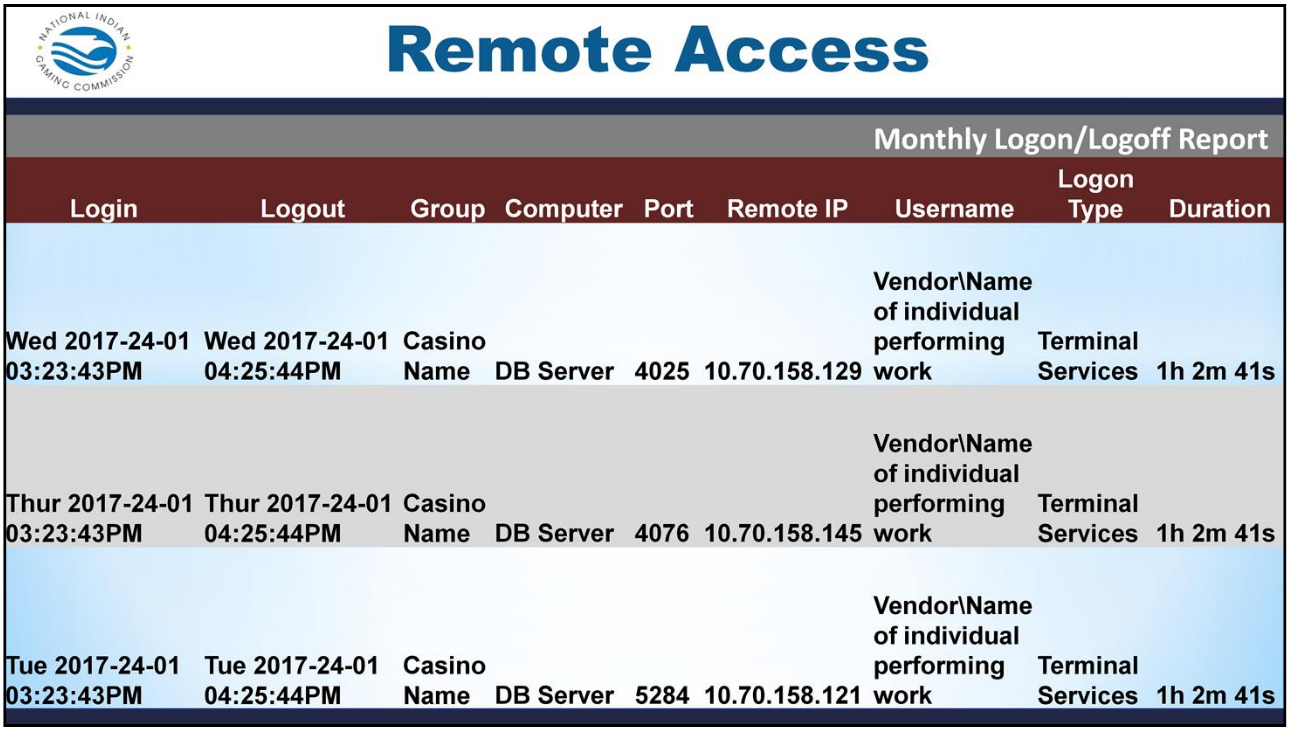
#41, #49

543.20 (h)(41) Is documentation for each remote access system support session maintained at the place of authorization? (Inquiry and review supporting documentation)

***543.20 (h)(49*)** Is all remote access performed via a secured method? (Inquiry and review supporting documentation)

- Look at remote access logging

- Look at secured remote access



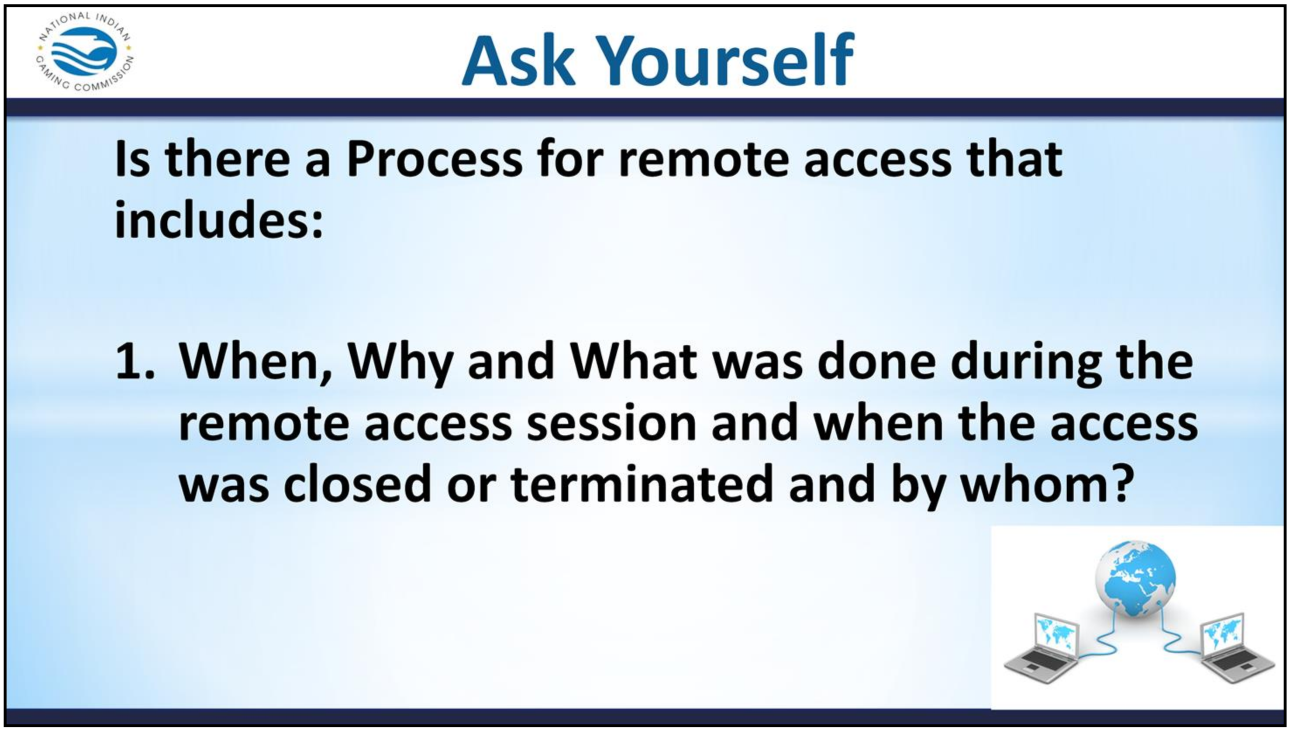
Remote Access

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

KEY POINTS

What is wrong with this picture?

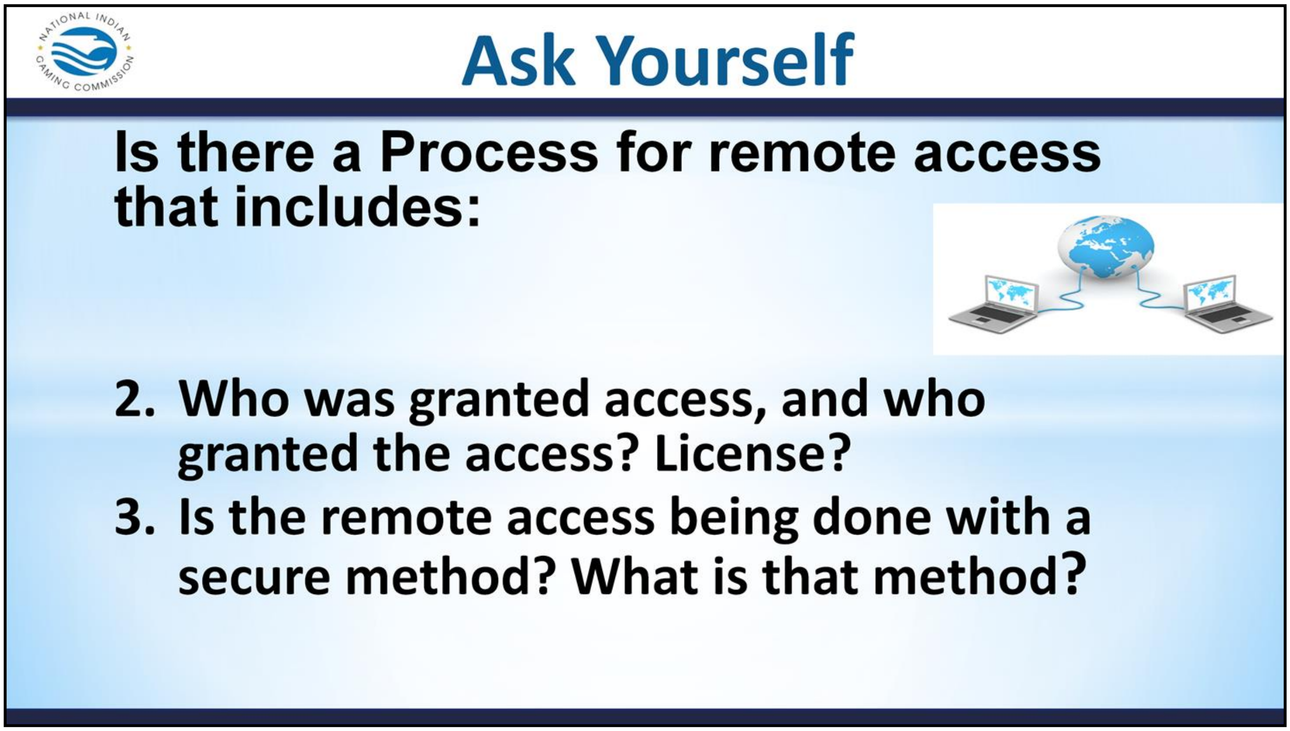


Ask Yourself

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?

KEY POINTS



Ask Yourself

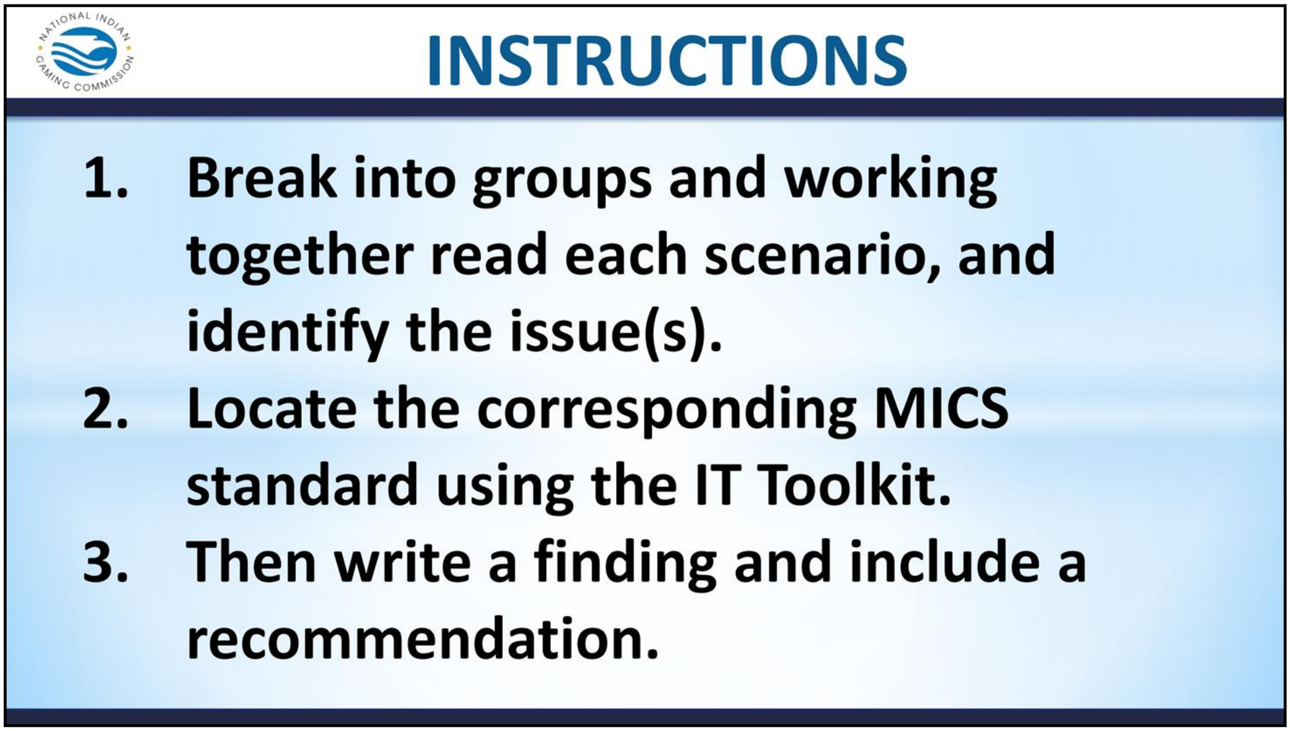
Is there a Process for remote access that includes:

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?

KEY POINTS

Exercise 3 – Handout #3

KEY POINTS



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.

KEY POINTS

Data Backup

KEY POINTS

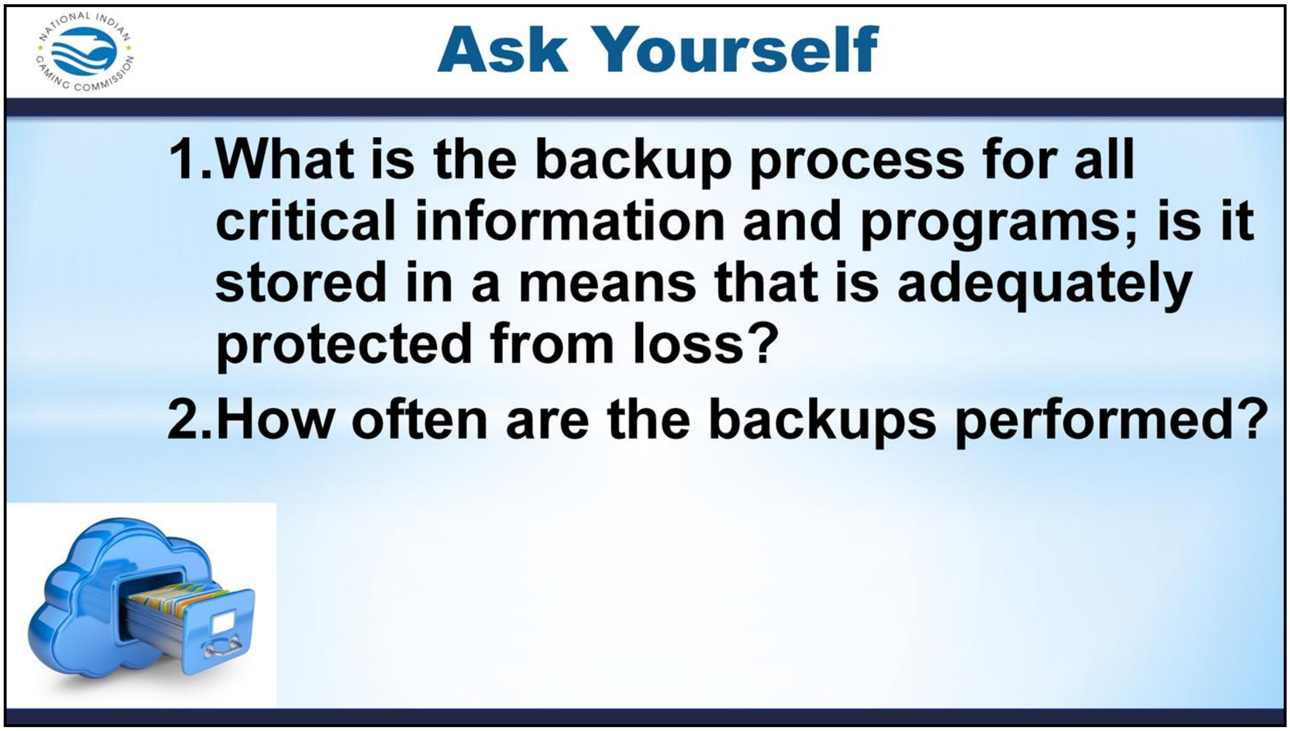
Checklist #53, #55, #59, #61

***543.20 (j)(53*)** Do controls include adequate backup, including, but not limited to, the following: Daily data backup of critical information technology systems? (Inquiry and review supporting documentation)

***543.20 (j)(55*)** Do controls include adequate backup, including, but not limited to, the following: Secured storage of all backup data files and programs, or other adequate protection? (Inquiry and observation)

***543.20 (j)(59*)** Do controls include recovery procedures , including, but not limited to, the following: Program restoration? (Inquiry and review supporting documentation)

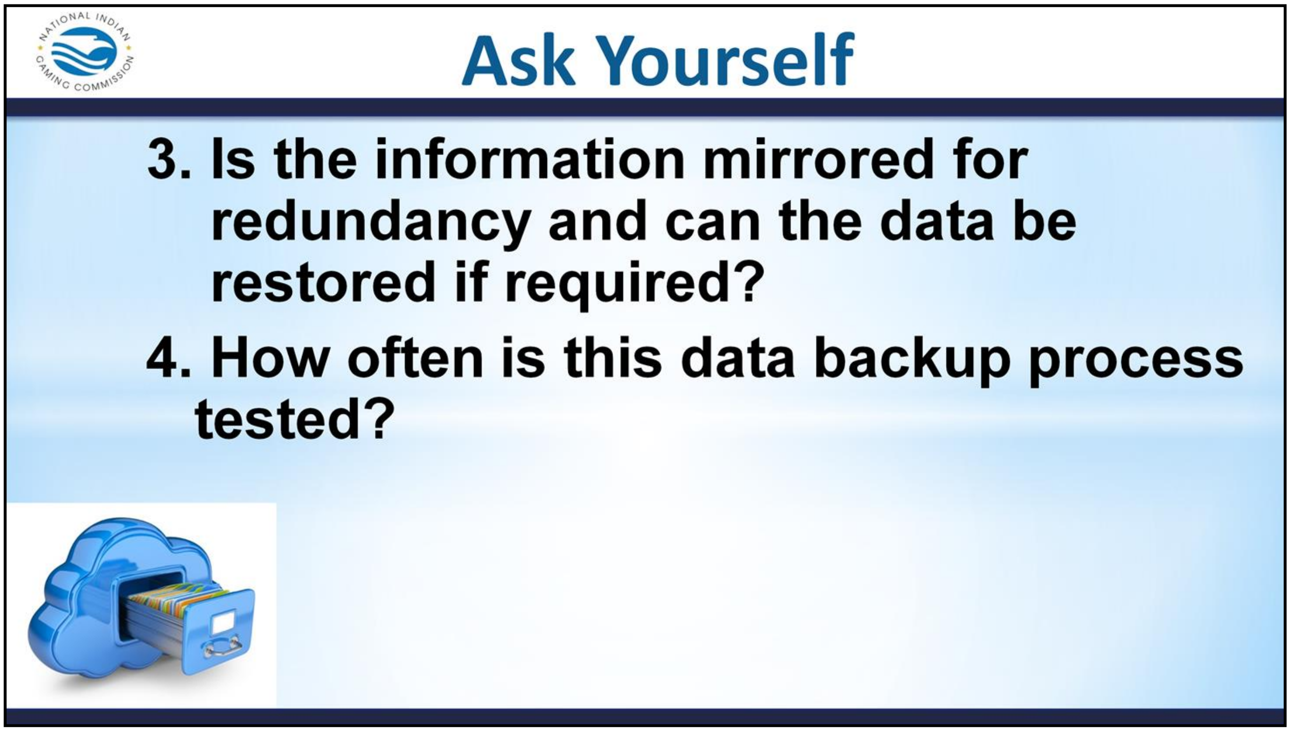
- Look at backup schedule
- Look at security of backups
- Look at restoration methods
- Look at recovery process and testing of process



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?

KEY POINTS



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?

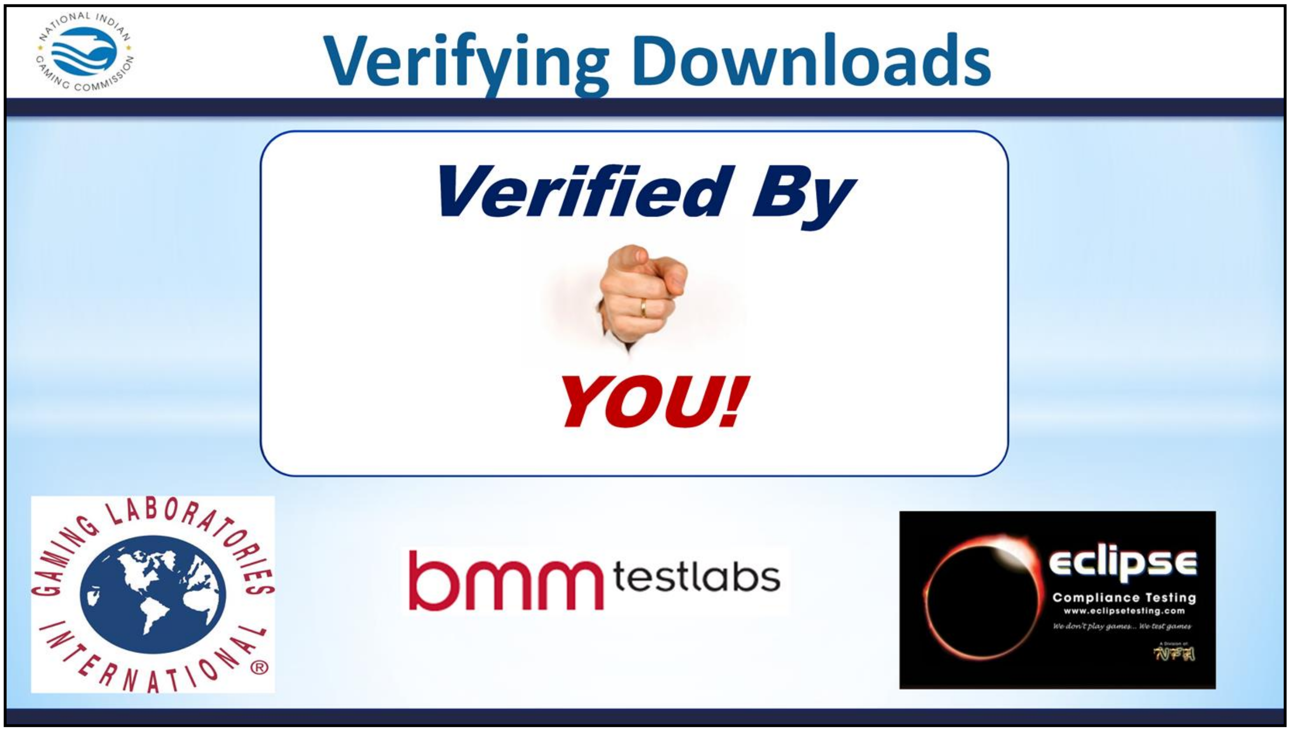
KEY POINTS

Software Downloads

KEY POINTS

543.20(k)(63) Are downloads, either automatic or manual, performed in accordance with 25 CFR 547.12? (Inquiry and review SICS)

1. Acceptable means of transporting APPROVED content
2. Use secure methodologies that will deliver data without alteration or modification
3. Downloads during operational periods will not affect game play
4. Must not affect integrity of accounting data
5. C2 gaming MUST be capable of providing
   - Time & date of initiated download
   - Time & date of completed download
   - C2 gaming system components to which software was downloaded
   - Versions of download package and any software. Logging unique software signature
   - Outcome of any software verification (Success or Failure)
   - Name and ID number, or other unique identifier, of any individuals conducting or scheduling a download



Verifying Downloads

Verified By

YOU!

GAMING LABORATORIES INTERNATIONAL®
bmm testlabs
eclipse
Compliance Testing
www.eclipsetesting.com
We don't play games... We test games

KEY POINTS

Verifying downloads – Software on C2 gaming system MUST be capable of verification by C2 Gaming system using a software signature verification method that meets 547.8(f)

543.20(l)(64) Following the download of any Class II gaming system software, does the Class II gaming system verify the downloaded software using a software signature verification method? (Inquiry and review supporting documentation)

- *Look at download process*
- *Look at signature verification*
- *Look at best practices.* *(Remember 542.16)*

Installations &/or Modifications

Casino Management System

Surveillance

Hotel Shops

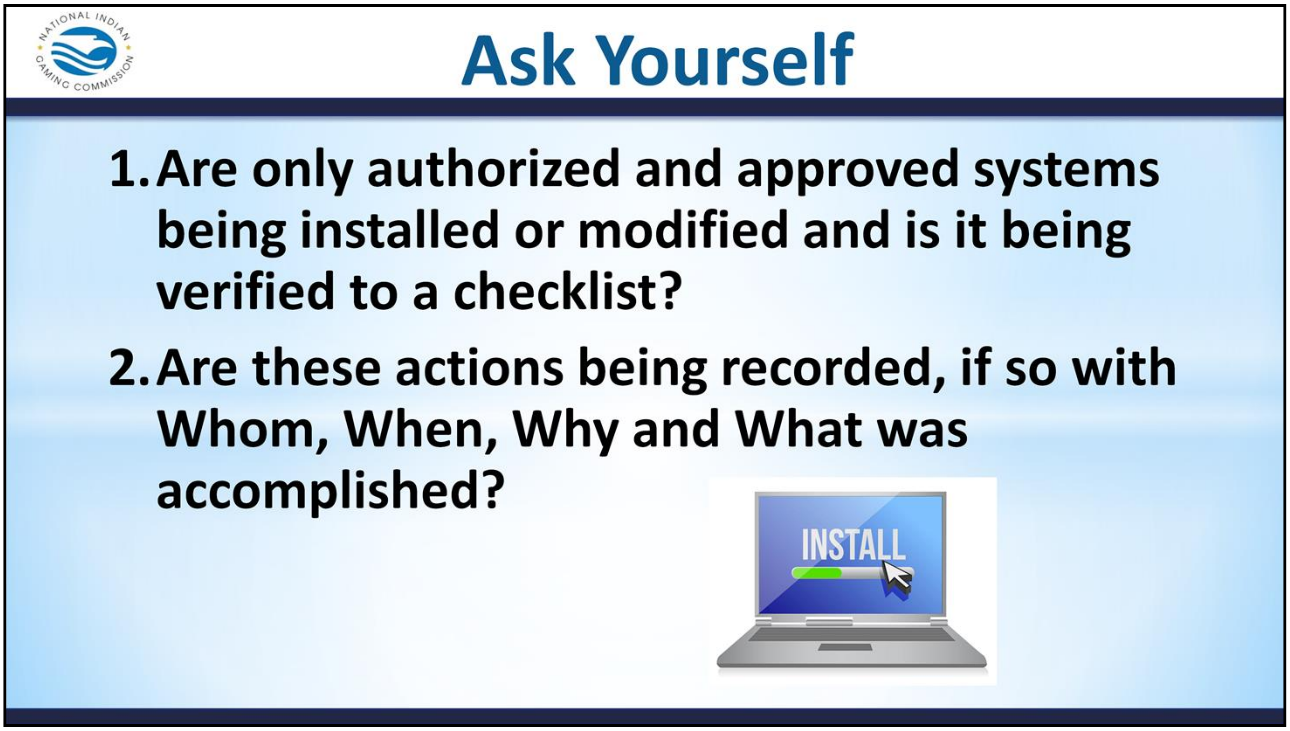
Hospitality

KEY POINTS

543.20(g)(36) Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum: The date of the installation or modification? (Inquiry and review supporting documentation)

543.20(g)(38) Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum: Evidence of verification that the installation or the modifications are approved? (Inquiry and review supporting documentation)

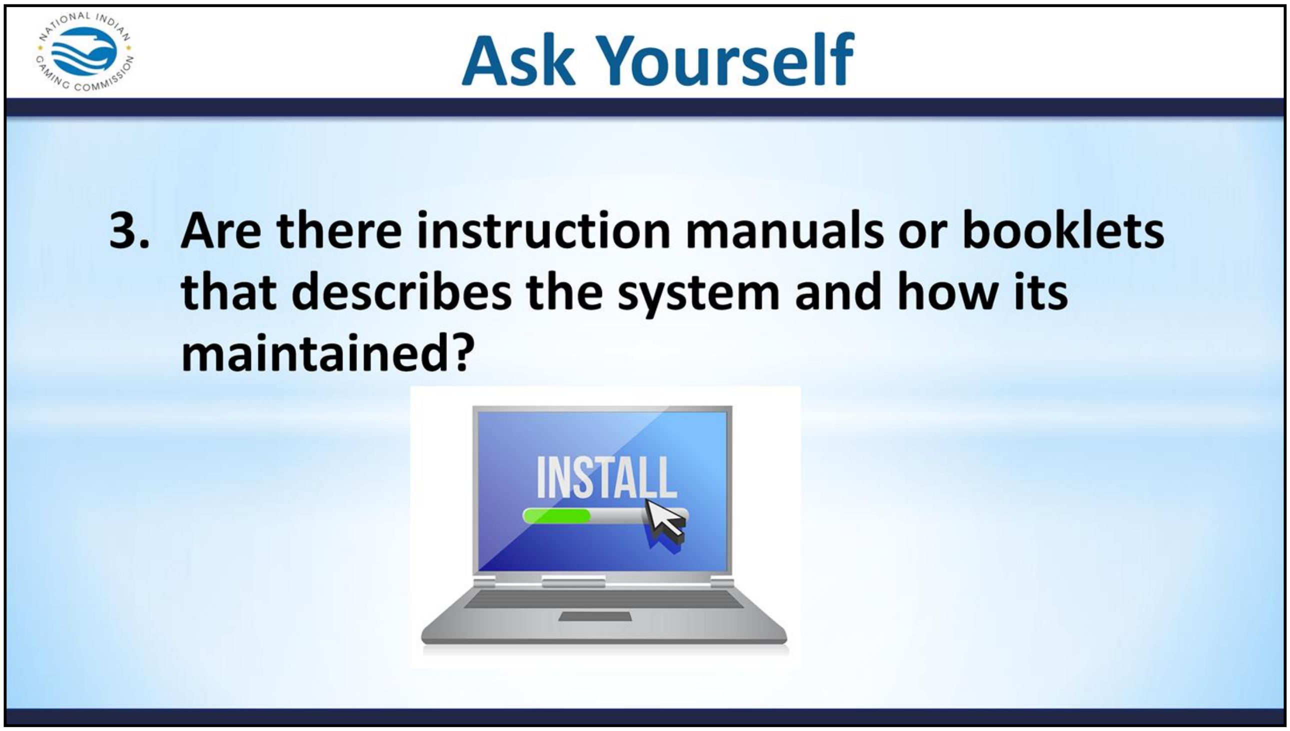
- *Look at records and versions of installs* - Is there a written record of the install
- *Look at records of all new installations and modifications* - Is there proof of the software verification?
- *Look at change management process*
  - Is there a documented process for testing new software or hardware
  - Is there a documented process for incorporating new software and hardware into the destination environment?
- Is there a process for vetting approved vendors?



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?

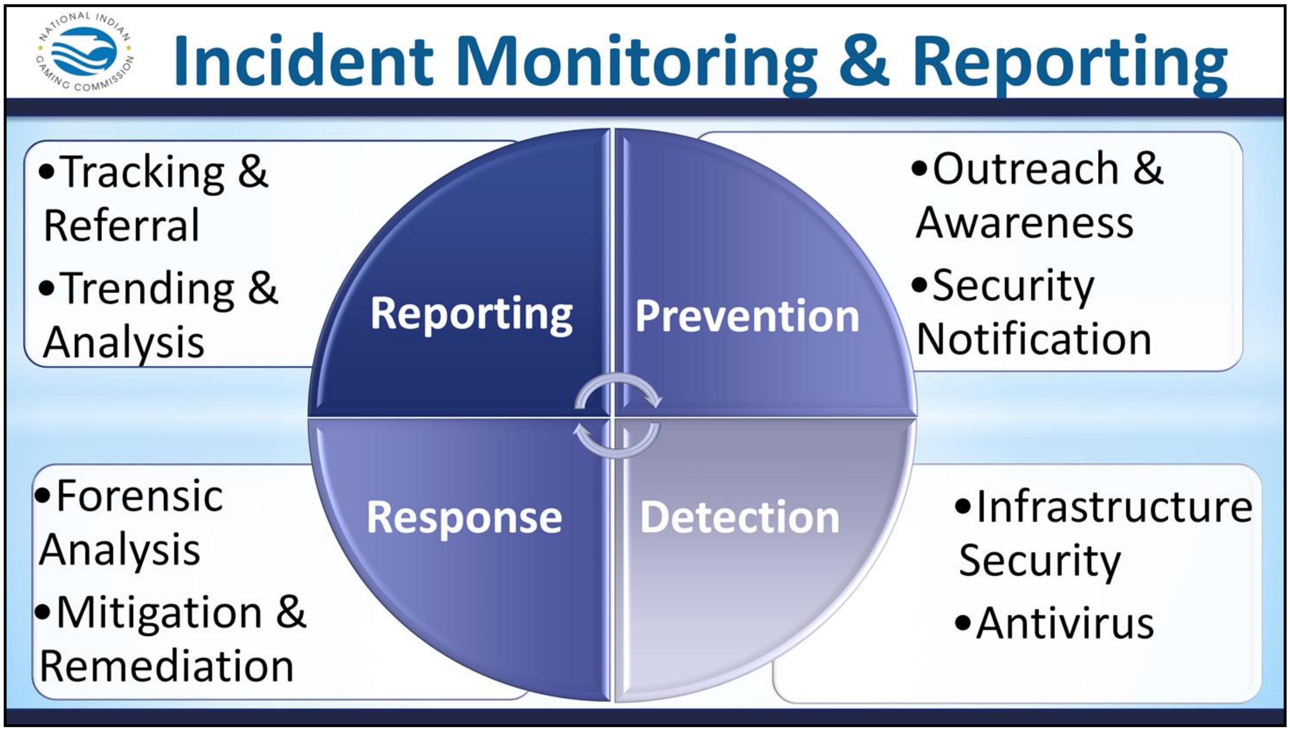
KEY POINTS



Ask Yourself

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

KEY POINTS



Incident Monitoring & Reporting

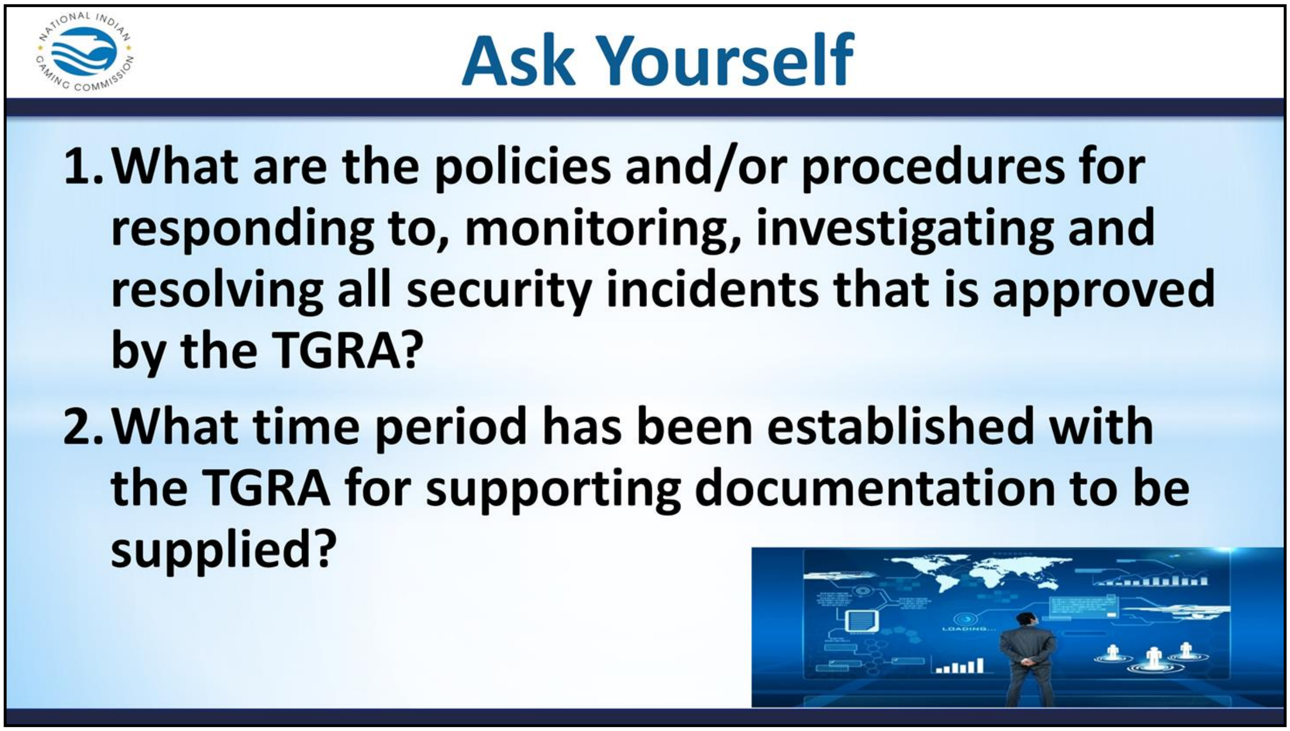
KEY POINTS

Incident Monitoring & Reporting

543.20(i)(51) Are all security incidents responded to within the established time period approved by the TGRA? State the time period_____.

(Inquiry, review TGRA approval, and review supporting documentation)

- What are the processes for responding to monitoring, investigating, resolving, documenting, and reporting security incidents?
  - Is there a documented response time period for incidents?
  - Is there a tracking system for **reporting** incidents and are they being utilized for data analysis?
  - What steps for outreach and notification are being taken to promote **prevention**?
- What **detection** methods are in place?
- What is the **response** system

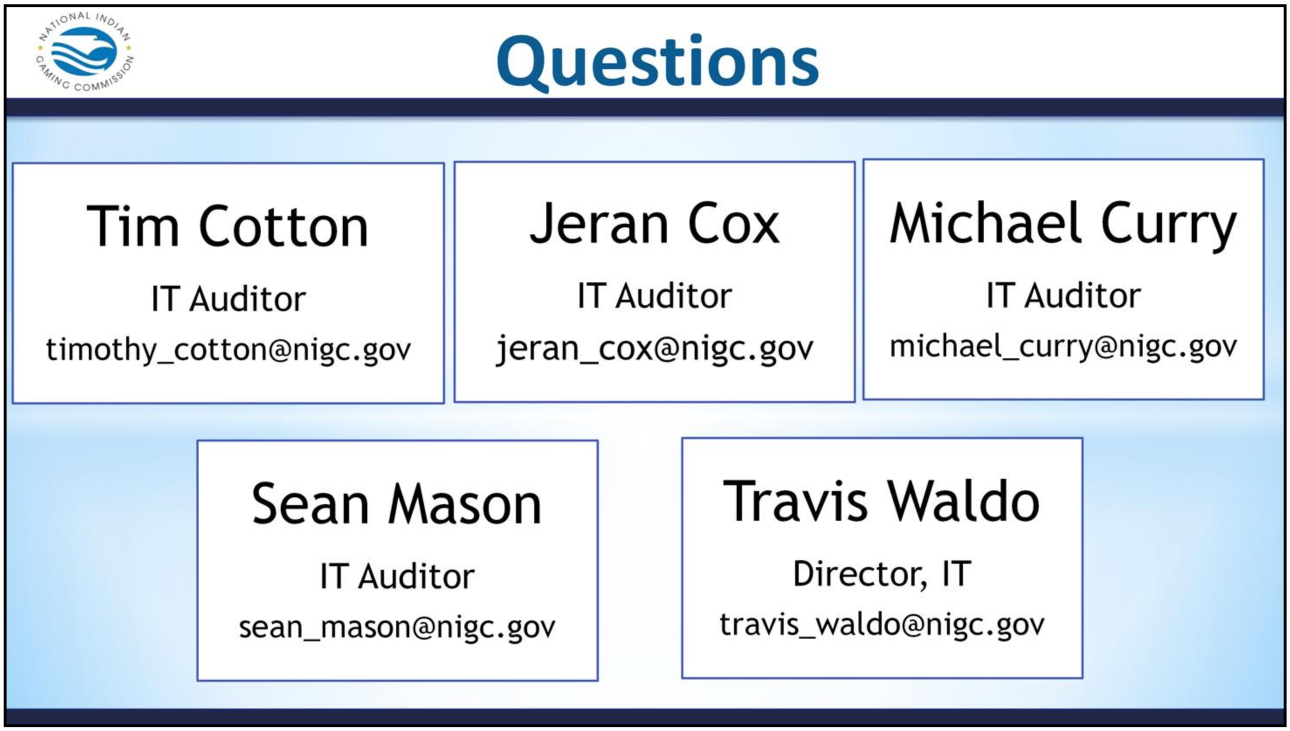


Ask Yourself

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?

KEY POINTS

Ask Yourself – Incident Monitoring and Reporting



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

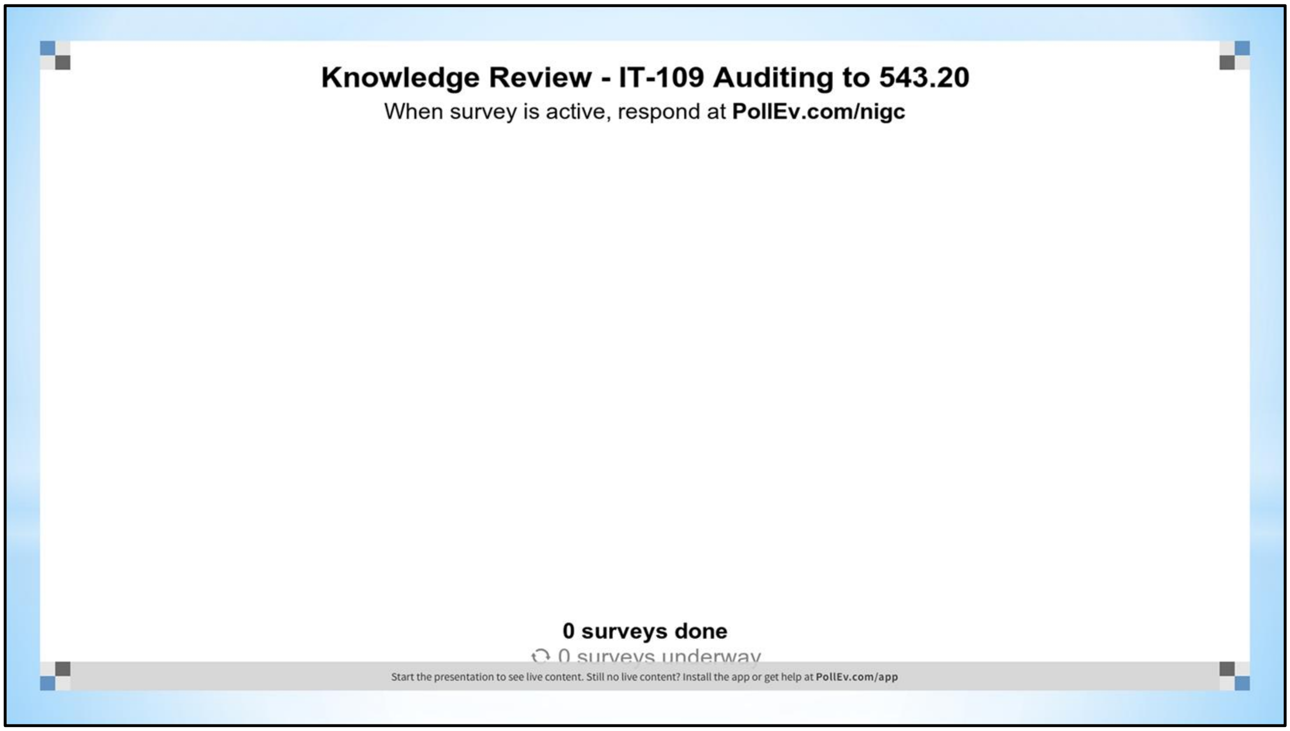
Travis Waldo
Director, IT
travis_waldo@nigc.gov

KEY POINTS

Course Evaluation

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

KEY POINTS



Knowledge Review - IT-109 Auditing to 543.20

When survey is active, respond at **PollEv.com/nigc**

0 surveys done

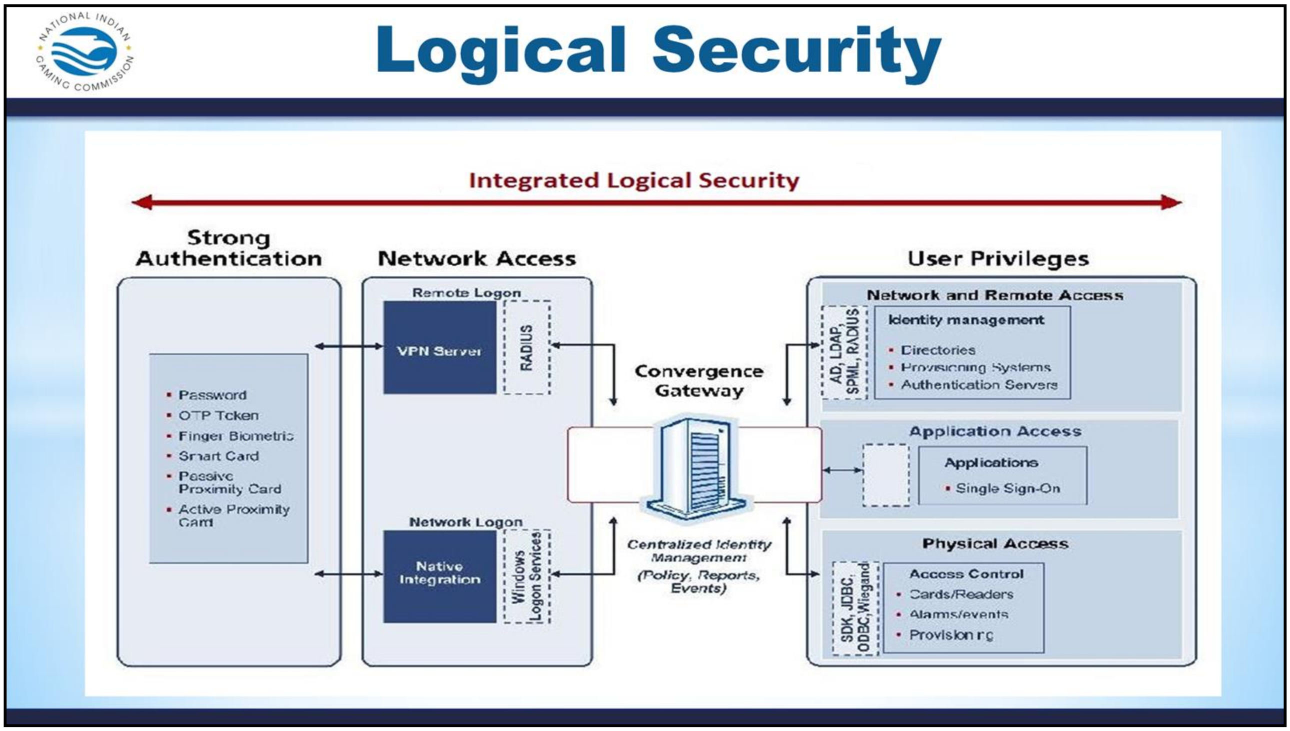
0 surveys underway

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

KEY POINTS

Poll Title: Knowledge Review - IT-109 Auditing to 543.20

https://www.polleverywhere.com/surveys/Qdj8myfmA



Logical Security

Integrated Logical Security

Strong Authentication
- Password
- OTP Token
- Finger Biometric
- Smart Card
- Passive Proximity Card
- Active Proximity Card

Network Access

Remote Logon
VPN Server
RADIUS

Network Logon
Native Integration
Windows Logon Services

Convergence Gateway

Centralized Identity Management (Policy, Reports, Events)

User Privileges

Network and Remote Access
AD, LDAP, SPML, RADIUS
Identity management
- Directories
- Provisioning Systems
- Authentication Servers

Application Access
Applications
- Single Sign-On

Physical Access
SDK, JDBC, ODBC,Wiegand
Access Control
- Cards/Readers
- Alarms/events
- Provisioning

KEY POINTS

Logical security – focus #17 and #18

> ***543.20 (e)(17)*** Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured: Systems' software and application programs? (Inquiry and review other – authorization lists)
>
> ***543.20 (e)(18)*** Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:
> Data associated with Class II gaming? (Inquiry and review other – authorization lists)

Look at SICS to protect all systems and ensure access is restricted

- Is there a process in place to grant or limit key access to various systems? – For example: Active Directory and Kerberos are two of the most common authentication services. But how are those utilized to give access to key servers, key folders, and key applications to users? Which IT personnel have access to each system? In a larger organization, you might have the floor operations support separate from the back-office operations support.
- Is the process of deciding who has access to what decided upon? – For example: When an individual requests access to a room or to an application how is it determined if they get it or not? Do you need a manager approval? Do you accept ANY manager's approval? Is there a process not just to add access but to grant or deny?
- Is the process of deciding access documented? – For example: When the head of IT leaves the org. will anyone understand the process when they are gone? And, will they do it the same way?