Fundamentals of IT Regulation and Gaming Technology

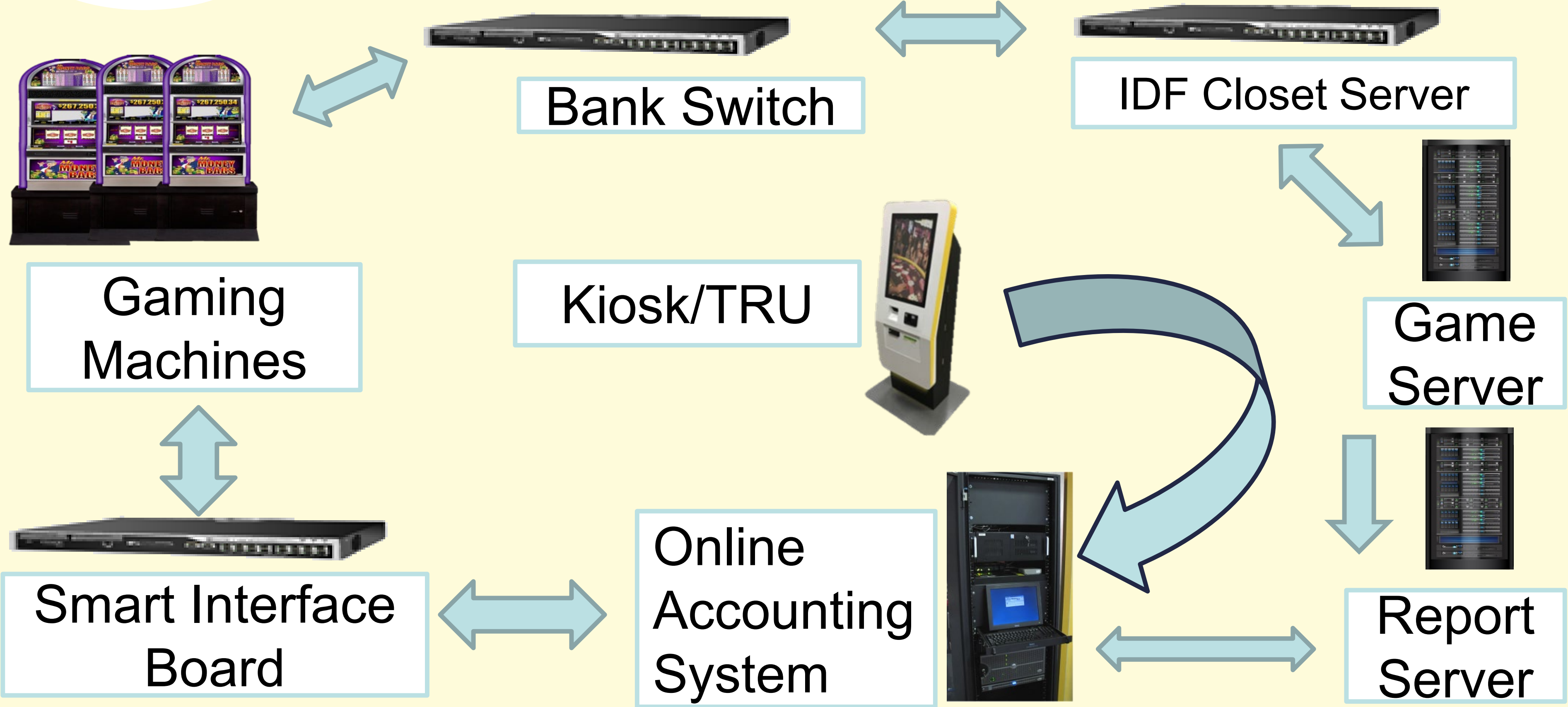
Division of Technology

NATIONAL INDIAN GAMING COMMISSION

Overview

- **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

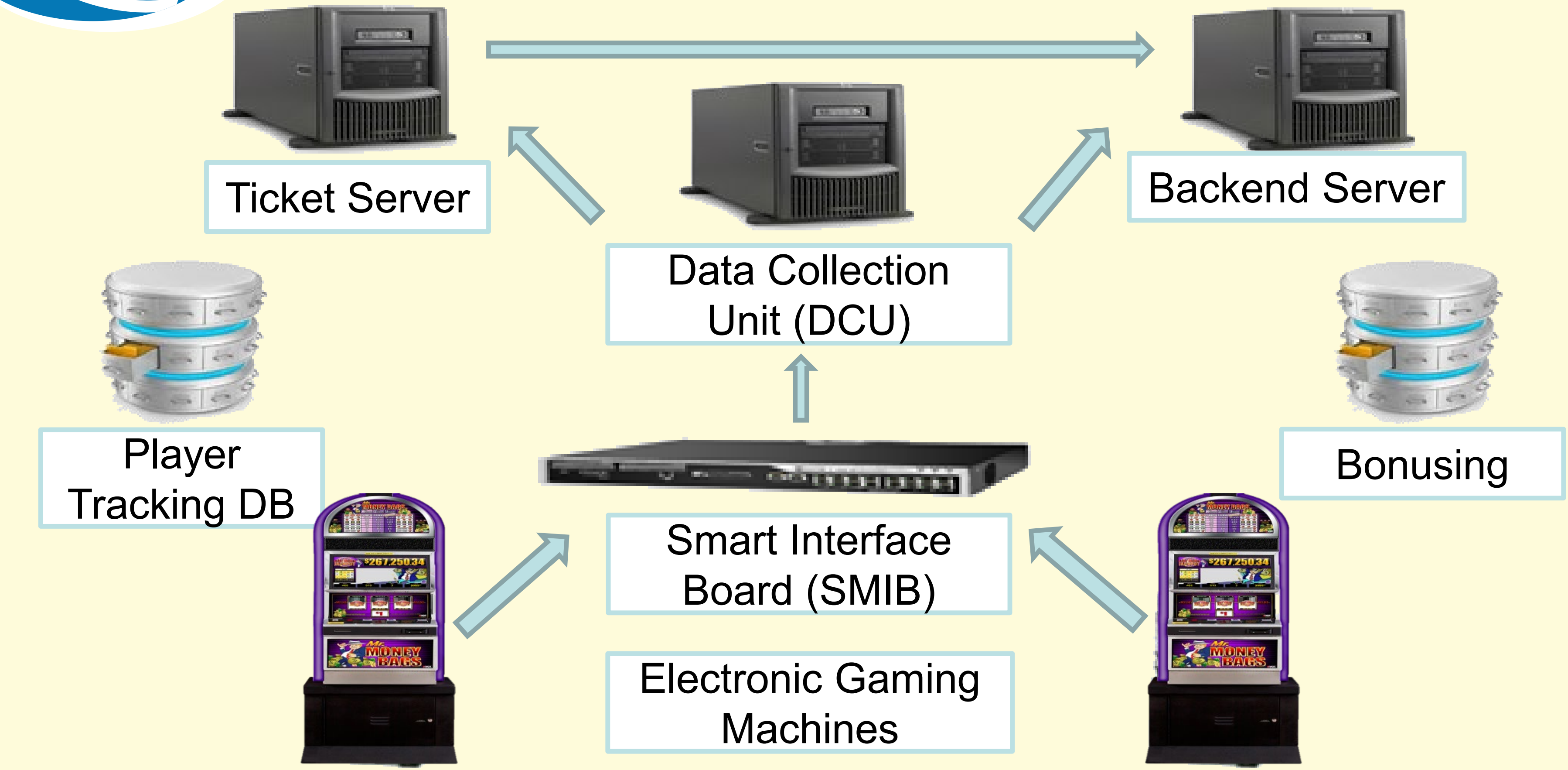
Game Server

Smart Interface Board

Online Accounting System

Report Server

The Why?


Ticket Server
Backend Server
Data Collection Unit (DCU)
Player Tracking DB
Bonusing
Smart Interface Board (SMIB)
Electronic Gaming Machines
$267,250.34
Mr. MONEY BAGS

The Why?

STANDARDS – refers to the principles behind work and values associated.

REGULATIONS – refers to the set of laws and rules that need to be followed while performing certain tasks.

Food & Medicine ☎

Communications

Trade

Air & Water

Typical Government Regulations

The Why? Insider Threats

59%

Of employees who leave voluntarily or involuntarily say they take sensitive data with them.

90%

Of IT employees indicate that if they lost their jobs, they'd take sensitive company data with them.

51%

Of employees involved in an insider threat incident had a history of violating IT security policies.

25%

Of employees have used email to exfiltrate sensitive data from an organization.

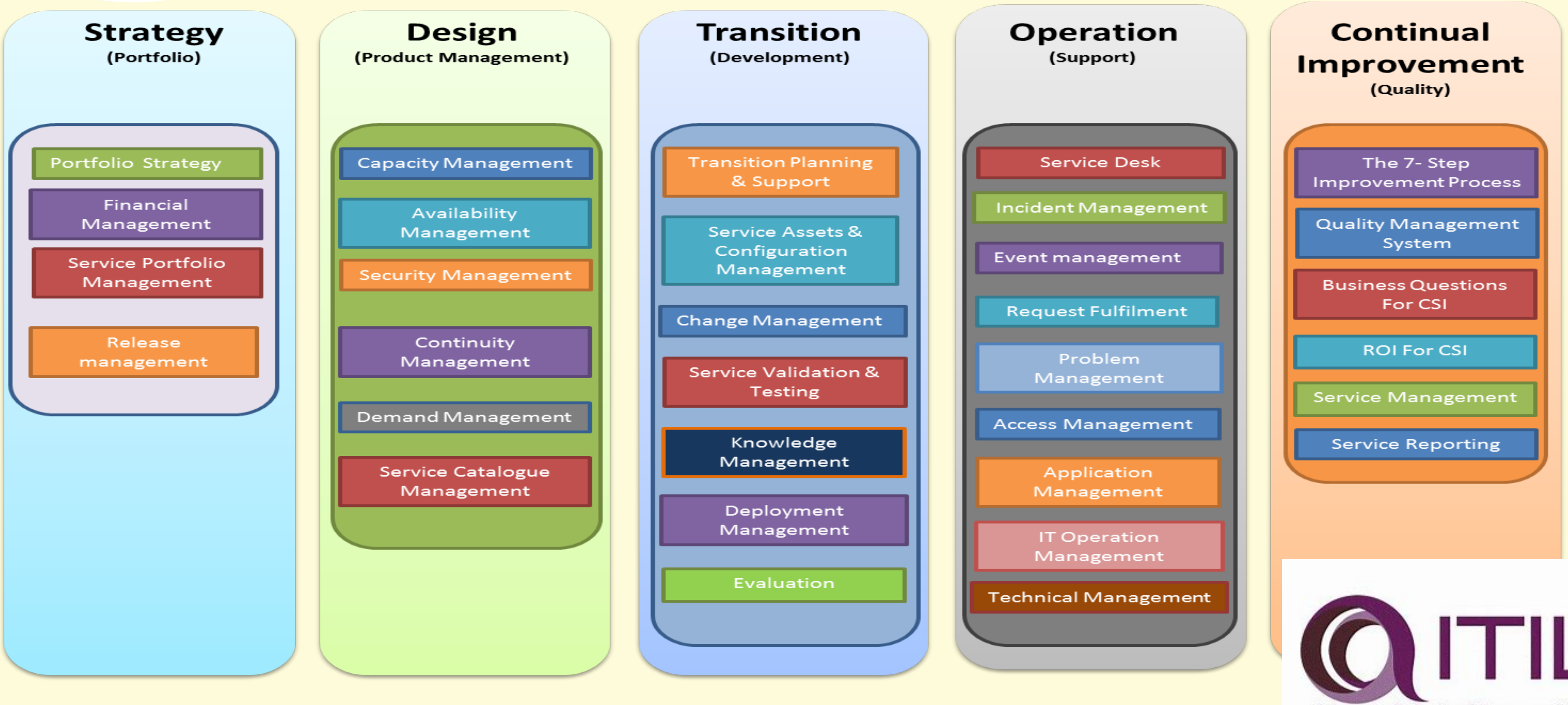
Source:Deloitte / WSJ

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
National Institute of Standards and Technology
U.S. Department of Commerce

IT Standards



Strategy
(Portfolio)

- Portfolio Strategy
- Financial Management
- Service Portfolio Management
- Release management

Design
(Product Management)

- Capacity Management
- Availability Management
- Security Management
- Continuity Management
- Demand Management
- Service Catalogue Management

Transition
(Development)

- Transition Planning & Support
- Service Assets & Configuration Management
- Change Management
- Service Validation & Testing
- Knowledge Management
- Deployment Management
- Evaluation

Operation
(Support)

- Service Desk
- Incident Management
- Event management
- Request Fulfilment
- Problem Management
- Access Management
- Application Management
- IT Operation Management
- Technical Management

Continual Improvement
(Quality)

- The 7- Step Improvement Process
- Quality Management System
- Business Questions For CSI
- ROI For CSI
- Service Management
- Service Reporting

ITIL®
Information Technology Infrastructure Library

NIGC MICS 543.20

Data Backups

Controls must include adequate backup, including, but not limited to, the following: Daily data backup of critical information technology systems

User Controls

Systems, including application software, must be secured with passwords or other means for authorizing access

Supervision

Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures

Incident Monitoring

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

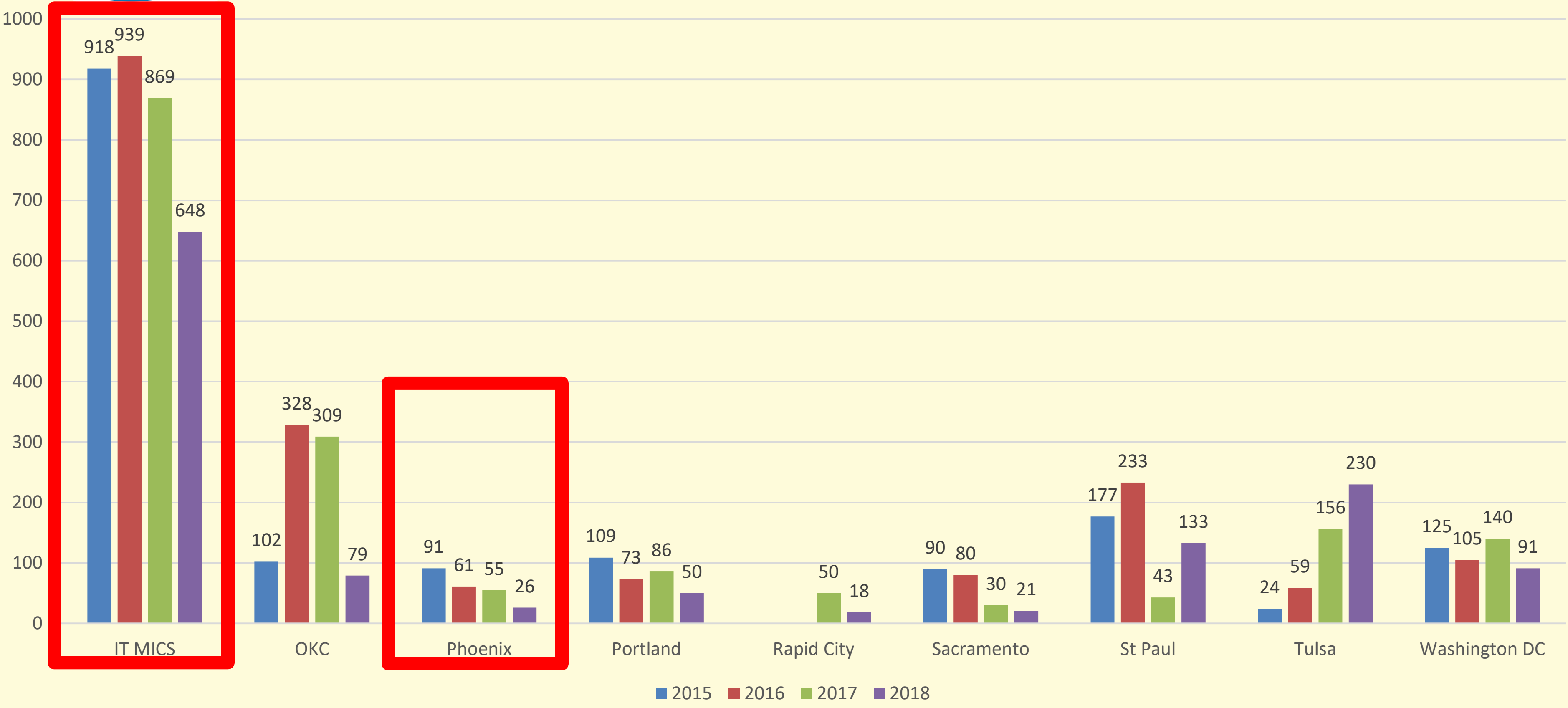
Logical Security

Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured

Map IT - NIST to 543.20

Supervision	User Controls	Logical Security	Incident Monitoring	Data Backups
Identify	Protect	Detect	Respond	Recover
Governance	Access Control	Security Monitoring	Response Planning	Recovery Planning

IT Agreed Upon Procedures



2018 AUP Common Finding #1

User Controls – f(5)

Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.

SAVE THE DATE

23
Findings

2018 AUP Common Finding #1

User Controls – f(5)

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

2018 AUP 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:

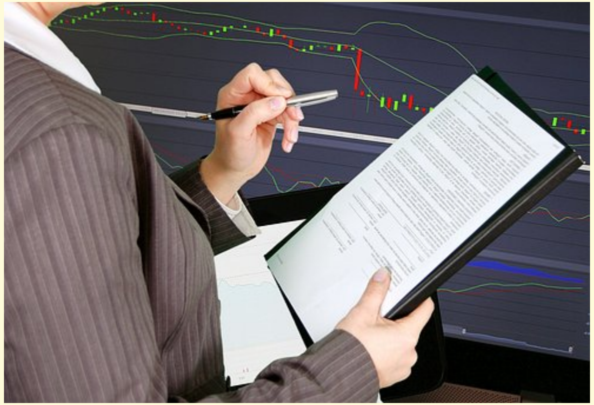
Record keeping and audit processes;

18 Findings

2018 AUP Common Finding #2

Class II gaming systems’ logical and physical controls c(4)

Testing: Review SICS and audit results with findings from previous internal and external audits and also any records kept by the IT operation.



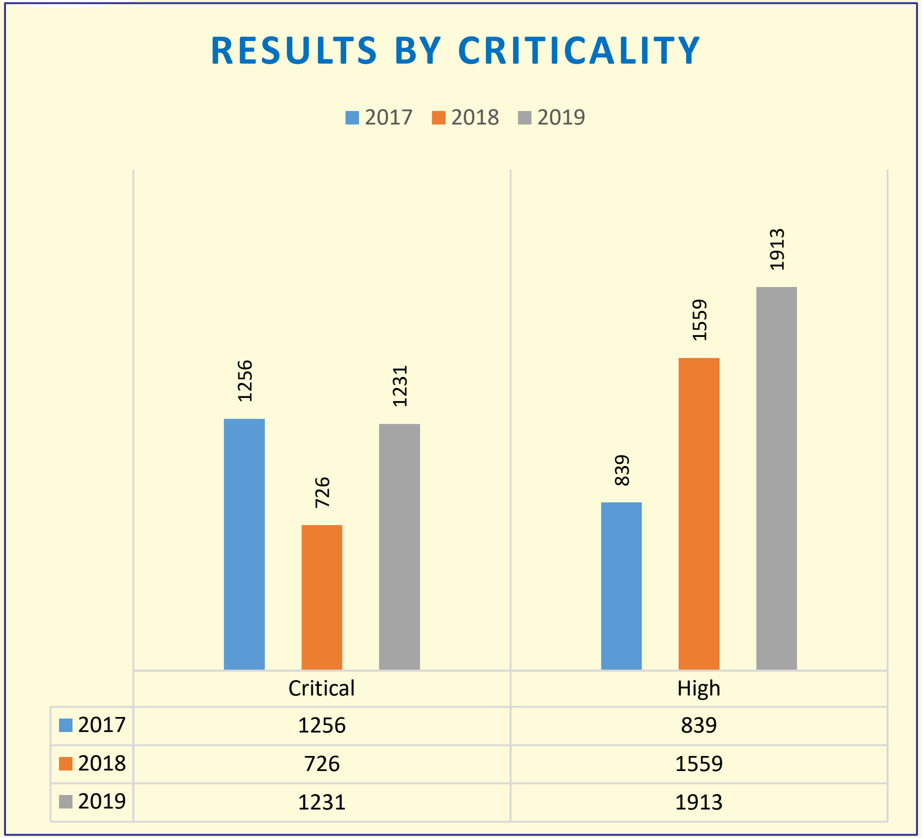
2018 AUP Honorable Mentions

Supervision a(1)

Class II gaming systems logical & physical controls c(1&5)

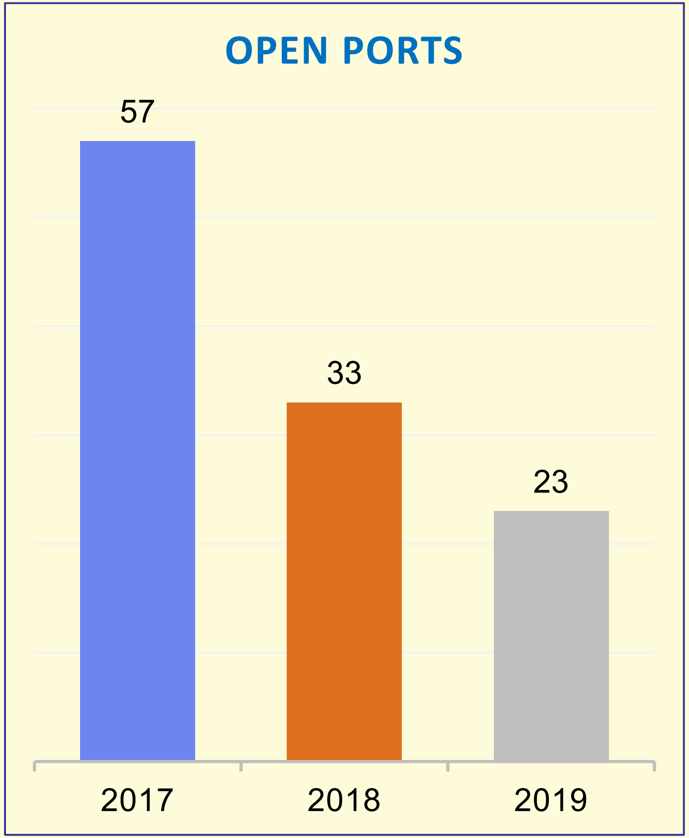
Data Backups j(3)

IT Vulnerability Assessment Metrics



RESULTS BY CRITICALITY

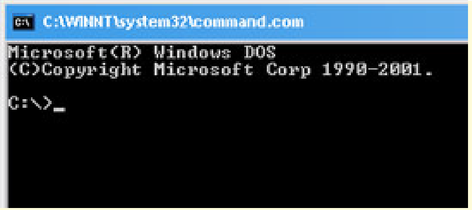
	Critical	High
🟦 2017	1256	839
🟧 2018	726	1559
⬜ 2019	1231	1913



OPEN PORTS

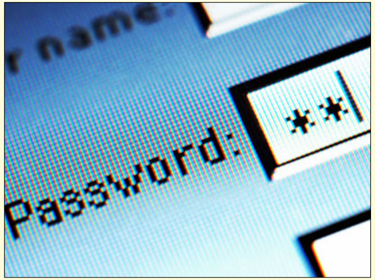
Vulnerability Scoring Calculator

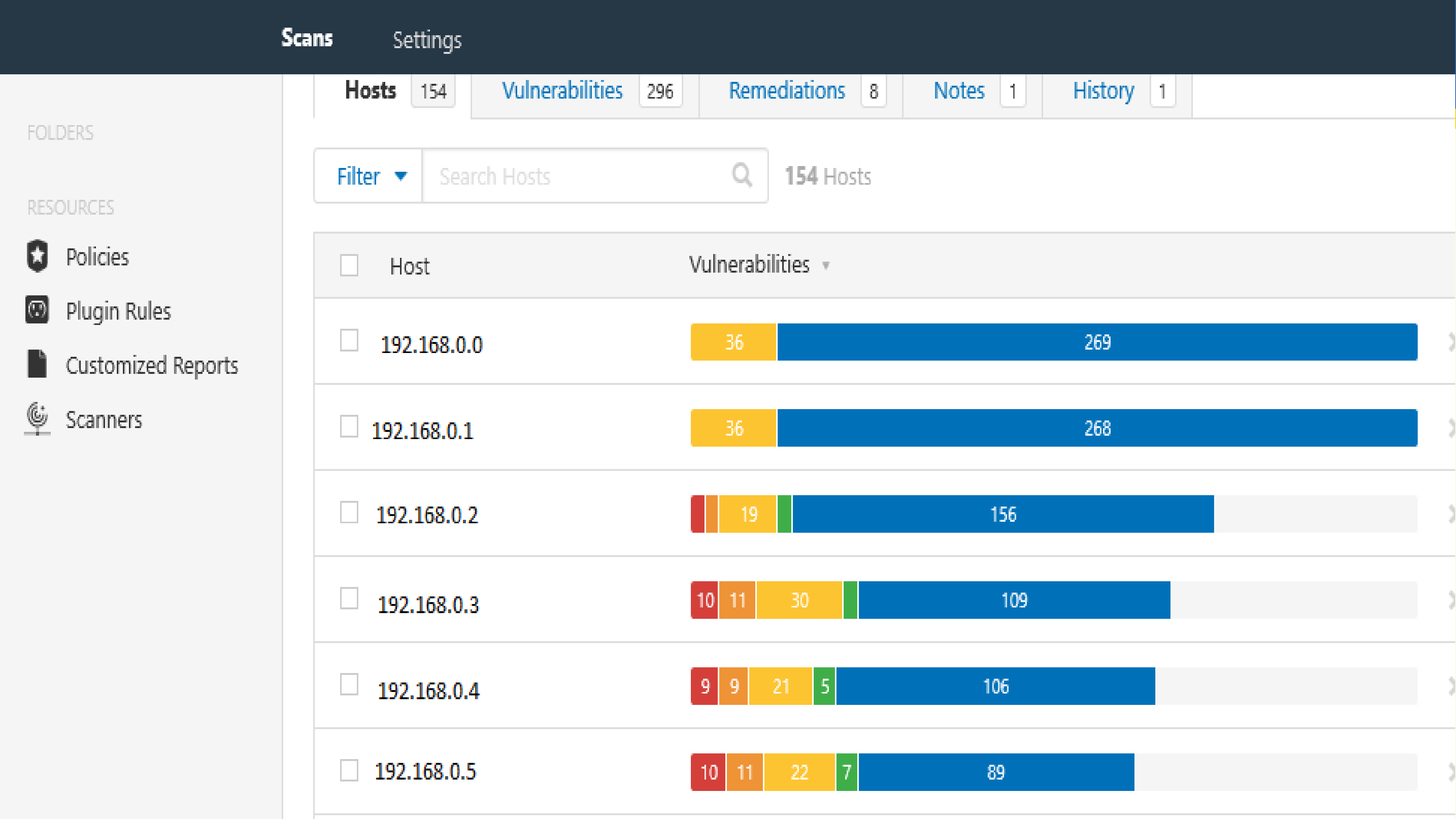
Critical	High	Medium	Low
Remote Execution of Code	DOS - Denial of Service	Information Disclosure	Lower quality encryption



```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\>_
```





□	Host	Vulnerabilities ▾
□	192.168.0.0	36 269
□	192.168.0.1	36 268
□	192.168.0.2	19 156
□	192.168.0.3	10 11 30 109
□	192.168.0.4	9 9 21 5 106
□	192.168.0.5	10 11 22 7 89

Common ITVA Concerns

Older Network Infrastructures

Windows XP/7/Old PC's

Missing Software Patches

Open Network Ports

Questions?

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