National Indian Gaming Commission

Division of Technology

FY 2020- Workbook

NATIONAL INDIAN GAMING COMMISSION

Division of Technology

Day 3: IT Conference Agenda

9:00 am to 10:20 am	Mobile Gaming & Auditing IT Systems
10:30 am to 12:00 pm	Fundamentals of IT Regs & Gaming Technology
12:00 pm to 1:00 pm	Lunch (on your own)
1:00 pm to 1:50 pm	Commission Preparation for GM Certification and Approval
2:00 pm to 4:00 pm	IT Threats Going into 2020

Information is downloadable from the nigc.gov website.

If you have any questions or concerns please email TRAININGINFO@NIGC.GOV.

Impact of Mobile Gaming

Division of Technology

Objectives:

- Types of Mobile Gaming Technology
- Basics of How Each Operates
- Considerations
  - Operational
  - Security
  - Regulatory
  - Alternate Technical Standards
- Auditing and Regulatory Tips and Practices

Use of Technological Aids:

547.1

Permits the use of Technologic Aids with the play of Class II Games

Casino Owned Device

- Safer Connection to Network
- Impractical

Notes:

Casino & Vendor Applications

- Casino Branded Application
- Promotional Marketing Apps
- Social Media Based Gaming

Notes:

Online Gaming

- Overseas
- Device as a user interface
- Uncommon in US
- Regulatory Hurdles
- Due Diligence

Notes:

Sports and Event Betting:

Various areas to consider when thinking about Sports Betting.

- Mainstream and traditional sports betting ____

  ____
- Fantasy sports betting____

  ____

- ESports betting____

  ____

- Non-sport related betting____

  ____

- Parlay bets____

  ____

- In-game and in-play bets____

  ____

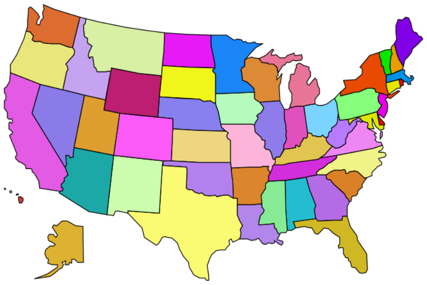
- Mobile betting____

  ____

- CFR 502.4(c)____

  ____

*Sports betting is listed in NIGC's regulations as Class III gaming, 25 CFR § 502.4(c)



Geofencing

What is it?

Types:

- Wi-Fi within a property
- GPS within a boundary
- Casino vs. BYOD

Resources:
547.15(b), 543.20(e)
GLI-33
NIST800-124r1

Issues:

- Inexperienced Developers____

  ____
- Mentioned the importance of strong experienced developers because most vendors don’t do this in house, and GLI / BMM can’t test that extensively. ____________________

  ____
- Design Flaw vs Feature?____

  ____
- Authentication issues____

  ____
- Link from one device to another (Safety? Responsibility? ____________________________

  ____
- Link to casino networks (SQL injection, Man in the middle attacks)____________________

  ____
- IP spoofing via VPNs a danger____

  ____
- GPS spoofing apps a danger____

  ____

Gaming with Cellular Phones:

Considerations:

Proper Configuration

*Fill in the blank from PowerPoint. All content is downloadable from www.nigc.gov

Resources:
547.15(b)
GLI-33
NIST800-124r1

Mobile Voucher:

Considerations:

New Vendors

Alternative Technical Standards:

More details are located at:

https://www.nigc.gov/news/detail/nigc-and-agua-caliente-band-of-cahuilla-indians-announce-approval-of-al

https://www.nigc.gov/general-counsel/alternate-technical-standards

Example of standards:

Before: 547.2 “Not limited to terminals, player stations, handhelds, fixed units, etc.”
After: Alternative Standard “not limited to terminals, player stations, handhelds such as Class II mobile devices, fixed units, etc.”

Notes:

547.2 -

“Not limited to terminals, player stations, handhelds, fixed units, etc.”

↓

Alternative Standard -

“Not limited to terminals, player stations, handhelds such as Class II mobile devices, fixed units, etc.”

Tips for Auditing

- Think Network Diagrams, what other systems and applications will this interact with?

  ____
  ____
  ____

- How does this (possibly new) technology work?

  ____
  ____
  ____

- Who has access?
- 543.20(f) User Controls
- RBAC- Role Based Access Control
- INCITS 359-2012- NIST access control standards
- How is access logged?

  ____
  ____
  ____

- How is access reviewed?

  ____
  ____
  ____

  - What procedures are in place to log and review access?

Questions? Email traininginfo@nigc.gov

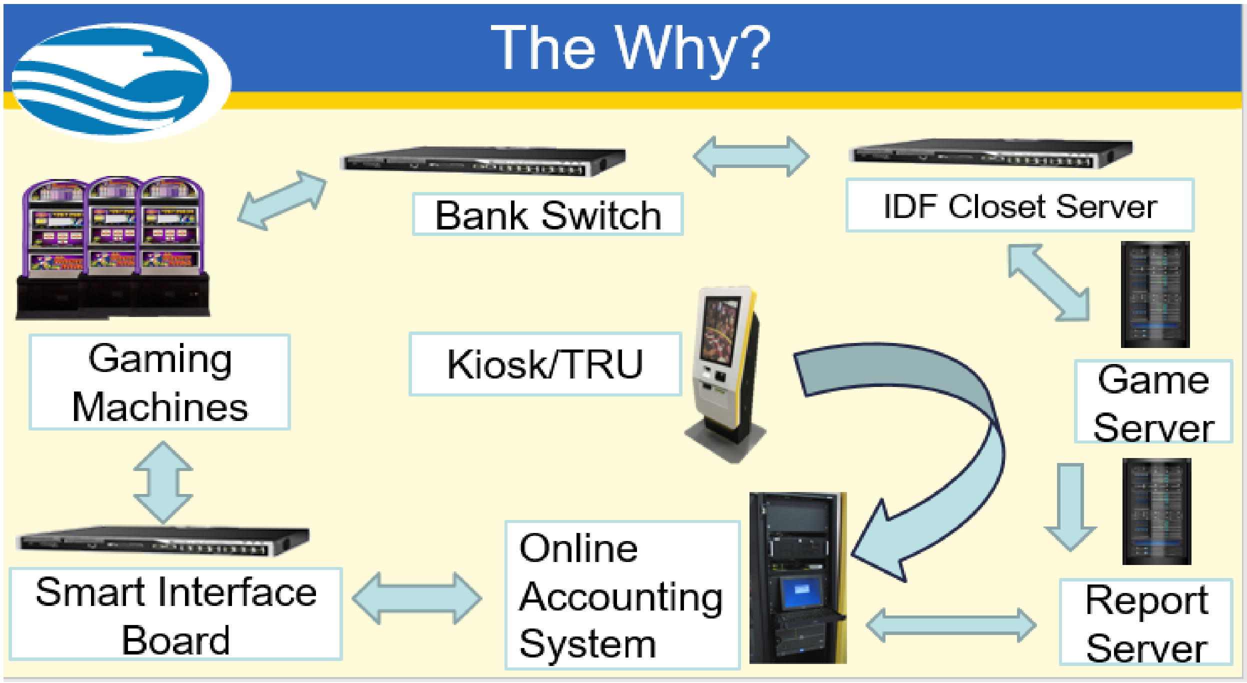
Fundamentals of IT Regulation and Gaming Technology

Division of Technology

NIGC.GOV - TRAININGINFO@NIGC.GOV

Objectives:

- **Regulations: The Why?**
    - Class II and III Networks
    - Typical Government Regulations
    - Insider Threat %'s
- **Industry IT Standards to NIGC Regulations**
    - Map IT Exercise
- **NIGC IT AUP Information**
    - ITVA Vulnerability Assessment
    - Common ITVA Concerns



The Why?

Bank Switch

IDF Closet Server

Gaming Machines

Kiosk/TRU

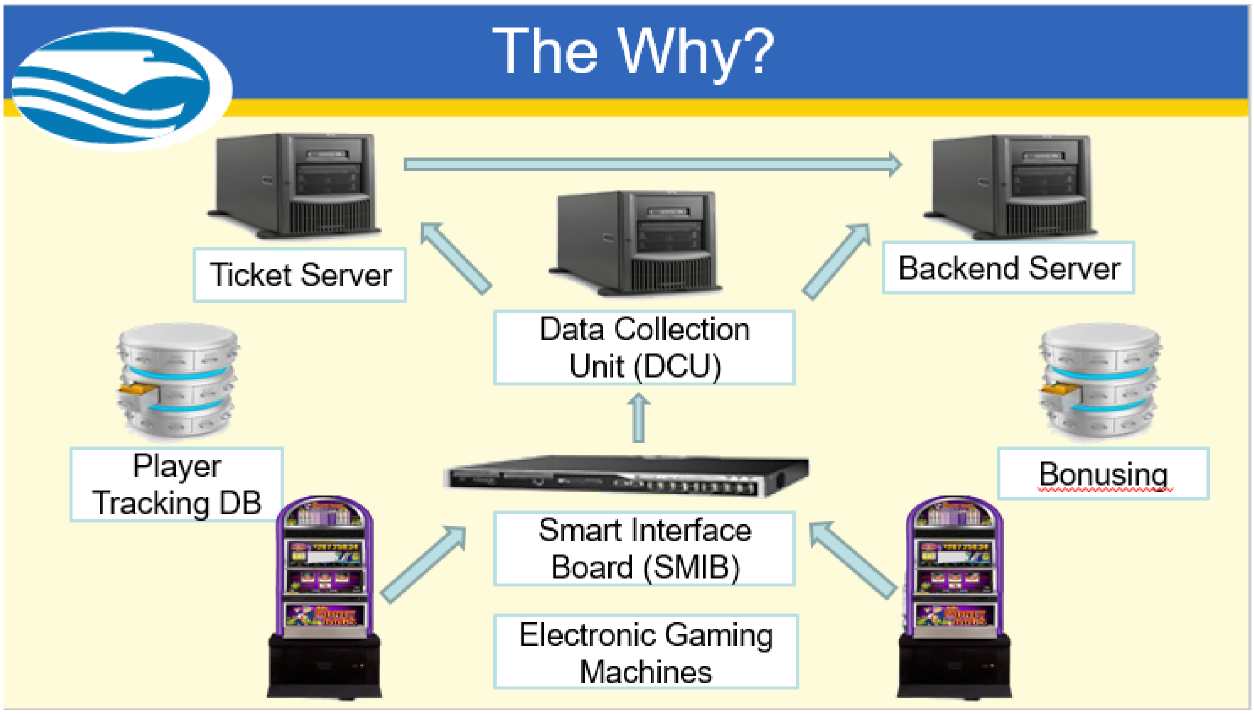
Game Server

Smart Interface Board

Online Accounting System

Report Server

- Is this a Class II or Class III Network Diagram?_______________________________________
- Is the Electronic Player Interface (EPI) receiving game determinations from the server to which it is attached? ____
- Do a minimum of two players need to be present to initiate game play?__________________
- Is the math model of the Class II game derived from a bingo ball draw? _________________
- If the EPI is disconnected from the server can I still play the game? ___________________



The Why?

Ticket Server
Backend Server
Data Collection Unit (DCU)
Player Tracking DB
Bonusing
Smart Interface Board (SMIB)
Electronic Gaming Machines

- Is this a Class II or Class III Network Diagram? ____
- Where does the technology reside? ____
- Is the Electronic Player Interface (EPI) receiving game determinations from the server to which it is attached? ____
- Do a minimum of two players need to be present to initiate game play? ______________
- Is the math model of the Class II game derived from a bingo ball draw? ______________
- If the EPI is disconnected from the server can I still play the game? _________________

Notes:

What are industry **standards** and what are **regulations**?

Standards: ____

____

____

Regulations: ____

____

____

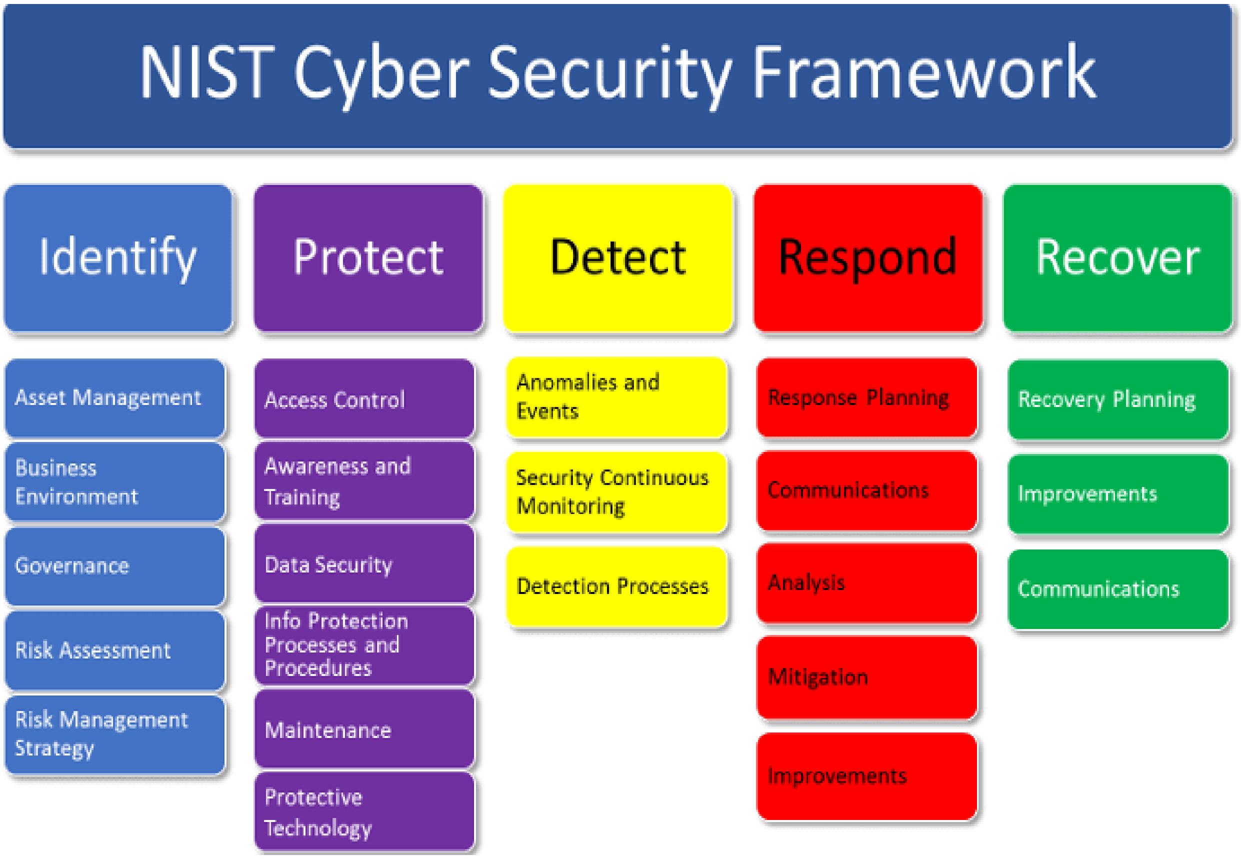
Typical Government Regulations

1. Food & Medicine – Created 1906 became Food and Drug Administration (FDA)
2. Communications – Federal Communications Commission (FCC) – What can and cannot be broadcast regulated by FCC including profanity, nudity and other objectionable content.
3. Trade – Federal Trade Commission (FTC) – Protect consumers from unfair practices & ensure competition is preserved.
4. Air & Water – Environmental Protection Agency (EPA) – regulating the safety of the air and public waterways.

Notes:

Inside Threats:

Additional information https://deloitte.wsj.com/cio/files/2016/04/2688954-Insider-Threat_4.pdf



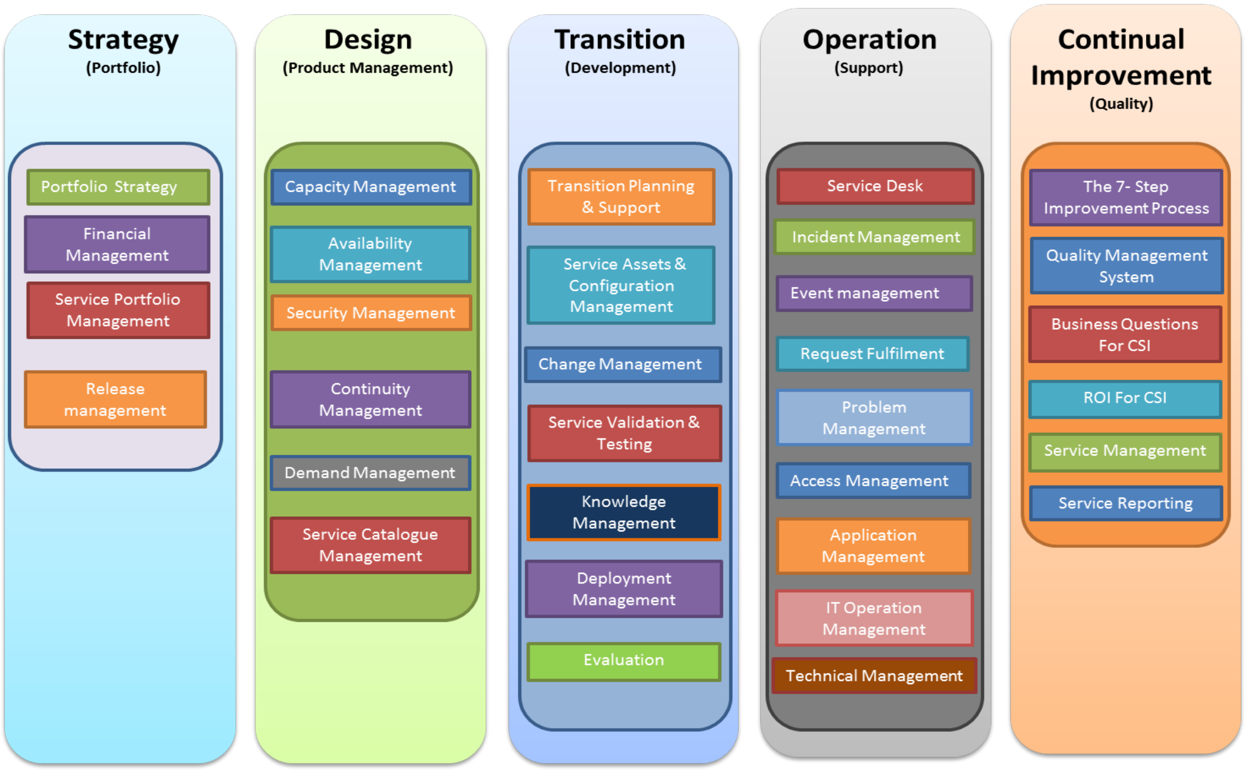
NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST – Physical sciences laboratory; its mission is to promote innovation and industrial competitiveness.

Resources: NIST Cyber Security Framework v1.1 < https://www.nist.gov/cyberframework >

Notes:



ITIL 4 – Framework designed to standardize the selection, planning, delivery and maintenance of IT services.

Resources: ITIL 4< https://www.axelos.com/best-practice-solutions/itil >

Additional standards: ISO 20000-1< https://www.iso.org/standard/51986.html >

ISACA / COBIT 2019 <http://www.isaca.org/COBIT/pages/default.aspx >

Notes:

Data Backups	
User Controls	
Supervision	
Incident Monitoring	
Logical Security	

IT Agreed Upon Procedures:

Notes:

Most Common finding #1:

User Controls f(5) - Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.

- Maintain updated Policy and Procedures on the who, what, when and where when dealing with access lists.
- **Testing: 1.** Review TICS, SICS, P&Ps and Employee Manuals for employee, IT Management and Human Resources action when compromised credentials are reported. **2.** Review user access lists for former employees

Most Common Finding #2:

Class II gaming systems' logical and physical controls c(4)- Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate: Record keeping and audit processes;

- What to test to better understand the outcome
- **Testing:** Review SICS and audit results with findings from previous internal and external audits and also any records kept by the IT operation.

NIGC performs IT Network Assessments and based on information gathered these are general metrics kept for trending purposes.

It is important to have a vulnerability assessment performed of your operations network infrastructure.

Benefit is having knowledge of where possible pain points reside in the network.

Open Ports on the casino floor is one of the easiest ways to resolve. i.e. port blockers & port management.

Critical	High	Medium	Low
Remote Execution of Code	DOS - Denial of Service	Information Disclosure	Lower quality encryption

NIGC uses industry standard software to automate much of the process of finding vulnerabilities.

Tenable Nessus and **Metasploit** are two of the most well known utilities.

The respective software bases the severity of the vulnerabilities off published databases from:

- NIST (National Institute of Standards and Technology)
- CVSS (Common Vulnerability Scoring System)
- NVD (National Vulnerability Database)

See also:

<https://nvd.nist.gov/vulnmetrics/cvss/v2calculator?vector=AV:N/AC:L/Au:N/C:P/I:P/A:P >

A vulnerability assessment is the **process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems**, applications and network infrastructures and **providing the organization** doing the assessment **with the necessary knowledge, awareness and risk** background **to understand the threats** to its environment and react appropriately.

Notes:

Common items identified during an ITVA visit:

1. **Older Network Infrastructures** – allow for easier access into player tracking data or cyber attacks
2. **Windows XP/7/Old PC's** – End of Life PCs with no software support allowing for security concerns and accessibility by unwanted online attackers
3. **Missing Software Patches** – Updated software patches assist with keeping software up to date to not allow vulnerabilities identified by the software vendor
4. **Open Network Ports** – Unmanaged ports or just open ports with connectivity allow for persons to possibly jump onto a network and cause harm

Notes:

Commission Preparation for GM Certification and Approval

Division of Technology

NIGC.GOV - TRAININGINFO@NIGC.GOV

Objectives:

Game/System Certification Process____

Certification vs. Approval____

Game Testing on the Floor____

Onsite System Testing____

Certifying Class II vs. Class III____

Changes to Game and System Testing over the years____

Why is verification so important?
• It is important to verify the software and or game to insure that it meets all the regulations required in the specific jurisdiction, it also insures that the wrong software is not installed that may or may not have regulation issues.
• 542.12(g)(1) • 543.08(I)(ii)(4)(i-iv)
•
•
•
•
• There may be 2-3 or more iterations of a single piece of software from a single submission.

As complex as this process is, it is an important one to insure the regulator that the software is being addressed for regulatory issues as well as future updates as well.

- The system software consists of variety of controlled files found in system, these are usually executables (.exe) or .DLL file or any file that control the accounting or functions of the game or system.
- This is to make sure they comply with your jurisdictional standards
- Using the tools to create the original signature that is present on the Certification Letter from the ITL
- A signature is generated on-site where the game or system is in use.

Certification vs. Approval

The Independent Testing Lab (ITL) does not “approve” a game or a system. They simply testing the game or system to see that it meets the requirements for compliance in a requested jurisdiction. The ITL is simply a extension of the regulator body.

Onsite Floor and System Testing:

An online accounting system is software that will manage the accounting, marketing, promotions, ticketing, player databases, etc.

Notes:

Gaming Floor Audits:

-
-
-
-
-

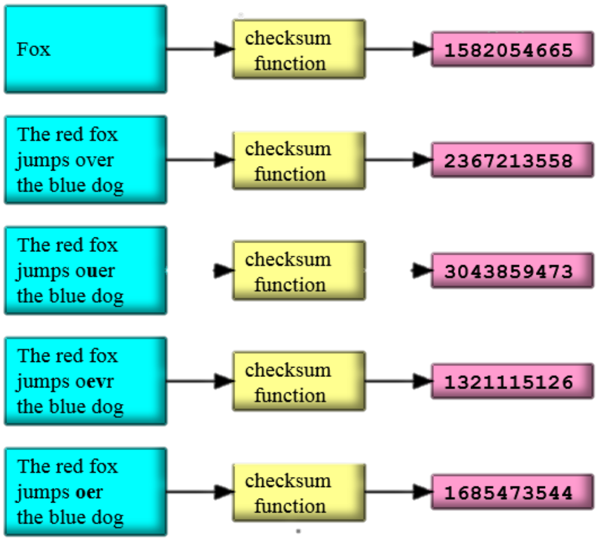
Floor audits are important in many ways. It helps insure that what was tested in the ITL is just what is being deployed on the floor.

Notes:

System Verification:

Each individual part in a gaming system is tested and assigned a signature. This signature will match the letter provided from the ITL in order to insure it is the same software tested in the lab as the software in the field.

- SHA-1
- SHA-256
- SHA-512
- MD5
- CRC-16 cyclic redundancy check
- CRC-32 cyclic redundancy check
- Checksum
- GAT


Fox
checksum function
1582054665
The red fox jumps over the blue dog
checksum function
2367213558
The red fox jumps ouer the blue dog
checksum function
3043859473
The red fox jumps oevr the blue dog
checksum function
1321115126
The red fox jumps oer the blue dog
checksum function
1685473544

*An electronic signature refers to data in electronic form, which is logically associated with the data. There are many signature types.

GAT

(Game Authentication Terminal)

GAT is a fairly new type of signature type that is embedded in the GSA protocol.

- As time and technology, moves forward the need to secure and verify software types have changed over the years this is an example of some older Signature tools.
- The industry has gone through many changes over the years from using EPROM, to hard drives to direct download. As the industry, moves forward, so does the verification tools used to verify the software this is just a sample of some of the tools used for verification.

Notes:

Questions? Email traininginfo@nigc.gov

IT Threats Going Into 2020

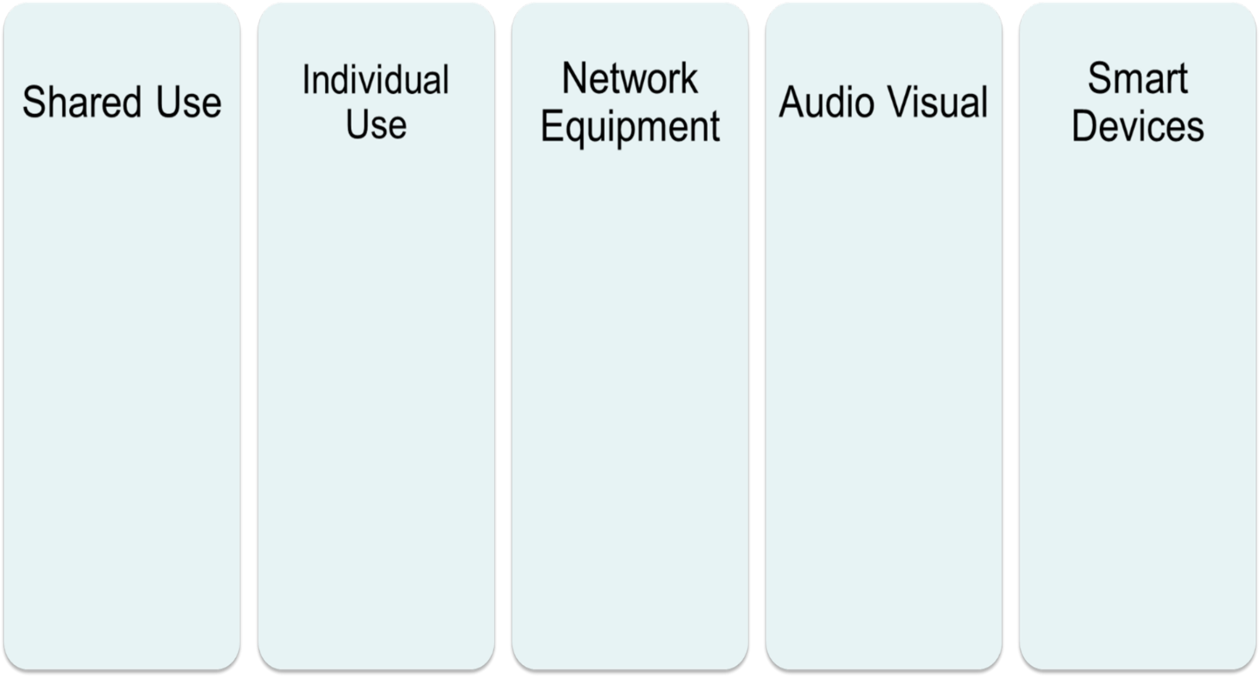
Division of Technology

NIGC.GOV - TRAININGINFO@NIGC.GOV

Objectives:

- Explain the scope of course and areas under threat
- Review new threats on the horizon
- Explore persistent and trending threats for 2020
- Define mitigation techniques

Notes:



Shared Use

Individual Use

Network Equipment

Audio Visual

Smart Devices

**All devices and Operating Systems are susceptible.

The rise of AI and automation as both a target of attacks and a tool for attacks.

The imminent release of 5G cellular networks and concerns over their safety and reliability.

Notes:

What is **Ransomware**?

____

____

____

Helpful link: https://www.rollcall.com/news/congress/cyber-hackers-lurking-longer-inside-computers-report-finds

Common causes for continued prevalence of Ransomware:

- Phishing/ Social engineering attacks: ____
- Weak User controls:____
- Lax Logical security controls:____
- Insufficient Data backup controls:____
- User education:____

Notes:

Social Engineering Targets

Many types of info can be used by attacker to facilitate an attack – the examples below are questions used in real-world hacking competitions. *Source Defcon/ Social-Engineer.org

Logistics
Is IT support handled in-house or outsourced?
Who do they use for delivering packages?
Do they have a cafeteria?
Who does the food service?
Other Technology
What is the name of the company VPN?
Do they block websites?
If website block = yes, which ones? (Facebook, eBay, etc
Is wireless in use onsite? (yes/no) If yes, what is the ESSID Name?
What make and model of computer do they use?
What anti-virus system is used?
Can Be Used for Onsite Pretext What is the name of the cleaning/janitorial service?
Who does their bug/pest extermination?
What is the name of the company responsible for the vending machines onsite?
Who handles their trash/dumpster disposal?
Name of their 3rd party security guard company or is it in-house?
What types of badges do they use for company access? (RFID, HID, None)
Company-Wide Technology
What operating system is in use?
What service pack/version?
What program do they use to open PDF documents and what version?
What browser do they use? What version?
What mail client is used?
Do they use disk encryption, if so what type
Fake URL (getting the target to go to a URL)
Employee-Specific Information
How long has the call recipient worked for the company?
What days of the month does the call recipient get paid?
Employee's schedule information (start/end times, breaks, lunches)
What is the name of the phone/PBX system?
When was the last time the call recipient had awareness training?

Notes:

Hacking is not limited to just breaking into a computer. VIA Social Engineering the process can be about:

Notes:

Ways to gather Open-Source Intel:

- Social Media____
- Job sites____
- Hacker sites____
- Dumpster diving____
- Red Team/ Pen Tests____

*Most sophisticated attacks and successful attacks involve planning and research.

Mitigated Risk:

Remember

543.20(g) Installations and Modifications

543.20(e) Logical Security

ITIL Change Management

Data Backups

- 543.20(j)
- Recovery procedures
- Tested Procedures

Incident Management

- 543.20(i)
- BCP (Backup Continuity Plan)

*To reduce the impact after an attack has already occurred and damage has been done, it is important to have strong controls regarding data backups and incident management.
Not just to have the controls, but to have documented the appropriate steps to take in the event of an attack.

For detailed steps and advice on formulating a Disaster Recovery Plan or Backup Continuity Plan see:
ITIL Continuity Management, also ISO 22301 and other industry standards.
Basic steps involve identifying critical areas, their Respective Responsible parties, and then documenting the recovery procedures.
Many of these policies and procedures may already be covered with 543.20(j)(3) in your annual testing of Data Backup procedures.

Know your assets	Know your people	Monitor activity	Apply analytics	Conduct forensic & Root Cause analysis
• 543.20(j)	• 543.20(a), (f)	• 543.20(i)	• 543.20(i)	• 543.20(e)

Tips:

Know your systems

Know your people and train them

- Have ways to monitor and catch suspicious activity
- Be on the lookout for patterns
- After the damage is done follow up and find the root cause

Notes:

Questions? –email traininginfo@nigc.gov

NATIONAL INDIAN GAMING COMMISSION

Jeran Cox

IT Auditor

jeran_cox@nigc.gov

Michael Curry

IT Auditor

michael_curry@nigc.gov

Sean Mason

IT Auditor

sean_mason@nigc.gov

Tim Cotton

IT Audit Manager

timothy_cotton@nigc.gov