



National Indian Gaming Commission

NATIONAL TRAINING CONFERENCE

**NTC
2023**





START TIME	NIGC National Training Conference Agenda	
DAY ONE		
8:30	Welcome/Ice Breaker	
9:00	Leadership Discussion	
10:00	30-Minute Break	
10:30	How to Avoid an IGRA Violation	
12:00	Lunch (On Your Own)	
	AUDIT TRACK	COMPLIANCE TRACK
1:00	IT Findings and Best Practices	Risk Assessments
2:00	15-Minute Break	
2:15	Cybersecurity Incident Response Plans	Risk Assessments (Continued)
3:15	15-Minute Break	
3:30	Cybersecurity Incident Response Plans (Continued)	Ethical Considerations for Regulators
4:30	DAY ONE: Wrap-up and Q&A	
DAY TWO		
8:30	Top 10 Audit Findings	Panel: The Regulatory Landscape
9:30	15-Minute Break	
9:45	Intent and Testing: Bingo Toolkit	Criminal History Record Information (CHRI) and Compliance with 25 CFR Part 558.3(e)
10:45	15-Minute Break	
11:00	Intent and Testing: Bingo Toolkit (Continued)	Essential Roles of a Regulator
12:00	Lunch (On Your Own)	
1:00	Panel: Roundtable Discussion with Internal Audit Professionals	Report Writing
2:00	15-Minute Break	
2:15	Critical Thinking: Enhancing the Internal Audit	Background Investigations: Eligibility Determination for Nuanced Standards
3:15	15-Minute Break	
3:30	Critical Thinking: Enhancing the Internal Audit (Continued)	Background Investigations: Eligibility Determination for Nuanced Standards (Continued)
4:30	DAY TWO: Wrap-up and Q&A	



DAY THREE	
8:30	Emergency Preparedness Roundtable
9:30	<i>15-Minute Break</i>
9:45	Introduction to Emergency Preparedness Planning
10:45	<i>15-Minute Break</i>
11:00	Table Top Exercise
12:00	<i>Lunch (On Your Own)</i>
1:00	Table Top Exercise (Continued)
2:00	<i>15-Minute Break</i>
2:15	Panel Discussion with Federal Agencies/OSHA and Indian Health Services (IHS)
3:15	<i>15-Minute Break</i>
3:30	Security Threat Assessments
4:30	Event Concludes

COURSE DESCRIPTIONS



Leadership Discussion

This regional and national update will give attendees on understanding of the hot button issues facing our industry, from areas of concern to technological updates, to an open format that welcomes your questions.

Intended Audience: All

How to Avoid an IGRA Violation

The Indian Gaming Regulatory Act has specific areas where non-compliance can lead a Tribe to a violation. The best way to ensure your operation remains compliant is to know the common problems and the best ways to avoid them. Join our Office of General Counsel as they point out the pitfalls and give you timely tips for success.

Intended Audience: All

Audit Track

Course listing in order of schedule



Information Technology Audit Findings and Best Practices to Remediate Risk

Information Technology issues continue to be one of the highest reported findings submitted to the NIGC through external reporting. This course provides an overview of the most repeated findings in the gaming industry. Hear from our IT professionals as they discuss the top findings and give you the tools to determine intent and testing requirements essential to remediate information technology non-compliance.

Intended Audience: IT Professionals, Internal Auditors, and Tribal Gaming Regulatory Authorities

Cyber Security Incident Response Plans

It is not a matter of if, but when! A cyber-attack can happen at any moment in an operation – will you know what to do? Incident response plans are critical to overcome and limit the damage an incident can cause. This interactive course will challenge you to bring your critical thinking skills, which will guide you in the development of an incident plan that you can take back to your facility.

Intended Audience: Tribal Gaming Regulators, Operations Personnel, IT Professionals, Risk and Safety Personnel

Top 10 Audit Findings

Do you have audit findings on our Top 10? Don't know? Find out in this presentation of the Top 10 most common audit findings as identified through annual AUP independent audit reports, internal audit reports and NIGC internal control assessments. This course will cover the intent of the control, and provides specific instructions and exercises focusing on identifying and correcting findings. You will leave with an increased understanding of and ability to identify and remedy like findings at your gaming operations.

Intended Audience: Tribal Regulators, Auditors, Casino Operations

Intent and Testing: Bingo Toolkit

Understanding the intent of a standard is the first step in ensuring appropriate testing is occurring. Join us as we go through the Bingo Tool Kit where we will discuss how it can be used, engage in practical exercises, and discuss the intent and testing process to help build better controls and testing methods. This course will help tribal regulators, internal auditors,

and operations personnel to better understand the MICS for class II gaming.

Intended Audience: Internal Auditors, Operations, and Regulator Personnel

Panel: Roundtable Discussion with Internal Audit Professionals

Join this panel of internal audit professionals as they discuss the current landscape of the Internal Audit process for their gaming operations. Dive into the issues they face and hear how they have overcome these challenges.

Intended Audience: Internal Auditors, Operations Personnel, Regulators, and those interested in Internal Audit

Critical Thinking: Enhancing the Internal Audit

Looking to improve your skills? Then we have the course for you. This course increases your understanding of objective and critical thinking skills necessary to evaluate and test a standard to ensure testing is appropriate. The course is intended for experienced operations and regulatory compliance personnel with a working understanding of the internal audit process.

Intended Audience: Internal Auditors, Operations and Regulatory Compliance



Risk Assessments

Not that risk is everywhere, but it is... In this course, we will discuss risk assessments and lead participants to discover their risk and apply resources over high-risk areas to limit exposure to potential violations. This activity-based session will help you start the conversation about strengths, weakness, opportunities and threats with your team!

Intended Audience: Tribal Leadership, Commissioners, and TGRA staff

Ethical Considerations for Regulators

The wonderful world of gaming is full of shinny things and freebees... or is it? In this course, we will dive into ethics and tools for navigating ethical situations. Daily, TGRA's and Commissioners may encounter situations where ethical decisions come into play. We will start the conversation on building an ethical culture within your department, and share real-life examples and lessons learned when encountering common ethical issues.

Intended Audience: Tribal Leadership, Commissioners, and Tribal Gaming Regulatory Authorities

Panel: The Regulatory Landscape

Join this panel of regulatory professionals as they discuss all the trending topics facing the Indian gaming industry. Hear from the panelist on how they are addressing the challenges as the landscape continues to change.

Intended Audience: All

Criminal History Record Information (CHRI) and Compliance with 25 CFR Part 558.3(e)

Join staff from the NIGC Criminal Justice Information Services Audit Unit (CAU) for a discussion about CHRI and compliance with 25 CFR Part 558.3(e).

Intended Audience: Background and Licensing Personnel, LASO's and other Regulatory Personnel

Essential Roles of a Regulator

Regulators like all staff in gaming operations are asked to perform many tasks. Being an expert in all things gaming is difficult, if not impossible. Let us break down some essential

roles of regulators to ensure compliance. We will also look at some areas throughout the gaming operation that have valuable reports (i.e. revenue audit, surveillance, internal audit) to help in your day-to-day activities.

Intended Audience: Tribal Leadership, Commissioners and Tribal Gaming Regulatory Authorities

Report Writing

Tired of the same old report writing class? Well, this is just like those... only fun! Designed for both experienced and new TGRA staff as well as any tribal gaming department that writes reports, we have filled this hands-on, activity-based course with information to improve report-writing skills.

Intended Audience: Tribal Gaming Regulatory Authorities, Security, Surveillance, and Commissioners

Background Investigations: Eligibility Determination for Nuanced Standards

What do you think when you hear Reputation, Habits, and Associations? What about Prior Activities? Join us as we look at the nuanced language of the Background Investigations for PMO/KE. You will work together in this interactive course, using critical thinking skills to develop a process to bring back to your operations.

Intended Audience: Background and Licensing Personnel, Regulatory Personnel, individuals interested in developing processes

Emergency Preparedness Workshop

Course listing in order of schedule



Emergency Preparedness Roundtable

In this session, you will hear from industry professionals, who lead emergency preparedness for their tribal casino organizations. They will discuss the importance of effective team building, training and collaboration to achieve emergency preparedness in addition to identifying who makes command decisions, the command structure and identify the primary decision makers.

Intended Audience: Risk and Safety Personnel, Operations, Security, and Regulator Personnel

Emergency Preparedness Plan

The Emergency Preparedness Plan is designed to guide casino team members, management and regulatory personnel in the response to critical and emergency situations. The primary purpose is to protect team members and guests. This plan establishes a command structure so sound decisions can be made and these decisions effectively communicated to team members and guests.

Intended Audience: Risk and Safety Personnel, Operations, Security, and Regulator Personnel

Introduction to Emergency Preparedness “Table Top Exercise”

In this session, you will learn the importance of creating and practicing your Emergency Preparedness Plan (EPP), and who to include in your plan inside and outside your organization. Given the increase of natural and man-made disasters, preparedness has never been more critical to our tribal gaming industry. You will take away best practices and the recently release EPP template. In conjunction with this exercise, you will learn, evaluate and validate plans and capabilities, develop individual performance, improve interagency coordination, and identify capability gaps and opportunities for improvement. This will strengthen your Emergency Preparedness Plan’s ability to prepare, respond to, and recover from various critical incidents. A Wildfire scenario worksheet will be discussed and filled out for interactive discussion.

Intended Audience: Risk and Safety Personnel, Operations, Security, and Regulator Personnel

Panel Discussion with Federal Agencies/OSHA and Indian Health Services (IHS)

In this session, you will hear from Federal/OSHA Region IX Area Director who will discuss OSHA’s commitment to worker safety and health while collaborating with tribal casinos on safe practices to reduce employee injury and raise health awareness in addition to OSHA updates. You will also hear from the IHS Division of Environmental Health Services who will

discuss their role in partnerships with tribal casino health and food safety among other topics.

Intended Audience: Risk and Safety Personnel, Operations, Security, and Regulator Personnel

Security Threat Assessments

In this session, you will hear from industry professionals and how they manage risks and threats through leadership, experience, assessments, and training. Join us as these experts discuss the latest technology used to keep guests and employees safe in addition to the physical security of their facilities.

Intended Audience: Risk and Safety Personnel, Operations, Security, and Regulator Personnel

Leadership Discussion

National Indian Gaming Commission



Leadership Discussion

Industry Integrity

Agency Accountability

Preparedness

Outreach



NIGC National Training Conference Evaluation
Course Name: Leadership Discussion

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.


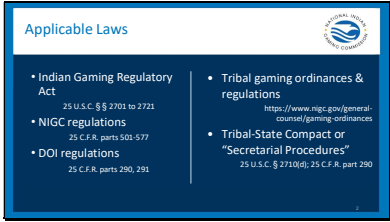
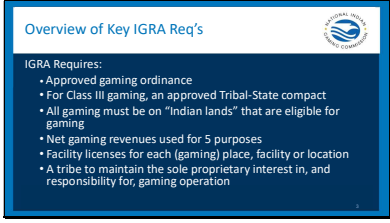
How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.






The Requirements of IGRA & How to Avoid a Violation Participant Guide




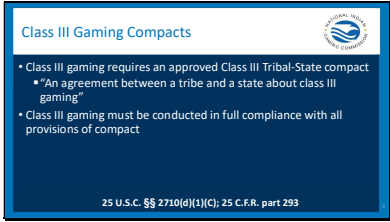

How to Avoid an IGRA Violation Participant Guide

<p>Slide 1</p>		
<p>Slide 2</p>		
<p>Slide 3</p>		

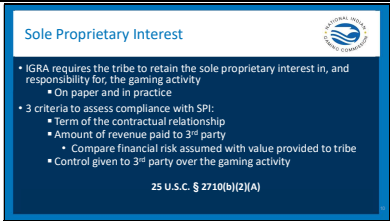
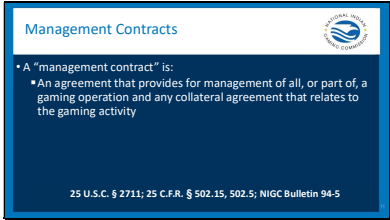

How to Avoid an IGRA Violation Participant Guide

<p>Slide 4</p>	<p>Overview of Key IGRA Req's Continued</p>  <ul style="list-style-type: none">• Safely construct, maintain and operate gaming facilities to adequately protect environment, public health & safety• Background investigations, eligibility determinations, and gaming license for every key employee and primary management officials• Annual audits of each gaming operations• Approved management contracts, if 3rd party will be managing gaming operation• Regulation of "Individually owned gaming"	
<p>Slide 5</p>	<p>Tribal Gaming Ordinances</p>  <ul style="list-style-type: none">• Class II or III gaming ordinance must be approved by NIGC Chair• Ordinance is effective only after approval• Must contain all provisions required by IGRA & NIGC regulations 	
<p>Slide 6</p>	<p>Tribal Gaming Ordinances Continued</p>  <ul style="list-style-type: none">• Amendments must be submitted to NIGC Chair for approval within 15 days of enactment• OGC will review the entire ordinance when reviewing an Amendment 	


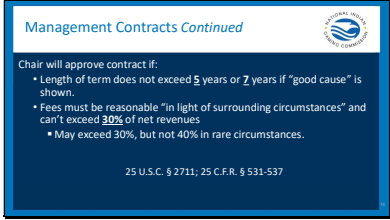
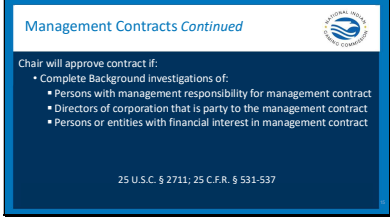
How to Avoid an IGRA Violation Participant Guide

<p>Slide 7</p>		
<p>Slide 8</p>		
<p>Slide 9</p>		

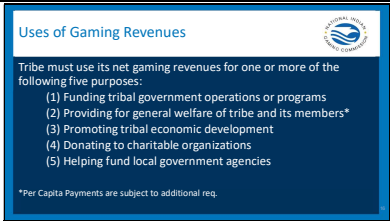
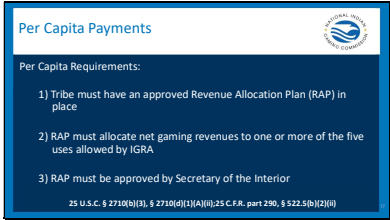
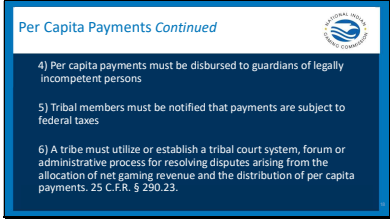
How to Avoid an IGRA Violation Participant Guide

Slide 10	 <p>Sole Proprietary Interest</p> <ul style="list-style-type: none">• IGRA requires the tribe to retain the sole proprietary interest in, and responsibility for, the gaming activity<ul style="list-style-type: none">• On paper and in practice• 3 criteria to assess compliance with SPI:<ul style="list-style-type: none">• Term of the contractual relationship• Amount of revenue paid to 3rd party• Compare financial risk assumed with value provided to tribe• Control given to 3rd party over the gaming activity <p>25 U.S.C. § 2710(b)(2)(A)</p>	
Slide 11	 <p>Management Contracts</p> <ul style="list-style-type: none">• A "management contract" is:<ul style="list-style-type: none">• An agreement that provides for management of all, or part of, a gaming operation and any collateral agreement that relates to the gaming activity <p>25 U.S.C. § 2711; 25 C.F.R. § 502.15, 502.5; NIGC Bulletin 94-5</p>	
Slide 12	 <p>Management Contracts Continued</p> <ul style="list-style-type: none">• A "collateral agreement" is:<ul style="list-style-type: none">• Contract that is related to management contract, either directly or indirectly• Any rights, duties or obligations created between tribe and management contractor or subcontractor <p>25 U.S.C. § 2711; 25 C.F.R. § 502.15, 502.5; NIGC Bulletin 94-5</p>	





How to Avoid an IGRA Violation Participant Guide

Slide 13	 <p>Management Contracts Continued</p> <ul style="list-style-type: none">• Must be submitted to NIGC Chair for review within 60 days of execution by parties• Is effective only when approved by NIGC Chair• Tribe may not allow Contractor to operate under management contract terms before approval <p>25 U.S.C. §§ 2710(d)(a), 2711; 25 C.F.R. Part 531, 533</p>	
Slide 14	 <p>Management Contracts Continued</p> <p>Chair will approve contract if:</p> <ul style="list-style-type: none">• Length of term does not exceed 5 years or 7 years if "good cause" is shown.• Fees must be reasonable "in light of surrounding circumstances" and can't exceed 30% of net revenues• May exceed 30%, but not 40% in rare circumstances. <p>25 U.S.C. § 2711; 25 C.F.R. § 531-537</p>	
Slide 15	 <p>Management Contracts Continued</p> <p>Chair will approve contract if:</p> <ul style="list-style-type: none">• Complete background investigations of:<ul style="list-style-type: none">• Persons with management responsibility for management contract• Directors of corporation that is party to the management contract• Persons or entities with financial interest in management contract <p>25 U.S.C. § 2711; 25 C.F.R. § 531-537</p>	




How to Avoid an IGRA Violation Participant Guide

<p>Slide 16</p>		
<p>Slide 17</p>		
<p>Slide 18</p>		

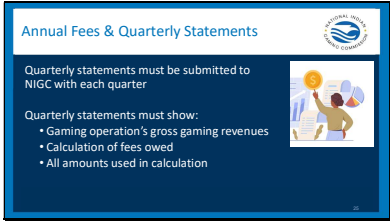

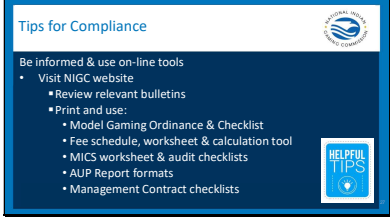
How to Avoid an IGRA Violation Participant Guide

<p>Slide 19</p>	<div data-bbox="386 226 773 445"> <p>Background Investigations</p>  <p>Tribes must conduct background investigations of all <i>primary management official (PMO)</i> and <i>key employee (KE)</i> applicants of the <i>gaming operation</i> before they can be licensed</p> <ul style="list-style-type: none"> • Must be conducted according to requirements in tribe's gaming ordinance and NIGC regulations Parts 536 & 538 • NIGC Regulations specify jobs that are PMO/KE • Tribe can designate additional PMO/KE who will need a full background investigation <p>25 C.F.R. §§ 522.5(b)(5), 502.14, 502.19</p> </div>	
<p>Slide 20</p>	<div data-bbox="386 760 773 978"> <p>Safe Construction & Operation of Gaming Facilities</p>  <p>Tribes must safely construct, maintain and operate gaming facilities to adequately protect environment, public health & public safety</p>  <p>25 U.S.C. § 2710(b)(2)(E), (d)(2)(A); 25 C.F.R. §§ 522.5(b)(7)</p> </div>	
<p>Slide 21</p>	<div data-bbox="386 1293 773 1512"> <p>Facility Licenses</p>  <ul style="list-style-type: none"> • Tribe must issue license for each place, facility, or location at which Class II or Class III gaming is conducted • The Tribe must provide notice to NIGC Chair that license is being considered 120 days before opening of new facility, place or location • Once license is issued, copy must be submitted to NIGC Chair within 30 days <p>25 C.F.R. part 559</p> </div>	


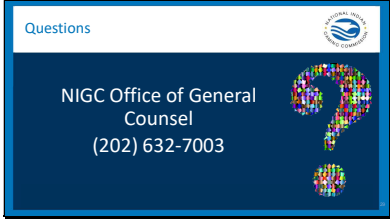
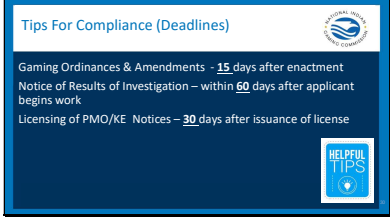
How to Avoid an IGRA Violation Participant Guide

<p>Slide 22</p>	<div data-bbox="386 224 773 443"> <p>Annual Audits & Financial Statements</p>  <ul style="list-style-type: none"> Annual audit must be conducted by <i>independent</i> Certified Public Accountant (CPA) conducted of each gaming operation <ul style="list-style-type: none"> Audit must be based on annual financial statements of each gaming operation Two copies of the annual audit must be submitted to NIGC within 120 days of end of fiscal year <p>28 U.S.C. § 2710(b)(2)(C)-(D); 25 C.F.R. §§ 522.5(b)(3)-(4), 571.12-13</p> </div>	
<p>Slide 23</p>	<div data-bbox="386 758 773 976"> <p>Agreed-Upon Procedures</p>  <ul style="list-style-type: none"> Agreed-Upon Procedures (AUPs) must be performed <i>annually</i> by independent CPA to verify that the Class II gaming operation is in compliance with Class II minimum internal control standards (MICS) CPA will prepare a report of their findings and present it to the Tribe Tribe must submit AUP reports to NIGC 120 days after the end of the fiscal year. <p>25 C.F.R. § 543.23(d)</p> </div>	
<p>Slide 24</p>	<div data-bbox="386 1291 773 1509"> <p>Annual Fees</p>  <p>Annual fees must be paid by each tribal gaming operation to NIGC</p> <ul style="list-style-type: none"> Fee rate set annually by NIGC and Published on or before November 1. Based on the gross gaming revenue for the fiscal year ending prior to January 1 of the current year. <p>Fee payments are calculated by each gaming operation in a "Quarterly Statement." http://www.nigc.gov/finance/Annual-fees</p> <p>25 U.S.C. § 2717; 25 C.F.R. part 514</p> </div>	

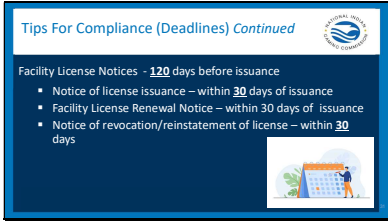
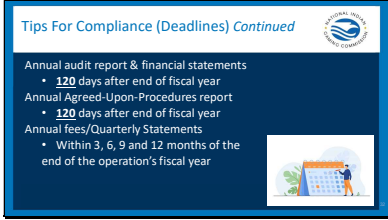

How to Avoid an IGRA Violation Participant Guide

<p>Slide 25</p>	 <p>Annual Fees & Quarterly Statements</p> <p>Quarterly statements must be submitted to NIGC with each quarter</p> <p>Quarterly statements must show:</p> <ul style="list-style-type: none"> • Gaming operation's gross gaming revenues • Calculation of fees owed • All amounts used in calculation 	
<p>Slide 26</p>	 <p>Tips for Compliance</p> <p>Know the laws that apply to you and your gaming operation and where to find them.</p> <p>Take advantage of NIGC expertise, services and on-line resources</p> <ul style="list-style-type: none"> • For compliance issues contact NIGC Regional staff • For legal questions contact OGC. <p>Learn from other examples</p> <ul style="list-style-type: none"> • www.nigc.gov/general-counsel 	
<p>Slide 27</p>	 <p>Tips for Compliance</p> <p>Be informed & use on-line tools</p> <ul style="list-style-type: none"> • Visit NIGC website <ul style="list-style-type: none"> • Review relevant bulletins • Print and use: <ul style="list-style-type: none"> • Model Gaming Ordinance & Checklist • Fee schedule, worksheet & calculation tool • MICS worksheet & audit checklists • AUP Report formats • Management Contract checklists 	

How to Avoid an IGRA Violation Participant Guide

Slide 28	 <p>Tips for Compliance</p> <p>Be informed & use on-line tools</p> <ul style="list-style-type: none">• Visit NIGC website• Review upcoming trainings and attend one• Access IGRA and NIGC & DOI regulations <p>HELPFUL TIPS</p>	
Slide 29	 <p>Questions</p> <p>NIGC Office of General Counsel (202) 632-7003</p>	
Slide 30	 <p>Tips For Compliance (Deadlines)</p> <p>Gaming Ordinances & Amendments - <u>15</u> days after enactment Notice of Results of Investigation – within <u>60</u> days after applicant begins work Licensing of PMO/KE Notices – <u>30</u> days after issuance of license</p> <p>HELPFUL TIPS</p>	

How to Avoid an IGRA Violation Participant Guide

<p>Slide 31</p>	 <p>Tips For Compliance (Deadlines) Continued</p> <p>Facility License Notices - 120 days before issuance</p> <ul style="list-style-type: none"> • Notice of license issuance – within 30 days of issuance • Facility License Renewal Notice – within 30 days of issuance • Notice of revocation/reinstatement of license – within 30 days 	
<p>Slide 32</p>	 <p>Tips For Compliance (Deadlines) Continued</p> <p>Annual audit report & financial statements</p> <ul style="list-style-type: none"> • 120 days after end of fiscal year <p>Annual Agreed-Upon-Procedures report</p> <ul style="list-style-type: none"> • 120 days after end of fiscal year <p>Annual fees/Quarterly Statements</p> <ul style="list-style-type: none"> • Within 3, 6, 9 and 12 months of the end of the operation's fiscal year 	
<p>Slide 33</p>	 <p>Tips For Compliance (Deadlines) Continued</p> <p>Management Contracts</p> <ul style="list-style-type: none"> • Within 60 days of execution <p>Amendments</p> <ul style="list-style-type: none"> • Within 30 days of execution 	



NIGC National Training Conference Evaluation
Course Name: How to Avoid an IGRA Violation

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

IT Findings and Best Practices Participant Guide

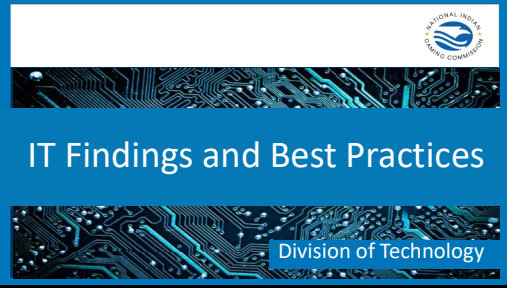



IT Findings and Best Practices

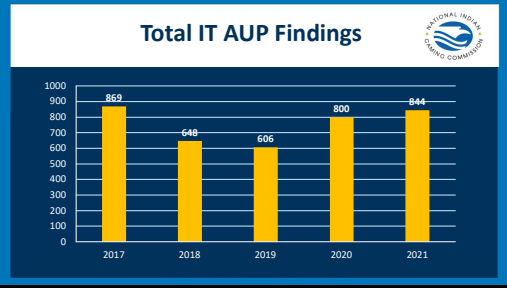
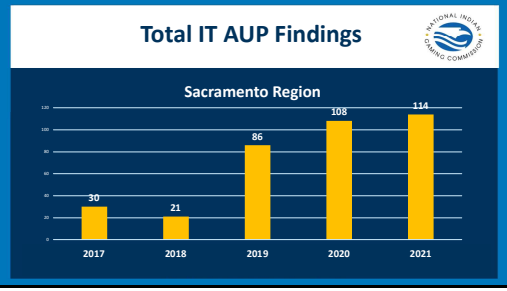
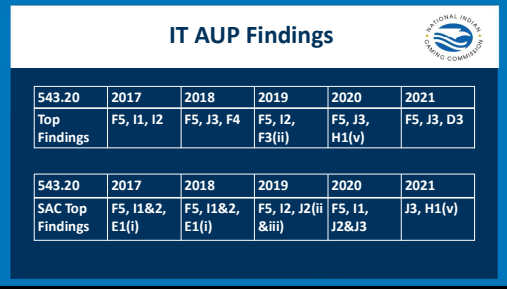


Division of Technology

IT Findings and Best Practices Participant Guide

Slide 1	 <p>IT Findings and Best Practices</p> <p>Division of Technology</p>	PARTICIPANT QUESTION CHALLENGE The time allotted for this virtual training will allow each of you to ask questions. I challenge each of you to ask a question! Your participation will make this training a success today!
Slide 2	 <p>Overview</p> <ul style="list-style-type: none">AUP IT Data ReviewIT MICS Top FindingsIT AUP Recap <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	Key Points Rather than discuss specific types of trending attacks and vulnerabilities, in this course we aim to take a different approach. We will be looking at specific data/events/timelines of successful cyber-attacks within Indian Country in recent years, and then by reviewing what happened in those attacks we will discuss lessons learned, ways to reduce the chance of a similar attack, and uncover possible lapses in compliance.

IT Findings and Best Practices Participant Guide

<p>Slide 3</p>		<p>Key Points Information Technology Agreed Upon Procedures number of findings by year.</p>																		
<p>Slide 4</p>		<p>Key Points Information Technology Agreed Upon Procedures number of findings by year for Sacramento Region.</p>																		
<p>Slide 5</p>	 <table border="1"> <thead> <tr> <th></th> <th>2017</th> <th>2018</th> <th>2019</th> <th>2020</th> <th>2021</th> </tr> </thead> <tbody> <tr> <td>543.20 Top Findings</td> <td>F5, I1, I2</td> <td>F5, J3, F4</td> <td>F5, I2, F3(ii)</td> <td>F5, J3, H1(v)</td> <td>F5, J3, D3</td> </tr> <tr> <td>543.20 SAC Top Findings</td> <td>F5, I1&2, E1(i)</td> <td>F5, I1&2, E1(i)</td> <td>F5, I2, J2(ii) & iii)</td> <td>F5, I1, J2&J3</td> <td>J3, H1(v)</td> </tr> </tbody> </table>		2017	2018	2019	2020	2021	543.20 Top Findings	F5, I1, I2	F5, J3, F4	F5, I2, F3(ii)	F5, J3, H1(v)	F5, J3, D3	543.20 SAC Top Findings	F5, I1&2, E1(i)	F5, I1&2, E1(i)	F5, I2, J2(ii) & iii)	F5, I1, J2&J3	J3, H1(v)	<p>Key Points Common IT Findings per year nationally and for the Sacramento Region.</p>
	2017	2018	2019	2020	2021															
543.20 Top Findings	F5, I1, I2	F5, J3, F4	F5, I2, F3(ii)	F5, J3, H1(v)	F5, J3, D3															
543.20 SAC Top Findings	F5, I1&2, E1(i)	F5, I1&2, E1(i)	F5, I2, J2(ii) & iii)	F5, I1, J2&J3	J3, H1(v)															

IT Findings and Best Practices Participant Guide

<p>Slide 6</p>	<div style="border: 1px solid black; padding: 10px;"> <div style="text-align: center;"> <h3>F(5) User Controls</h3> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">Citation</th> <th style="width: 30%;">Language</th> <th style="width: 50%;">Intent and Testing</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="text-align: center;">§ 543.20 (f-g)</td> </tr> <tr> <td>543.20 (f)(4)</td> <td>Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.</td> <td> Intent: To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. Testing: Review TICS, SICs, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported. </td> </tr> <tr> <td>543.20(g)</td> <td>Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.</td> <td> Intent: To ensure that access credentials of terminated users are deactivated in the minimum time period stated by the TGRA. Testing: 1. Review TICS, SICs, Policies and Procedures and Employee Manuals for employee, IT Management and Human Resources action when compromised credentials are reported. 2. Review user access lists for former employees. </td> </tr> </tbody> </table> </div>	Citation	Language	Intent and Testing	§ 543.20 (f-g)			543.20 (f)(4)	Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.	Intent: To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. Testing: Review TICS, SICs, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported.	543.20(g)	Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.	Intent: To ensure that access credentials of terminated users are deactivated in the minimum time period stated by the TGRA. Testing: 1. Review TICS, SICs, Policies and Procedures and Employee Manuals for employee, IT Management and Human Resources action when compromised credentials are reported. 2. Review user access lists for former employees.	<p>Key Points</p> <p>Over the past 5 years, User Controls is a common finding that continue to show up on the AUPs. Why are User Controls a finding to overcome?</p>
Citation	Language	Intent and Testing												
§ 543.20 (f-g)														
543.20 (f)(4)	Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.	Intent: To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. Testing: Review TICS, SICs, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported.												
543.20(g)	Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.	Intent: To ensure that access credentials of terminated users are deactivated in the minimum time period stated by the TGRA. Testing: 1. Review TICS, SICs, Policies and Procedures and Employee Manuals for employee, IT Management and Human Resources action when compromised credentials are reported. 2. Review user access lists for former employees.												
<p>Slide 7</p>	<div style="border: 1px solid black; padding: 10px;"> <div style="text-align: center;"> <h3>F(5) User Controls</h3> </div> <ol style="list-style-type: none"> 1. Are user's access secured with passwords/MFA? 2. Who is assigned to control, update or modify system functions? 3. Are there roles and responsibilities for controls and are they approved by the TGRA? 4. Are user controls recorded with Who, When, Why and What was completed? </div>	<p>Key Points</p> <p>Some thoughts to think about when reviewing policies and procedures around User Controls.</p>												
<p>Slide 8</p>	<div style="border: 1px solid black; padding: 10px;"> <div style="text-align: center;"> <h3>F(5) User Controls</h3> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>As TGRA what would be the best time period (in hours) for assuring lost, compromised or access credentials of terminated users be deactivated?</p> <p>A. 8 B. 12 C. 24 D. 48</p> </div> </div>	<p>Key Points</p> <p>Answer question</p>												




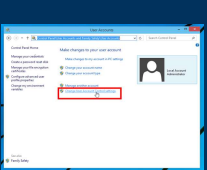
IT Findings and Best Practices Participant Guide

<p>Slide 9</p>	<div style="border: 2px solid blue; padding: 5px;"> <p style="text-align: center;">I(1) Incident Monitoring & Reporting </p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">Citation</th> <th style="width: 35%;">Language</th> <th style="width: 50%;">Intent and Testing</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="text-align: center;">§ 543.20 (g-1)</td> </tr> <tr> <td>543.20(i)</td> <td>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.</td> <td> <p>Intent: To ensure expedient and appropriate response to computerized incidents, faults, errors or cyber attacks.</p> <p>Testing: 1. Review TICS, SICS, IT Policies and Procedures and review sampling of Incident Responses and the courses of action taken. 2. Review relevant work orders, job orders or work requests completed to address the incident(s).</p> </td> </tr> </tbody> </table> </div>	Citation	Language	Intent and Testing	§ 543.20 (g-1)			543.20(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.	<p>Intent: To ensure expedient and appropriate response to computerized incidents, faults, errors or cyber attacks.</p> <p>Testing: 1. Review TICS, SICS, IT Policies and Procedures and review sampling of Incident Responses and the courses of action taken. 2. Review relevant work orders, job orders or work requests completed to address the incident(s).</p>	<p>Key Points</p> <p>Do you have procedures implemented for responding to, monitoring, investigating, resolving, documenting and reporting security incidents and/or cyberattacks?</p>
Citation	Language	Intent and Testing									
§ 543.20 (g-1)											
543.20(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.	<p>Intent: To ensure expedient and appropriate response to computerized incidents, faults, errors or cyber attacks.</p> <p>Testing: 1. Review TICS, SICS, IT Policies and Procedures and review sampling of Incident Responses and the courses of action taken. 2. Review relevant work orders, job orders or work requests completed to address the incident(s).</p>									
<p>Slide 10</p>	<div style="border: 2px solid blue; padding: 5px;"> <p style="text-align: center;">I(2) Incident Monitoring & Reporting </p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">Citation</th> <th style="width: 35%;">Language</th> <th style="width: 50%;">Intent and Testing</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="text-align: center;">§ 543.20 (g-1)</td> </tr> <tr> <td>543.20(i)(2)</td> <td>All security incidents must be responded to within an established time period approved by the TGRA and formally documented.</td> <td> <p>Intent: To ensure all security incidents are responded to and addressed within a practical time period to mitigate the associated incident risk.</p> <p>Testing: Review TICS, SICS, or P&P for a time period established by security incidents should be responded to as soon as possible from the moment of notification.</p> </td> </tr> </tbody> </table> </div>	Citation	Language	Intent and Testing	§ 543.20 (g-1)			543.20(i)(2)	All security incidents must be responded to within an established time period approved by the TGRA and formally documented.	<p>Intent: To ensure all security incidents are responded to and addressed within a practical time period to mitigate the associated incident risk.</p> <p>Testing: Review TICS, SICS, or P&P for a time period established by security incidents should be responded to as soon as possible from the moment of notification.</p>	<p>Key Points</p> <p>Security Incidents should be responded to within a timeframe from the moment of notification.</p>
Citation	Language	Intent and Testing									
§ 543.20 (g-1)											
543.20(i)(2)	All security incidents must be responded to within an established time period approved by the TGRA and formally documented.	<p>Intent: To ensure all security incidents are responded to and addressed within a practical time period to mitigate the associated incident risk.</p> <p>Testing: Review TICS, SICS, or P&P for a time period established by security incidents should be responded to as soon as possible from the moment of notification.</p>									
<p>Slide 11</p>	<div style="border: 2px solid blue; padding: 5px; background-color: #0056b3; color: white;"> <p style="text-align: center;">Incident Response Review </p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px; vertical-align: top;"> <p>Do I understand my business risk? Have I identified the types of assets and information that need to be protected?</p> <p>Has my organization developed a security strategy and communicated it effectively?</p> </td> <td style="width: 50%; padding: 5px; vertical-align: top;"> <p>Do I have the right tools in place to ensure timely incident detection and response?</p> <p>Have I developed a formal incident response plan? Have I tested the efficacy of my current incident response plan and processes?</p> </td> </tr> </table> <p style="text-align: right; font-size: small;">Source: OWG</p> </div>	<p>Do I understand my business risk? Have I identified the types of assets and information that need to be protected?</p> <p>Has my organization developed a security strategy and communicated it effectively?</p>	<p>Do I have the right tools in place to ensure timely incident detection and response?</p> <p>Have I developed a formal incident response plan? Have I tested the efficacy of my current incident response plan and processes?</p>	<p>Key Points</p> <p>Some questions to consider when reviewing incident response plan?</p>							
<p>Do I understand my business risk? Have I identified the types of assets and information that need to be protected?</p> <p>Has my organization developed a security strategy and communicated it effectively?</p>	<p>Do I have the right tools in place to ensure timely incident detection and response?</p> <p>Have I developed a formal incident response plan? Have I tested the efficacy of my current incident response plan and processes?</p>										






IT Findings and Best Practices Participant Guide

<p>Slide 12</p>		<p>Key Points</p> <p>See Handout insert at end of the slide pages. Fill in the blank with one of the phrases in the white box for each description with one of the 5 elements for each portion of the pie chart. Use this handout to collect your thoughts and gather notes to take back to use at your property.</p>
<p>Slide 13</p>		<p>Key Points</p> <p>Do we have controls including recovery procedures with restoration and redundant backup?</p>
<p>Slide 14</p>		<p>Key Points</p> <p>Review recovery testing documentation for performance and results of recovery testing.</p>

IT Findings and Best Practices Participant Guide

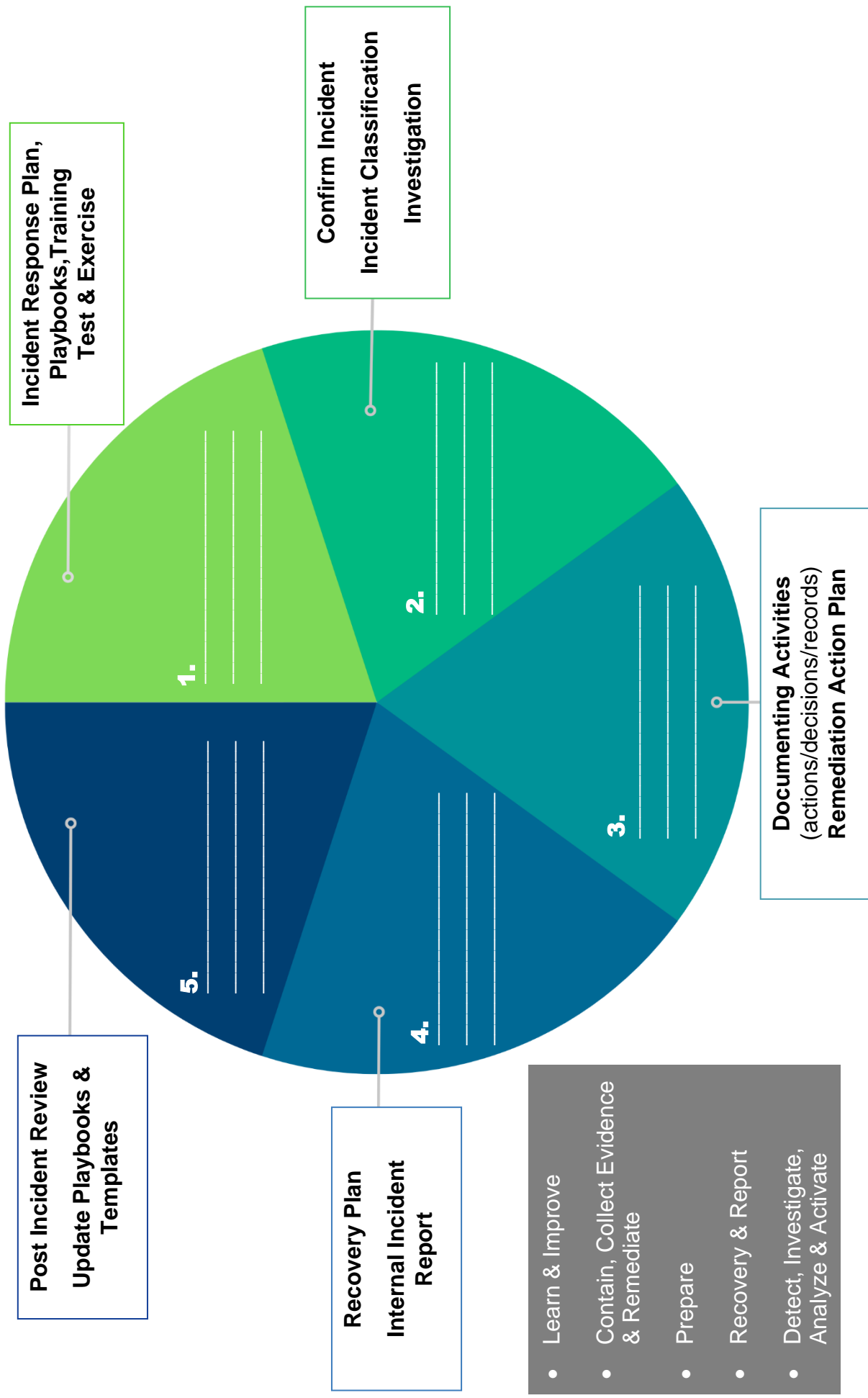
<p>Slide 15</p>	<div data-bbox="391 275 894 558"> <h3 style="text-align: center;">NIGC Data Backup Finding</h3>  <p>...it was determined recovery procedures are not tested on a sample basis at specified intervals.</p> <p>...personnel be trained on the early stages of restoring an IT Department to functional operation as a result of a significant or catastrophic negative event.</p> <p>This should include the ability to perform the image replacement of servers if need be, the transfer or restoration of data from an offsite location, etc. Training should extend to the verification that the data backup and recovery architectural network, with accompanying hardware, will be functional when needed.</p> <p>A 'test' environment, or a sandbox testing environment set-up to utilize 'dummy' or test servers, switches, routers, software, etc., provides a test/training environment for technicians to hone their skills in anticipation of a real and significant event.</p> <p>Pass/Fail evaluation should be documented for both the personnel under annual training/evaluation, as well as Pass/Fail for the infrastructure that those personnel will be required to perform</p> </div>	<h3>Key Points</h3> <p>Portion of an actual NIGC finding on data backups along with recommendation.</p>
<p>Slide 16</p>	<div data-bbox="391 806 894 1089"> <h3 style="text-align: center;">Data Backup Steps</h3>  <ol style="list-style-type: none"> 1. Familiarize yourself with your backup and recovery systems 2. Run tests to recover & restore deleted or corrupted files 3. Test the backup of your applications 4. Test your database recovery & restoration 5. Time how long it takes to back up your data 6. Try testing your backup, recovery & restoration plan; remotely if possible 7. Continue to test your database backup and recovery plan regularly <p style="text-align: right; font-size: small;">Source: Technology Advisor</p> </div>	<h3>Key Points</h3> <p>Review of Data Backup processes to ensure all bases are covered.</p>
<p>Slide 17</p>	<div data-bbox="391 1337 894 1621"> <h3 style="text-align: center;">IT AUP Recap</h3>  <div data-bbox="402 1455 672 1545"> <p>F(S) User Controls For lost or compromised access credentials as well as access credentials of terminated users are deactivated with an <i>established time period approved by the TGRA</i></p> </div>  </div>	

IT Findings and Best Practices Participant Guide

<p>Slide 18</p>	<div data-bbox="391 275 894 558"> <p style="text-align: center;">IT AUP Recap</p>  <p>I(1 & 2) Incident Monitoring & Reporting For responding to, monitoring, investigating, resolving and documenting security/IT incidents be sure procedures are implemented in an established time period approved by the TGRA.</p>  </div>							
<p>Slide 19</p>	<div data-bbox="391 808 894 1092"> <p style="text-align: center;">IT AUP Recap</p>  <p>J(2 & 3) Data Backup For controls including recovery procedures should include program restoration and redundancy of backup hardware restoration. Recovery procedures need to be tested at specified intervals with documented results.</p>  </div>							
<p>Slide 20</p>	<div data-bbox="391 1341 894 1625"> <p style="text-align: center;">Questions</p>  <table border="1" style="width: 100%; text-align: center;"> <tr> <td data-bbox="407 1411 558 1507"> <p>Eddie Hall IT Auditor eddie.hall@nigc.gov</p> </td> <td data-bbox="565 1411 716 1507"> <p>Michael Curry IT Auditor michael.curry@nigc.gov</p> </td> <td data-bbox="722 1411 873 1507"> <p>Jeran Cox IT Auditor jeran.cox@nigc.gov</p> </td> </tr> <tr> <td data-bbox="477 1516 628 1612"> <p>Tim Cotton IT Audit Manager timothy.cotton@nigc.gov</p> </td> <td colspan="2" data-bbox="662 1516 836 1612"> <p>Training Technical Assistance traininginfo@nigc.gov</p> </td> </tr> </table> </div>	<p>Eddie Hall IT Auditor eddie.hall@nigc.gov</p>	<p>Michael Curry IT Auditor michael.curry@nigc.gov</p>	<p>Jeran Cox IT Auditor jeran.cox@nigc.gov</p>	<p>Tim Cotton IT Audit Manager timothy.cotton@nigc.gov</p>	<p>Training Technical Assistance traininginfo@nigc.gov</p>		
<p>Eddie Hall IT Auditor eddie.hall@nigc.gov</p>	<p>Michael Curry IT Auditor michael.curry@nigc.gov</p>	<p>Jeran Cox IT Auditor jeran.cox@nigc.gov</p>						
<p>Tim Cotton IT Audit Manager timothy.cotton@nigc.gov</p>	<p>Training Technical Assistance traininginfo@nigc.gov</p>							

Information Technology Findings and Best Practices – Handout

Instructions: Review the process wheel below. Using the phrases in the grey box, write the correct phrase matching the corresponding process indicated.





NIGC National Training Conference Evaluation
Course Name: IT Findings and Best Practices

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.



Lined writing area consisting of multiple horizontal lines for text entry.



A series of horizontal lines for writing, spaced evenly down the page.

Cyber Security Incident Response Plans Participant Guide


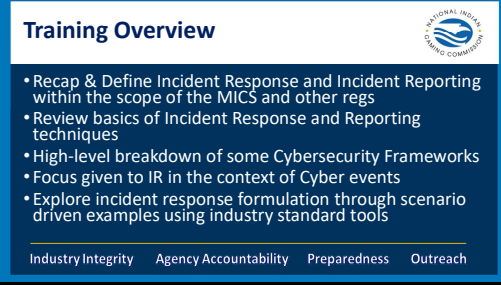
National Indian Gaming Commission





Cyber Security Incident Response Plans




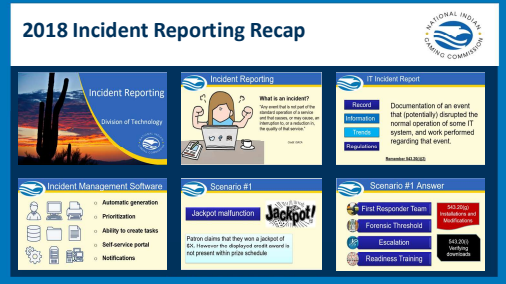
Cyber Security Incident Response Plans Participant Guide

<p>Slide 1</p>		<p>KEY POINTS</p> <p>It is not a matter of if but when! A cyber-attack can happen at any moment in an operation, will you know what to do?</p> <p>Incident response plans are critical to overcome and limit the damage an incident can cause.</p> <p>This interactive course will challenge you to bring your critical thinking skills, and assist in the development of an incident plan that you can take back to your facility.</p>
<p>Slide 2</p>		<p>KEY POINTS</p> <p>Recap & Define Incident Response and Incident Reporting within the scope of the MICS and cyber security frameworks</p> <p>Identify why we need Incident Reporting</p> <p>Review basics of Incident Response and Reporting techniques</p> <p>Explore incident response formulation through scenario driven examples using industry standard tools.</p>

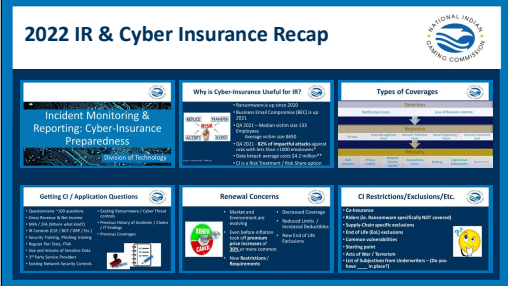
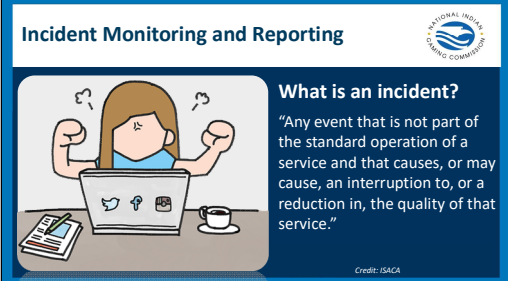
Cyber Security Incident Response Plans Participant Guide

<p>Slide 3</p>	<div data-bbox="391 275 889 558" style="border: 1px solid black; padding: 5px;"> <p style="text-align: right;"></p> <p>MICS Requirements</p> <p>Incident Monitoring & Reporting - 25 CFR 543.20(i)(1)</p> <p>“Procedures <i>must</i> be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.”</p>  </div>	<p>KEY POINTS</p> <p>(i) <i>Incident monitoring and reporting.</i></p> <ul style="list-style-type: none"> • Procedures must be implemented (SICS need to be developed) for <i>responding</i> to, <i>monitoring</i>, <i>investigating</i>, <i>resolving</i>, <i>documenting</i>, and <i>reporting</i> security incidents associated with information technology systems. <p>(2) All security incidents must be responded to within an established time period approved by the TGRA and formally documented.</p> <p>A lot contained in 543.20(i)(1)</p> <p>Responding Monitoring Investigating Resolving Documenting Reporting</p> <p>Many Different things can constitute a security incident. Hardware failure, weather events, internal threats, external threat actors just to name a few.</p> <p>How do we deal with this, by having robust procedures in places to deal with the variety of incidents</p>
----------------	--	---

Cyber Security Incident Response Plans Participant Guide

<p>Slide 4</p>	 <p>FBI CSP rev. 5.9.2 Requirements</p> <ul style="list-style-type: none"> • 5.3.1 Reporting Security Events • 5.3.2 Management of Security Incidents • 5.3.2.1 Incident Handling • 5.3.3 Incident Response Training • 5.3.4 Incident Monitoring • 5.13.5 Incident Response (Mobile) 	<p>KEY POINTS</p> <p>Here are a few of the additional requirements laid out in the FBI’s CSP 5.9.1</p> <p>5.3.1 Reporting Security Events 5.3.2 Management of Security Incidents 5.3.2.1 Incident Handling 5.3.3 Incident Response Training 5.3.4 Incident Monitoring 5.13.5 Incident Response (Mobile)</p> <p>https://www.fbi.gov/file-repository/cjis_security_policy_v5-9-1_20221001.pdf/view</p>
<p>Slide 5</p>	 <p>2018 Incident Reporting Recap</p> <p>Incident Reporting Incident Reporting IT Incident Report Incident Management Software Scenario #1 Scenario #1 Answer</p>	<p>KEY POINTS</p> <p>A recap of the 2018/2019 training on Incident Reporting: We covered the importance of Incident Response and dove into one responsibility within the MICS... Incident Reporting</p> <p>While we did cover many different scenarios and IR steps and types of remediation...we did not cover every imaginable one. One we did not get into enough detail in was the topic of cyber security incidents so...</p>

Cyber Security Incident Response Plans Participant Guide

<p>Slide 6</p>	 <p>The slide is a grid of six topics related to 2022 IR and Cyber Insurance. The topics are: Incident Monitoring & Reporting: Cyber-Insurance Preparedness; Why is Cyber-Insurance Useful for IR?; Types of Coverages; Getting CI / Application Questions; Renewal Concerns; and CI Restrictions/Exclusions/Etc. Each topic has a small icon and a brief description of the content.</p>	<p>KEY POINTS</p> <p>A recap of the 2022 training on IR and Cyber Insurance:</p> <p>We covered the importance of one aspect of IR and the value of Cyber Insurance as a tool to supplement and fortify your Incident response policies and procedures and some of the tips and challenges of obtaining or renewing an insurance policy.</p>
<p>Slide 7</p>	 <p>The slide features a cartoon illustration of a woman sitting at a desk with a laptop, looking thoughtful. To the right of the illustration, the text reads: "What is an incident? 'Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.'" The credit "Credit: ISACA" is at the bottom right.</p>	<p>KEY POINTS</p> <ul style="list-style-type: none"> • A very broad definition of what is an incident - ISACA's definition of Incident. • Additional resources for official strategies: <ul style="list-style-type: none"> • NIST Special Publication 800-61-r2 • NIST Special Publication 800-184 • ISACA Incident Management and Response • ITIL Service Operation • ITIL IM • ISO 20000-1

Cyber Security Incident Response Plans Participant Guide

Slide 8

Path to Incident Response (Part 1)



Incident response plan
The operational component of incident management. Including **documented procedures** and guidelines for **defining the criticality of incidents**, reporting and escalation process, and recovery procedures.

Credit: ISACA

1) Define types of Incidents

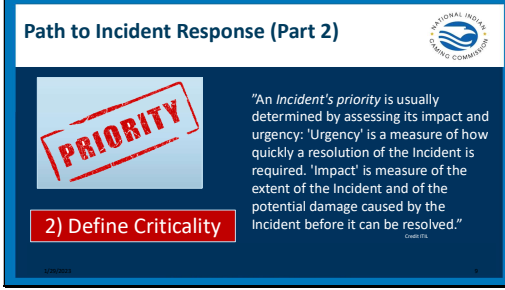
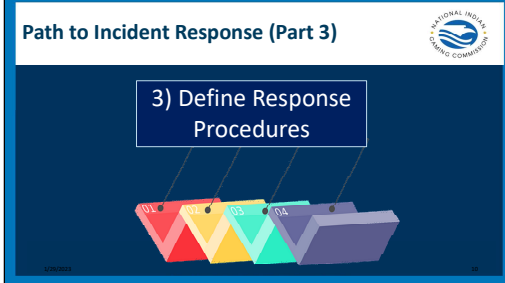
KEY POINTS

- ISACA's definition of **Incident response plan**
- An incident Response Plan is the operational component of incident management.
- The plan includes documented procedures and guidelines for defining the criticality of incidents, reporting and escalation process, and recovery procedures.

Possible IT Incident categories:

- Multiple Player Card failures
 - Unauthorized access to CHRI
- Public facing website down
 - IDF switch outage
- Floor switch outage
 - Outage in virtual server environment
- Power outage that results in system failure
- Hardware cooling outage
 - Portion of any gaming floor outage
- POS outage
- Kiosk / ATM outage
- Check / Cash Advance outage
 - Phone outages
- Radio outage
 - Surveillance infrastructure outage
- Any additional item at *discretion* of IT/GC/Operations management


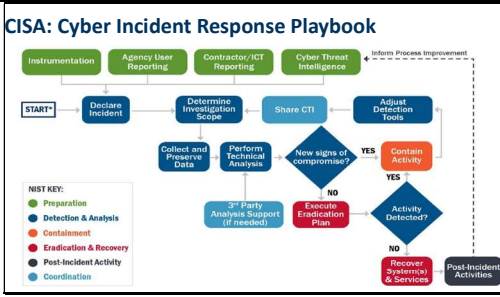
Cyber Security Incident Response Plans Participant Guide

<p>Slide 9</p>		<p>KEY POINTS</p> <ul style="list-style-type: none"> To cover incidents with the correct resources we need to define how critical the incident is. The ITIL's (Information Technology Infrastructure Library) definition of Incident's Priority. ITIL looks at Urgency, Urgency can be defined within the SICS and SOPs, or if allowed by the SICS at the discretion of IT Management. <p>In summary: What is the Priority and who is provides the initial support? NOTE: Remember 543.20(a)(1) Supervision</p>
<p>Slide 10</p>		<p>KEY POINTS</p> <ul style="list-style-type: none"> Another important step in the Incident Response process is defining the appropriate procedures for each type of incident. <p>While IT staff may know how to respond to various incidents, those response procedures are frequently lacking or nonexistent.</p> <p>In summary</p> <ul style="list-style-type: none"> How do you respond? – Answer depends on the kind of issue Who is involved? – Depends on the criticality and affected teams Resolution and Record keeping Ownership, monitoring, tracking, customer communication Incident closure

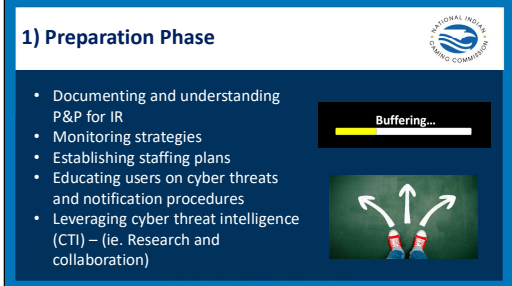
Cyber Security Incident Response Plans Participant Guide

		<p>Note: Best practices also deal with root cause analysis and remediation strategies, but those are typically not involved in the process at this stage.</p>
<p>Slide 11</p>	<div data-bbox="386 804 889 1087"> <p>Incident Response (IR) Standards</p> <ul style="list-style-type: none"> • NIST CSF (Cyber Security Framework) -- Evolution of NIST 800-53 Rev5 • SOC 2 Control Framework -- AICPA (Compliance / Auditing focus) • CIS v8 -- (Cyber Defense focus) • IEC 62443 -- (Mechanical focus) • NERC CIP v5 -- (Critical Infrastructure focus) • ISO 27001 -- (Industrial focus) </div>	<p>KEY POINTS</p> <p>We have to implement IR P&P, but do not have to start from scratch. Many effective standards exist. Such as IT / IR standards and frameworks.</p> <ul style="list-style-type: none"> - NIST – National Institute of Standards and Technology - CSF used extensively, advised by CISA (circa 2021) - SOC 2 -- System and Organization Controls: (AICPA) American Institute of Certified Professional Accountants - (Auditing Focused) (circa 2020) - CIS v8 – Center for Internet Security Critical Security Controls for Effective Cyber Defense - SANS Institute / Council on Cyber Security (CCS) – (circa 2021) - IEC 62443 – ISAC - International Society of Automation Cybersecurity Standard (circa 2009-2020) - NERC CIP v5 - North American Electric Reliability Corp - Critical





Cyber Security Incident Response Plans Participant Guide

		<p>Infrastructure Protection (circa 2013-2014) - ISO/IEC 27001 – International Organization for Standardization / International Electrotechnical Commission (circa 2017-2019)</p>
<p>Slide 12</p>	 <p>The slide thumbnail shows the title 'CISA: Cyber Incident Response Playbook' with the National Indian Gaming Commission logo. It features a dark blue background with a network diagram and the URL https://www.cisa.gov/cyber-incident-response. Logos for the Cybersecurity & Infrastructure Security Agency and the National Indian Gaming Commission are also present.</p>	<p>KEY POINTS Today we will focus on one specific playbook published by CISA that has a strong focus on cybersecurity events.</p> <p>CISA: Cybersecurity Incident and Vulnerability Response Playbook</p> <p>https://www.cisa.gov/cyber-incident-response</p>
<p>Slide 13</p>	 <p>The flowchart, titled 'CISA: Cyber Incident Response Playbook', details the incident response process. It starts with 'START*' leading to 'Declare Incident'. This is followed by 'Determine Investigation Scope', which branches into 'Collect and Preserve Data' and 'Perform Technical Analysis'. 'Perform Technical Analysis' leads to a decision 'New signs of compromise?'. If 'YES', it leads to 'Contain Activity', then 'Execute Eradication Plan', and finally 'Recover Systems & Services'. If 'NO', it leads to '3rd Party Analysis Support (if needed)'. A second decision 'Activity Detected?' follows 'Execute Eradication Plan'. If 'YES', it leads to 'Contain Activity'. If 'NO', it leads to 'Recover Systems & Services'. The process concludes with 'Post-Incident Activities' and 'Inform Process Improvement'. A 'NIST KEY' is provided at the bottom left, defining colors for Preparation (green), Detection & Analysis (blue), Containment (orange), Eradication & Recovery (red), Post-Incident Activity (grey), and Coordination (light blue).</p>	<p>KEY POINTS CISA: Cybersecurity Incident and Vulnerability Response Playbook</p> <p>Preparation Detection & Analysis Containment Eradication & Recovery Post-Incident Activity Coordination</p> <p>https://www.cisa.gov/cyber-incident-response</p>

Cyber Security Incident Response Plans Participant Guide

Slide 14		KEY POINTS <ul style="list-style-type: none">• Documenting and understanding policies and procedures for incident response• Instrumenting the environment to detect suspicious and malicious activity• Establishing staffing plans• Educating users on cyber threats and notification procedures• Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity

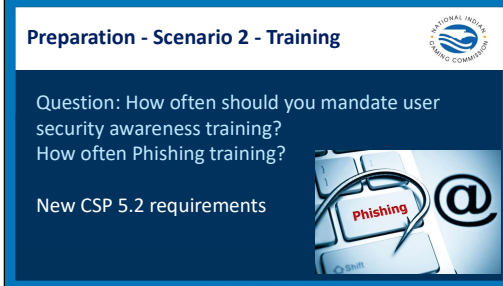
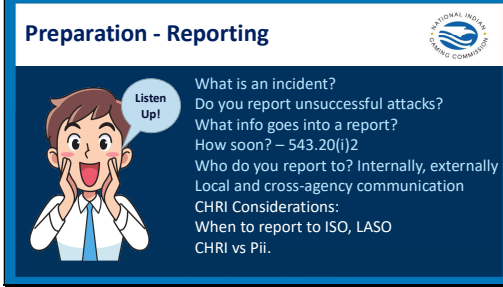
Cyber Security Incident Response Plans Participant Guide

<p>Slide 15</p>	<p>Preparation - Monitoring</p>  <p>How to monitor?</p> <p>Tools: AV, IDS, EDR, SOC</p> <p>Techniques: Audit reviews, access review, deactivated user reviews</p>  <p>CJIS considerations: CSP 5.4 access reviews CSP 5.10.1.3 Intrusion Detection Tools and Techniques</p>	<p>KEY POINTS</p> <ul style="list-style-type: none"> • Documenting and understanding policies and procedures for incident response • Instrumenting the environment to detect suspicious and malicious activity • Establishing staffing plans • Educating users on cyber threats and notification procedures • Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity <p>Keywords:</p> <p>AV (Anti-virus) — Looks for certain processes on a device</p> <p>IDS (Intrusion Detection Systems) — Looks for certain activity on a network</p> <p>EDR (Endpoint Protection Response) – - Looks for certain activity on a device</p> <p>SOC (Security Operation Center) --: SOC =/ SOC2</p>
<p>Slide 16</p>	<p>Preparation - Scenario 1</p>  <p>Which of these should be monitored / reviewed to reduce the risk of a cyber event? Why?</p> <p>a) VPN Access logs e) Firewall settings b) Fingerprinting systems f) All of the above c) User access lists g) Something else d) Data Backup integrity</p> 	<p>KEY POINTS</p> <ul style="list-style-type: none"> • Documenting and understanding policies and procedures for incident response • Instrumenting the environment to detect suspicious and malicious activity • Establishing staffing plans • Educating users on cyber threats and notification procedures • Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity


Cyber Security Incident Response Plans Participant Guide

Slide 17	<p>Preparation – Monitoring (Cont.)</p> <p>What to monitor? Logs, PCAP (packet capture), Cloud, Remote devices OPSEC (operational security, BCP)</p> <p>CSP 5.4.1.1 Events CSP 5.10.1.1 Boundary Protection CSP 5.10.3.1 Partitioning</p>	<p>KEY POINTS</p> <ul style="list-style-type: none"> • Documenting and understanding policies and procedures for incident response • Instrumenting the environment to detect suspicious and malicious activity • Establishing staffing plans • Educating users on cyber threats and notification procedures • Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity
Slide 18	<p>Preparation – Staffing and Training</p> <p>Trained Response Personnel</p> <p>Communication and Logistics</p> <p>Question: Only IT Staff are responsible for the security of IT systems - True / False?</p>	<p>KEY POINTS</p> <ul style="list-style-type: none"> • Documenting and understanding policies and procedures for incident response • Instrumenting the environment to detect suspicious and malicious activity • Establishing staffing plans • Educating users on cyber threats and notification procedures • Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity

Cyber Security Incident Response Plans Participant Guide

Slide 19		<p>KEY POINTS</p> <ul style="list-style-type: none"> • Documenting and understanding policies and procedures for incident response • Instrumenting the environment to detect suspicious and malicious activity • Establishing staffing plans • Educating users on cyber threats and notification procedures • Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity
Slide 20		<p>KEY POINTS</p> <ul style="list-style-type: none"> • What is an incident? • Do you report unsuccessful attacks? • What info goes into a report? (More on next slide) • How soon? (Think 543.20(i)2) • Who do you report to? Internally, externally • Local and cross-agency communication <p>www.ic3.gov -> Automatically goes to CISA and FBI</p>

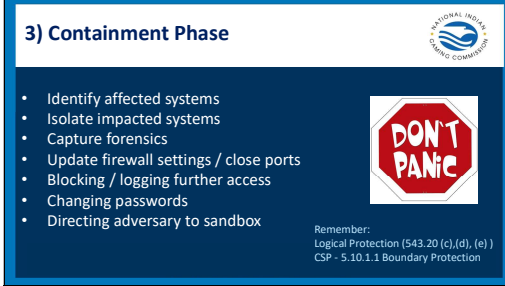
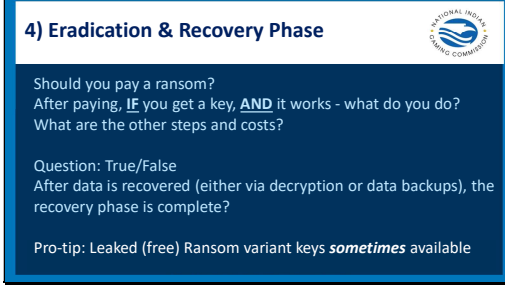
Cyber Security Incident Response Plans Participant Guide

		<p>https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20Contacting%20Law%20Enforcement%20v%201.0.pdf</p>
<p>Slide 21</p>		<p>KEY POINTS: Know before whom to contact!</p> <p>www.ic3.gov</p> <p>More detailed lists available online:</p> <p>https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident</p> <p>Logs, drive images, timeline, network topology, emails, URLs, contacted parties, etc.</p>


Cyber Security Incident Response Plans Participant Guide

Slide 22	<p>2) Detection & Analysis Phase</p> <p>What was the attack vector (access method)? Does the threat actor still have access (persistence)? If so, what is the method of persistence, (Credentials, malware)? Which accounts are compromised? (User Controls CFR 543.20(f)) Attacker's reconnaissance method? (Think: for detection, intent) Lateral movement? (Network shares, Remote access, etc.) Data exfiltration? (Ransom can become blackmail)</p>  <p><small>CIJS Considerations: CSP – 5.5 Access Control, 5.3.4 Incident Monitoring OS – 2.09 Notification of PII breach</small></p>	<p>KEY questions to answer</p> <ul style="list-style-type: none">• What was the initial attack vector? (i.e., How did the adversary gain initial access to the network?)• How is the adversary accessing the environment?• Is the adversary exploiting vulnerabilities to achieve access or privilege?• How is the adversary maintaining command and control?• Does the actor have persistence on the network or device?• What is the method of persistence (e.g., malware backdoor, webshell, legitimate credentials, remote tools, etc.)?• What accounts have been compromised and what privilege level (e.g., domain admin, local admin, user account, etc.)?• What method is being used for reconnaissance? (Discovering the reconnaissance method may provide an opportunity for detection and to determine possible intent.)• Is lateral movement suspected or known? How is lateral movement conducted (e.g., RDP, network shares, malware, etc.)?• Has data been exfiltrated and, if so, what kind and via what mechanism?
----------	--	--

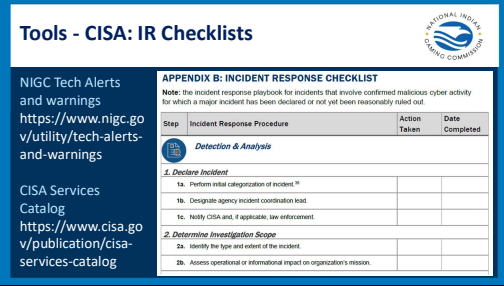
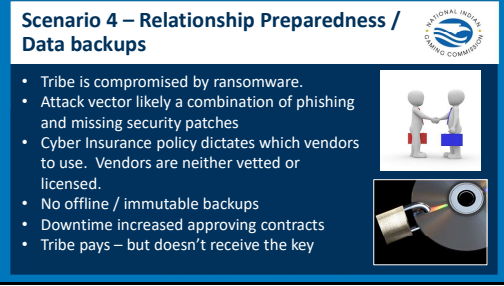
Cyber Security Incident Response Plans Participant Guide

<p>Slide 23</p>	 <p>3) Containment Phase</p> <ul style="list-style-type: none"> Identify affected systems Isolate impacted systems Capture forensics Update firewall settings / close ports Blocking / logging further access Changing passwords Directing adversary to sandbox <p>Remember: Logical Protection (543.20 (c),(d), (e)) CSP - 5.10.1.1 Boundary Protection</p>	<p>KEY POINTS</p> <ul style="list-style-type: none"> Any additional adverse impacts to mission operations, availability of services (e.g., network connectivity, services provided to external parties), Duration of the containment process, resources needed, and effectiveness (e.g., full vs. partial containment; full vs. unknown level of containment), and Any impact on the collection, preservation, securing, and documentation of evidence.
<p>Slide 24</p>	 <p>4) Eradication & Recovery Phase</p> <p>Should you pay a ransom? After paying, IF you get a key, AND it works - what do you do? What are the other steps and costs?</p> <p>Question: True/False After data is recovered (either via decryption or data backups), the recovery phase is complete?</p> <p>Pro-tip: Leaked (free) Ransom variant keys <i>sometimes</i> available</p>	<p>KEY POINTS</p> <p>Preparation Detection & Analysis Containment Eradication & Recovery Post-Incident Activity Coordination</p>

Cyber Security Incident Response Plans Participant Guide

<p>Slide 25</p>	<p>5) Post Incident Activities Phase</p>  <p>Adjust Sensors , Alerts, Log Collection</p> <p>Finalize Incident Reports – Escalate to TGRA? Law Enforcement?</p> <p>Perform a “Hotwash”</p>	<p>KEY POINTS</p> <p>Not as important as Preparation phase, but knowing what to do after an incident is complete is also important.</p> <ul style="list-style-type: none">• Adjust Sensors, Alerts, and Log Collection (IDS, EDR, Log review/retention/protection policies)• Finalize Reports• Perform Hotwash -Ensuring root-cause has been eliminated or mitigated.<ul style="list-style-type: none">> Identifying infrastructure problems to address.> Identifying organizational policy and procedural problems to address.> Reviewing and updating roles, responsibilities, interfaces, and authority to ensure clarity.> Identifying technical or operational training needs.> Improving tools required to perform protection, detection, analysis, or response actions.
-----------------	---	--


Cyber Security Incident Response Plans Participant Guide

<p>Slide 26</p>	 <p>Tools - CISA: IR Checklists</p> <p>NIGC Tech Alerts and warnings https://www.nigc.gov/utility/tech-alerts-and-warnings</p> <p>CISA Services Catalog https://www.cisa.gov/publication/cisa-services-catalog</p> <p>APPENDIX B: INCIDENT RESPONSE CHECKLIST Note: The incident response playbooks for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.</p> <table border="1"> <thead> <tr> <th>Step</th> <th>Incident Response Procedure</th> <th>Action Taken</th> <th>Date Completed</th> </tr> </thead> <tbody> <tr> <td colspan="4">Detection & Analysis</td> </tr> <tr> <td colspan="4">1. Declare Incident</td> </tr> <tr> <td>1a.</td> <td>Perform initial categorization of incident **</td> <td></td> <td></td> </tr> <tr> <td>1b.</td> <td>Designate agency incident coordination lead</td> <td></td> <td></td> </tr> <tr> <td>1c.</td> <td>Notify CISA and, if applicable, law enforcement</td> <td></td> <td></td> </tr> <tr> <td colspan="4">2. Determine Investigation Scope</td> </tr> <tr> <td>2a.</td> <td>Identify the type and extent of the incident</td> <td></td> <td></td> </tr> <tr> <td>2b.</td> <td>Assess operational or informational impact on organization's mission</td> <td></td> <td></td> </tr> </tbody> </table>	Step	Incident Response Procedure	Action Taken	Date Completed	Detection & Analysis				1. Declare Incident				1a.	Perform initial categorization of incident **			1b.	Designate agency incident coordination lead			1c.	Notify CISA and, if applicable, law enforcement			2. Determine Investigation Scope				2a.	Identify the type and extent of the incident			2b.	Assess operational or informational impact on organization's mission			<p>KEY POINTS</p> <p>Where to start writing my Policies and Procedures?</p> <p>Many Tools and Resources: NIGC Tech Alerts and warnings https://www.nigc.gov/utility/tech-alerts-and-warnings</p> <p>CISA Services Catalog https://www.cisa.gov/publication/cisa-services-catalog</p>
Step	Incident Response Procedure	Action Taken	Date Completed																																			
Detection & Analysis																																						
1. Declare Incident																																						
1a.	Perform initial categorization of incident **																																					
1b.	Designate agency incident coordination lead																																					
1c.	Notify CISA and, if applicable, law enforcement																																					
2. Determine Investigation Scope																																						
2a.	Identify the type and extent of the incident																																					
2b.	Assess operational or informational impact on organization's mission																																					
<p>Slide 27</p>	 <p>Scenario 4 – Relationship Preparedness / Data backups</p> <ul style="list-style-type: none"> • Tribe is compromised by ransomware. • Attack vector likely a combination of phishing and missing security patches • Cyber insurance policy dictates which vendors to use. Vendors are neither vetted or licensed. • No offline / immutable backups • Downtime increased approving contracts • Tribe pays – but doesn't receive the key 	<p>KEY POINTS</p> <ul style="list-style-type: none"> - Reliant on cyber insurer for all aspects of resolving issue - Everything lost. No offline backups. - When you pay you may not get the key - Even if you pay....you still have to rebuild everything. - Disaster recovery plan missing, relationships and actions not predetermined. - Incident monitoring and reporting - 543.20(i)(1) 																																				

Cyber Security Incident Response Plans Participant Guide

Slide 28

Post Incident Activities – Scenario 4 - Checklist



Step	Incident Response Procedure	Action Taken
Post-Incident Activities		
5.0. Post-Incident Activities		
Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.		
Adjust Sensors, Alerts, and Log Collection		
10a.	Add enterprise-wide detectors to mitigate against adversary TTPs that were successfully executed.	
10b.	Identify and address operational "blind spots" to adequate coverage moving forward.	
10c.	Continue to monitor the agency environment for evidence of persistent presence.	

- Divide into groups
- Designate a writer and a speaker
- List ways to adjust Monitoring practices (aka. "blind spots") from this scenario or others.

KEY POINTS

- **Adjust Sensors, Alerts, and Log Collection**
- **Finalize Reports**
- **Perform Hotwash** -Ensuring root-cause has been eliminated or mitigated.

- > **Identifying infrastructure problems to address.**

- > Identifying organizational policy and procedural problems to address.

- > Reviewing and updating roles, responsibilities, interfaces, and authority to ensure clarity.




- > Identifying technical or operational training needs.

- > Improving tools required to perform protection, detection, analysis, or response actions.

TTP = Tactics, techniques, Procedures (aka. P&P)

Discuss and list possible monitoring blind spots from this scenario or others.

Cyber Security Incident Response Plans Participant Guide

<p>Slide 29</p>	<p>Post Incident Activities – Scenario 4 – Checklist (Continued)</p>  <p>Write example IR control (P&P)</p> <p>Example: "After the event is resolved, operations/IT will provide a root-cause analysis report to TGRA within X days."</p> <table border="1"> <thead> <tr> <th>Step</th> <th>Incident Response Procedure</th> <th>Action Taken</th> </tr> </thead> <tbody> <tr> <td colspan="3">Finalize Reports</td> </tr> <tr> <td>10e.</td> <td>Provide post-incident updates as required by law and policy.</td> <td></td> </tr> <tr> <td>10f.</td> <td>Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.</td> <td></td> </tr> <tr> <td colspan="3">Perform Retrospect</td> </tr> <tr> <td>11a.</td> <td>Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process (recently experienced).</td> <td></td> </tr> <tr> <td>11g.</td> <td>Identify if agency IR processes were followed and if they were sufficient.</td> <td></td> </tr> <tr> <td>11d.</td> <td>Identify any policies and procedures in need of modification to prevent similar incidents from occurring.</td> <td></td> </tr> <tr> <td>11en.</td> <td>Identify any gaps in incident responder training.</td> <td></td> </tr> <tr> <td>11e.</td> <td>Identify any unclear or undefined roles, responsibilities, interfaces, and activities.</td> <td></td> </tr> </tbody> </table>	Step	Incident Response Procedure	Action Taken	Finalize Reports			10e.	Provide post-incident updates as required by law and policy.		10f.	Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.		Perform Retrospect			11a.	Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process (recently experienced).		11g.	Identify if agency IR processes were followed and if they were sufficient.		11d.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.		11en.	Identify any gaps in incident responder training.		11e.	Identify any unclear or undefined roles, responsibilities, interfaces, and activities.		<p>KEY POINTS</p> <p>Each team will write a sample control aligning with an item on the CISA checklist regarding the Post Incident Activities for a hypothetical cyber scenario.</p>
Step	Incident Response Procedure	Action Taken																														
Finalize Reports																																
10e.	Provide post-incident updates as required by law and policy.																															
10f.	Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.																															
Perform Retrospect																																
11a.	Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process (recently experienced).																															
11g.	Identify if agency IR processes were followed and if they were sufficient.																															
11d.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.																															
11en.	Identify any gaps in incident responder training.																															
11e.	Identify any unclear or undefined roles, responsibilities, interfaces, and activities.																															
<p>Slide 30</p>	<p>6) Coordination</p>  <p>Who to call? How to report?</p> <ul style="list-style-type: none"> Contact FBI Contact CISA Contact local authorities Review intelligence to update scope, timelines, etc. Collaboration with other tribes / groups? Review / update timeline for outside services (ITVA, Pen-test, etc.) <p>Don't forget NIGC ISO, and others.</p>	<p>KEY POINTS</p> <p>Inform and Update NIGC / CISA / FBI</p> <p>Review provided intelligence</p> <p>Update scope, timelines, etc.</p> <p>CISA and FBI determine escalation</p> <p>CISA, NIGC and others can assist with validation of received agency and 3rd party vendor reports</p>																														
<p>Slide 31</p>	<p>Questions & Contact Information</p>  <table border="1"> <tbody> <tr> <td> <p>Jeran Cox IT Auditor Jeran.Cox@nigc.gov</p> </td> <td> <p>Michael Curry IT Auditor Michael.Curry@nigc.gov</p> </td> <td> <p>Derek Holbert CJIS Systems ISO Derek.Holbert@nigc.gov</p> </td> </tr> <tr> <td> <p>Eddie Hall IT Auditor Eddie.Hall@nigc.gov</p> </td> <td> <p>Tim Cotton IT Audit Manager Timothy.Cotton@nigc.gov</p> </td> <td> <p>Training Technical Assistance traininginfo@nigc.gov</p> </td> </tr> </tbody> </table>	<p>Jeran Cox IT Auditor Jeran.Cox@nigc.gov</p>	<p>Michael Curry IT Auditor Michael.Curry@nigc.gov</p>	<p>Derek Holbert CJIS Systems ISO Derek.Holbert@nigc.gov</p>	<p>Eddie Hall IT Auditor Eddie.Hall@nigc.gov</p>	<p>Tim Cotton IT Audit Manager Timothy.Cotton@nigc.gov</p>	<p>Training Technical Assistance traininginfo@nigc.gov</p>	<p>KEY POINTS</p> <p>If you would like more information or would like to request this training in person, please go to www.nigc.gov and hit the "Request Training" link.</p>																								
<p>Jeran Cox IT Auditor Jeran.Cox@nigc.gov</p>	<p>Michael Curry IT Auditor Michael.Curry@nigc.gov</p>	<p>Derek Holbert CJIS Systems ISO Derek.Holbert@nigc.gov</p>																														
<p>Eddie Hall IT Auditor Eddie.Hall@nigc.gov</p>	<p>Tim Cotton IT Audit Manager Timothy.Cotton@nigc.gov</p>	<p>Training Technical Assistance traininginfo@nigc.gov</p>																														



NIGC National Training Conference Evaluation
Course Name: Cybersecurity Incident Response Plans

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.


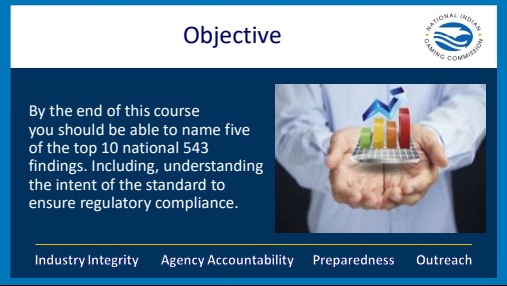
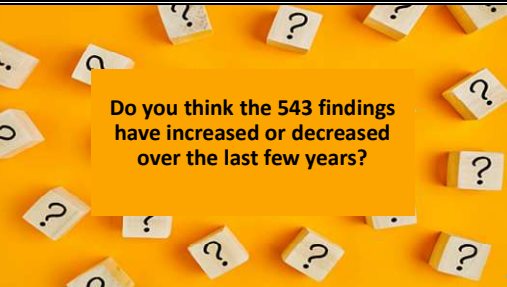
How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

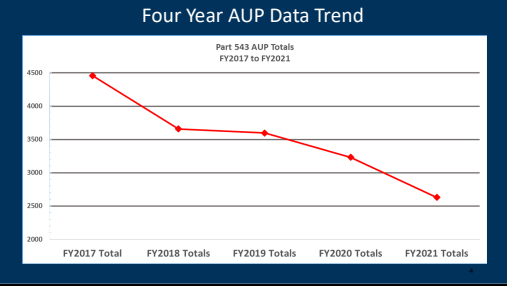

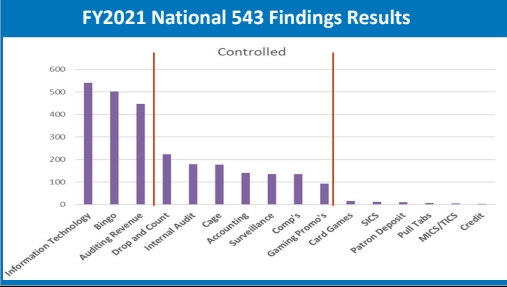
Top 10 Audit Findings Participant Guide



Top 10 Audit Findings Participant Guide

Slide 1		Key Points Welcome to Top 10 Audit Findings.
Slide 2	 <p>Objective</p> <p>By the end of this course you should be able to name five of the top 10 national 543 findings. Including, understanding the intent of the standard to ensure regulatory compliance.</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	Key Points <ul style="list-style-type: none">• Understanding the common exceptions.• Determine the Intent of the standard.• Once Intent is determined, establish the control to ensure regulatory compliance.
Slide 3	 <p>Do you think the 543 findings have increased or decreased over the last few years?</p>	

Top 10 Audit Findings Participant Guide

<p>Slide 4</p>	 <p>Four Year AUP Data Trend</p> <p>Part 543 AUP Totals FY2017 to FY2021</p> <table border="1"> <thead> <tr> <th>Fiscal Year</th> <th>Total AUP</th> </tr> </thead> <tbody> <tr> <td>FY2017 Total</td> <td>~4500</td> </tr> <tr> <td>FY2018 Totals</td> <td>~3700</td> </tr> <tr> <td>FY2019 Totals</td> <td>~3600</td> </tr> <tr> <td>FY2020 Totals</td> <td>~3300</td> </tr> <tr> <td>FY2021 Totals</td> <td>~2700</td> </tr> </tbody> </table>	Fiscal Year	Total AUP	FY2017 Total	~4500	FY2018 Totals	~3700	FY2019 Totals	~3600	FY2020 Totals	~3300	FY2021 Totals	~2700	<p>Key Points</p> <p>This line graph provides a better look at the decrease from FY 2017 to 2021 based on AUP data.</p>																						
Fiscal Year	Total AUP																																			
FY2017 Total	~4500																																			
FY2018 Totals	~3700																																			
FY2019 Totals	~3600																																			
FY2020 Totals	~3300																																			
FY2021 Totals	~2700																																			
<p>Slide 5</p>	 <p>Which areas do you think have the highest findings?</p>																																			
<p>Slide 6</p>	 <p>FY2021 National 543 Findings Results</p> <p>Controlled</p> <table border="1"> <thead> <tr> <th>Category</th> <th>Number of Findings</th> </tr> </thead> <tbody> <tr> <td>Information Technology</td> <td>~550</td> </tr> <tr> <td>Bingo</td> <td>~500</td> </tr> <tr> <td>Auditing Revenue</td> <td>~450</td> </tr> <tr> <td>Drop and Count</td> <td>~450</td> </tr> <tr> <td>Internal Audit</td> <td>~250</td> </tr> <tr> <td>Cage</td> <td>~180</td> </tr> <tr> <td>Accounting</td> <td>~150</td> </tr> <tr> <td>Surveillance</td> <td>~150</td> </tr> <tr> <td>Camp's</td> <td>~150</td> </tr> <tr> <td>Gaming Programs</td> <td>~150</td> </tr> <tr> <td>Card Games</td> <td>~100</td> </tr> <tr> <td>SIC</td> <td>~50</td> </tr> <tr> <td>Personnel</td> <td>~50</td> </tr> <tr> <td>Pool Tables</td> <td>~50</td> </tr> <tr> <td>WCS/TCS</td> <td>~50</td> </tr> <tr> <td>Credit</td> <td>~50</td> </tr> </tbody> </table>	Category	Number of Findings	Information Technology	~550	Bingo	~500	Auditing Revenue	~450	Drop and Count	~450	Internal Audit	~250	Cage	~180	Accounting	~150	Surveillance	~150	Camp's	~150	Gaming Programs	~150	Card Games	~100	SIC	~50	Personnel	~50	Pool Tables	~50	WCS/TCS	~50	Credit	~50	<p>Key Points</p> <ul style="list-style-type: none"> This chart shows the areas with the top national findings for all regions. It is listed in descending order by the number of 543 findings noted in 2021. Because of this data, we have been providing trainings for Auditing Revenue, Bingo, and Internal Audit over the last few years. We hope our efforts in providing those specific trainings help reduce the number of findings and the operations
Category	Number of Findings																																			
Information Technology	~550																																			
Bingo	~500																																			
Auditing Revenue	~450																																			
Drop and Count	~450																																			
Internal Audit	~250																																			
Cage	~180																																			
Accounting	~150																																			
Surveillance	~150																																			
Camp's	~150																																			
Gaming Programs	~150																																			
Card Games	~100																																			
SIC	~50																																			
Personnel	~50																																			
Pool Tables	~50																																			
WCS/TCS	~50																																			
Credit	~50																																			

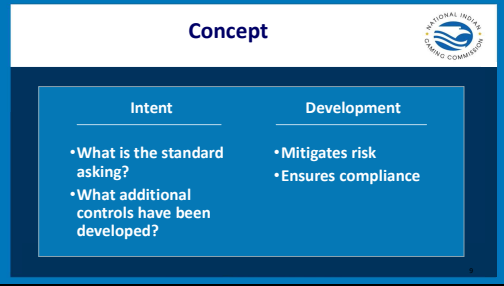

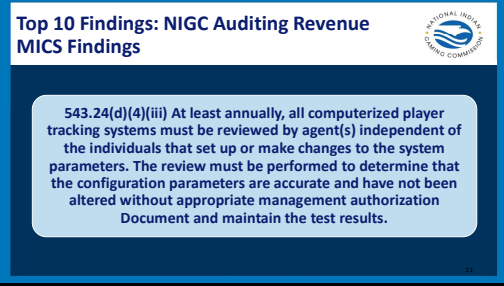
Top 10 Audit Findings Participant Guide

		reach compliance with those standards.
--	--	--




Slide 7	<table border="1"> <thead> <tr> <th colspan="10">AUP Data for 2021</th> </tr> <tr> <th>Section</th> <th>Oklahoma City</th> <th>Phoenix</th> <th>Portland</th> <th>Rapid City</th> <th>Sacramento</th> <th>St. Paul</th> <th>Tulsa</th> <th>Washington DC</th> <th>Grand Total</th> </tr> </thead> <tbody> <tr> <td>Information Technology</td> <td>122</td> <td>4</td> <td>65</td> <td>38</td> <td>93</td> <td>84</td> <td>66</td> <td>69</td> <td>541</td> </tr> <tr> <td>Bingo</td> <td>72</td> <td>22</td> <td>54</td> <td>42</td> <td>147</td> <td>45</td> <td>50</td> <td>71</td> <td>503</td> </tr> <tr> <td>Auditing Revenue</td> <td>112</td> <td>27</td> <td>67</td> <td>34</td> <td>64</td> <td>80</td> <td>32</td> <td>32</td> <td>448</td> </tr> <tr> <td>Drop and Count</td> <td>55</td> <td>4</td> <td>19</td> <td>29</td> <td>46</td> <td>33</td> <td>17</td> <td>21</td> <td>224</td> </tr> <tr> <td>Internal Audit</td> <td>20</td> <td>21</td> <td>19</td> <td>36</td> <td>6</td> <td>47</td> <td>2</td> <td>28</td> <td>179</td> </tr> <tr> <td>Cage</td> <td>42</td> <td>9</td> <td>19</td> <td>14</td> <td>35</td> <td>16</td> <td>19</td> <td>23</td> <td>177</td> </tr> <tr> <td>Accounting</td> <td>38</td> <td>13</td> <td>33</td> <td>32</td> <td>5</td> <td>12</td> <td>3</td> <td>5</td> <td>141</td> </tr> <tr> <td>Surveillance</td> <td>28</td> <td>2</td> <td>18</td> <td>34</td> <td>12</td> <td>32</td> <td>3</td> <td>7</td> <td>136</td> </tr> <tr> <td>Comps</td> <td>27</td> <td>3</td> <td>14</td> <td>1</td> <td>44</td> <td>28</td> <td>3</td> <td>15</td> <td>135</td> </tr> <tr> <td>Gaming Promo's</td> <td>7</td> <td></td> <td>6</td> <td>17</td> <td>16</td> <td>11</td> <td>33</td> <td>3</td> <td>93</td> </tr> </tbody> </table>	AUP Data for 2021										Section	Oklahoma City	Phoenix	Portland	Rapid City	Sacramento	St. Paul	Tulsa	Washington DC	Grand Total	Information Technology	122	4	65	38	93	84	66	69	541	Bingo	72	22	54	42	147	45	50	71	503	Auditing Revenue	112	27	67	34	64	80	32	32	448	Drop and Count	55	4	19	29	46	33	17	21	224	Internal Audit	20	21	19	36	6	47	2	28	179	Cage	42	9	19	14	35	16	19	23	177	Accounting	38	13	33	32	5	12	3	5	141	Surveillance	28	2	18	34	12	32	3	7	136	Comps	27	3	14	1	44	28	3	15	135	Gaming Promo's	7		6	17	16	11	33	3	93	<p>Key Points</p> <p>This information breaks down the FY2021 AUP data by section and region.</p> <p>The section with the most AUP findings for the region for FY2021 is in red text.</p>
AUP Data for 2021																																																																																																																										
Section	Oklahoma City	Phoenix	Portland	Rapid City	Sacramento	St. Paul	Tulsa	Washington DC	Grand Total																																																																																																																	
Information Technology	122	4	65	38	93	84	66	69	541																																																																																																																	
Bingo	72	22	54	42	147	45	50	71	503																																																																																																																	
Auditing Revenue	112	27	67	34	64	80	32	32	448																																																																																																																	
Drop and Count	55	4	19	29	46	33	17	21	224																																																																																																																	
Internal Audit	20	21	19	36	6	47	2	28	179																																																																																																																	
Cage	42	9	19	14	35	16	19	23	177																																																																																																																	
Accounting	38	13	33	32	5	12	3	5	141																																																																																																																	
Surveillance	28	2	18	34	12	32	3	7	136																																																																																																																	
Comps	27	3	14	1	44	28	3	15	135																																																																																																																	
Gaming Promo's	7		6	17	16	11	33	3	93																																																																																																																	

Slide 8	<table border="1"> <thead> <tr> <th>Area</th> <th>Total AUP findings</th> </tr> </thead> <tbody> <tr> <td>Information Technology</td> <td>541</td> </tr> <tr> <td>Bingo</td> <td>503</td> </tr> <tr> <td>Auditing Revenue</td> <td>448</td> </tr> <tr> <td>Drop and Count</td> <td>224</td> </tr> <tr> <td>Internal Audit</td> <td>179</td> </tr> <tr> <td>Cage</td> <td>177</td> </tr> <tr> <td>Accounting</td> <td>141</td> </tr> <tr> <td>Surveillance</td> <td>136</td> </tr> <tr> <td>Comps</td> <td>135</td> </tr> <tr> <td>Gaming Promos</td> <td>93</td> </tr> </tbody> </table>	Area	Total AUP findings	Information Technology	541	Bingo	503	Auditing Revenue	448	Drop and Count	224	Internal Audit	179	Cage	177	Accounting	141	Surveillance	136	Comps	135	Gaming Promos	93	<p>Key Points</p> <p>How do we come up with the data?</p> <p>The NIGC Audit Group compiles yearly Gross Gaming Revenues from submitted annual audited financial statements, performs analysis of the financial statements and Agreed Upon Procedures (AUP) reports for assessment of technical assistance, all to ensure regulatory compliance, gaming integrity and that tribes are the primary beneficiaries of their gaming revenues.</p>
Area	Total AUP findings																							
Information Technology	541																							
Bingo	503																							
Auditing Revenue	448																							
Drop and Count	224																							
Internal Audit	179																							
Cage	177																							
Accounting	141																							
Surveillance	136																							
Comps	135																							
Gaming Promos	93																							

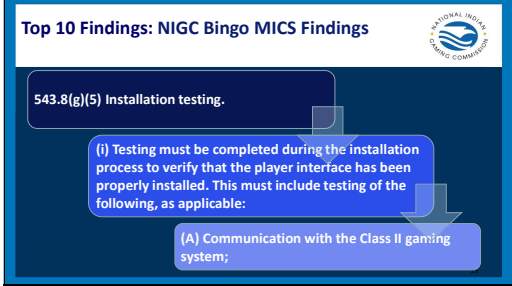
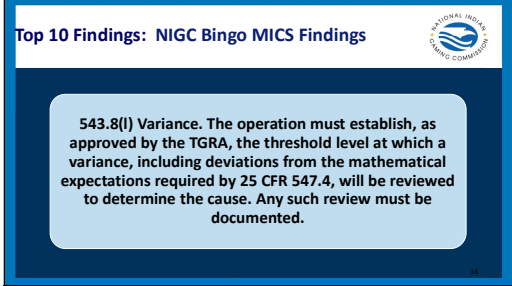
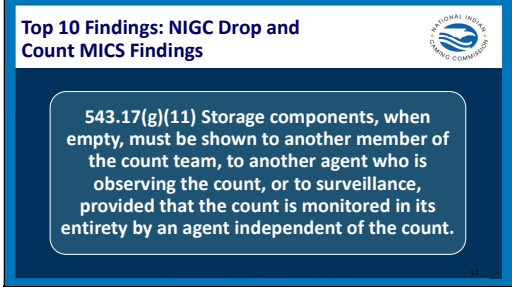
Top 10 Audit Findings Participant Guide

<p>Slide 9</p>		<p>Key Points Controls can basically have three functions:</p> <ul style="list-style-type: none"> ▪ Prevent something undesired from happening ▪ Detect when something undesired happened ▪ Corrective Action that should be taken in the event that something undesired happened <p>Standards should be written in a way that help ensure the intent is met.</p>
<p>Slide 10</p>		<p>Key Points A top finding for Auditing Revenue is NIGC MICS 543.24(d)(4)(ii)(C) Gaming promotions and player tracking.</p>
<p>Slide 11</p>		<p>Key Points Another top finding for Revenue Audit is NIGC MICS 543.24(d)(4)(iii).</p>

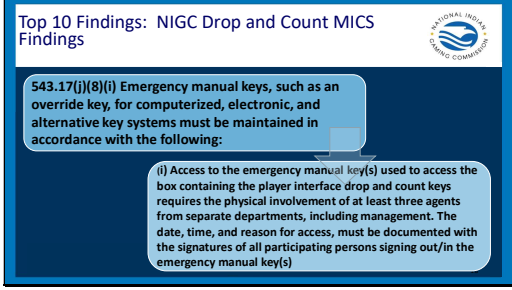
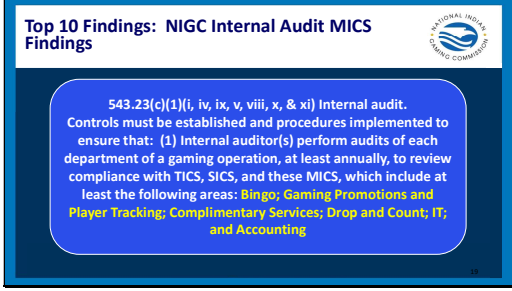
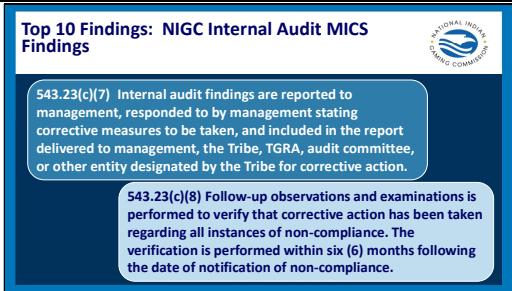
Top 10 Audit Findings Participant Guide

<p>Slide 12</p>	<p>Top 10 Findings: NIGC Auditing Revenue MICS Findings</p>  <p>543.24(d)(8)(i) At least quarterly, unannounced currency counter and currency counter interface (if applicable) tests must be performed, and the test results documented and maintained. All denominations of currency and all types of cash out tickets counted by the currency counter must be tested. This test may be performed by internal audit or the TGRA. The result of these tests must be documented and signed by the agent(s) performing the test</p>	<p>Key Points This is a top and recurring finding for Revenue Audit NIGC MICS 543.24(d)(8)(i).</p>
<p>Slide 13</p>	<p>Top 10 Findings: NIGC Auditing Revenue MICS Findings</p>  <p>543.24(d)(8)(iv) At least quarterly, an inventory of all controlled keys must be performed and reconciled to records of keys made, issued, and destroyed. Investigations must be performed for all keys unaccounted for, and the investigation documented.</p>	<p>Key Points Another top and common finding for Revenue Audit is NIGC MICS 543.24(d)(8)(iv)</p>
<p>Slide 14</p>	<p>Top 10 Findings: NIGC Bingo MICS Findings</p>  <p>543.8(f) Cash and cash equivalent controls</p> <p>(1) Cash or cash equivalents exchanged between two persons must be counted independently by at least two agents and reconciled to the recorded amounts at the end of each shift or session. Unexplained variances must be documented and maintained. Unverified transfers of cash or cash equivalents are prohibited.</p>	<p>Key Points Bingo has some common and top findings included in our list. Here is one of the top bingo findings: NIGC MICS 543.8(f) Cash and cash equivalent controls.</p>

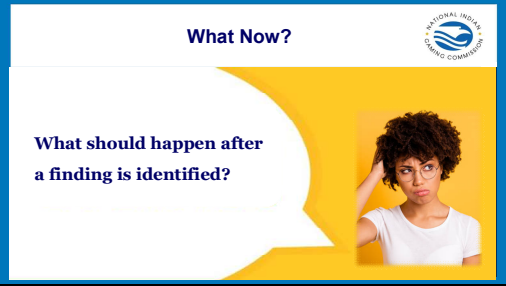
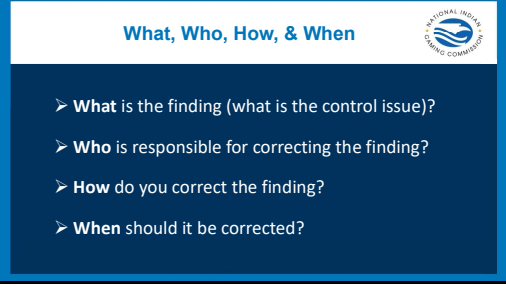

Top 10 Audit Findings Participant Guide

<p>Slide 15</p>		<p>Key Points Another top finding for Bingo is NIGC MICS 543.8(g)(5) Installation testing.</p>
<p>Slide 16</p>		<p>Key Points This standard continues year after year to be a recurring finding for Bingo: NIGC MICS 543.8(l) Variance.</p>
<p>Slide 17</p>		<p>Key Points Let's look at Drop and Count Top Findings by starting with NIGC MICS 543.17(g)(11)</p>


Top 10 Audit Findings Participant Guide

<p>Slide 18</p>		<p>Key Points This is a recurring top finding for the Drop and Count area: NIGC MICS 543.17(j)(8)(i)</p>
<p>Slide 19</p>		<p>Key Points Internal Audits are critical to provide assurance of an organizations risk management, compliance, and internal control effectiveness. This area is a top finding as it is critical for an organization to have in place to determine the overall effectiveness.</p>
<p>Slide 20</p>		<p>Key Points This part of 543.23 (c) is a common recurring finding for Internal Audit.</p>

Top 10 Audit Findings Participant Guide

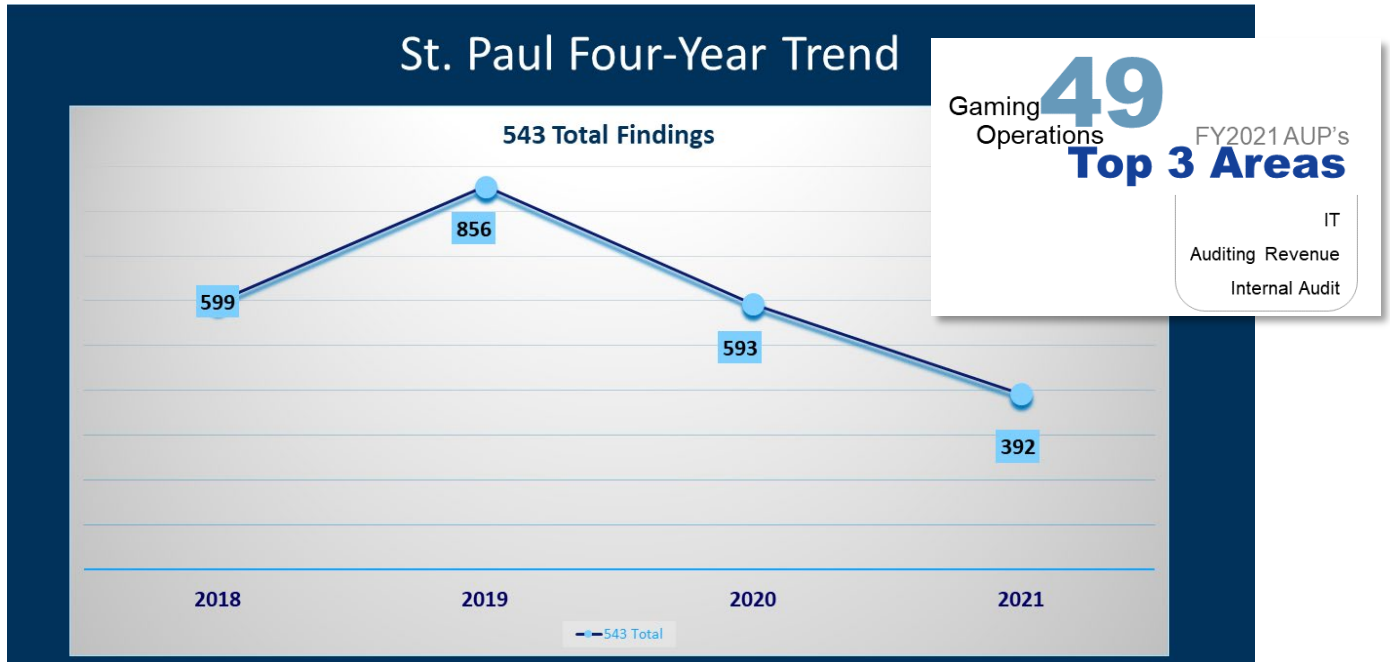
Slide 21	 <p>What Now?</p> <p>What should happen after a finding is identified?</p> <p>NATIONAL INDIAN GAMING COMMISSION</p>	Key Points What should happen after a finding is identified?
Slide 22	 <p>What, Who, How, & When</p> <ul style="list-style-type: none">➤ What is the finding (what is the control issue)?➤ Who is responsible for correcting the finding?➤ How do you correct the finding?➤ When should it be corrected? <p>NATIONAL INDIAN GAMING COMMISSION</p>	Key Points What – what is the finding Who – who is responsible How – who will it be corrected When – when should it be completed
Slide 23	 <p>Address Cause</p> <p>NATIONAL INDIAN GAMING COMMISSION</p>	Key Points Understanding the cause of the finding will always help address the issue and help with writing the corrective action plan.

Top 10 Audit Findings Participant Guide

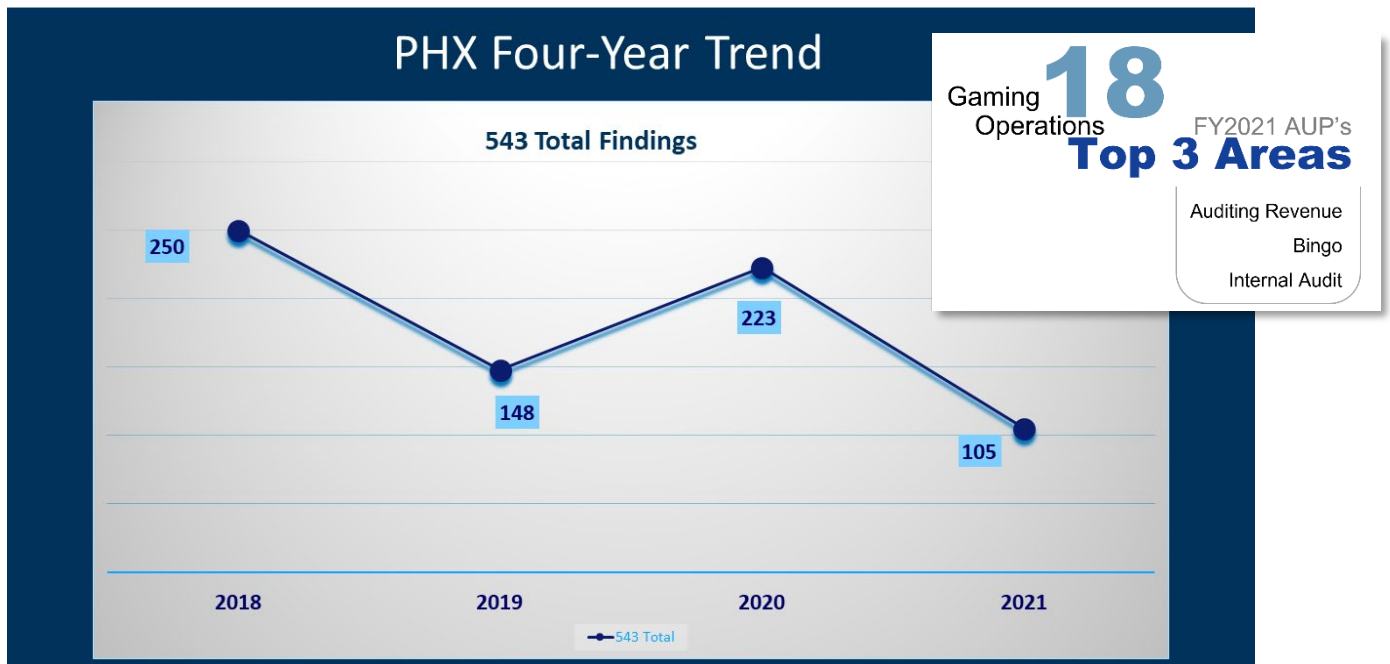
Slide 24		Key Points <p>Thank you for attending.</p> <p>If you have any questions or comments please send them to TRAININGINFO@nigc.gov</p>
----------	---	---

Top 10 Audit Findings - HANDOUT #1

The following graphs show the regions' trend for the last four years.

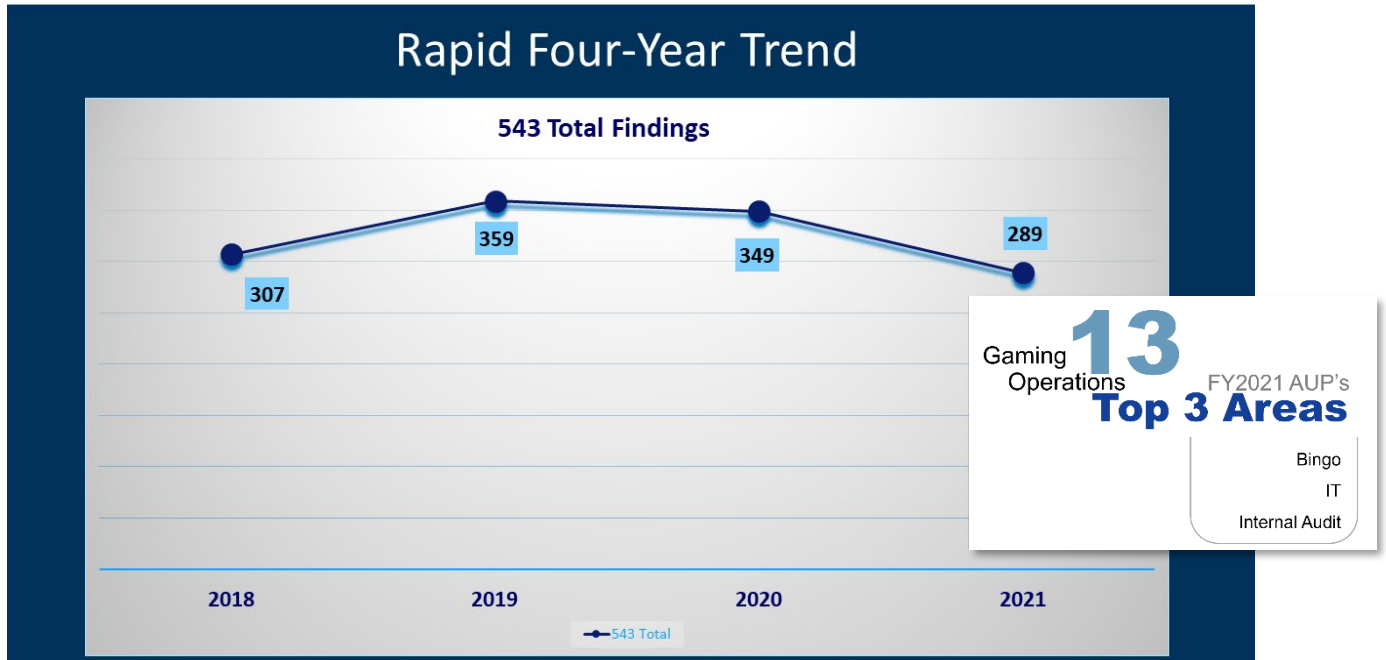


Above: There's been an overall gradual decrease from 2019 to 2021. With a period during 2019 where the region seen it's highest number of findings.

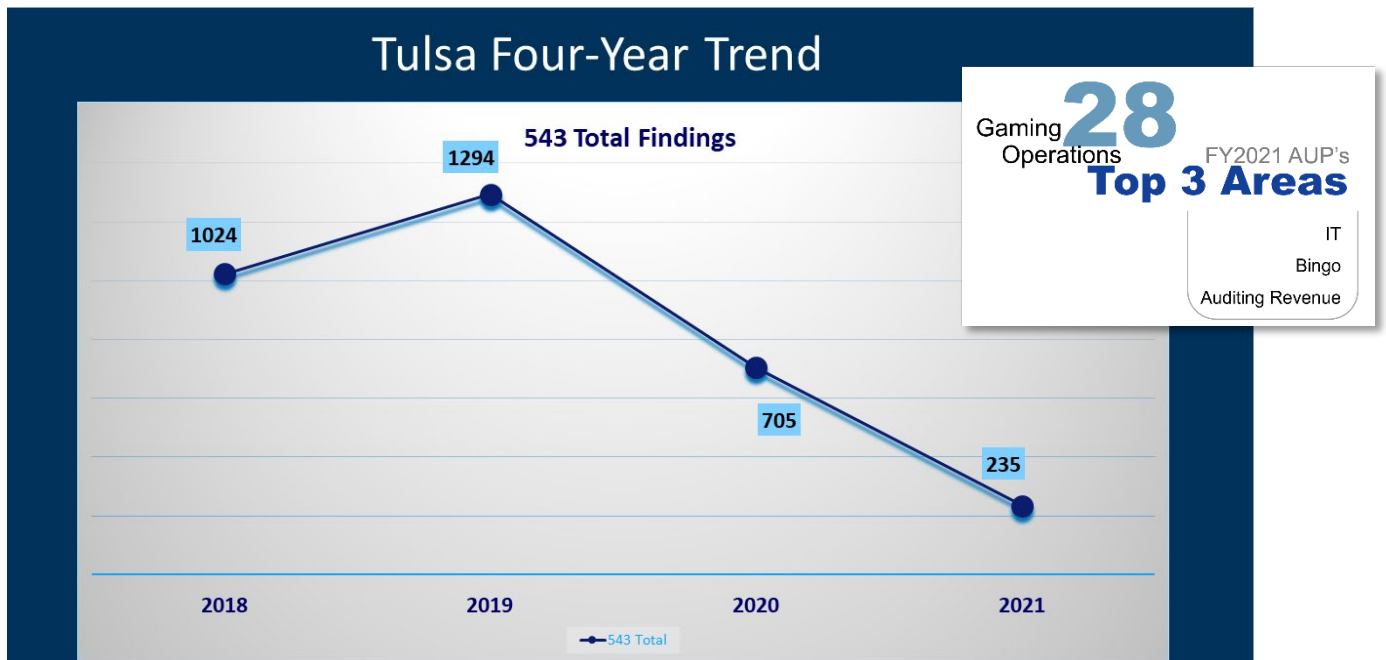


Above: There's been an overall gradual decrease from 2018 to 2021. With a period during 2020 where the region seen it's highest number of findings.

Top 10 Audit Findings - HANDOUT #1

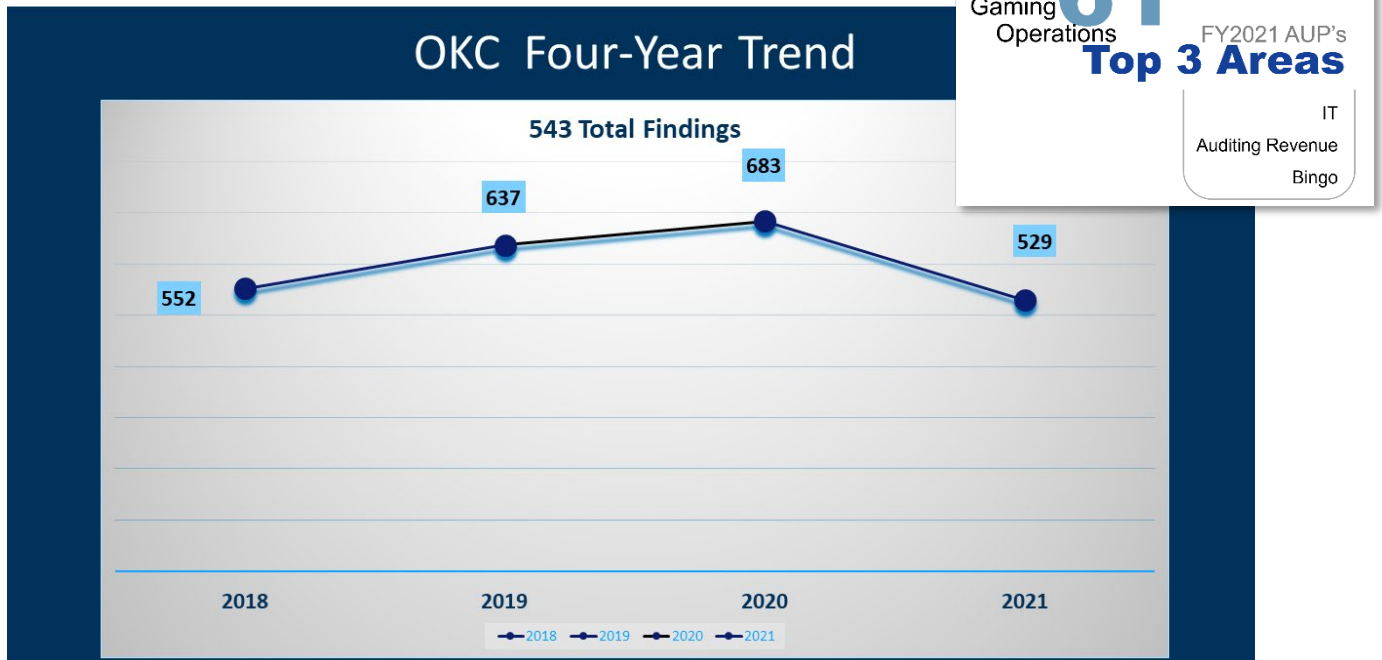


Above: The region has stayed fairly steady from 2018 to 2021. With a period between 2019 and 2020 where the region seen it's highest number of findings.

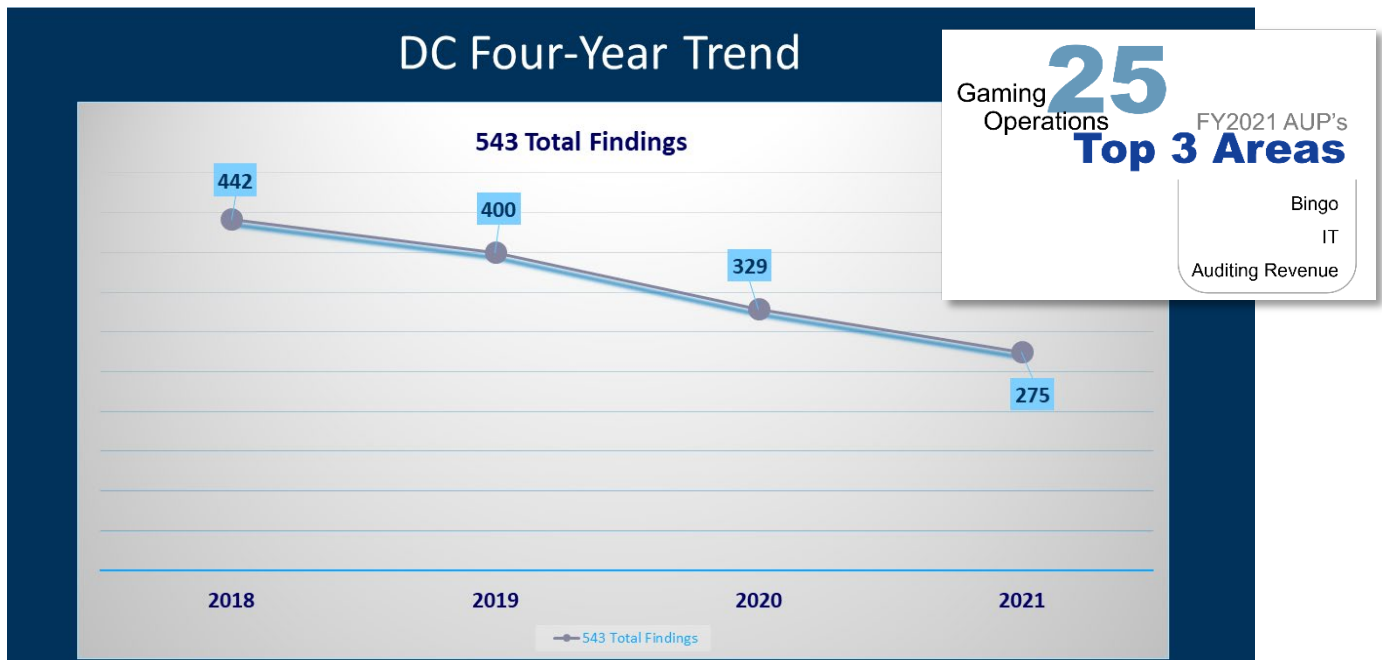


Above: There's been a large decrease from 2019 to 2021. With a period during 2019 where the region seen it's highest number of findings.

Top 10 Audit Findings - HANDOUT #1

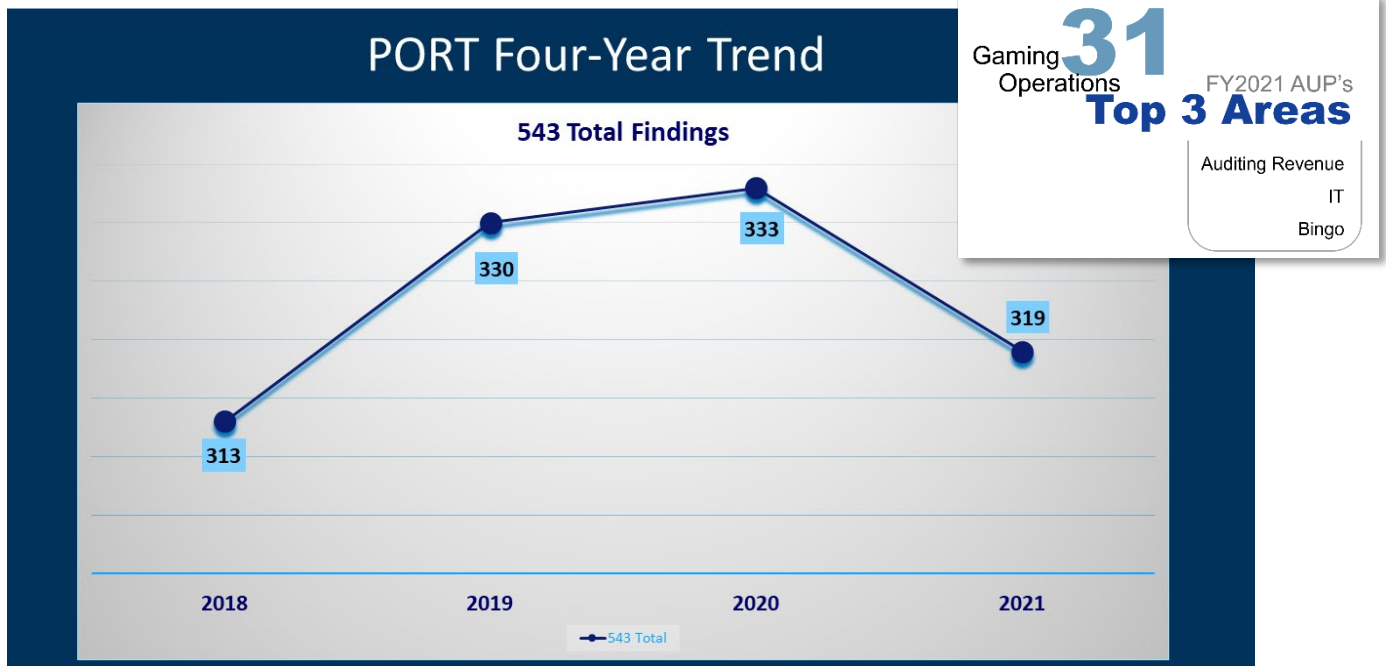


Above: There's been an overall gradual increase from 2018 to 2020. With a period during 2020 where the region seen it's highest number of findings.

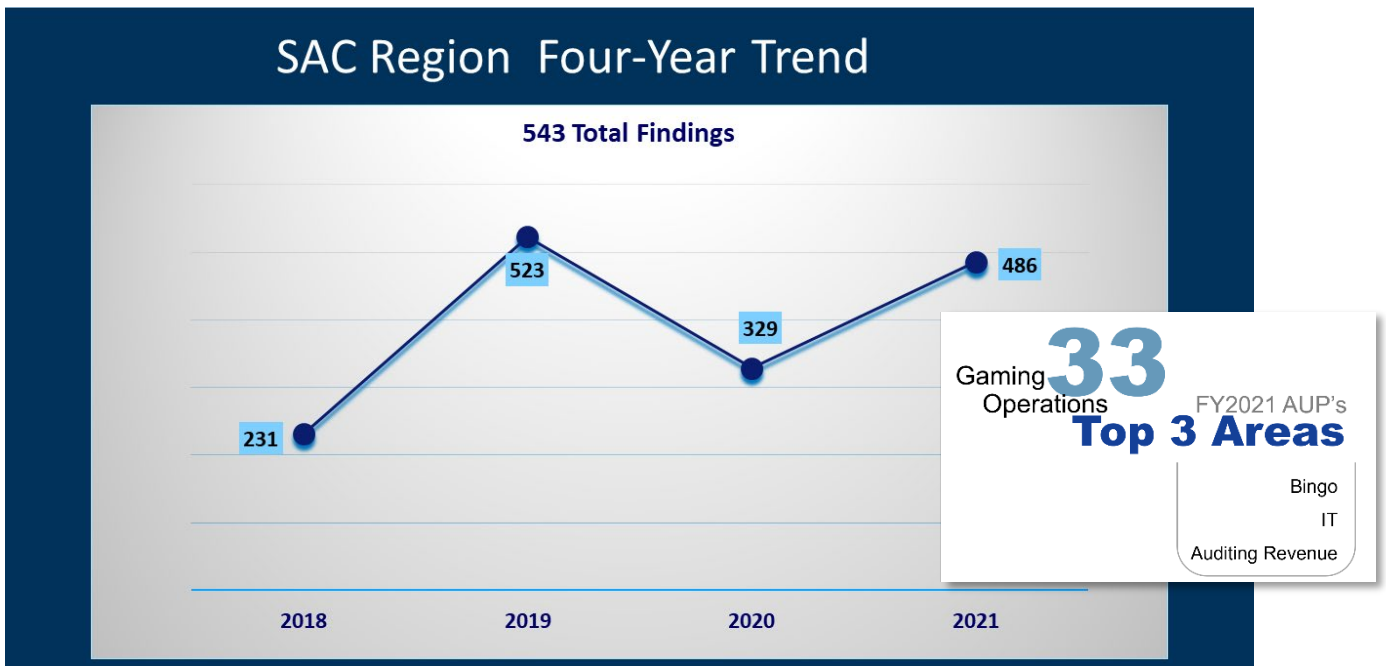


Above: There's been an overall gradual decrease from 2018 to 2021. With a period during 2018 where the region seen it's highest number of findings.

Top 10 Audit Findings - HANDOUT #1



Above: We see a steady increase from 2018 to 2020 with a decrease in findings for 2021.



Above: There's been an overall increase from 2018 to 2021. With a period during 2019 where the region seen it's highest number of findings.



NIGC National Training Conference Evaluation
Course Name: Top 10 Audit Findings

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Intent and Testing: Bingo Toolkit


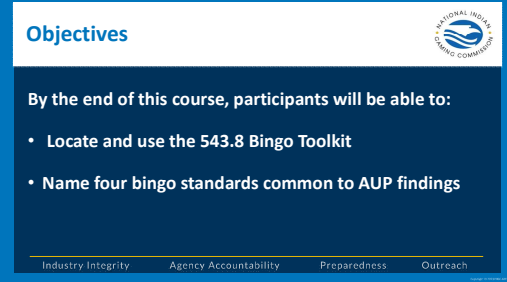
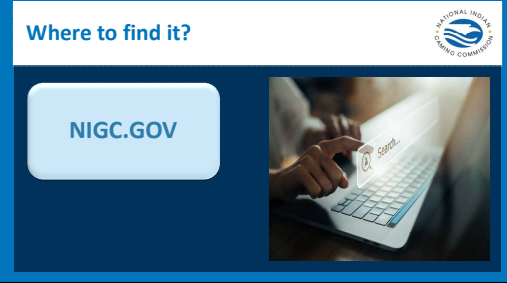
National Indian Gaming Commission



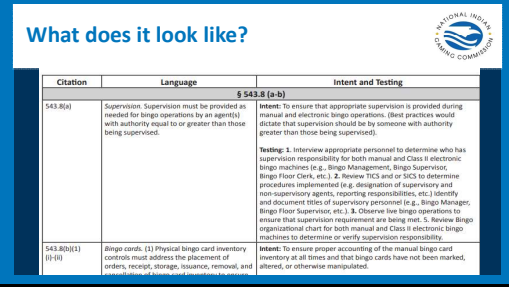

**Intent and Testing:
Bingo Toolkit**



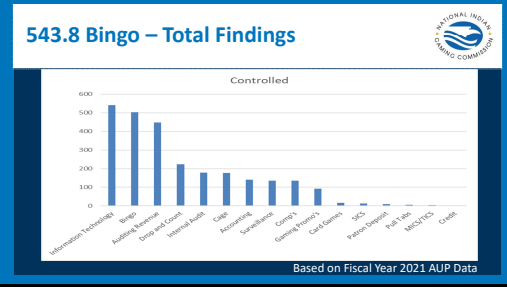
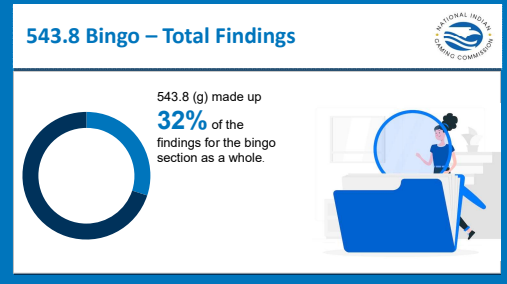

Intent and Testing: Bingo Toolkit Participant Guide

Slide 1		
Slide 2		<p>Key Points: By the end of this course, participants will be able to:</p> <ul style="list-style-type: none">• Locate and use the 543.8 Bingo Toolkit• Name four bingo standards common to AUP findings
Slide 3		<p>Key Points: The 543.8 Bingo Toolkit can be found on the NIGC webpage</p> <p>Direct link: https://www.nigc.gov/images/uploads/training/Bingo_Flipbook_Rev12_6.pdf</p>

Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 4</p>		<p>Key Points:</p> <ul style="list-style-type: none"> • Example of a page from the Toolkit.
<p>Slide 5</p>		<p>Key Points:</p> <p>The toolkit layout lists the:</p> <ul style="list-style-type: none"> • Standard – the requirement as stated in Part 543 Minimum Internal Control Standards • Intent – the goal of the standard • Testing – steps listed to assist with the auditing process or with developing Tribal Internal Control Standards (TICS) or operational System of Internal Control Standards (SICS)

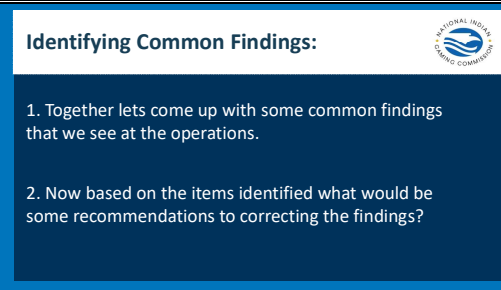
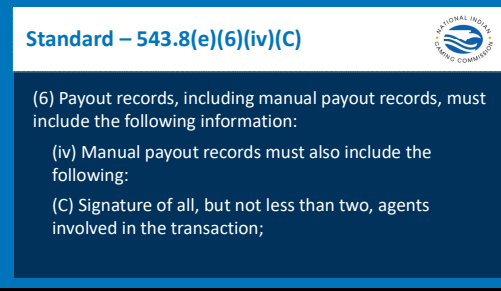
Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 6</p>	 <p>543.8 Bingo – Total Findings</p> <p>Controlled</p> <p>Based on Fiscal Year 2021 AUP Data</p>	<p>Key Points:</p> <p>543.8 Bingo had 503 findings identified nationally. It is the second largest areas with the most findings. However, keep in mind bingo is one of the larger sections within the MICS. The largest section within 543.8 Bingo with the most findings was 543.8(g) Technologic aids to the play of bingo.</p>
<p>Slide 7</p>	 <p>543.8 Bingo – Total Findings</p> <p>543.8 (g) made up 32% of the findings for the bingo section as a whole.</p>	
<p>Slide 8</p>	 <p>Standard – 543.8(e)(5)</p> <p>Authorization and Signatures</p>	<p>Key Points:</p> <p>Find the standard 543.8(e)(5) in your Bingo Toolkit</p> <p>Common Finding</p> <p>543.8(e)(5) Authorization and Signatures.</p> <ul style="list-style-type: none"> At least two agents must authorize, sign, and witness all manual prize payouts above \$1,200, or a lower threshold as authorized by management and approved by the TGRA.



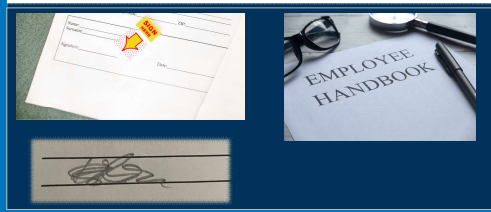

Intent and Testing: Bingo Toolkit Participant Guide

		<ul style="list-style-type: none">• Manual prize payouts above the following threshold (or a lower threshold, as authorized by management and approved by TGRA) must require one of the two signatures and verifications to be a supervisory or management employee independent of the operation of Class II Gaming System bingo: (A) \$5,000 for a Tier A facility; (B) \$10,000 at a Tier B facility; (C) \$20,000 for a Tier C facility; or (D) \$50,000 for a Tier C facility with over \$100,000,000 in gross gaming revenues.• The predetermined thresholds, whether set at the MICS level or lower, must be authorized by management, approved by the TGRA, documented, and maintained.• A Class II gaming system may substitute for one authorization/signature verifying, validating or authorizing a winning card, but may not substitute for a supervisory or management authorization/signature.
--	--	--



Intent and Testing: Bingo Toolkit Participant Guide

Slide 9		<p>Key Points: Activity #1 Identifying Common Findings 1. Together let's come up with some common findings that we see at the operations. 2. Now based on the items identified what would be some recommendations to correcting the findings?</p>
Slide 10		<p>Key Points: 543.8(e)(6)(iv)(C) Authorization and Signatures (6) Payout records, including manual payout records, must include the following information: (iv) Manual payout records must also include the following: (C) Signature of all, but not less than two, agents involved in the transaction</p>

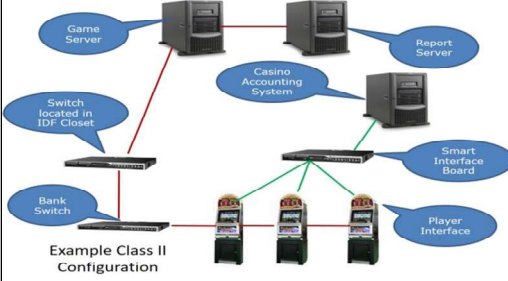
Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 11</p>	<p>Common Issues Noted – 543.8(e)(6)(iv)(C) </p> <p>Does anyone have any issues they have seen relating to this particular standard?</p>	<p>Key Points: 543.8(e)(6)(iv)(C) Authorization and Signatures (C) Payout records, including manual payout records, must include the following information: Signature of all, but not less than two, agents involved in the transaction;</p>
<p>Slide 12</p>	<p>Common Issues Noted – 543.8(e)(6)(iv)(C) </p> 	<p>Key Points: 543.8(e)(6)(iv)(C) Authorization and Signatures (C) Payout records, including manual payout records, must include the following information: Signature of all, but not less than two, agents involved in the transaction</p>
<p>Slide 13</p>	<p>543.8(f)(1) </p> <p>(f) Cash and cash equivalent controls.</p> <p>(1) Cash or cash equivalents exchanged between two persons must be counted independently by at least two agents and reconciled to the recorded amounts at the end of each shift or session. Unexplained variances must be documented and maintained. Unverified transfers of cash or cash equivalents are prohibited.</p>	<p>Key Points: 543.8 (f)(1) (f) Cash and cash equivalent controls. (1) Cash or cash equivalents exchanged between two persons must be counted independently by at least two agents and reconciled to the recorded amounts at the end of each shift or session. Unexplained variances must be documented and maintained. Unverified transfers of cash or cash equivalents are prohibited.</p>


Intent and Testing: Bingo Toolkit Participant Guide

Slide 14	<p>Common Issues Noted: 543.8 (f)(1)</p>  <p>The image shows a woman and a man standing behind a counter, both focused on counting stacks of cash. The woman is on the left, and the man is on the right. They appear to be in a retail or service environment.</p>	<p>Key Points: 543.8 (f)(1) (f) Cash and cash equivalent controls. (1) Cash or cash equivalents exchanged between two persons must be counted independently by at least two agents and reconciled to the recorded amounts at the end of each shift or session. Unexplained variances must be documented and maintained. Unverified transfers of cash or cash equivalents are prohibited.</p>
Slide 15	<p>Questions before we take a break?</p>  <p>The image shows a desk setup with a white keyboard, a white mouse, a spiral notebook, and a sign that reads "TAKE A BREAK". The sign is made of white cards with black text.</p>	<p>Key Points: Break time!</p>

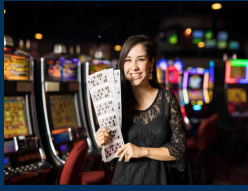
Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 16</p>	<p>543.8(g)(5)(i)(A)</p> <p>(5) Installation testing.</p> <p>(i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable:</p> <p>(A) Communication with the Class II gaming system;</p>	<p>Key Points:</p> <p>543.8(g)(5)(i)(A)</p> <p>(5) Installation testing.</p> <p>(i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable:</p> <p>(A) Communication with the Class II gaming system;</p>
<p>Slide 17</p>	 <p>Example Class II Configuration</p>	<p>Key Points:</p> <p>543.8(g)(5)(i)(A)</p> <p>(5) Installation testing.</p> <p>(i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable:</p> <p>(A) Communication with the Class II gaming system;</p>


Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 18</p>	<p>Activity #2</p> <p>As a group let's come up with the intent and testing for this standard.</p> 	<p>Key Points: Activity #2: As a group lets come up with the intent and testing for this standard. (No cheating please) 543.8 (5) Installation testing. (i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable: (I) All buttons, to ensure that all are operational and programmed appropriately;</p>
<p>Slide 19</p>	<p>543.8(g)(5)(i)(I)</p> <p>(5) Installation testing.</p> <p>(i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable:</p> <p>(I) All buttons, to ensure that all are operational and programmed appropriately;</p>	<p>Key Points: 543.8(g)(5)(i)(I) (5) Installation testing. (i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable: (I) All buttons, to ensure that all are operational and programmed appropriately;</p>


Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 20</p>	<p>Common Issues Noted: 543.8(g)(5)(i)(I)</p>  <p><small>NATIONAL INDIAN GAMING COMMISSION</small></p>	<p>Key Points: 543.8(g)(5)(i)(I) (5) Installation testing. (i) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable: (I) All buttons, to ensure that all are operational and programmed appropriately;</p>
<p>Slide 21</p>	<p>543.8(h)(1)(i) & (ii)</p> <p>(1) Malfunctions. Procedures must be implemented to investigate, document and resolve malfunctions. Such procedures must address the following:</p> <p>(i) Determination of the event causing the malfunction; (ii) Review of relevant records, game recall, reports, logs, surveillance records;</p> <p><small>NATIONAL INDIAN GAMING COMMISSION</small></p>	<p>Key Points: 543.8(h)(1)(i)&(ii) (1) Malfunctions. Procedures must be implemented to investigate, document and resolve malfunctions. Such procedures must address the following: (i) Determination of the event causing the malfunction; (ii) Review of relevant records, game recall, reports, logs, surveillance records;</p>

Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 22</p>	<p>Common Issues Noted: 543.8(h)(1)(i) & (ii)</p> <p>"The machine being played by Robert Taylor malfunctioned due to a "communication error" and neither he nor the Treasure Island Hotel & Casino realized that he'd won a progressive jackpot the evening of Jan. 8, the Nevada Gaming Control Board said Friday in a statement."</p> <p><small>FEBRUARY 7, 2022 / 7:59 AM / CBS/A https://www.cbsnews.com/news/las-vegas-jackpot-slot-machine-malfunction-winner-located-arizona/</small></p>	<p>Key Points:</p> <p>543.8(h)(1)(i)&(ii)</p> <p>(1) Malfunctions. Procedures must be implemented to investigate, document and resolve malfunctions. Such procedures must address the following:</p> <ul style="list-style-type: none"> (i) Determination of the event causing the malfunction; (ii) Review of relevant records, game recall, reports, logs, surveillance records;
<p>Slide 23</p>	<p>Intent & Testing</p> 	<p>Key Points:</p> <p>It's important to understand the intent of a standard to be able to write a control, implement a procedure, identify errors, or test for compliance.</p> <p>It's important to understand how to test for compliance with the standards to ensure the safety and integrity of the gaming operation along with mitigating the risk for fraudulent activity and protection of tribal assets.</p> <p>Understanding intent moves you past just checking a box on a checklist to understanding why a control is important and how it protects tribal assets.</p>

Intent and Testing: Bingo Toolkit Participant Guide

<p>Slide 24</p>		<p>Key Points: Thank you for joining us today.</p> <p>If you have any questions or comments regarding the training, please send them to TRAININGINFO@nigc.gov</p>
-----------------	---	---



NIGC National Training Conference Evaluation
Course Name: Intent and Testing: Bingo Toolkit

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

A series of horizontal lines for writing, consisting of 25 parallel black lines spaced evenly down the page.

Panel: Roundtable Discussion with Internal Audit Professionals Participant Guide

National Indian Gaming Commission



Panel: Roundtable Discussion with Internal Audit Professionals

Industry Integrity Agency Accountability Preparedness Outreach



NIGC National Training Conference Evaluation

Course Name: Panel: Roundtable Discussion with Internal Audit Professionals

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Critical Thinking: Enhancing the Internal Audit Participant Guide

National Indian Gaming Commission


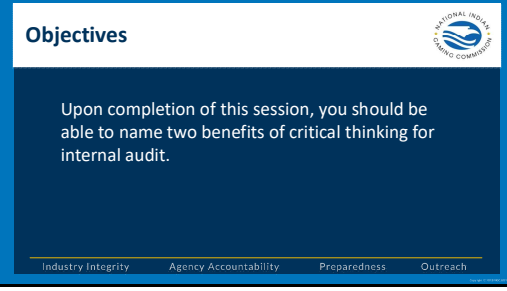



Critical Thinking:
Enhancing Internal Audit

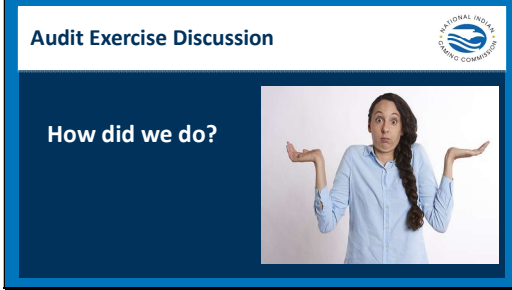
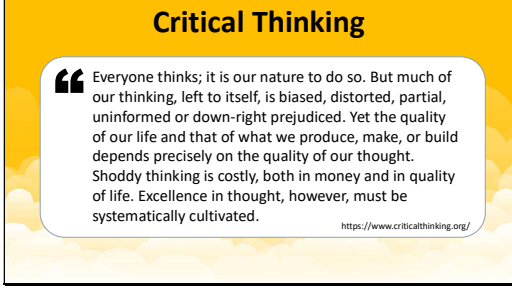


A graphic showing several glowing lightbulbs with the words "Skill", "judgment", "method", "problem", "strategy", and "tools" written on them.

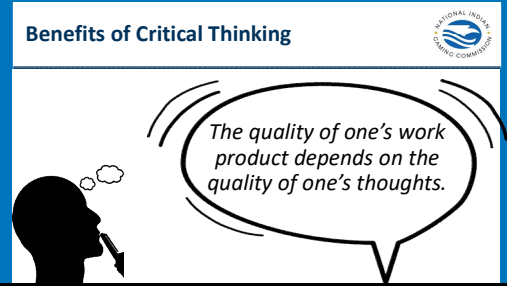

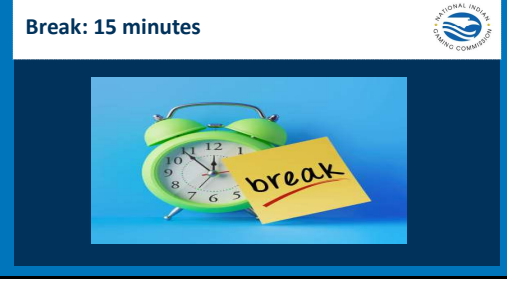
Critical Thinking: Enhancing the Internal Audit Participant Guide

<p>Slide 1</p>		
<p>Slide 2</p>		<p>KEY POINTS You should be able to name two benefits of critical thinking for internal audit.</p>
<p>Slide 3</p>		<p>KEY POINTS Activity (Ice Breaker) Supplies:</p> <ul style="list-style-type: none"> • Handout #1 Ice Breaker • Pen <p>Directions: At your tables read through the standard and come up with questions or testing that you would complete to verify compliance.</p>

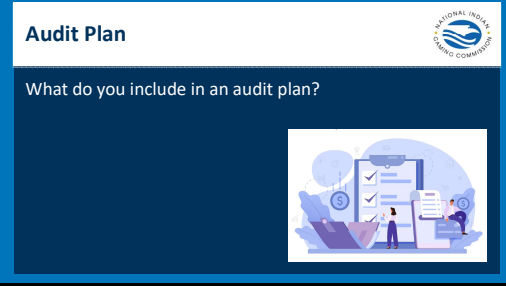
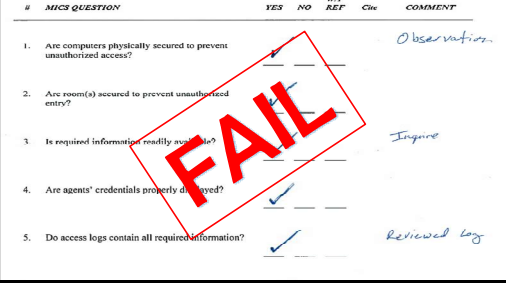
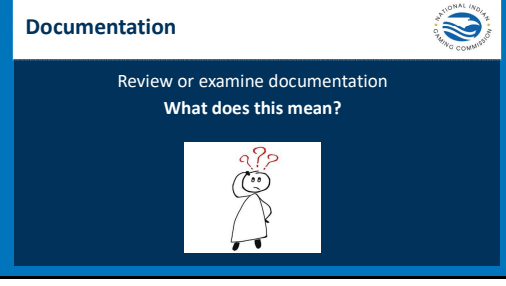
Critical Thinking: Enhancing the Internal Audit Participant Guide

<p>Slide 4</p>	 <p>Audit Exercise Discussion</p> <p>How did we do?</p>	<p>KEY POINTS How did we do?</p>
<p>Slide 5</p>	 <p>Critical Thinking</p> <p>“ Everyone thinks; it is our nature to do so. But much of our thinking, left to itself, is biased, distorted, partial, uninformed or down-right prejudiced. Yet the quality of our life and that of what we produce, make, or build depends precisely on the quality of our thought. Shoddy thinking is costly, both in money and in quality of life. Excellence in thought, however, must be systematically cultivated.</p> <p>https://www.criticalthinking.org/</p>	<p>KEY POINTS Everyone thinks; it is our nature to do so. However, much of our thinking, left to itself, is biased, distorted, partial, uninformed or downright prejudiced. Yet the quality of our life and that of what we produce, make, or build depends precisely on the quality of our thought. Shoddy thinking is costly, both in money and in quality of life. Excellence in thought, however, must be systematically cultivated - https://www.criticalthinking.org/</p>

Critical Thinking: Enhancing the Internal Audit Participant Guide

<p>Slide 6</p>		<p>KEY POINTS</p> <p>Benefits of critical thinking:</p> <ul style="list-style-type: none"> • It helps Internal Auditors successfully scope, assess and report on risk • Improves decision-making by Internal Auditors that can result in better organizational performance
<p>Slide 7</p>		<p>KEY POINTS</p> <p><u>(1) Internal auditor(s) perform audits of each department of a gaming operation, at least annually, to review compliance with TICS, SICS, and these MICS, which include at least the following areas:</u></p>
<p>Slide 8</p>		<p>KEY POINTS</p> <p>Break</p>

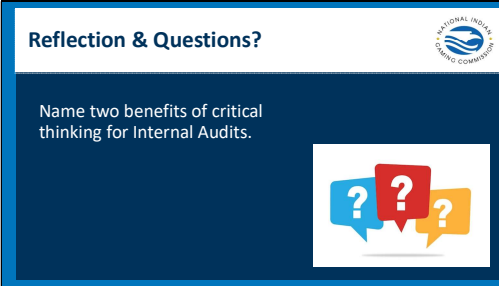
Critical Thinking: Enhancing the Internal Audit Participant Guide

<p>Slide 9</p>		<p>KEY POINTS (1) Internal auditor(s) perform audits of each department of a gaming operation, at least annually, to review compliance with TICS, SICS, and these MICS, which include at least the following areas:</p>
<p>Slide 10</p>		<p>KEY POINTS Fieldwork: Here is an example of a poorly completed checklist.</p>
<p>Slide 11</p>		<p>KEY POINTS <u>(4) Documentation such as checklists, programs, reports, etc. is prepared to evidence all internal audit work and follow-up performed as it relates to compliance with TICS, SICS, and these MICS, including all instances of noncompliance.</u></p>

Critical Thinking: Enhancing the Internal Audit Participant Guide

<p>Slide 12</p>		<p>KEY POINTS Critical thinking will help you determine what issues to include in the report.</p>
<p>Slide 13</p>		<p>KEY POINTS Let's practice what we have learned.</p> <p>Activity – Scenario Supplies:</p> <ul style="list-style-type: none"> • Handout #2 • Pen <p>Time: 15 minutes</p> <p>Instructions: Read the scenario and answer the questions on your handout. What other actions should be done to measure risk? Why?</p>

Critical Thinking: Enhancing the Internal Audit Participant Guide

<p>Slide 14</p>	 <p>Reflection & Questions?</p> <p>Name two benefits of critical thinking for Internal Audits.</p>	<p>Key Points: Name two benefits of critical thinking for Internal Audit.</p> <ol style="list-style-type: none">1.2. <p>Thank you for attending “Critical Thinking: Enhancing Internal Audit”.</p> <p>If you have any questions or comments please send them to TRAININGINFO@nigc.gov</p>
-----------------	--	--



Critical Thinking: Enhancing the Internal Audit – Handout #1

Exercise: You, the Internal Auditor is tasked with ensuring compliance with the below internal control standard 543.24(d)(4)(iii). When completing an audit of the Revenue Audit Department. What questions and testing should you conduct to have a successful audit? Try to think of five and write your answers in the lines below.

Scenario:

543.24(d)(4)(iii) At least annually, all computerized player tracking systems must be reviewed by agent(s) independent of the individuals that set up or make changes to the system parameters. The review must be performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization Document and maintain the test results.

1. _____

2. _____

3. _____

4. _____

5. _____

Critical Thinking: Enhancing the Internal Audit – Handout #2

RELEVANT STANDARDS:

25 CFR 543.17(j) **Controlled keys.** Controls must be established, and procedures implemented to safeguard the use, access, and security of keys in accordance with the following:

- (1) Each of the following requires a separate and unique key lock or alternative secure access method:
 - (i) Drop cabinet;
 - (ii) Drop box release;
 - (iii) Drop box content; and
 - (iv) Storage racks and carts used for the drop
- (2) Access to and return of keys or equivalents must be documented with the date, time, and signature or other unique identifier of the agent accessing or returning the key(s).
 - (i) For Tier A and B operations, at least two (2) drop team agents are required to be present to access and return keys. For Tier C operations, at least three (3) drop team agents are required to be present to access and return keys.
 - (ii) For Tier A and B operations, at least two (2) count team agents are required to be present at the time count room and other count keys are issued for the count. For Tier C operations, at least three (two for card game drop box keys in operations with three tables or fewer) count team agents are required to be present at the time count room and other count keys are issued for the count.
- (3) Documentation of all keys, including duplicates, must be maintained, including:
 - (i) Unique identifier for each individual key;
 - (ii) Key storage location;
 - (iii) Number of keys made, duplicated, and destroyed; and
 - (iv) Authorization and access
- (4) Custody of all keys involved in the drop and count must be maintained by a department independent of the count and the drop agents as well as those departments being dropped and counted.
- (5) Other than the count team, no agent may have access to the drop box content keys while in possession of storage rack keys and/or release keys.
- (6) Other than the count team, only agents authorized to remove drop boxes are allowed access to drop box release keys.
- (7) Any use of keys at times other than the scheduled drop and count must be properly authorized and documented.
- (8) Emergency manual keys, such as an override key, for computerized, electronic, and alternative key systems must be maintained in accordance with the following:
 - (i) Access to the emergency manual key(s) used to access the box containing the player interface drop and count keys requires the physical involvement of at least three agents from separate departments, including management. The date, time, and reason for access, must be documented with the signatures of all participating persons signing out/in the emergency manual key(s);
 - (ii) The custody of the emergency manual keys requires the presence of two agents from separate departments from the time of their issuance until the time of their return; and
 - (iii) Routine physical maintenance that requires access to the emergency manual key(s), and does not involve accessing the player interface drop and count keys, only requires the presence of two agents from separate departments. The date, time, and reason for access must be documented with the signatures of all participating agents signing out/in the emergency manual key(s).

Critical Thinking: Enhancing the Internal Audit – Handout #2

Exercise: You, the Internal Auditor, is tasked with ensuring compliance with the above internal control standards. Below is the scene.

Scenario:

You are given a monthly inventory sheet for the 3 months (Jan, April, July) along with sign out/in key logs for three days (test days). Upon your review of the documents, you determine the key inventory was completed with no issues. The sign in/out logs also indicate that keys were signed out/in according to procedure. The next day you are watching the drop and count process. You notice keys are signed out from an electronic key box in the cage. You continue to watch the drop process and conclude the key removal and replacement process is according to procedure.

Using our critical thinking skills: **What other actions should be done to measure risk? Why?**

1. _____

2. _____

3. _____

4. _____

5. _____



NIGC National Training Conference Evaluation
Course Name: Critical Thinking: Enhancing the Internal Audit

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.



Lined writing area consisting of 28 horizontal black lines on a white background, intended for text entry.

Risk Assessments Participant Guide


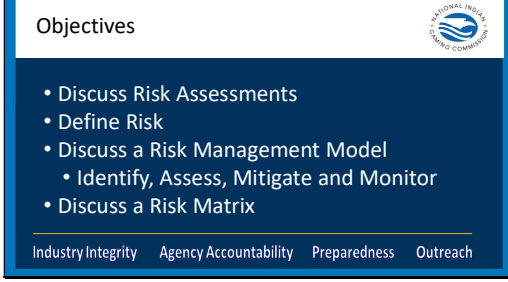
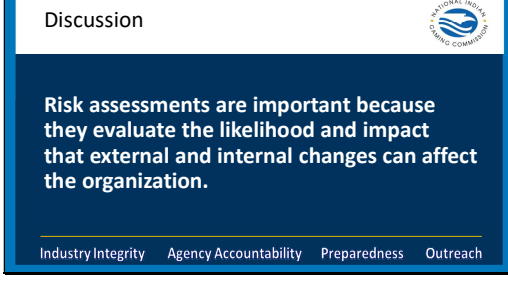
National Indian Gaming Commission



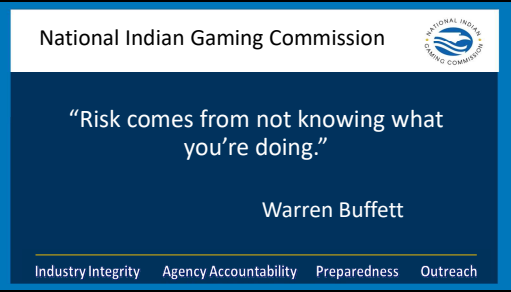
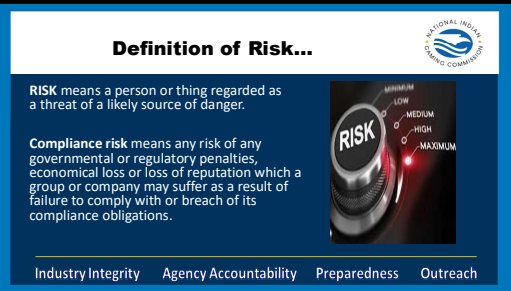

Risk Assessment approach to Regulatory Monitoring

Industry Integrity Agency Accountability Preparedness Outreach


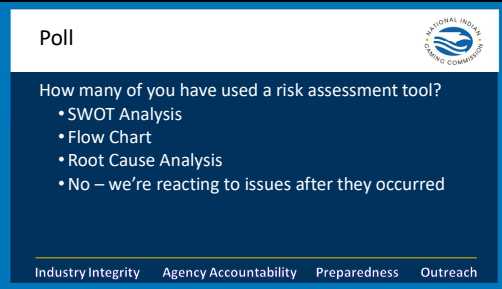

Risk Assessments Participant Guide

Slide 1	 <p>National Indian Gaming Commission</p> <p>Risk Assessment approach to Regulatory Monitoring</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	KEY POINTS Risk Assessments are necessary so one can understand the risk associated with a process or activity. Risk assessments can reduce the likelihood of something occurring or reoccurring.
Slide 2	 <p>Objectives</p> <ul style="list-style-type: none">• Discuss Risk Assessments• Define Risk• Discuss a Risk Management Model<ul style="list-style-type: none">• Identify, Assess, Mitigate and Monitor• Discuss a Risk Matrix <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	
Slide 3	 <p>Discussion</p> <p>Risk assessments are important because they evaluate the likelihood and impact that external and internal changes can affect the organization.</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	KEY POINTS Working in groups, write out risks taken to be here today.

Risk Assessments Participant Guide

<p>Slide 4</p>		
<p>Slide 5</p>		<p>KEY POINTS What is your TGRA compliance risk? RISK means a person or thing regarded as a threat of a likely source of danger. There are many categories of risk involved in a casino or TGRA. Let us focus Compliance Risk. This involves the government or regulatory penalties, economical loss or loss of reputation a company may suffer because of failing to comply with a breach of compliance.</p>
<p>Slide 6</p>		<p>KEY POINTS Elements of the risk model include Identify, Assess, Respond to Risk, and Monitoring Risk. Make sure the right people are involved in risk discussions and the policy is clear. Create a culture around risk management and communicate risks as they arise. Continuously monitor for risks.</p>


Risk Assessments Participant Guide

<p>Slide 7</p>		<p>Time for an activity.</p>
<p>Slide 8</p>		
<p>Slide 9</p>		<p>KEY POINTS Your organization needs to understand... what you are good at, to understand how big a threat any risks are to your organization. Through a third party contract, you are not in 100% control of the third party, there would be high risk, and without the knowledge, it is possible the third party may begin manage. Putting your organization at risk for IGRA Violations.</p>

Risk Assessments Participant Guide

Slide 10

Risk Matrix – Assess Activity



Risk Assessment Table		Severity of Harm (Impact)		
		Low (L)	Medium (M)	High (H)
Likelihood	High (H)	3	4	5
	Medium (M)	2	3	4
	Low (L)	1	2	3

Industry Integrity Agency Accountability Preparedness Outreach

KEY POINTS
 A risk matrix is a visual representation of risks laid out in a diagram or a table, hence its alternate name as a risk diagram. Here, risks are divided and sorted based on their probability of happening and their effects or impact. A risk matrix is often used to help prioritize which risk to address first, what safety measures and risk mitigation plans to take, and how a certain task should be done. Risk matrices can come in any size and number of columns and rows, depending on the project and risks being discussed.

Slide 11


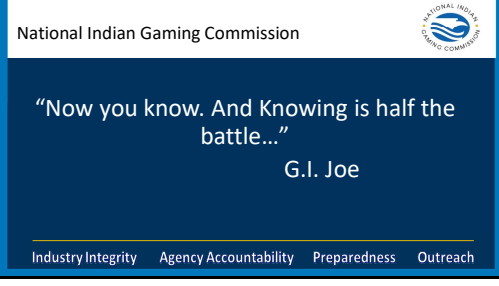
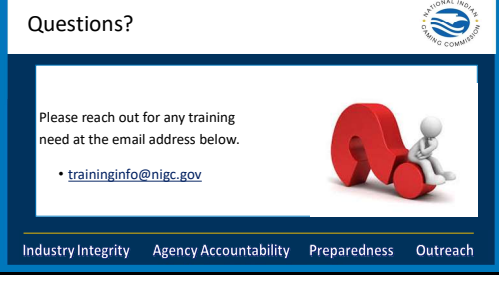
Mitigate Risk Activity




Industry Integrity Agency Accountability Preparedness Outreach

KEY POINTS
 Risk Mitigation is the practice of reducing identified risks. It is one of the four ways to treat risk: avoid, transfer, accept or mitigate. The tools or techniques you use depends on the type of risk you want to mitigate. Way to reduce include: Audits, Backups, Independence, Policies, Training, Communication, Insurance , Contingency plans, Equipment, Due Diligence and Training

Risk Assessments Participant Guide

<p>Slide 12</p>		<p>KEY POINTS</p> <p>Will we accept it? Will we avoid it by not implementing? Will we transfer it to another party or third party? Will we reduce it enough and are happy with the controls we added?</p>
<p>Slide 13</p>		
<p>Slide 14</p>		



Identifying Risk - Group Exercise

Scenario: The TGRA receives information that the Gaming Operation plans to implement Cashless Wagering, using a third-party vendor. This is new to the gaming operation. Taking the time to understand what risks and potential threats are associated with implementing a new process is an important step in assessing risk.

Directions: Discuss with those in your group and determine a list of individuals who should be involved in assessing and then brainstorm all the possible threats that exist. Select someone to document the group's results and share the responses.

Who needs to be involved in assessing the risk?

What are the risks?



Activity – Assess and Analyze Risk

Scenario: The TGRA determined the risks associated with implementing cashless wagering using a third-party vendor. The next step is to analysis your current organization. **Directions:** As a group, conduct a SWOT analysis on your gaming operation to determine risks of implementing cashless wagering, using a third-party vendor.

Aid: **Strengths** – what you do well: **Weakness** – where you need improvement: **Opportunities** – what changes could occur to help you: **Threats** – what changes could cause issues.

SWOT analysis is a framework for identifying and analyzing an organizations strengths, weakness, opportunities and threats.

Strengths

Weakness

Opportunity

Threats

Activity: Risk assessment table

	Severity of Harm (Impact)		
	Low (L)	Medium (M)	High (H)
Likelihood	High (H)		
	Medium (M)		
	Low (L)		

Directions: This stage of a risk assessment involves estimating the likely impacts of the risks your group identified in the last activity. Select one of the risks identified. Based on your assessment of the strengths and weaknesses, determine the likelihood it will occur and the severity of harm. Select someone to record the group's responses and be prepared to discuss.

- 1. Risk (from previous activity):** _____
- 2. Describe the likelihood this is to occur and provide your reasoning (Ex: Highly, Moderate, very unlikely):**
- 3. Describe the severity of impact to the organization if it were to occur and reasoning:**

Part B: Completed when prompted: Mitigating Risk

- 4. Relying on your analysis above determine how to mitigate the risk to reduce its impact. (Ex: reduce, transfer, accept)**

Ultimately, every organization must define and determine how they will rate risk. Regardless of how you have rated your risk, continuous evaluating and monitoring is necessary even with little risk to determine if risks have changed.



NIGC National Training Conference Evaluation
Course Name: Risk Assessments

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.



Note Pages

Lined writing area consisting of 25 horizontal lines.

Ethical Considerations for Regulators Participant Guide

National Indian Gaming Commission



Regulatory Ethical Considerations

Ethical Decision Making and Company Ethics


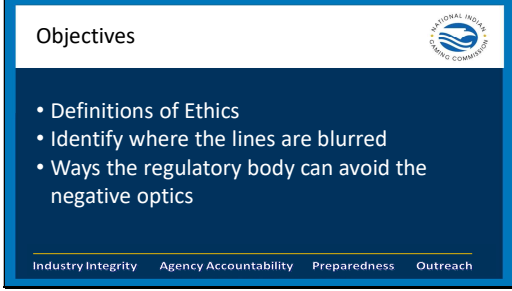
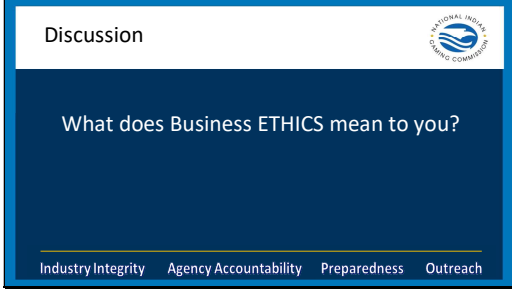
Industry Integrity

Agency Accountability


Preparedness

Outreach

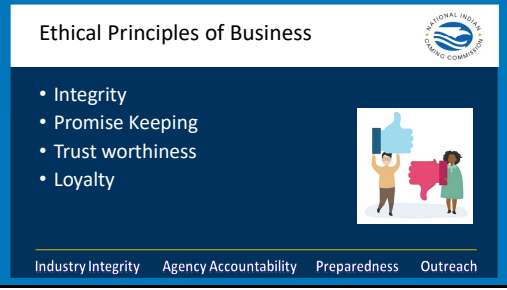

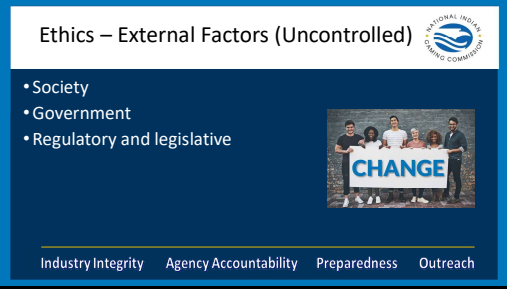
Ethical Considerations for Regulators

<p>Slide 1</p>		<p>KEY POINTS Do you have an ethics policy and is your staff trained on ethics?</p>
<p>Slide 2</p>		
<p>Slide 3</p>		<p>KEY POINTS Large Post It Write out thoughts from the collective group, each table.</p>

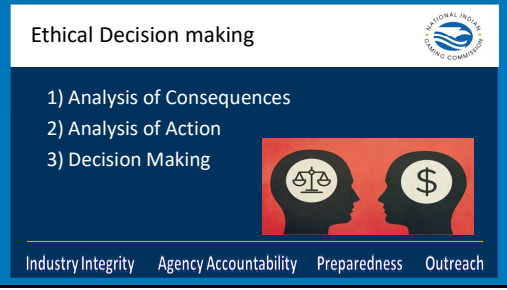

Ethical Considerations for Regulators

Slide 4		
Slide 5	<p>Definition of Business Ethics...</p> <p>The implementation of policies and procedures regarding topics such as fraud, bribery, discrimination and corporate governance.</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS</p> <p>Business ethics concerns ethical dilemmas or controversial issues faced by a company. Often, business ethics involve a system of practices and procedures that help build trust with the consumer. On one level, some business ethics are embedded in the law, such as minimum wages, insider trading restrictions, and environmental regulations. On another, business ethics can be influenced by management behavior, with wide-ranging effects across the company.</p>

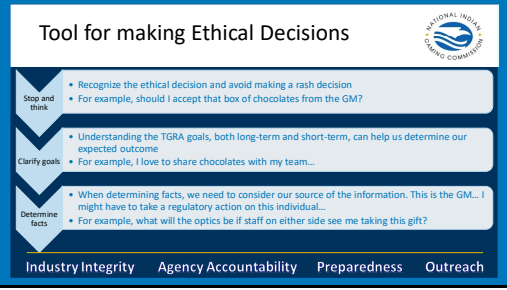
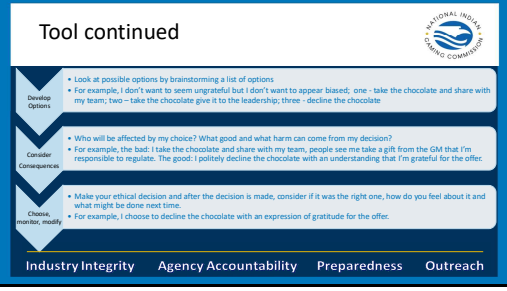

Ethical Considerations for Regulators

<p>Slide 6</p>		<p>KEY POINTS The basis for ethics comes from the above slide: There are numerous principles of ethics apply the ones that work for you.</p>
<p>Slide 7</p>		<p>KEY POINTS Starting point for an ethics policy; Areas where the TGRA has control</p>
<p>Slide 8</p>		<p>KEY POINTS External Factors can be fluid Your Ethics policy should be a living document.</p>



Ethical Considerations for Regulators

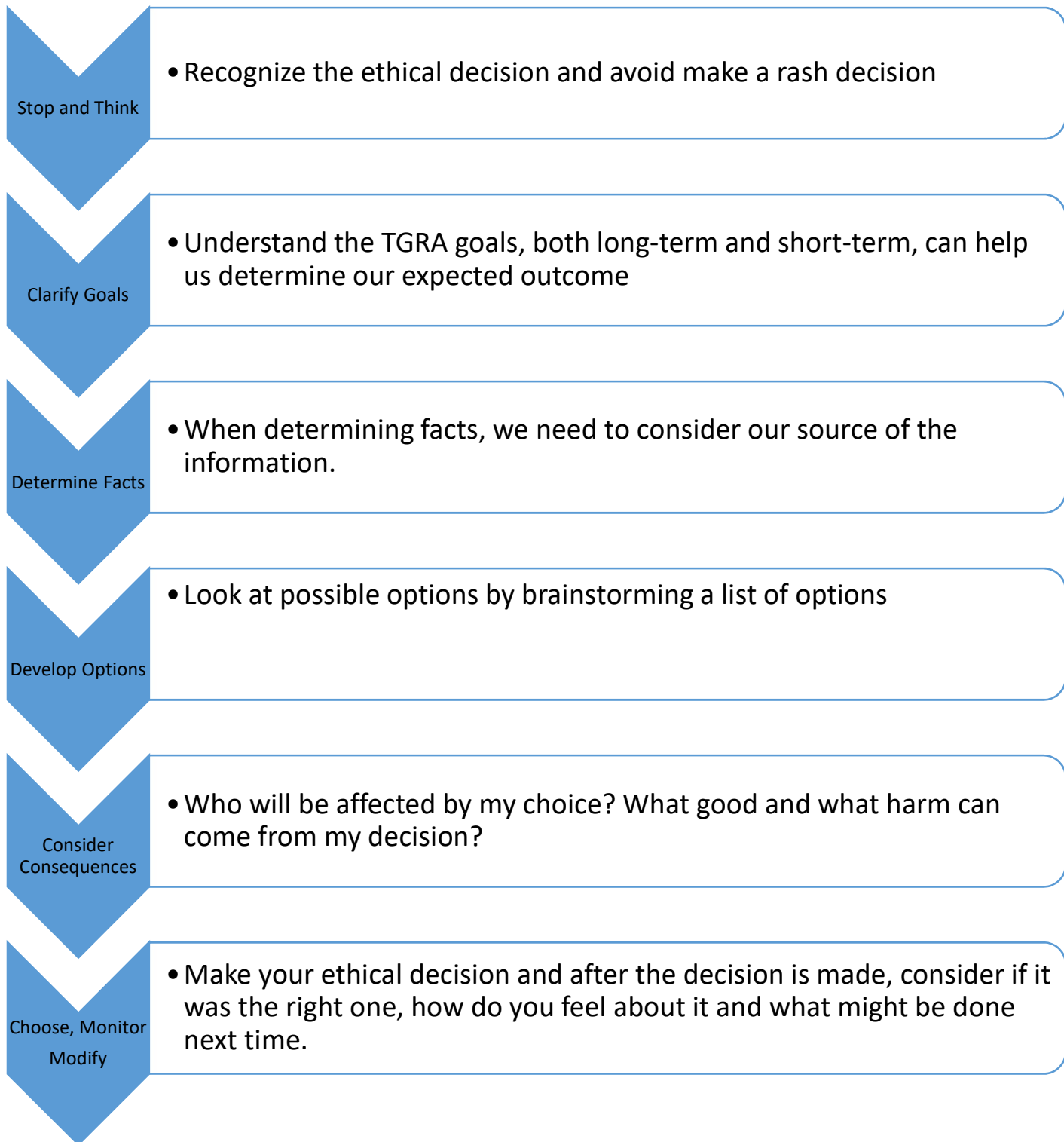
<p>Slide 9</p>	 <p>Ethical Decision making</p> <ol style="list-style-type: none"> 1) Analysis of Consequences 2) Analysis of Action 3) Decision Making <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS</p> <p>Consequences in detail, listing both the pro's and con's; an Analysis of the action, what are the potential outcomes; making a decision.</p>
<p>Slide 10</p>	 <p>Key Elements of Organizational Ethics</p> <ul style="list-style-type: none"> ✓ Morality ✓ Customer Prioritization ✓ Integrity ✓ Respect ✓ Risk-taking <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS</p> <p>Morality – a set of standards that enable people to live cooperatively in groups.</p> <p>Customer Prioritization - an individual is to act in good faith and advance the employers interest.</p> <p>Integrity – honesty</p> <p>Respect – treat all staff with respect, trust engenders trust, positive outcomes, good working conditions so everyone feels able to give their best</p> <p>Risk taking – although not a norm for TGRA's and Commissions, but changing things up a bit are bold and often necessary to make change in long rooted organizations. The core values of course remain the same.</p>

Ethical Considerations for Regulators

<p>Slide 11</p>	 <p>Tool for making Ethical Decisions</p> <p>Stop and think</p> <ul style="list-style-type: none"> Recognize the ethical decision and avoid making a rash decision For example, should I accept that box of chocolates from the GM? <p>Clarify goals</p> <ul style="list-style-type: none"> Understanding the TGRA goals, both long-term and short-term, can help us determine our expected outcome For example, I love to share chocolates with my team... <p>Determine facts</p> <ul style="list-style-type: none"> When determining facts, we need to consider our source of the information. This is the GM... I might have to take a regulatory action on this individual... For example, what will the optics be if staff on either side see me taking this gift? <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	
<p>Slide 12</p>	 <p>Tool continued</p> <p>Develop Options</p> <ul style="list-style-type: none"> Look at possible options by brainstorming a list of options For example, I don't want to seem ungrateful but I don't want to appear biased, one - take the chocolate and share with my team, two - take the chocolate give it to the leadership, three - decline the chocolate <p>Consider Consequences</p> <ul style="list-style-type: none"> Who will be affected by my choice? What good and what harm can come from my decision? For example, the bad: I take the chocolate and share with my team, people see me take a gift from the GM that I'm responsible to regulate. The good: I politely decline the chocolate with an understanding that I'm grateful for the offer. <p>Check, monitor, modify</p> <ul style="list-style-type: none"> Make your ethical decision and after the decision is made, consider if it was the right one, how do you feel about it and what might be done next time. For example, I choose to decline the chocolate with an expression of gratitude for the offer. <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	
<p>Slide 13</p>	 <p>Tool for making ethical decisions</p> <p>ACTIVITY</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS</p> <p>Activity: Tool for making ethical decisions</p> <p>Small Group Activity</p> <p>Supplies: (per group)</p> <ul style="list-style-type: none"> Using the model provided

Ethical Considerations for Regulators

<p>Slide 14</p>	<p>Questions?</p>  <p>For more training opportunities or questions please contact us:</p> <p>Traininginfo@NIGC.GOV</p>  <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	
-----------------	---	--





NIGC National Training Conference Evaluation
Course Name: Ethical Considerations for Regulators

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Panel: The Regulatory Landscape



National Indian Gaming Commission

Panel: The Regulatory Landscape

Industry Integrity Agency Accountability Preparedness Outreach



NIGC National Training Conference Evaluation
Course Name: Panel: The Regulatory Landscape

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Criminal History Record Information (CHRI) and Compliance with 25 CFR Part 558.3(e)

National Indian Gaming Commission



NIGC CJIS Audit

CHRI and Part 558.3 (e)

Industry Integrity

Agency Accountability

Preparedness

Outreach

Slide 1



National Indian Gaming Commission

NIGC CJIS Audit Unit

◆

CHRI and Part 558.3 (e)

Industry Integrity Agency Accountability Preparedness Outreach

PARTICIPANT GUIDE

Chairman Simermeyer promotes four emphasis areas in the Agency’s work. This training reinforces these four emphasis areas and the agency’s commitment to the Indian gaming industry and Indian Country.

The NIGC Criminal Justice Information Services (CJIS) Audit Unit (CAU) is responsible for the implementation of the NIGC’s external and internal compliance strategies to achieve and demonstrate compliance with the Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and NIGC concerning Noncriminal Justice Fingerprint Submissions. CAU audit staff deliver trainings, technical assistance and conduct selective audits / investigations of those tribes with an executed, suspended, or terminated MOU with the NIGC regarding CHRI.

Slide 2



National Indian Gaming Commission




➤ Is this CHRI?

Industry Integrity Agency Accountability Preparedness Outreach

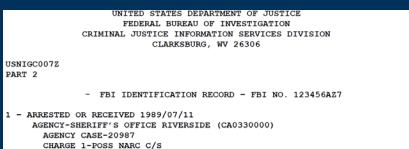
PARTICIPANT GUIDE

There are two fingerprinting processes to obtain CHRI results through the NIGC—electronic fingerprint and hard card fingerprint submissions. Tribes submit fingerprint *images* and receive Criminal History Record Information (CHRI).

Slide 3



National Indian Gaming Commission




Industry Integrity Agency Accountability Preparedness Outreach

PARTICIPANT GUIDE

This is Criminal History Record Information (CHRI).

CHRI means information collected by criminal justice agencies about individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. CHRI also includes information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI. CHRI includes any media that contains it, such as: Letters, emails, documents, notes, conversations – in person or via phone/text, and spreadsheets or tables. Examples of CHRI potentially include: notice of results (NORs), investigative reports (IRs), licensing objection letters, and other summaries of CHRI. Updating the NOR to remove the FBI CHRI results can help eliminate summary CHRI.

Slide 4



National Indian Gaming Commission



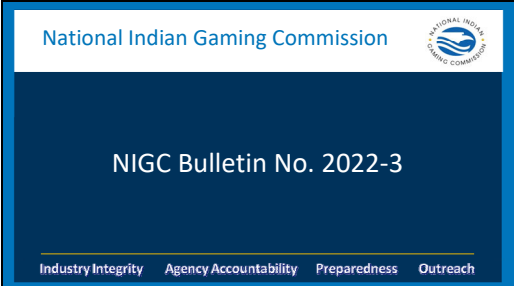

Is CHRI required to comply with Part 558.3 (e)?

Industry Integrity Agency Accountability Preparedness Outreach

PARTICIPANT GUIDE

Is CHRI required to be maintained to comply with Part 558.3(e)? What do you need to know about the CJIS Security Policy 4.2.4?

CJIS Security Policy (CJISSECPOL) Section 4.2.4, Storage
When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.
See <https://le.fbi.gov/cjis-division-resources/cjis-security-policy-resource-center>

<p>Slide 5</p>	 <p>National Indian Gaming Commission</p> <p>Investigative reports ❖ Eligibility determinations</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>PARTICIPANT GUIDE §558.3 Notification to NIGC of license decisions and retention obligations. (e) A tribe shall retain the following for inspection by the Chair or his or her designee for no less than three years from the date of termination of employment: (1) Applications for licensing; (2) Investigative reports; and (3) Eligibility determinations.</p> <p>See https://nigc.gov/general-counsel/commission-regulations</p>
<p>Slide 6</p>	 <p>National Indian Gaming Commission</p> <p>➤ Sanitize CHRI?</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>PARTICIPANT GUIDE How do you sanitize CHRI?</p> <p>Information is not considered CHRI if it is obtained as a result of using CHRI received from a national FBI check as a lead to reach out to source record owners such as local courts or state criminal history record repositories. As a prerequisite, both the process used to obtain the source record information and the resulting source record information itself must not directly reference or be attributed to the national FBI check.</p> <p>Information is considered CHRI if it confirms the existence or nonexistence of CHRI.</p> <p>See https://www.nigc.gov/images/uploads/ngi-audit-noncriminal-policy-reference-guide-june-2022.pdf</p>
<p>Slide 7</p>	 <p>National Indian Gaming Commission</p> <p>NIGC Bulletin No. 2022-3</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>PARTICIPANT GUIDE See https://nigc.gov/images/uploads/bulletins/NIGCBulletin2022-3_CHRI_Retention_20220603.pdf</p>
<p>Slide 8</p>	 <p>National Indian Gaming Commission</p> <p>NIGC CJIS Resource Materials</p> <p>❖ https://nigc.gov/technology/cjis-resource-materials</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>PARTICIPANT GUIDE The NIGC has spent the past couple of years providing CJIS training and has a multitude of resources available at https://nigc.gov/technology/cjis-resource-materials</p> <p>If you need CJIS technical assistance, please email us at cau@nigc.gov</p>



BULLETIN

No. 2022-3

June 3, 2022

Subject: Criminal History Record Information (CHRI) Retention

The NIGC processes fingerprints submitted by tribes for background investigations of primary management officials (PMO) and key employees (KE). Prior to issuing a gaming license to a PMO or KE, a tribe is required to perform a fingerprint check through the FBI¹ records system as part of the background investigation on each applicant. The criminal history record information CHRI² obtained as a result of the check assists the tribe in determining the applicant's eligibility for employment.

This bulletin addresses FBI CHRI retention obligations and how these obligations may intersect with the National Indian Gaming Commission (NIGC) regulatory mandates for retaining primary management official and key employee licensing applications, eligibility determinations, and investigation reports.

I. CHRI & CHRI Dissemination

Initially, it is important to understand the functions and purpose of the CHRI. CHRI comprises “information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information[], or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual’s involvement with the criminal justice system.”³ CHRI is also information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI.⁴ CHRI includes

¹ Federal Bureau of Investigation.

² Criminal History Record Information.

³ 28 C.F.R. § 20.3.

⁴ See Next Generation Identification Audit, Noncriminal Justice Access to Criminal History Record Information, Policy Reference Guide (hereinafter NGI) at 1 (Apr. 6, 2020).

any media that contains CHRI, such as: letters, emails, documents, notes, conversations—in person or via phone/text, and spreadsheets or tables.⁵

In order to assist, TGRAs⁶ determine the eligibility of applicants for key employee (KE) or primary management official (PMO) positions in their gaming operation(s), the NIGC obtains CHRI from the FBI on these applicants and disseminates it to the TGRAs. The NIGC provides this assistance pursuant to a joint MOU⁷ between the agency and TGRAs, which memorializes the parties' understandings and responsibilities regarding the submission of noncriminal justice fingerprints and the transmittal, receipt, storage, use, and dissemination of CJJ⁸ and CHRI. As noted, this bulletin's focus is retention of CHRI after its proper use.

II. CHRI Retention Obligations

A. CHRI retention

So how long must TGRAs retain CHRI? CHRI may be destroyed as soon as practicable by TGRAs—potentially at the conclusion of a licensing appeal process or the CHRI audit process (whichever comes later), in accordance with the TGRA's media sanitization and destruction policy. The FBI CJIS Security Policy instructs that CHRI “records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal records.”⁹ Further, the policy indicates that “[p]hysical media shall be securely disposed of when no longer required”¹⁰

B. CHRI & NIGC regulatory retention requirements

i. Investigation reports & sanitizing CHRI

NIGC regulations do not require that CHRI itself be retained,¹¹ just summary CHRI if it is transferred into an investigation report.¹² Specifically, NIGC regulations, Sections 556.6 (b)(2)(iii)(C) and (D) require that an investigation report include “every known criminal charge . . .” and “every felony” So TGRAs may put summary CHRI in an investigation report. Under NIGC regulations, an investigation report must be retained by a TGRA for three (3) years from the date of the primary management official (PMO) or key employee's (KE) employment termination date.¹³

⁵ *Id.*

⁶ Tribal Gaming Regulatory Agencies.

⁷ Memorandum of Understanding.

⁸ Criminal Justice Information is the term used for the FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

⁹ See CJIS Security Policy, Section 4.2.4.

¹⁰ *Id.* at Section 5.8.4.

¹¹ See 25 C.F.R. parts 556 and 558.

¹² See 25 C.F.R. §§ 556.6 (a) & (b)(2)(iii)(C) and (D); 558.3(e).

¹³ 25 C.F.R. § 558.3(e).

But TGRAs may avoid putting summary CHRI in investigation reports—and maintaining CHRI for a significant period of time with its required protections¹⁴—by sanitizing the CHRI. To sanitize CHRI, TGRAs use it as a lead to reach out to source record-owners, such as local courts or state criminal history record repositories, and obtain the original criminal history¹⁵. Importantly, both the process used to acquire the source record information and the resulting original criminal history information must not directly reference or be attributed to the national FBI check. This is because information is considered CHRI if it confirms the existence or nonexistence of CHRI.

ii. Licensing applications & eligibility determinations

The other documents that NIGC regulations direct be held for three years after a KE or PMO's termination do not necessitate the inclusion of CHRI or a summary of it.¹⁶ Applications for KE and PMO licensing explicitly contain only information *from* the applicant.¹⁷ NIGC regulations require that “[a] tribe shall request from each primary management official and from each key employee [certain] information . . . ,” including felony, misdemeanor, and criminal charges.¹⁸ Such information is not CHRI though, because it is not from a criminal justice agency.¹⁹ And fingerprints given as part of that application also are not CHRI.²⁰

Eligibility determinations simply require that the TGRA review a person's criminal record and determine if they are suitable.²¹ So eligibility determinations should not include CHRI or a summary of it. Of course TGRAs need to be careful not to summarize, reproduce, or confirm the existence or nonexistence of CHRI in eligibility determinations, as that constitutes summary CHRI.²² If TGRAs do include CHRI in the eligibility determination, then it must be maintained for three (3) years from the date of the PMO or KE's employment termination.

iii. Abbreviated background investigations

Finally, CHRI results also may be destroyed as soon as practicable when TGRAs implement an abbreviated background investigation process. This occurs when after the

¹⁴ See CJIS Security Policy, Sections 4 and 5; see also NIGC Bulletin No. 2020-2, *Fingerprint processing — applicant Privacy Act rights and protecting CHRI* at 3-4 (Feb. 18, 2020), [https://www.nigc.gov/images/uploads/bulletins/Bulletin - Privacy Act rights protecting CHRI - FINAL FINAL.pdf](https://www.nigc.gov/images/uploads/bulletins/Bulletin_-_Privacy_Act_rights_protecting_CHRI_-_FINAL_FINAL.pdf)

¹⁵ Or, in other words, source record information.

¹⁶ See 25 C.F.R. § 558.3(e).

¹⁷ See 25 C.F.R. § 556.6(a) (“the tribe shall maintain a complete application file containing the information listed under 556.4(a)(1) through (14)”).

¹⁸ See 25 C.F.R. § 556.4(a).

¹⁹ See 28 C.F.R. § 20.3(g)(2).

²⁰ See National Identity Services Audit Noncriminal Justice Access to CHRI, Policy Reference Guide at 1 (07/22/2019) (CHRI “does not include identification information such as fingerprint records if such information does not indicate the individual's involvement in the criminal justice system.”).

²¹ See 25 C.F.R. § 556.5.

²² See National Identity Services Audit Noncriminal Justice Access to CHRI, Policy Reference Guide at 1 (07/22/2019) (“Information is considered CHRI if it is transferred or reproduced directly from CHRI received as a result of a national FBI Check Information is considered CHRI if it confirms the existence or nonexistence of CHRI.”).

submission of a completed application, CHRI is requested, evaluated, and then used to ask the applicant to withdraw their application. In those cases, TGRAs do not prepare an investigation report, make an eligibility determination, or create and submit a Notice of Results (NOR). Consequently, summary CHRI is not contained in any of those documents and may be destroyed upon the application's withdrawal, in accordance with the TGRA's media sanitization and destruction policy.

III. Conclusion

In sum, NIGC regulations do not require that CHRI results themselves be retained, and such results may be destroyed as soon as practicable by a TGRA. Also, TGRAs must be careful to sanitize CHRI for purposes of investigation reports and avoid including summary CHRI or confirming its existence or nonexistence in eligibility determinations. Doing so ensures that CHRI is not subject to the NIGC regulatory retention requirements for investigation reports and eligibility determinations.

Should you have any questions regarding the information covered in this bulletin, please contact a [NIGC Region Office](#) or the CJIS Audit Unit at cau@nigc.gov.



NIGC National Training Conference Evaluation
Course Name: Criminal History Record Information (CHRI)
and Compliance with 25 CFR Part 558.3(e)

NIGC greatly appreciates your feedback to aid in our Training offerings.

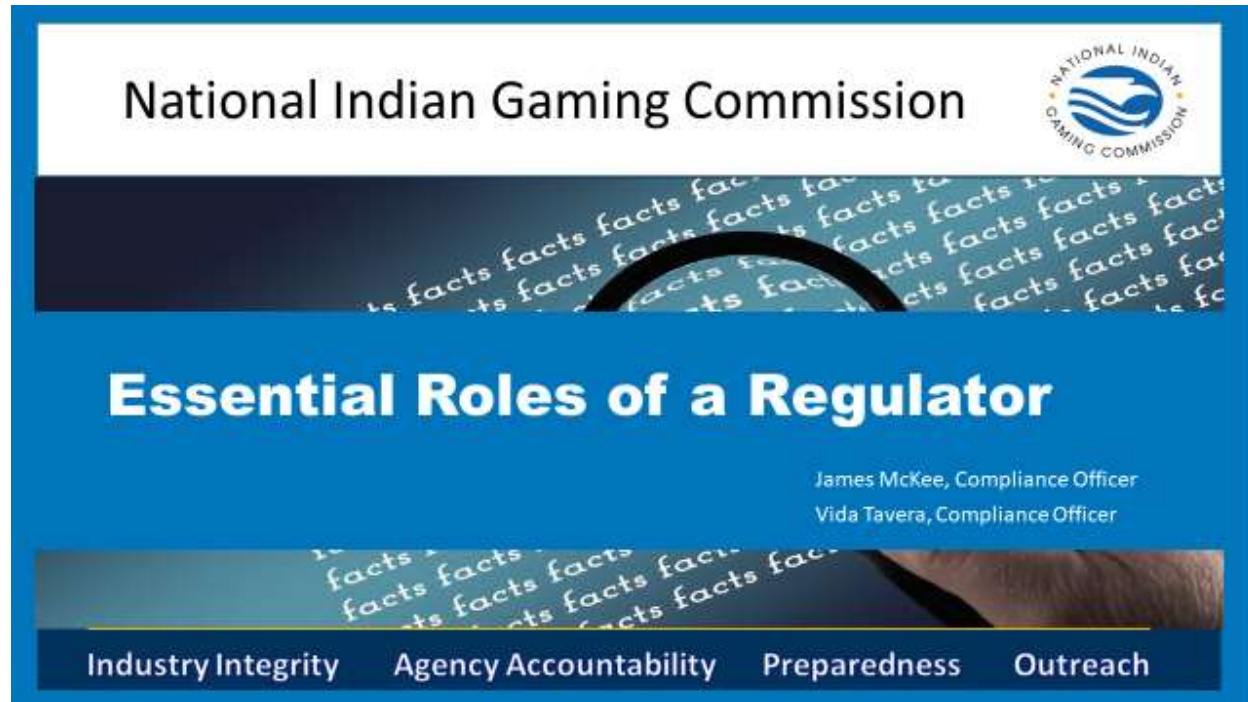
<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Essential Roles of a Regulator Participant Guide



The image shows the cover of a report titled "Essential Roles of a Regulator" from the National Indian Gaming Commission. The cover features a blue background with a pattern of the word "facts" repeated in various orientations. At the top, the National Indian Gaming Commission logo is visible, which includes a stylized eagle and the text "NATIONAL INDIAN GAMING COMMISSION". Below the logo, the title "Essential Roles of a Regulator" is prominently displayed in white. Underneath the title, the names of the authors, James McKee and Vida Tavera, are listed as Compliance Officers. At the bottom of the cover, four key roles are highlighted: Industry Integrity, Agency Accountability, Preparedness, and Outreach.




National Indian Gaming Commission

Essential Roles of a Regulator

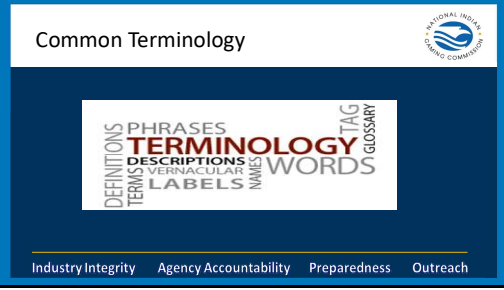
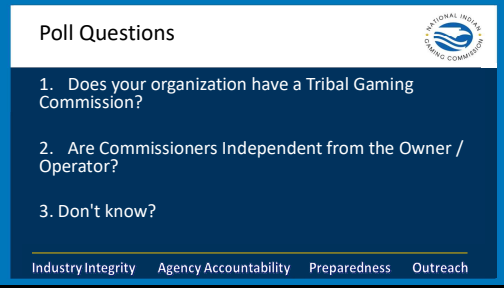
James McKee, Compliance Officer
Vida Tavera, Compliance Officer

Industry Integrity Agency Accountability Preparedness Outreach

Essential Roles of a Regulator Participant Guide

<p>Slide 1</p>		
<p>Slide 2</p>		<p>Key Points Define and discuss common terminology Identify and discuss IGRA Review gaming ordinances Review structural organization and function of TGRA Explore Authority and Responsibilities of the TGRA</p>
<p>Slide 3</p>		<p>Key Points If something is said or a term is used you are unfamiliar with, please let us know.</p>

Essential Roles of a Regulator Participant Guide

<p>Slide 4</p>		<p>Key Points</p> <p>Agency Names Tribal Gaming Commission Tribal Gaming Agency Tribal Gaming Authority Tribal Gaming Regulatory Authority</p> <p>Titles and Terms Commissioner Gaming Inspector Compliance Officer Internal Auditor MICS, TICS, SICS Owner (Tribe) Operations(Mgmt.)</p>
<p>Slide 5</p>		<p>Key Points</p> <ol style="list-style-type: none">1. Yes / No2. Yes / No3. Yes

Essential Roles of a Regulator Participant Guide

Slide 6



Key Points

The Indian Gaming Regulatory Act's (IGRA) History

IGRA (25 U.S.C. §§ 2701 – 2721) was enacted in 1988 in the wake of *Cabazon*

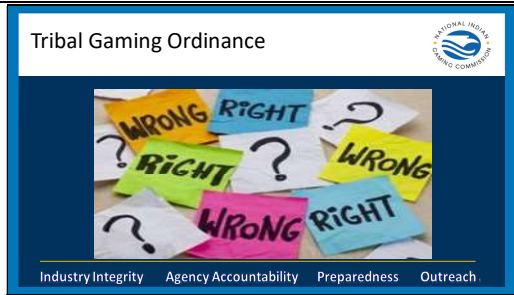
- maintains Tribes as primary regulators
- Established the regulatory role of the National Indian Gaming Commission (NIGC) for Class II gaming (States regulate Class III) The tribal/state compact defines who regulates class III, it could be State, Tribe or both.
- Established the legal framework Tribes' are required to comply with in regards to gaming on tribal lands.

Purpose of IGRA (25 U.S.C. §2702):

- Promote tribal economic development, self-sufficiency, and strong tribal governments
- Shield tribes from organized crime
- Ensure tribes are the primary beneficiary of the gaming activities
- Ensure gaming is conducted fairly and honestly
- Establish federal regulatory authority for gaming on Indian lands

Essential Roles of a Regulator Participant Guide

Slide 7




Key Points

Tribal law creates TGRA authority to regulate gaming. Before gaming commences, a tribe must have a gaming ordinance approved by the NIGC Chair. A gaming ordinance provides the foundation in which a tribe may regulate gaming. Each tribe is encouraged to tailor a gaming ordinance that best suits their needs.



- Incorporating IGRA & NIGC regulation requirements.
 - Example – Model Gaming Ordinance (www.nigc.gov/compliance/bulletins)
 - Published January 10, 2018

Separate from the gaming ordinance/code are the tribal rules and regulations. The rules and regulations are more in-depth as opposed to the ordinance informing the public about the law. The rules and regulations inform the public how the law will be carried out. Tribal rules and regulations do not need NIGC approval. Tribal rules and regulations may be revised at any time and do not need to be reviewed by the NIGC.


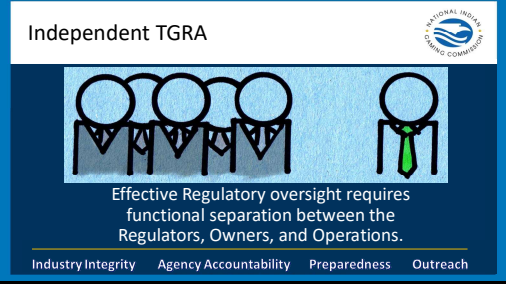

Essential Roles of a Regulator Participant Guide

<p>Slide 8</p>	 <p>Tribal Gaming Regulatory Authority</p> <p>Structural Organization & Operational Function</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>Key Points</p> <p>Structural Organization and Operational Function</p> <p>Matters to be considered and possibly included in the Ordinance or Laws establishing the TGRA:</p> <ul style="list-style-type: none">• Clearly defined responsibilities, powers, and enforcement Authority• Number of Commissioners, term length, selection process, removal process, time commitment, and continuity of the Commission• Funding should be appropriated from the Government, not by the Gaming Operation• Procedures for conducting official commission business and appeal/hearing procedures for Commission Action• Procedures for regular reports to Tribal Government on the health of the gaming operation from the Regulatory perspective (Monthly Stats on Incidents, Crimes, Internal Control Violations, etc.)
----------------	---	--

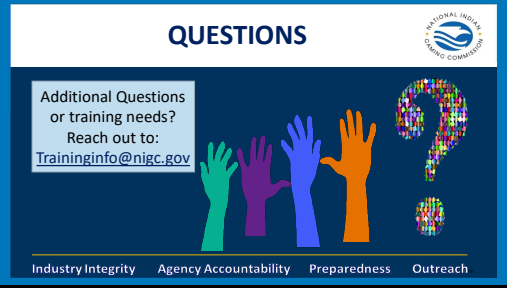
Essential Roles of a Regulator Participant Guide

<p>Slide 9</p>	 <p>TGRA Structure</p> <p>Working Commission</p> <p>Board Style</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>Key Points</p> <p>*Common Structures</p> <p>*Working Commission - Commissioners have offices on-site and participate with the day-to-day regulation of the facility. Act as permanent employees of the TGRA.</p> <p>*Board Style - Delegates the day-to-day regulatory oversight to regulatory employees on site. Meets periodically and often has term limits.</p> <p>Combination working and board – Where some commissioners are full time capacity and others on stipend for meetings.</p>
<p>Slide 10</p>	 <p>Round Table Discussion</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>Key Points</p> <p>In a round table: Select someone to write and someone to present to the group. Using the large post-IT, discuss and write out your day-to-day responsibilities.</p>

Essential Roles of a Regulator Participant Guide

<p>Slide 11</p>	 <p>The slide features a blue background with a white cloud at the top containing the letters T, G, R, and A. Below the cloud are three blue water droplets labeled 'Writing Regulations', 'Monitoring', and 'Investigations'. These droplets are positioned above a brown woven basket labeled 'Regulatory Bucket'. At the bottom of the slide, four categories are listed: 'Industry Integrity', 'Agency Accountability', 'Preparedness', and 'Outreach'. The National Indian Gaming Commission logo is in the top right corner.</p>	<p>Key Points The TGRA has authority in regulating gaming. The passing of IGRA provided some specific requirements and submissions. The bulk of the responsibilities are left to the Tribe.</p>
<p>Slide 12</p>	 <p>The slide shows four stylized human figures in suits. The first three are identical, while the fourth is slightly larger and has a green tie. Below the figures, the text reads: 'Effective Regulatory oversight requires functional separation between the Regulators, Owners, and Operations.' The bottom of the slide lists 'Industry Integrity', 'Agency Accountability', 'Preparedness', and 'Outreach'. The National Indian Gaming Commission logo is in the top right corner.</p>	<p>Key Points</p> <ul style="list-style-type: none"> • Clearly defined and established by Ordinance or Tribal law • Separate arm of the Tribal Government • Exclusively for regulation and monitoring of the gaming operations
<p>Slide 13</p>	 <p>The slide features a rocket ship launching upwards. The rocket is labeled 'TGRA Mission Statement'. Above the rocket, the word 'Responsibilities' is written, with 'Regulations' and 'Authorities' positioned on either side. Below the rocket, the words 'Management' and 'Duties' are written. The bottom of the slide lists 'Industry Integrity', 'Agency Accountability', 'Preparedness', and 'Outreach'. The National Indian Gaming Commission logo is in the top right corner.</p>	<p>Key Points Try to maintain a focus on regulatory issues and achieve the organization's goals. TGRA's do not manage the facility, their job is to make sure that the facility operates within Tribal, Federal laws and if applicable within the regulations set forth in the State Compact. Ask yourself, How does each task or TGRA responsibility help meet your regulatory mission and organizational goals?</p>

Essential Roles of a Regulator Participant Guide

<p>Slide 14</p>		<p>Key Points If you have any questions or would like information about additional topics and training please contact the NIGC training department at traininginfo@nigc.gov.</p>
-----------------	---	--



NIGC National Training Conference Evaluation
Course Name: Essential Roles of a Regulator

NIGC greatly appreciates your feedback to aid in our Training offerings.


<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.


How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Report Writing Participant Guide



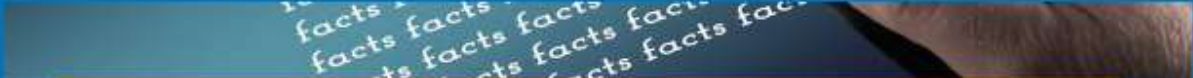
National Indian Gaming Commission



How to Write an Effective Report

JoElle Thompson, Compliance Officer

Sam Wetzler, Compliance Training



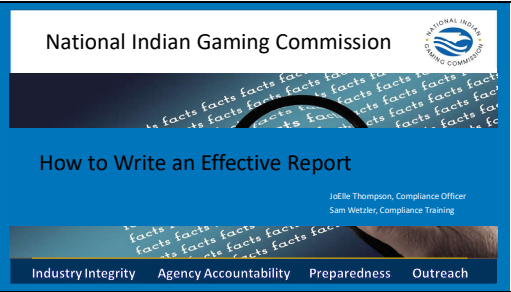


Industry Integrity

Agency Accountability



Preparedness

Outreach



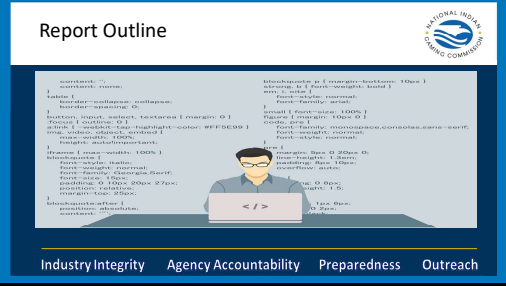
Report Writing Participant Guide

<p>Slide 1</p>		<p>KEY POINTS Welcome to "How to Write an Effective Report"</p>
<p>Slide 2</p>		<p>KEY POINTS General Principle of report writing, helpful hints and understanding best practices is the goal of this session.</p>
<p>Slide 3</p>		<p>KEY POINTS Eschew Obfuscation means to avoid ambiguity, adopt clarity</p>




Report Writing Participant Guide

<p>Slide 4</p>		<p>KEY POINTS</p> <p>Definition of a Report: Verb: Give a spoken or written account of something that one has observed, heard, done, or investigated. <i>Noun:</i> An account given of a particular matter, especially in the form of an official document, after thorough investigation or consideration by an appointed person or body.</p>
<p>Slide 5</p>		<p>KEY POINTS</p> <p>Provide decision makers with information to reach a disposition.</p>






Report Writing Participant Guide

<p>Slide 6</p>		<p>KEY POINTS Please see handout "how to write an effective report."</p>
<p>Slide 7</p>		<p>KEY POINTS Major Components:</p> <ul style="list-style-type: none"> • The facts • The policy, procedure, regulation, law • The evidence • The analysis • The conclusion
<p>Slide 8</p>		<p>KEY POINTS Introduction – summary Body- detailed facts Conclusion – wraps up the analysis that guided the results of the investigation</p>


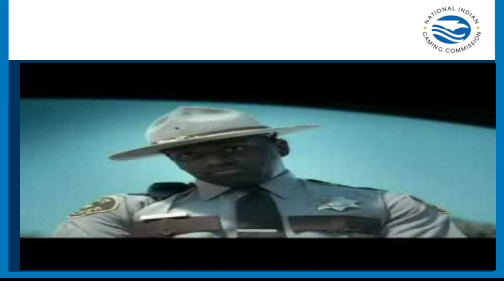
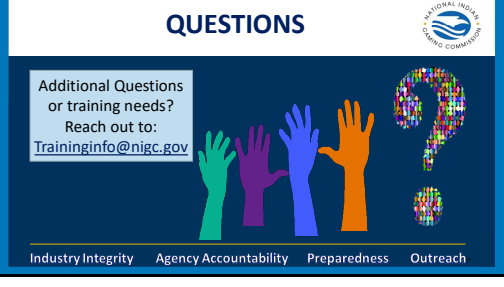
Report Writing Participant Guide

<p>Slide 9</p>		<p>KEY POINTS Do – use third person voice, document, use paragraphs if necessary Don't – use slang, opinions for facts, judgement before completion or submission without proofreading.</p>
<p>Slide 10</p>		<p>KEY POINTS See attachment "how to write an effective report"</p>
<p>Slide 11</p>		<p>KEY POINTS See attachment "how to write an effective report"</p>

Report Writing Participant Guide

<p>Slide 12</p>	<p>Who, What, When, Where, Why and How </p>  <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS See handout "how to write an effective report"</p>
<p>Slide 13</p>	<p>National Indian Gaming Commission </p> <p>The NIGC does not promote or endorse products or services. The use of these videos are for instructional purposes on how to observe and document activities.</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	
<p>Slide 14</p>	<p>Good vs. Bad Reports </p>  <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS Individual Activity Time: 15-30 mins.</p>

Report Writing Participant Guide

Slide 15		
Slide 16		
Slide 17		<p>KEY POINTS If you have any questions or would like information about additional topics and training please contact the NIGC training department at traininginfo@nigc.gov.</p>



How to Write an Effective Report Course Handout


I. Purpose

- a) To document an impartial account of the facts and circumstances of an event.
- b) Defend Investigation

II. Helpful Hints

- a) Write the report in a Microsoft Word or similar Software and copy the text into the final report format.
- b) Complete every section of the report form, if utilized. Include the date, time, location, and the reason for the report in the text of the report.
- c) Be detailed as it relates to the facts. If someone was helpful or uncooperative, describe the actions of the person.
- d) Outline Components
- e) Introduction (the beginning) – The introduction should include a summary of the event and investigation. Describe the event, investigation plan, relevant regulations or laws and the result.
- f) The body (the middle) - of the report should detail the facts of the event, the scope of the investigation, the evidence gathered, the evidence reviewed and the analysis of the evidence.
- g) The conclusion (the end) should explain how, the analysis guided the results of the investigation.

III. Effective Characteristics

- a) Well organized
 - b) Grammatically correct
 - c) Defines all necessary terms, abbreviations and acronyms
 - d) Accurate
 - e) Specific Objective
- 

- f) Clear, Complete, Concise

IV. Common Problems

- a) Confusing
- b) Lack organization
- c) Not enough relevant details
- d) Not concise
- e) Poor grammar, punctuation, spelling
- f) Incorrect word use
- g) Use of terms, abbreviation and acronyms without explanation

V. WWWWWH

- a) Noticing details that matter – Height, clothing, speech, accent, things in the hand. Notice things, don't focus too much on describing them.
- b) Surroundings – Place, weather, crowded or not, temperature
- c) Action – What was happening, what are you describing?
- d) Subject – Who is the center of the action, the person doing the activity or the person who is the subject of the activity?
- e) Result – What happened as a result between the subject of the action and the object of the action?

Notes:





NIGC National Training Conference Evaluation
Course Name: Report Writing

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

National Indian Gaming Commission



556.6 Tribal Eligibility Determination

NIGC Training


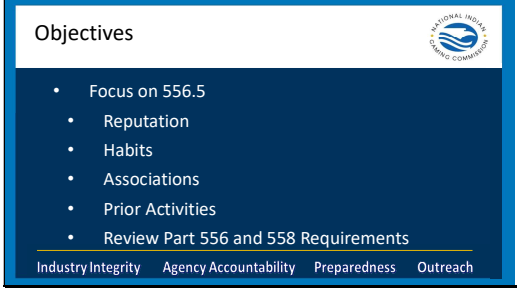
Industry Integrity

Agency Accountability

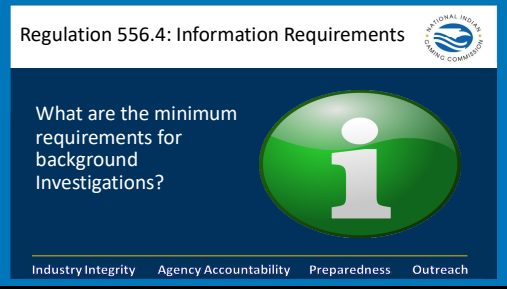
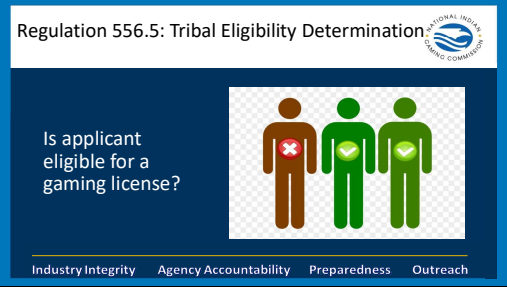
Preparedness

Outreach

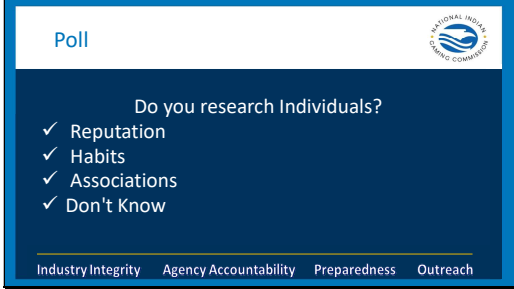
Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 1</p>		<p>KEY POINTS Welcome to Tribal Eligibility Determination.</p>
<p>Slide 2</p>		<p>KEY POINTS Going beyond the bear minimum Focus on 556.5 “Tribal Eligibility Determination” with a focus on the Reputation, Habits and Associations as well as prior activities.</p>

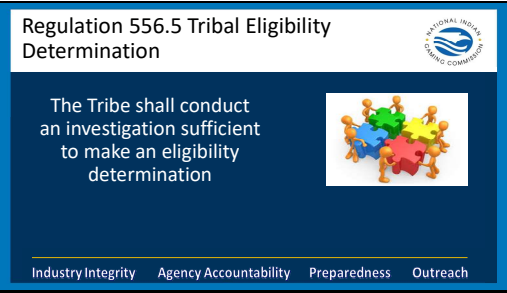
Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 3</p>		<p>KEY POINTS</p> <ul style="list-style-type: none"> • Touch on Notification requirement to NIGC (NOR, and Licensing notifications) and this is only a small piece of a much larger process • 556.4 details the specific information that must at a minimum be requested from every applicant applying for KE or PMO position. • This required information provides a starting point in the background investigative work
<p>Slide 4</p>		<p>KEY POINTS</p> <p>How do you decide if an applicant is eligible for a gaming license?</p> <p>NIGC 556.5 says A Tribe shall conduct an investigation sufficient to make an eligibility determination.</p> <ul style="list-style-type: none"> • To make a finding concerning the eligibility of a key employee or primary management official for granting of a gaming license, an authorized tribal official shall review a person's: <ol style="list-style-type: none"> (1) Prior activities; (2) Criminal record, if any; and <ol style="list-style-type: none"> (3) Reputation, habits and associations. <p>(b) If the authorized tribal official, in applying the standards adopted in a tribal ordinance, determines that</p>



Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

		<p>licensing of the person poses a threat to the public interest or to the effective regulation of gaming, or creates or enhances the dangers of unsuitable, unfair, or illegal practices and methods and activities in the conduct of gaming, an authorizing Tribal official shall not license that person in a key employee or primary management official position.</p>
Slide 5		<p>Show of Hands</p> <ul style="list-style-type: none"> • Reputation • Habits • Activities • Don't know?



Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 6</p>	 <p>Regulation 556.5 Tribal Eligibility Determination</p> <p>The Tribe shall conduct an investigation sufficient to make an eligibility determination</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS What is considered sufficient and adequate?</p> <p><u>§ 556.5 Tribal eligibility determination.</u></p> <p>A tribe shall conduct an investigation sufficient to make an eligibility determination.</p> <p>(a) To make a finding concerning the eligibility of a key employee or primary management official for granting of a gaming license, an authorized tribal official shall review a person's:</p> <ul style="list-style-type: none">(1) Prior activities;(2) Criminal record, if any; and(3) Reputation, habits, and associations. <p>(b) If the authorized tribal official, in applying the standards adopted in a tribal ordinance, determines that licensing of the person poses a threat to the public interest or to the effective regulation of gaming, or creates or enhances the dangers of unsuitable, unfair, or illegal practices and methods and activities in the conduct of gaming, an authorizing tribal official shall not license that person in a key employee or primary management official position.</p>
----------------	--	--



Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 7</p>		<p>Setting a licensing standard for PMO's/Key/Non-Key licensee's:</p> <p>Activity #1</p> <p>Directions: Working as a group, determine and develop a list of Prior activities, Crime(s), Reputation, Habits, or Associations, that would disqualify an applicant from being licensed.</p>
<p>Slide 8</p>		<p>KEY POINTS</p> <p>Let's brainstorm some avenues we might be able to make use of in making an eligibility determination</p>



Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 9</p>		<p>KEY POINTS Criminal records may include fingerprinting, State, City, County or governing jurisdiction...</p>
<p>Slide 10</p>		<p>PARTICIPANT GUIDE Free records checks can help you verify information provided from your applicant.</p> <ul style="list-style-type: none"> • Pacer • State courts • NIGC Tribal Access Portal • Other TGRA's- you can develop a reference form to send to other TGRA's to verify licensing information from them.



Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 11</p>		<p>KEY POINTS</p> <p>Your reputation precedes you...</p>
<p>Slide 12</p>		<p>Activity #2</p> <p>Let's look up a name using google and see what we can simply see by opening a page or two associated with the name:</p>



Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 13</p>	 <p>National Indian Gaming Commission</p> <p>so-cial me-di-a: <i>noun</i> websites and applications that enable users to create and share content or to participate in social networking.</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS</p> <p>Why should you consider utilizing social media? Studies have shown a majority of Facebook, Snapchat and Instagram users say they visit these platforms on a daily basis.</p>
<p>Slide 14</p>	 <p>National Indian Gaming Commission</p> <p>Where do you look?</p> <p>Industry Integrity Agency Accountability Preparedness Outreach</p>	<p>KEY POINTS</p> <ul style="list-style-type: none"> • Google • LinkedIn • Facebook • Instagram

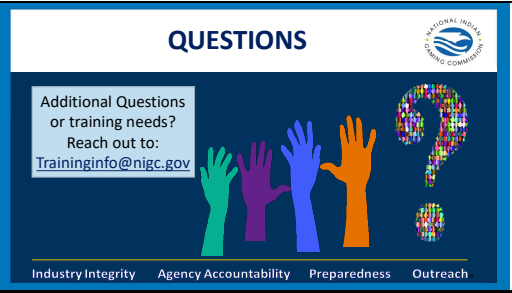
Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 15</p>		<p>KEY POINTS</p> <p>How do you discern individual's habits?</p>
<p>Slide 16</p>		<p>KEY POINTS</p> <p>How do you note or look into an individual's associations?</p>

Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 17</p>		<p>Activity #3</p> <p>Activity: Using the first activity of setting a criteria or standards to obtain a license: Based upon the information reviewed and verified and the investigative findings, and taking into consideration the applicant’s prior activities, criminal record, if any, reputation, habits, associations, the applicant/licensee is Eligible or Not Eligible for a license.</p>
<p>Slide 18</p>		<p>KEY POINTS</p> <p>Before issuing a license to a primary management official or a key employee, a Tribe shall:</p> <ul style="list-style-type: none"> • Create and maintain an investigative report on each background investigation. An investigative report shall include all of the following: <ul style="list-style-type: none"> (i) Steps taken in conducting a background investigation; (ii) Results obtained; (iii) Conclusions reached; and (iv) The basis for those conclusions.

Background Investigations: Eligibility Determination for Nuanced Standards Participant Guide

<p>Slide 19</p>		<p>KEY POINTS</p> <p>If you have any questions or would like information about additional topics and training please contact the NIGC training department at traininginfo@nigc.gov.</p>
-----------------	---	---



Course: Background Investigations: Eligibility Determination for Nuanced Standards

Activity 1: Disqualifying Standards for PMO/KEY/Non-Key licensee

Directions: Working as a group, determine and develop a list of Prior activities, Crime(s), Reputation, Habits, or Associations, that would disqualify an applicant from being licensed.

Example: Multiple assault convictions



Activity: Eligibility Determination (25 C.F.R. 558.3)

Using the first activity of setting a criteria or standards to obtain a license: Based upon the information reviewed and verified and the investigative findings, and taking into consideration the applicant's prior activities, criminal record, if any, reputation, habits, associations, the applicant/licensee is ELIGIBLE or NOT ELIGIBLE for a license:

Scenario #1	Eligible	Not Eligible
Background investigator provided TGRA with social media images of applicant hanging out with known gang members		
A review of the applicants RAP sheet indicated 10 charges in the past 8 years for theft or writing of worthless checks but all charges were dismissed		
Work and residence history shows nothing negative		

Scenario #2	Eligible	Not Eligible
Routine search of social media found images from the The Blue Knights motor cycle club. Additionally active in toys for tots program, big brother and sisters.		
A review of the applicants' RAP sheet indicated 1 charge 23 years for grand theft, deferred charge.		
Work and residence history shows nothing negative		

Scenario #3	Eligible	Not Eligible
Background investigator documented from social media, images of applicant hanging out with known drug dealers whom are relatives		



A review of the applicants' RAP sheet indicated 2 charges in the past 10 years for misdemeanor theft.		
Review of work history shows 7 jobs with 3 non-responsive contacts 4 responsive noting they would not hire them back		

Scenario #4	Eligible	Not Eligible
Background investigator provided information that the individual in question is associated with the South West Easterly 102 nd St Crips.		
A review of the applicants RAP sheet indicated no criminal charges		
Review of work and residence history shows no negative results		

For licensing actions including revocation, denial, suspensions, do you have an appeal process in place?





NIGC National Training Conference Evaluation

Course Name: Background Investigations: Eligibility Determination for Nuanced Standards

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.



Lined writing area consisting of 26 horizontal black lines.

Emergency Preparedness Roundtable Participant Guide

National Indian Gaming Commission



Emergency Preparedness Roundtable

Industry Integrity

Agency Accountability

Preparedness

Outreach



NIGC National Training Conference Evaluation
Course Name: Emergency Preparedness Roundtable

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Introduction to Emergency Preparedness Planning Participant Guide

National Indian Gaming Commission



Introduction to Emergency Preparedness Planning

Industry Integrity

Agency Accountability

Preparedness

Outreach



NIGC National Training Conference Evaluation
Course Name: Introduction to Emergency Preparedness Planning

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Table Top Exercise Participant Guide

National Indian Gaming Commission



Emergency Preparedness: Table Top Exercise

Industry Integrity

Agency Accountability

Preparedness

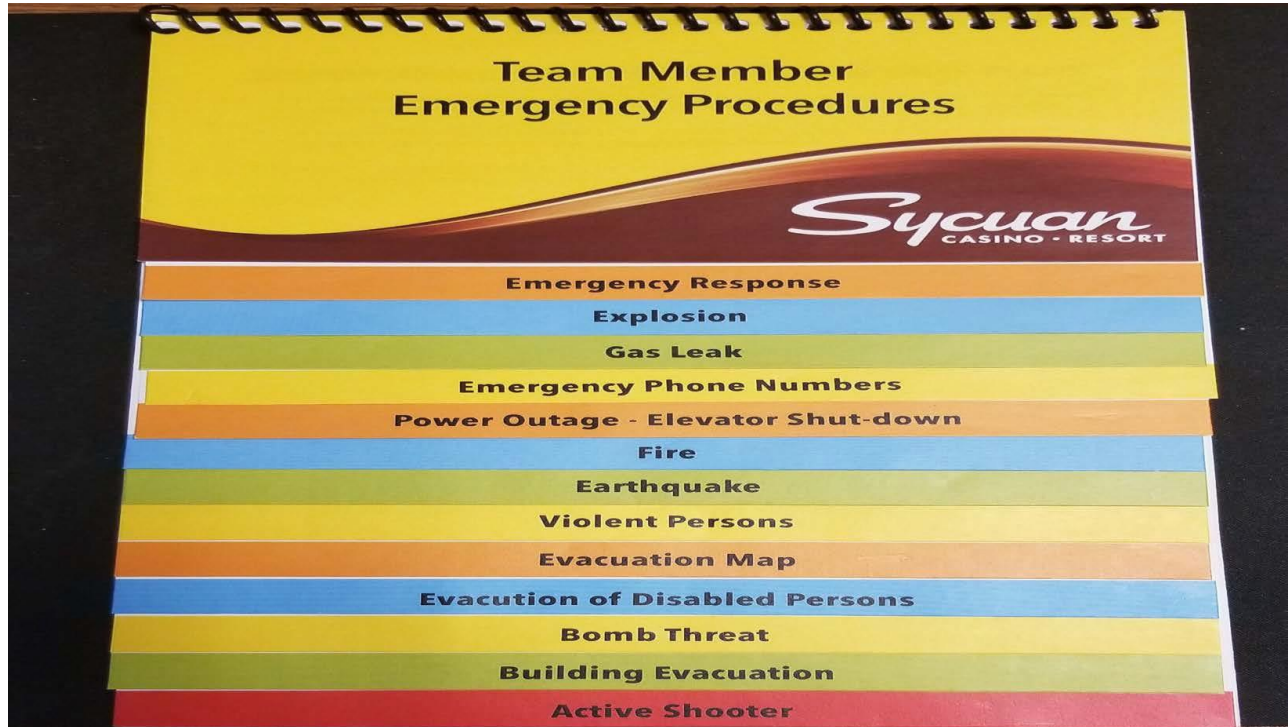
Outreach

NIGC Wildfire Exercise



VIEJAS
BAND OF KUMEYAY INDIANS





Example Emergency Flip Chart



Example Emergency App

NIGC Wildfire Scenario

BREAKOUT EXERCISE

Wildfire Worksheet:

1. Who will take immediate responsibility to make the command decisions and list the command structure?
2. List the other primary contacts that will be involve in any decision making?
3. What are the immediate priorities based on the current situation?
4. What is the status of the initial casino injects?
5. Based on the current wildfire situation. What are the contingency plans for the scheduled concert and fireworks display?

Develop the contingency plans to guide the response for the continuing wildfire disaster.

- How should an evacuation be coordinated?
- How would a shelter in place be implemented?

Disaster Management Resources

Federal Emergency Management Assistance grant program

This grant program provides funding to Indian tribes to strengthen tribes' capacity to prepare for and respond to emergency situations. Additional FEMA grant programs are also available to tribal governments.

Tribal Funding, Mitigation, and Planning Resources:

<https://www.fema.gov/about/organization/tribes/funding-mitigation-planning-resources>

External Resources

- FEMA Tribal Affairs
- FEMA Tribal Liaisons
- FEMA and Tribal Nations: A Pocket Guide
- National Recovery Framework Tribal Relations Support Annex
- Indian Health Service
- Indian Reservations in the Continental United States
- Native American Consultation Database
- Bureau of Indian Affairs- Emergency Management Division
- U.S. Census Bureau – American Indian and Alaska Native Resources

Suggested Training

Tribal Curriculum Resident Courses

- FEMA IS-650.A: Building Partnerships with Tribal Governments (online) This training provides an understanding, appreciation, and respect for tribal cultures so that effective relationships can be formed and evolve.

American Red Cross

www.redcross.org/contact-us.html

www.redcross.org/get-help/how-to-prepare-for-emergencies.html

www.redcross.org/get-help/disaster-relief-and-recovery-services.html



NIGC National Training Conference Evaluation
Course Name: Emergency Preparedness - Table Top Exercise

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

Panel Discussion with Federal Agencies/OSHA and Indian Health Services (IHS) Participant Guide

National Indian Gaming Commission



Panel Discussion with Federal Agencies/OSHA and Indian Health Services (IHS)

Industry Integrity

Agency Accountability

Preparedness

Outreach



NIGC National Training Conference Evaluation

Course Name: Panel Discussion with Federal Agencies: OSHA and Indian Health Services (IHS)

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.



A series of 25 horizontal lines spanning the width of the page, providing a template for writing.

Security Threat Assessments Participant Guide

National Indian Gaming Commission



Security Threat Assessments

Industry Integrity

Agency Accountability

Preparedness

Outreach



NIGC National Training Conference Evaluation
Course Name: Security Threat Assessments

NIGC greatly appreciates your feedback to aid in our Training offerings.

<i>When filling out the evaluation, please use the ranking scale of 1-5 as noted.</i>	1 Extremely Dissatisfied	2 Dissatisfied	3 Neutral	4 Satisfied	5 Extremely Satisfied
Did the training meet your expectations?					
Presentation materials were useful/effective. (i.e., PowerPoint, videos, handouts, etc.)					
Presentations and materials are clear.					
Overall I would rate the presentations:					
Was the presenter(s) knowledgeable in the subject matter?					
Overall, I would rate the presenter(s):					

Please provide additional details relevant to your scores above.

How do you feel NIGC can improve for future trainings?

Please list any recommendations for future training topics.

