# Improve your State Revenue Agencies IT Security Posture

FTA Technology
July 31, 2013
Presented by Tim Blevins

CGI

Experience the commitment®

# IT Security Overview

- How do we think about IT Security?
  - What are IT Security Standards?
- Security Policies and Procedures
- What does a Security Control Group Look Like
- How do we access the Security Control
- Automated tools to continually test and access
- Improving IT Security in your operations?

**Please Ask Questions Along the Way**

# Question to Ask Yourselves ?

How do you plan to address the growing regulatory requirements?

You audit the books why don’t you audit the networks?

Do you have a clear picture of the risks you are exposed to?

Are you confident you have the protection you need from your offshoring, outsourcing or shared services provider?

Are you sure the cost of your security matches your business needs?

Have you bench marked your security posture?

Are you confident that your digital services are protected from external threats?

# Latest market trends in cyber security

**What do we mean by cyber security? : Technology, services and policies that protect public sector and commercial organizations from the risk of electronic attacks in order to minimize business disruption and data loss.**

## The more connected the more vulnerable

- Homes, industrial control systems, remote workers, critical infrastructure
- Purchasing Technology can create new vulnerabilities

## New IT sourcing models are being implemented

- Large scale public cloud computing
- Connectivity to clients, vendors, employees seen as key

## Heightened awareness and complexity surrounding personal information

- Significant increase in use of personal information
- Clients and citizen need to trust businesses and governments to keep their personal data secure

## Threat landscape is changing

- Professionalism of cyber crime industry
- Motivation of threat actors very broad: financial, activism, state sponsored

# SANS Top 20 Security Critical Security Controls

**Description of Controls**

**Critical Control 1: Inventory of Authorized and Unauthorized Devices**

**Critical Control 2: Inventory of Authorized and Unauthorized Software**

**Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**

**Critical Control 4: Continuous Vulnerability Assessment and Remediation**

**Critical Control 5: Malware Defenses**

**Critical Control 6: Application Software Security**

**Critical Control 7: Wireless Device Control**

**Critical Control 8: Data Recovery Capability**

**Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps**

**Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**

Source : SANS Institute

# SANS Top 20 Security Critical Security Controls

**Description of Controls**

**Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services**

**Critical Control 12: Controlled Use of Administrative Privileges**

**Critical Control 13: Boundary Defense**

**Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs**

**Critical Control 15: Controlled Access Based on the Need to Know**

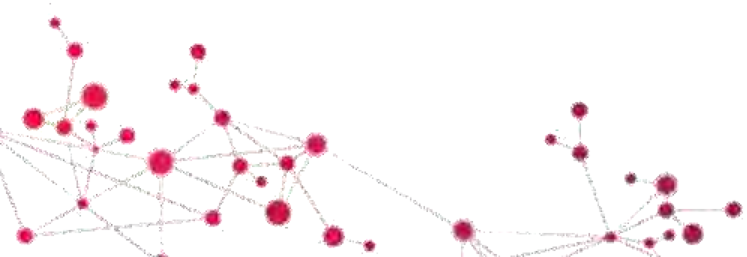
**Critical Control 16: Account Monitoring and Control**

**Critical Control 17: Data Loss Prevention**

**Critical Control 18: Incident Response and Management**

**Critical Control 19: Secure Network Engineering**

**Critical Control 20: Penetration Tests and Red Team Exercises**



Source : SANS Institute

# It’s all about risk management

## Clients are keen to understand the risk to their organization:

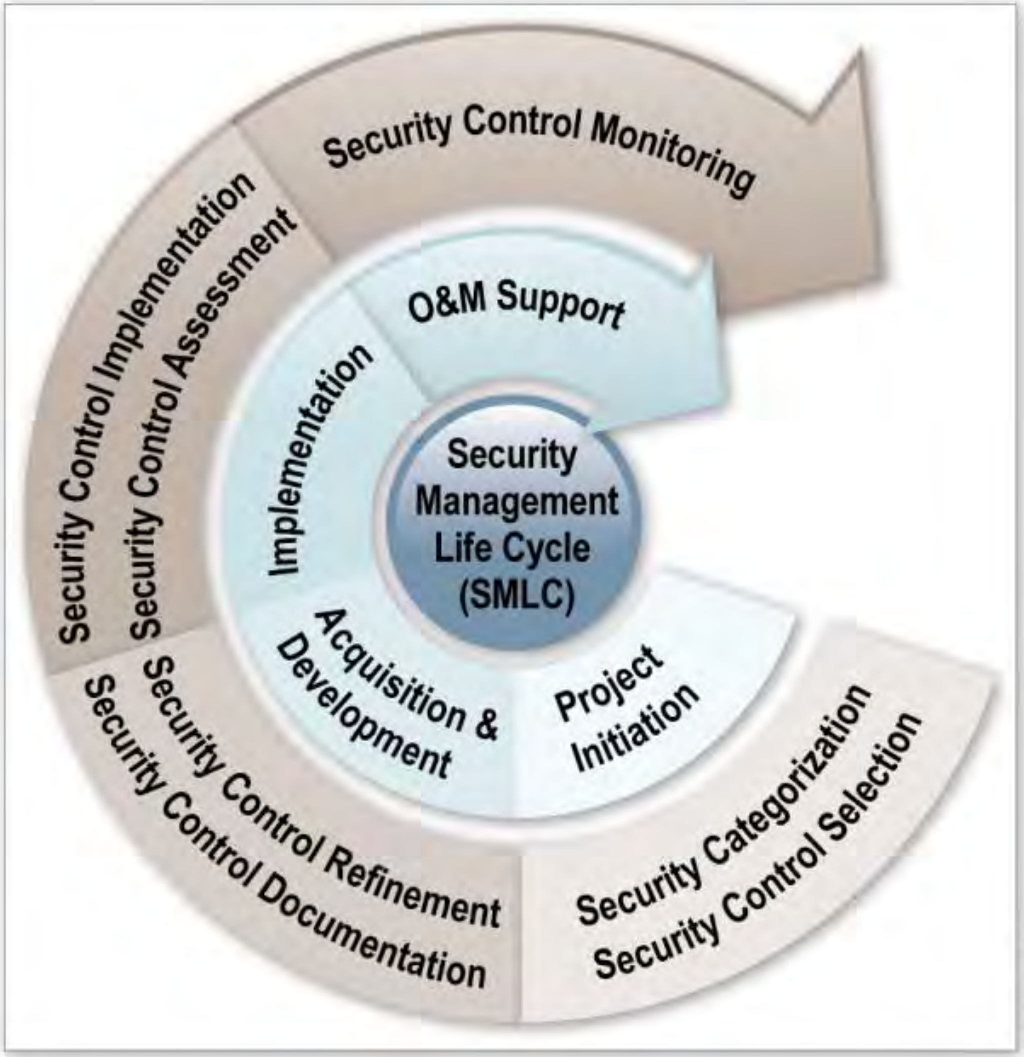
- Strategic Risk
- Financial Risk
- Reputational Risk
- IP Risk
- Identity breach Risk
- Regulatory Risk (SOX, Privacy Regs etc.)
- Corporate Liability
- Availability Risk
- Hostile geo-political Risk

**I need to understand the possible risk to my business (impact on profit, brand reputation)and how to manage it**

## There are four major categories of dealing with risk:

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)

# Security Lifecycle


Security Control Monitoring
Security Control Implementation
Security Control Assessment
O&M Support
Implementation
Security Management Life Cycle (SMLC)
Acquisition & Development
Project Initiation
Security Control Refinement
Security Control Documentation
Security Categorization
Security Control Selection
10-016-003

Balances risk management with security considerations in each System Development Life Cycle (SDLC) phase.

Includes developing and maintaining standard operating procedures and staff training to:

- Secure the environment in accordance with production controls.
- Monitor, document, report status, respond to incidents, and trigger re-authorization continually during operations and maintenance.
- Plan, review and respond to audits and annual tests.
- Plan contingency and capacity for infrastructure, telecommunications and environmental support during crisis situations.

# Enterprise IT Security (National, State, Agency) How do we think about it?

## FISMA Federal Information Security Management Act

- N.I.S.T. National Institute of Standards
- IRS Publication 1075

## State Enterprise IT Security Policy

- N.I.S.T. or I.S.O. Based Controls
- Standard Enterprise Policy
- Standard Enterprise Procedures

## Agency Level Enterprise Policy

- Specific Agency Policy and Procedures related to their mission

## Department Level Policies and Procedures at the Granule Level

# Security Policies and Procedures

- **Over reliance** on technology to achieve security controls
- Well documented **Security Policy** will provide **governance and oversight** over rapid response to ever changing threats
- Control groups should drive enterprise Security Policy as **fourteen** are either **operational or management** related
- Each control will have its own **procedures, standards and tools** identified (**site specific**)
- Implement, test and yearly assess procedure, standards and compliance

# N.I.S.T 800-53 Security Controls
# What does a Security Control Group Look Like?

| | | | |
|---|---|---|---|
| AC | Access Control | MP | Media Protection |
| AT | Awareness and Training | PE | Physical and Environmental Protection |
| AU | Audit and Accountability | PL | Planning |
| CA | Security Assessment and Authorization | PS | Personnel Security |
| CM | Configuration Management | RA | Risk Assessment |
| CP | Contingency Planning | SA | Systems and Services Acquisition |
| IA | Identification and Authorization | SC | Systems and Communications Protection |
| IR | Incident Response | SI | Security and Information Integrity |
| MA | Maintenance | PM | Program Management |

# N.I.S.T 800-53A Security Controls Assessment
# How do we access the Security Control?

0- We do not do at all

1- We have an Informal Practice Only

2- We have written Policy or Procedures

3- We have Written Policy & Procedures Implemented

4- We have Written Procedures  Reviewed & Tested

| | | | |
|---|---|---|---|
| **AC-3 Access Enforcement**<br>**Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.** | | | |
| AC-3.1. | | | |
| Examine organizational records or documents to determine if user access to the information system is authorized. | | | |
| AC-3.2. | | | |
| Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy. | | | |
| AC-3.3. | | | |
| Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations. | | | |
| AC-3.4. | | | |
| Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented. | | | |

# Penetration and Vulnerability Analysis Testing

- Separate penetration and vulnerability analysis should be conducted
- Research and analyze each result by security level and location within the application
- Combined common resultants from the scans
- Prioritized by likelihood of incident, impact, and location (Development, Test, Production) and level of effort
- Prioritized highest likelihood, impact, and immediate production exposure
- Understand the vulnerability to resolve all incidents and prepare for retests
- Institutionalize best coding practices for ongoing development and support

# Automated tools to continually test and access

## Security Content Automation Protocol (SCAP)

- Currently, US government SCAP content is
- primarily focused on Windows operating systems

## Safeguard Computer Security Evaluation Matrix (SCSEM)

- Unix Systems , HP-UX, AIX, Red Hat Linux, SuSE Linux
- Windows (Windows 2000, 2003, and 2008)
- Open VMS,
- VmWare
- MOT (Management, Operational, and Technical Controls)

# Improving IT Security in your operations

- Security Awareness Training
- Access and Authorization Controls
- Authorization Levels
- Understand and Manage Compliance Data
- Best Practices on Usage without Comingling
- Understand the IT Security Plan and Assessment
- Participate in Assessment Process
- Communicate Agency CSO/Compliance Officer

# Cloud Security

CGI

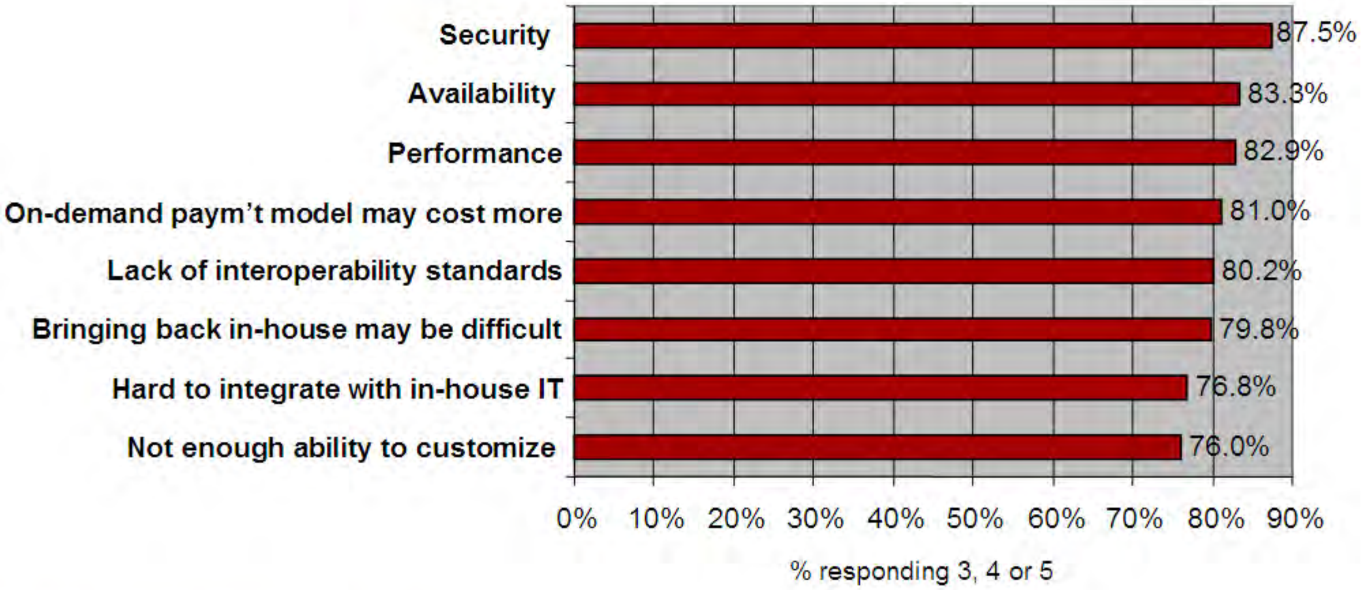
Experience the commitment®

# Security is the Highest Ranking Challenge to the Cloud

- The International Data Corporation (IDC) survey of IT executives and their line-of-business (LOB) colleagues shows Security as the top challenge/issue
- Security is a key consideration for how to enter the cloud rather than an impediment to the cloud
- CGI received provisional Authority to Operate from the Federal Risk Authorization and Management Program (FedRAMP$^{SM}$) on January 31, 2013

**Q: Rate the *challenges/issues* of the 'cloud'/on-demand model**

(Scale: 1 = Not at all concerned 5 = Very concerned)



Source: IDC Enterprise Panel, 3Q09, n = 263

# FedRAMP$^{SM}$ Eases the Security Path to Cloud

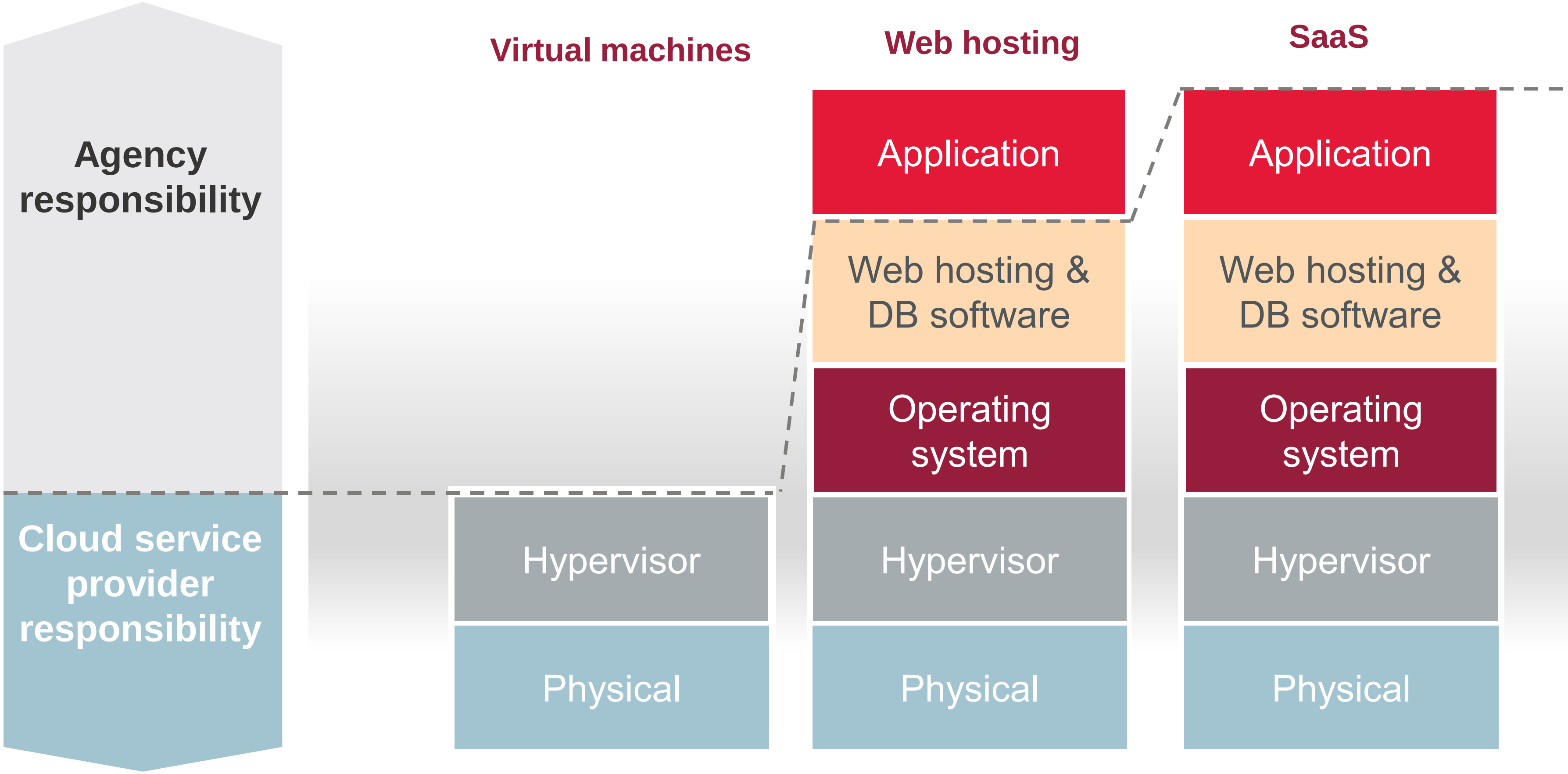
## In October 2010, the White House launched FedRAMP

- Provides framework for a standard and secure approach to Assessing and Authorizing (A&A) cloud computing services and products
- Allows joint authorizations and continuous security monitoring services for government/private cloud computing systems intended for multi-agency use

## Governance: Roles & Responsibilities

- Joint Authorization Board (JAB)
  - Comprised of DOD, DHS, and GSA
  - Grants provisional Authority to Operate (ATO) with sponsoring agency having final say
  - Runs Third Party Assessment Organization (3PAO) program (accredits independent third-party assessors)
  - Sets minimum standards
- Program Management Office (PMO)
  - GSA serves as the FedRAMP PMO
  - Develops guidance and templates; coordinates activities
- Sponsoring Agencies
  - Grant ATO
  - Conduct FISMA reporting

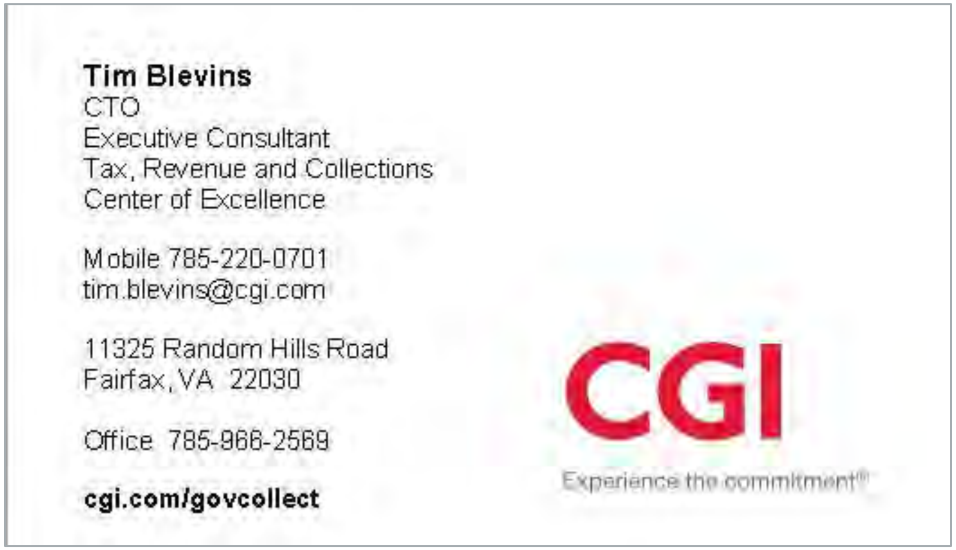
# FedRAMP Grants Provisional ATO To Cloud Solutions From Virtual Machines Through Applications



For web hosting: vulnerability scanning and patch management provides embedded security to close the most common exploits

# Questions/Discussion

# Contact Information



**Tim Blevins**
CTO
Executive Consultant
Tax, Revenue and Collections
Center of Excellence

Mobile 785-220-0701
tim.blevins@cgi.com

11325 Random Hills Road
Fairfax, VA  22030

Office  785-966-2569

**cgi.com/govcollect**

CGI

Experience the commitment®

## About the Presenter

- National Association of Chief Information Officers Security and Privacy Committee 2013
- IRS Electronic Tax Administration Advisory Committee (ETAAC)   2012-2014
- CIO Kansas DOR 11 Years
- FTA/IRS State Co-Chair TAG  2005-2007
- FTA/IRS State Co-Chair TAG Security Committee 2006-2008
- MTC Technology Committee Chair  2000-2008
- FTA National Service and Leadership Award in State Tax Administration 2008
- Kansas IT Security Council Co-Chair 2000-2008
- Experience with Local, State, Federal, and International tax agencies
- 32 Years in Information Technology Development, Management, and Leadership in State Government