# Nevada Information Technology Advisory Board

Security Subcommittee Report

6/11/2012

# Agenda

- Objective
- Key Findings
- Strategy/ISMS
- Security Maturity
- Security Governance
- Risks

# Objective

- Identify high level IT Security opportunities for the State of Nevada IT organization
- Research sources:
  - IGT
  - Gartner research organization
  - NIST
- Present findings and recommendations

# IT Security Committee

- Key Findings
  - Where to start:
    - Don’t start in the middle
    - Step #1 Create IT Strategy and/or ISMS (Information Management Security System) via adopted framework
      - ISO 27001 and 27002
      - NIST
      - COBIT
      - Other
    - IT Security Strategy may include the following disciplines:
      - Security Governance
      - Planning & Budgeting
      - Organization
      - Controls framework
      - Architecture & Engineering
      - Operations and Process
      - Communications, Education, and Awareness
      - Event detection and response (Advanced “Situational Awareness”)
      - Threat and vulnerability management
      - Risk and controls assessment

# IT Security Committee

- ISMS may include:
  - Security Policy
  - Security Management Plan (Scope, Perimeter, Gateways, Application, Data level, Desktop, etc.)
  - Asset Management
  - Physical Security (Perimeter Security)
  - Operations Management (Patch Management, constant monitoring)
  - Proactive Vulnerability Management (Ethical hacks, Data loss prevention tools, etc.)
  - Access Management
  - Incident Management
  - Business Continuity and Disaster Recovery
  - Compliance Management

# IT Security Committee

- Step #2 Conduct “current state” assessment of IT Security maturity level
  - In house or
  - Commission independent assessment/audit
    - Assess current state
    - Identify gaps
    - Set maturity targets
    - Plan improvements
    - Continuously improve the ISMS
  - Define desired maturity level (Gartner/NIST 1 – 6)
  - Define timeline to reach maturity levels
    - Example: level 2 in 2 years, level 4 in 4 years, etc.

# IT Security Committee

- Step #3 Create IT Security Governance Committee
  - Business Unit Owners
  - IT Security responsible for researching, assessing, and articulating solution risk levels to the ISGC
    - Present mitigating options
  - ISGC Accepts or rejects risk

# IT Security Committee

- Risks
  - Must have commitment from line-of-business owners and Executives (In this case Governor)