


# IT-110 Refining & Enhancing IT TICS



Information Technology Division

## KEY POINTS



## What does your facility offer

- Class III only
- Class II only
- Mixed of Class III and Class II

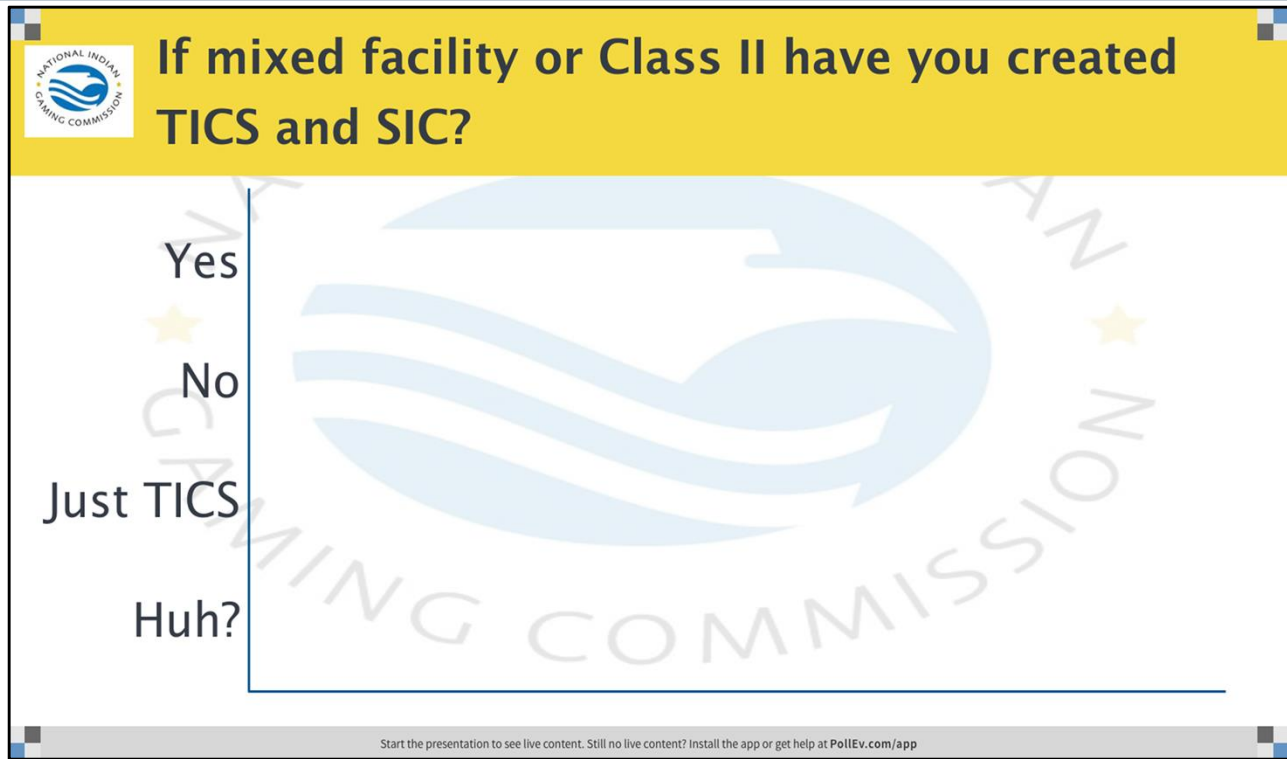
Start the presentation to see live content. Still no live content? Install the app or get help at [PolleEv.com/app](https://www.polleverywhere.com/app)


### KEY POINTS

Poll Title: What does your facility offer

[https://www.polleverywhere.com/multiple\\_choice\\_polls/NNFvAQgmzJeMpBw](https://www.polleverywhere.com/multiple_choice_polls/NNFvAQgmzJeMpBw)

## IT-110 Refining & Enhancing Your IT TICS Course Participant Guide



 **If mixed facility or Class II have you created TICS and SIC?**

Yes

No

Just TICS

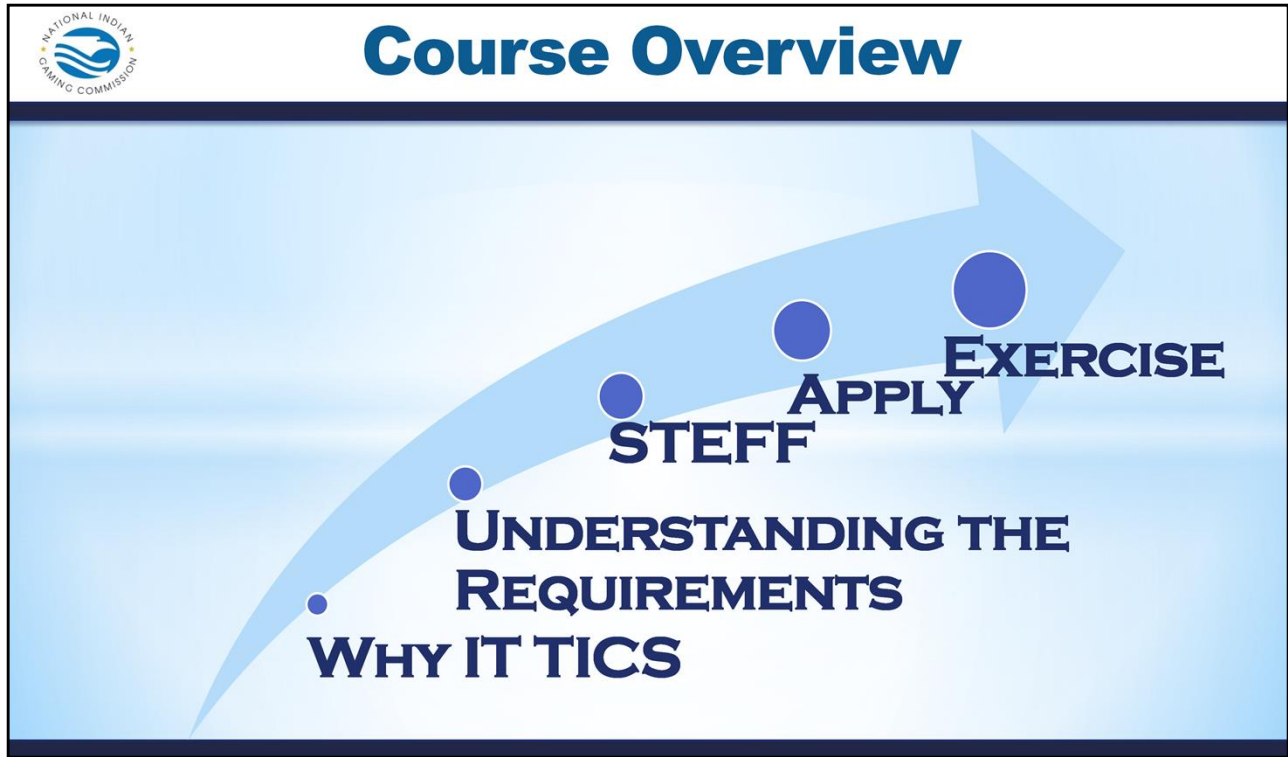
Huh?

Start the presentation to see live content. Still no live content? Install the app or get help at [PollEv.com/app](http://PollEv.com/app)

### KEY POINTS

Poll Title: If mixed facility or Class II have you created TICS and SIC?

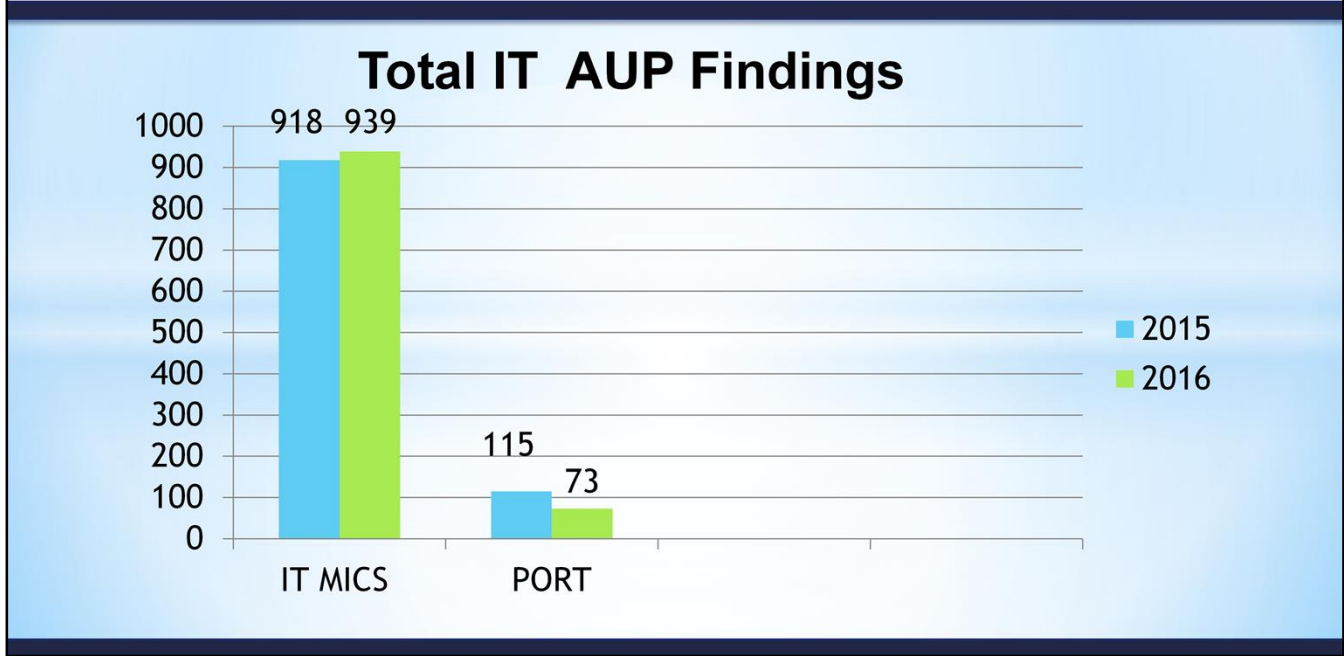
[https://www.polleverywhere.com/multiple\\_choice\\_polls/GFJu2NGRQGmiFI3](https://www.polleverywhere.com/multiple_choice_polls/GFJu2NGRQGmiFI3)



KEY POINTS



## The Why



### KEY POINTS

Comparing years 2015 & 2016 for IT Findings.

Enhancing IT TICS are based on the findings from Compliance Audits from all 7 NIGC regions and in this case your individual region.



## Common Findings

- Of the 6245 total AUP findings IT accounts for 15% of all the MICS.
- 543.20(i)(2) is the most common finding



### KEY POINTS

Overview of Agreed Upon Procedures (AUP) and the importance of reducing critical IT Findings for operations



### 543.20(i)(2)

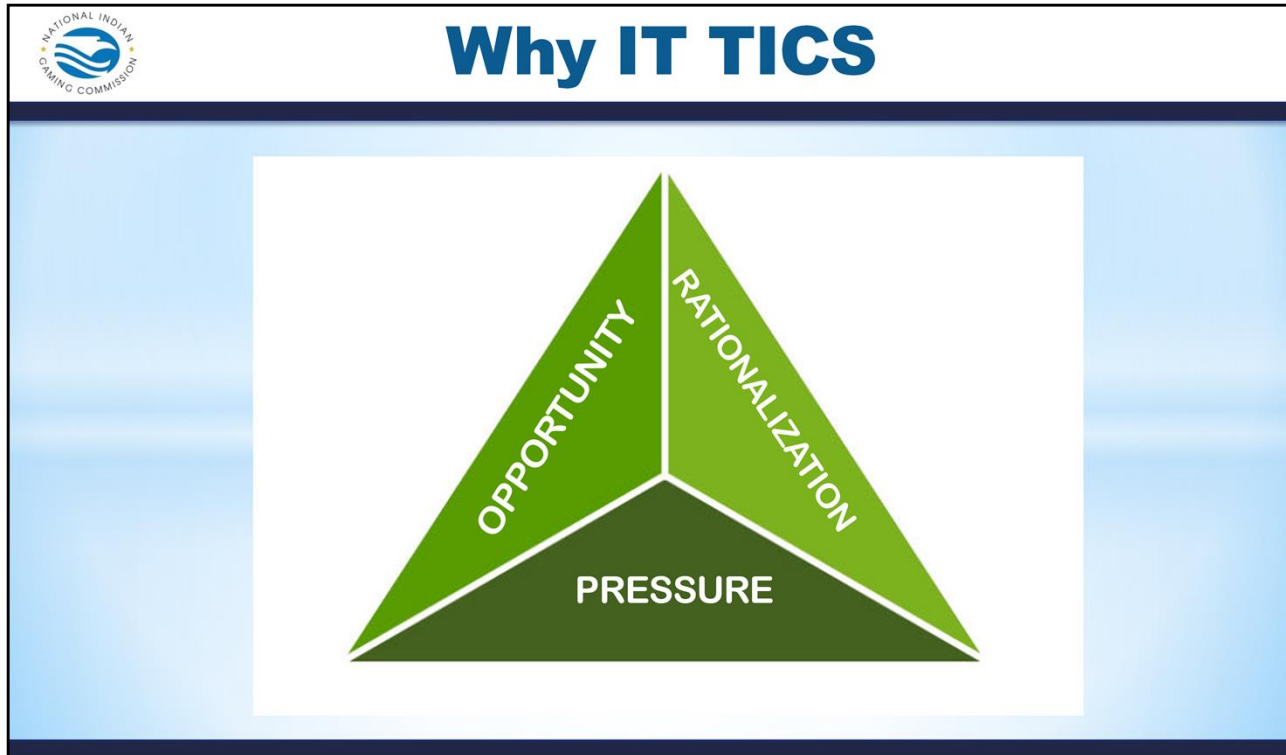
**(i) Incident monitoring and reporting.**

**(1) Procedures must be implemented** for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.

(2) All security incidents must be responded to within an established time period approved by the TGRA and formally documented.

#### KEY POINTS

543.20(i)(2) is the most common IT finding by all 7 regions. This finding is around the lack of procedures implemented during the TICS/SICS process by operations.



### KEY POINTS

- Internal controls provide reasonable assurances for asset protection, risk mitigation, and reduction in opportunities.
- Pressure - Motivation can be personal financial pressure such as debt problems and/or workplace debt to steal from the operations. i.e. gambling debt or maintaining a certain lifestyle
- Opportunity – An clear case of abuse of their position to solve their financial problems.
- Rationalization - A means of how an individual can/will defraud the operation. Many criminals are first time fraudsters and don't see themselves as criminals but rather a victim of circumstance. i.e. taking care of family or a dishonest employer





# MICS - §543.20

**What are the minimum internal control standards for information technology and information technology data?**

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate...

### KEY POINTS

Looking at Section C of 543.20 what does this one standard mean?

Is this standard enough to ensure proper coverage of your operations.



## Language - Internal Control Standards

**TRIBAL**  
**TICS**

Controls Must Be  
Established

**SYSTEM**  
**SICS**

And Procedures  
Implemented to  
ensure adequate...

PRESS

### KEY POINTS

Importance of TICS and implementing SICS the procedures associated to internal TICS



# MICS §543.20

### **(c) Class II gaming systems' logical and physical controls.**

- (1) Control of physical and logical access to the information technology environment,
- (2) Physical and logical protection of storage media and its contents
- (3) Access credential control methods
- (4) Record keeping and audit processes
- (5) Departmental independence

#### **KEY POINTS**

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

- (1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;
- (2) Physical and logical protection of storage media and its contents, including recovery procedures;
- (3) Access credential control methods;
- (4) Record keeping and audit processes; and
- (5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments



## Exercise #1 – Handout #1

1. Review Exercise #1 Handout #1
2. Answer these questions:

**Should the TGRA expand on this Control ?  
Why or Why Not?**



### KEY POINTS

**Activity:** Discussion - Expanding Controls

**TIME:** 5 minutes

### Instructions:

1. Working at your tables, review this control:

#### **§543.20**

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:


(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

2. Discuss and answer these questions:

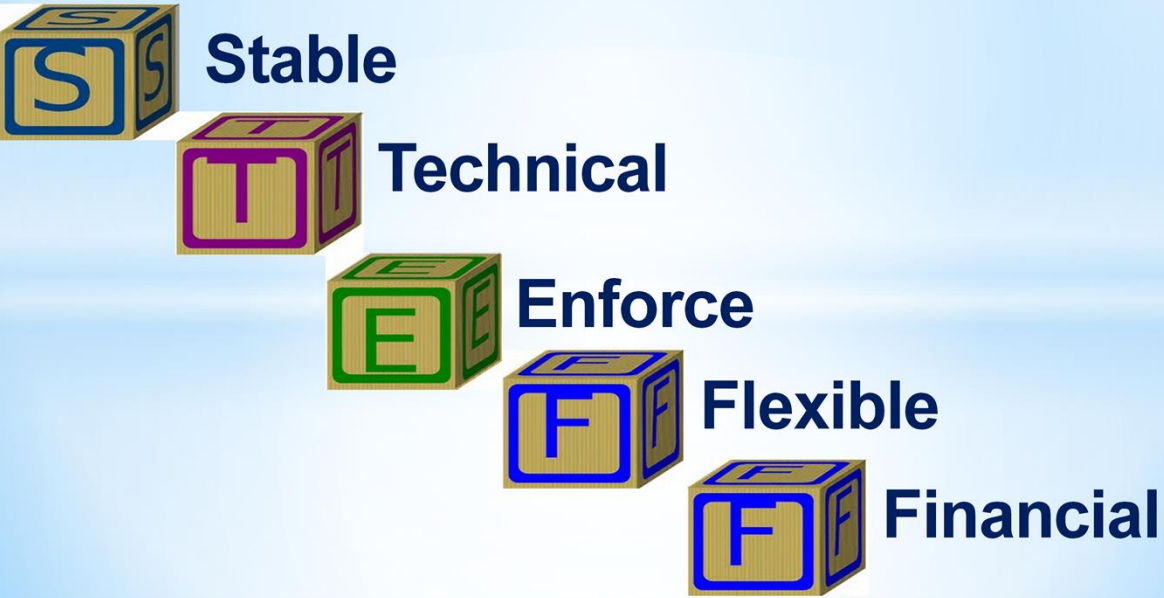
**Should the TGRA expand on this Control?**

**-and-**

**Why or Why Not?**



## Building Blocks



**Stable**

**Technical**

**Enforce**

**Flexible**

**Financial**

### KEY POINTS

Stable – Firm, Established, Secure, Solid, Steady

Technical – Practical, Scientific, High-tech, maybe mechanical (according to a strict application or interpretation of the rules)

Enforce – Impose, Apply, Administer, Implement, mandatory, binding, contractual

Flexible – pliable, stretch, springy, adaptable, adjustable, versatile, variable, open-ended, cooperative

Financial – Economic impact, fiscal, banking, investment



# Stable

### IT TICS should:

- Promote a regulatory environment
- Outcome focused

### Accomplished by:

- Employing individuals with requisite IT experience with
- In-depth knowledge of IT systems



### KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Stability the initial building block for STEFF should provide a foundation for creating your TICS/SICS.



## Technical

### IT TICS should provide:

- Proper technical intelligence for IT TIC enhancement and
- Fostering objective, and transparent procedures

**Greater Transparency  
&  
Increased Accountability**



### KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Technical the second foundational principle of STEFF is important to ensure your team has reviewed and included all pertinent technical aspects to your TICS/SICS.



# Enforcement

## IT TICS should contain:

- Consistency
- Execution
- Governance
- Independence



### KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Enforcement the third principle in the STEFF model should include the ability to execute and/or enforce the TICS/SICS within your operations.





## Flexible

### Sufficient and malleable TICS

- Respond promptly to technical changes
- Emerging IT threats



#### KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Flexible the fourth principle in STEF infers that all of your TICS/SICS should have enough movement to change with the IT world without having to change them all of the time.



# Financial

## TICS should

- Be cost-effective
- Not encumber your IT team
- Protect assets with resilient IT TICS



### KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Financial the fifth and final principle of STEFF should always play an important role in the building blocks in either cost effectiveness of hardware/software required as well as not be constricted in applying the pertinent IT components.



## The MICS

**Should the TGRA expand on this Control?  
Why or Why Not?**



### KEY POINTS

See 543.20(c) 1-5



# MICS §543.20

### **(c) Class II gaming systems' logical and physical controls.**

- (1) Control of physical and logical access to the information technology environment,
- (2) Physical and logical protection of storage media and its contents
- (3) Access credential control methods
- (4) Record keeping and audit processes
- (5) Departmental independence

#### **KEY POINTS**

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

- (1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;
- (2) Physical and logical protection of storage media and its contents, including recovery procedures;
- (3) Access credential control methods;
- (4) Record keeping and audit processes; and
- (5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments



## Exercise #2 – Handout #1

**1. Review Exercise #1 Handout #1.**

**2. Write additional controls for this standard.**



### KEY POINTS

**Activity:** Discussion - Expanding Controls

**TIME:** 20 minutes

### Instructions

1. Choose a note taker and presenter.
2. Working at your tables, review this control:

### §543.20

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

- (1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

## Applying Knowledge

### TIC 1 with STEFF

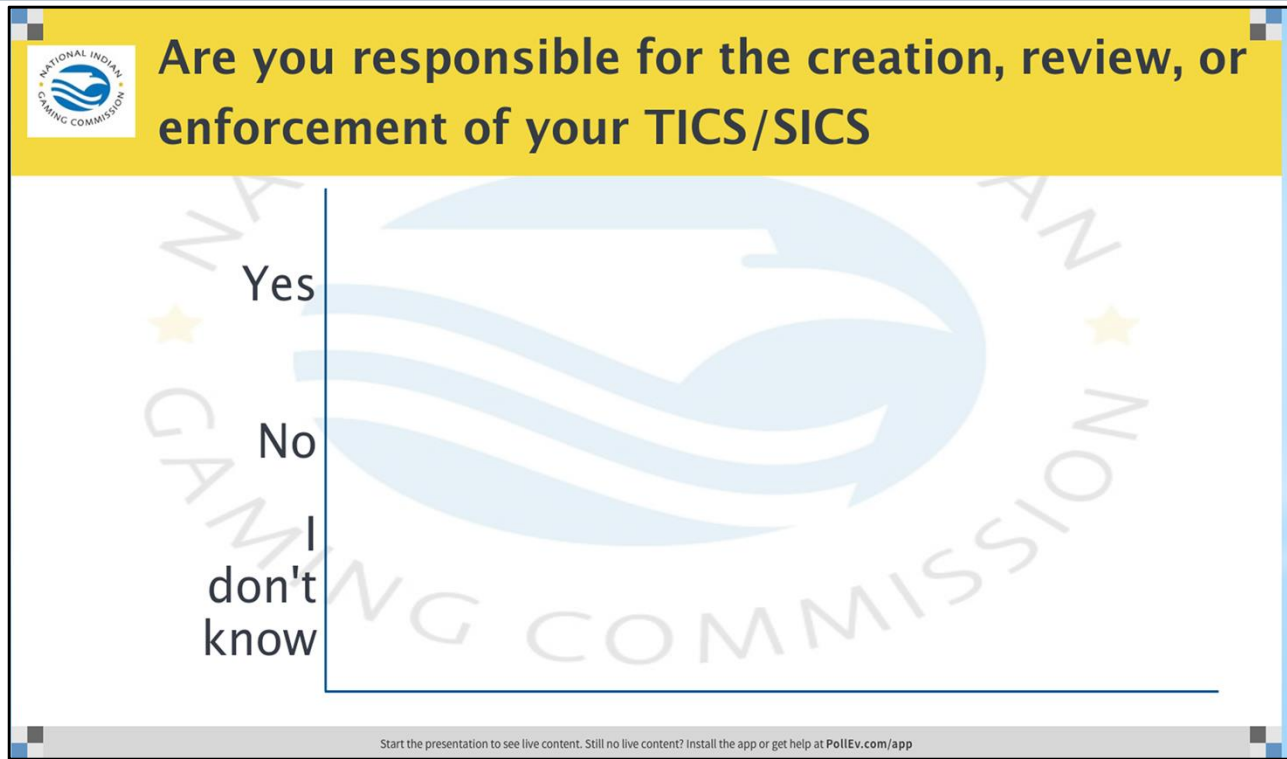
All aspects of a wireless network, including all hardware and software used therein, shall be subject to testing by the commission or an approved independent testing laboratory designated by the commission, and review and approval by the commission prior to the sale, installation, or use of the network by a licensed organization. The cost for which in all cases shall be borne by the licensed manufacturer.

22

#### KEY POINT

A TIC/SIC that demonstrates the STEFF principle

## IT-110 Refining & Enhancing Your IT TICS Course Participant Guide



The screenshot shows a poll interface with a yellow header containing the National Indian Gaming Commission logo and the poll title. The poll options are listed on the left side of a white area. A large, faint watermark of the commission's logo is visible in the background.

**Are you responsible for the creation, review, or enforcement of your TICS/SICS**

Yes

No

I don't know

Start the presentation to see live content. Still no live content? Install the app or get help at [PolleEv.com/app](https://www.polleverywhere.com/app)

### KEY POINTS

Poll Title: Are you responsible for the creation, review, or enforcement of your TICS/SICS

[https://www.polleverywhere.com/multiple\\_choice\\_polls/CEjhhc4JyBOPAax](https://www.polleverywhere.com/multiple_choice_polls/CEjhhc4JyBOPAax)



## 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 appreciated and allow us to improve your experience



### KEY POINTS