



---

---

---

---

---

---

---

---

**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

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---



---

---

---

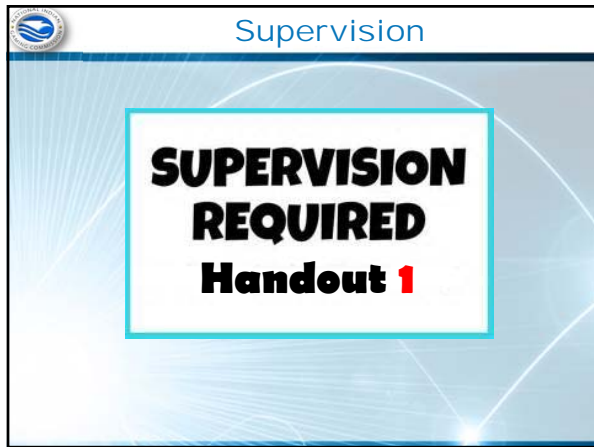
---

---

---

---

---



---

---

---

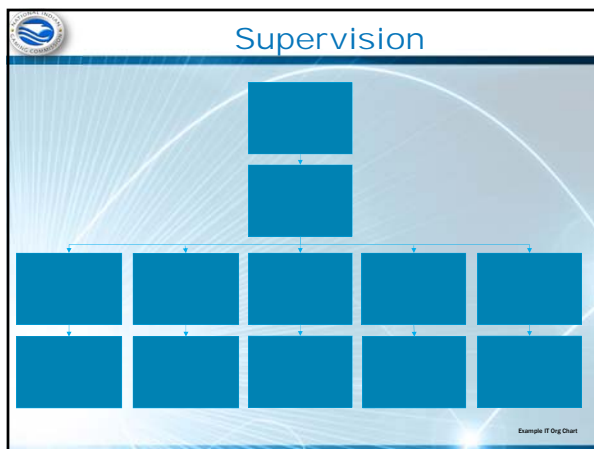
---

---

---

---

---



---

---

---

---

---

---


---

---

Class II Gaming Systems Logical and Physical Controls

Importance Of :

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



A diagram showing three overlapping circles labeled 'Threat', 'Asset', and 'Vulnerability'. The intersection of all three is shaded red and labeled 'Risk'. A hand is pointing to the 'Risk' area.

---

---

---

---

---


---

---

---

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?



A diagram with 'HELP' in the center, surrounded by colorful arrows pointing to 'SOLUTION', 'CUSTOMER', 'SERVICE', 'QUALITY', 'GROWTH', and 'BUSINESS'.

---

---

---

---

---

---

---

---

Physical Security



A photograph of a hallway with white lockers. A large metal chain is draped across the hallway, secured by a large brass padlock in the center.

---

---

---

---

---


---

---

---

**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/vendors checked before access is granted?




---

---

---

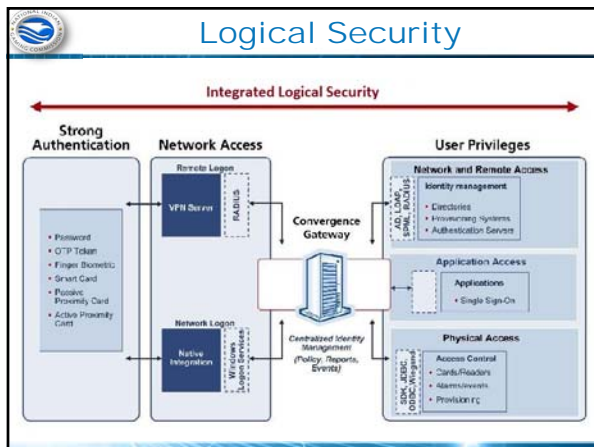
---

---

---

---

---




---

---

---

---

---

---

---

---

**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 data 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



**Handout 2**

---

---

---

---

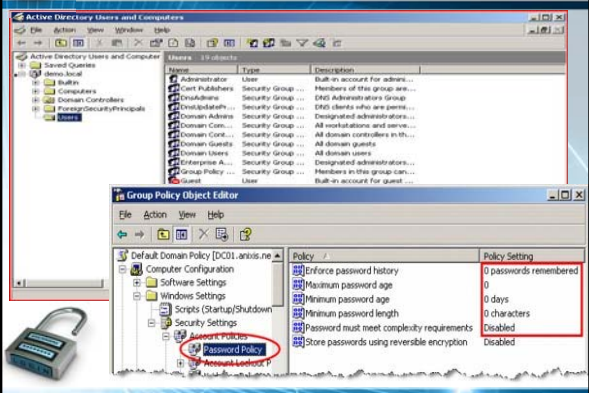
---

---

---

---

## User Controls



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

---

---

---

---

---

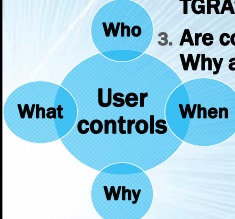
---

---

---

## 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

Username  
**username**

Password  
**\*\*\*\*\***

**Handout 3**

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p><b>Tr0ub4dor&amp;3</b></p> <p>CAPS? COMMON SUBSTITUTIONS NUMERICAL PUNCTUATION</p> <p>(Who can guess a password, has to know the order of the characters)</p>	<p>~28 BITS OF ENTROPY</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PASSWORD STRONG ON A WEBSITE AND OFFICE PC, WEAK ON OTHER WEBSITES)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~14 BITS OF ENTROPY</p> <p><math>2^{14} = 500 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>

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

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

---

---

---

---

---

---

---

---

---

---

---

---

### Remote Access

---

---

---

---

---

---

---

---

---

---

---

---

### Remote Access

Monthly Logon/Logoff Report

Logon	Logout	Group	Computer	Port	Remote IP	Username	Logon Type	Duration
							VendorName of individual performing work	Terminal Services
Wed 2017-24-01 03:23:43PM	Wed 2017-24-01 04:25:44PM	Casino Name	DB Server	4025	10.70.158.129		work	1h 2m 41s
							VendorName of individual performing work	Terminal Services
Thur 2017-24-01 03:23:43PM	Thur 2017-24-01 04:25:44PM	Casino Name	DB Server	4076	10.70.158.145		work	1h 2m 41s
							VendorName of individual performing work	Terminal Services
Tue 2017-24-01 03:23:43PM	Tue 2017-24-01 04:25:44PM	Casino Name	DB Server	5284	10.70.158.121		work	1h 2m 41s
							VendorName of individual performing work	Terminal Services
Mon 2017-24-01 03:23:43PM	Mon 2017-24-01 04:25:44PM	Casino Name	DB Server	3845	10.70.158.102		work	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!**



---

---

---

---

---

---

---

---



 **Installation &/or Modifications**



The slide features four images arranged in a 2x2 grid. The top-left image is titled 'Casino Management System' and shows a person's hands on a computer keyboard with a monitor displaying a software interface. The top-right image is titled 'Surveillance' and shows a person's silhouette in front of a wall of security camera monitors. The bottom-left image is titled 'Hotel Shops' and shows a retail store interior with clothing racks. The bottom-right image is titled 'Hospitality' and shows a person standing in a modern hallway.

---

---

---


---

---


---

---

---

 **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?**



The slide includes a small image of a laptop with the word 'INSTALL' on its screen and a mouse cursor pointing at it.

---

---

---


---

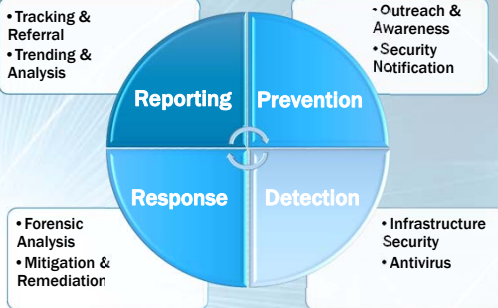
---

---

---

---

 **Incident Monitoring & Reporting**



The diagram is a circle divided into four quadrants. The top-left quadrant is labeled 'Reporting' and lists 'Tracking & Referral' and 'Trending & Analysis'. The top-right quadrant is labeled 'Prevention' and lists 'Outreach & Awareness' and 'Security Notification'. The bottom-left quadrant is labeled 'Response' and lists 'Forensic Analysis' and 'Mitigation & Remediation'. The bottom-right quadrant is labeled 'Detection' and lists 'Infrastructure Security' and '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?**



---

---

---


---

---

---

---

---

 **Questions**

<b>Tim Cotton</b> IT Auditor timothy_cotton@nigc.gov	<b>Jeran Cox</b> IT Auditor jeran_cox@nigc.gov	<b>Michael Curry</b> IT Auditor michael_curry@nigc.gov
<b>Sean Mason</b> IT Auditor sean_mason@nigc.gov	<b>Travis Waldo</b> Director, IT travis.waldo@nigc.gov	

---

---

---

---

---

---

---

---