IT Compliance Framework for Institutions of Higher Ed

Presented by

Carlos S. Lobato, CISA, CIA

IT Compliance Officer

Information & Communication Technologies Department

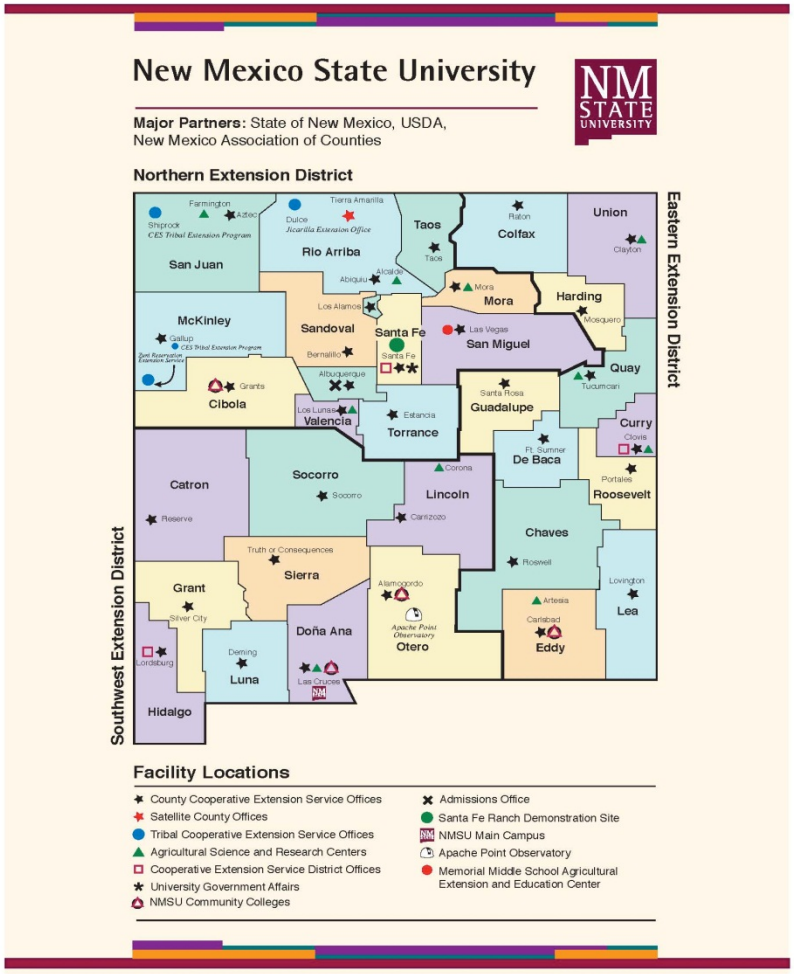
Agenda

- Background and Overview
- Development of the IT Compliance Framework for Institutions of Higher Ed
  - Overview of Laws & Regulations
- Summary of Results
- Ongoing Activities
- Questions

Background Context

- Some context before we proceed:
  - IT Compliance Officer – It was a New Position
  - There was **NO** specific guidance.
  - Where do I start ? ? ? And where should I focus my effort ? ? ?
  - CIO has University-wide Responsibility

CIO's Scope of Responsibility



Background Context Cont'd

- Some context before we proceed:
  - Luckily – Have an Audit Background
    - Reviewed existing IT Policies&Procedures
    - Needed to identify applicable federal & state laws and regulations to NMSU IT Activities (FERPA, HIPAA, etc.)
    - Needed to perform a University-wide IT Risk Assessment

Background Context Cont'd

- Some context before we proceed:
  - Luckily–NMSU used to have an IT Auditor
    - Requested access to working papers
    - Met with University Auditor who made me aware of an existing University-wide IT Risk Assessment (MADE ME HAPPY ! !)
    - NMSU ICT Employees very helpful, mindful of the need and supported the initiative – Self-Assessment

Development of Framework

- Start of Journey:
  - Mindset – **Hackers** generally want **Data**
  - Need to work in **two** areas in tandem:
    - Identify laws or regulations applicable to a University IT Environment
    - Re-perform or update/revalidate the existing University-wide IT Risk Assessment

Development of Framework

- Identification of Laws & Regulations:
  - Asked University Legal Counsel, University Auditor, Police Chief, CIO, Registrar's, VP of Research and other Key Employees
  - Asked EDUCAUSE-Higher Ed IT Association
  - Asked ACUA (Association of College & University Auditors)
  - Did research – browsed websites of other Universities

Development of Framework

- Identified Laws, Regulations & Other:
  - Federal **Data** Privacy Laws:
    - FERPA (Family Educational Rights and Privacy Act)
    - HIPAA (Health Insurance Portability and Accountability Act)
    - GLBA (Gramm-Leach-Bliley Act)
    - RFR (Red Flags Rule) – From Federal Trade Commission
  - Industry Regulations
    - PCI DSS (Payment Card Industry Data Security Standard)
  - Sponsored Projects (Grants, Contracts, etc.)
    - Special terms & conditions – Research Compliance
    - FISMA and ITAR

Development of Framework

➢Other related laws:

Federal Privacy Act of 1974	The Privacy Act states in part: No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains....
Electronic Communications Privacy Act	From a rights perspective, the ECPA protects individuals' communications against government surveillance conducted without a court order, from third parties without legitimate authorization to access the messages, and from the carriers of the messages, such as Internet service providers. However it appears to provide little privacy protection to employees with respect to their communications as conducted on the equipment owned by their employer.
Computer Fraud and Abuse Act of 1986	The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1986 intended to reduce "hacking" of computer systems. It was amended in 1994, 1996 and in 2001 by the USA PATRIOT Act. The USA PATRIOT Act increased the scope and penalties of this act.
The Computer Security Act of 1987	The Computer Security Law of 1987, Public Law No. 100-235 (H.R. 145), (Jan. 8, 1988), was passed by the United States Congress. It was passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. It requires the creation of computer security plans, and the appropriate training of system users or owners where the systems house sensitive information.
Federal Information Security Management Act of 2002	The Federal Information Security Management Act of 2002 (FISMA) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The act is meant to bolster computer and network security within the federal government.
International Traffic in Arms Regulations (ITAR)	Government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). These regulations implement the provisions of the Arms Export Control Act (AECA). Its goal is to safeguard U.S. national security.
Digital Millennium Copyright Act of 1998	Many people see unauthorized music downloading as harmless and don't fully understand its consequences. Illegal downloading presents a serious issue on college campuses and can be costly to the university administration in terms of resources, such as excessive use of bandwidth and time spent responding to infringement notices sent by the RIAA (Recording Industry Association of America). The RIAA is very active in enforcing DCMA for their clients. For more information on how the RIAA works with Universities, go to the FAQ's on the RIAA site.
U.S. Copyright Law, October 2007	Copyright protection is afforded to any work that is in a form that can be seen, reproduced, or otherwise communicated.

Laws – FERPA - What is it?

- FERPA (Family Educational Rights and Privacy Act of 1974) – Revised 12/2/11
- A United States Federal Law
- Administered by U.S. Department of Ed
- Requires protecting the privacy of Educational Records/Student Data
- Noncompliance can result: **Withholding payments or termination of funding**

FERPA - What is it? Cont'd

- Excerpts from FERPA (Family Educational Rights and Privacy Act)
- Protecting student privacy is paramount to the effective implementation of FERPA.
- All education data holders must act responsibly and be held accountable for safeguarding students' personally identifiable information (PII) from education records.

FERPA - What is it? Cont'd

- Excerpts from FERPA (Family Educational Rights and Privacy Act)
- The need for clarity surrounding privacy protections and data security continues to grow as data systems are built and more education records are digitized and shared electronically.

FERPA - What is it? Cont'd

- Excerpts from FERPA (Family Educational Rights and Privacy Act)
- The need for clarity surrounding privacy protections and data security continues to grow as data systems are built and more education records are digitized and shared electronically.

FERPA - What is it? Cont'd

- In ~2011 U.S. Department of Ed Launched Initiatives to Safeguard Student Privacy
  - Hired a Chief Privacy Officer
  - Established the Privacy Technical Assistance Center (PTAC)
    - PTAC serves as a one-stop resource for the education community on privacy, confidentiality, and data security
    - The center has developed a privacy toolkit and checklists for data governance

FERPA – How to comply?

- PTAC Checklists:
  - Data Governance Checklist (Dec 2011)
    - Responsibility, Policies & Procedures at a High Level
  - Data Security Checklist (Dec 2011)
    - Technical controls i.e. Strong Passwords, etc.
  - Data Breach Response (Sept 2012)
    - Responding to the breach (Policy, Plan & Procedures)
    - Notification to affected parties & U.S. Dept. of Ed
  - Ask PTAC for Guidance/assessment.

FERPA – Main Requirements

- Designate Information Security Responsibility
- Establish an Information Security Program
- Establish Policies & Procedures
- Monitoring/Incident Handling/Compliance
- Establish Training and Awareness

Laws – HIPAA - What is it?

- HIPAA (Health Insurance Portability and Accountability Act of 1996) – Revised 1/25/13 (Changes effective 3/26/13)
- Administered by U.S. Department of Health & Human Services (DHHS)
- Covered entities must comply with the applicable requirements of final rule by 9/23/13.

HIPAA - What is it? Cont'd

- HIPAA (Health Insurance Portability and Accountability Act)
- Privacy Rule - protects the privacy of individually identifiable health information
- Security Rule, sets national standards for the security of electronic protected health information – Technical Detailed Controls
- Noncompliance can result in FINES
  - Civil Monetary Penalties (See next)

HIPAA - What is it? Cont'd

- Excerpt from HIPAA (Health Insurance Portability and Accountability Act)

TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE		
Violation category—Section 1176(a)(1)	**Each violation**	**All such violations of an identical provision in a calendar year**
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect-Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect-Not Corrected	50,000	1,500,000

HIPAA - What is it? Cont'd

- The "Privacy Rule" standards address the use and disclosure of individuals' health information
  - Administrative **Requirements** main focus for IT
    - Privacy Personnel – Designate a Privacy Official
    - Privacy Policies and Procedures
    - Workforce Training
    - Data Safeguards
    - Documentation and Record Retention, etc.

HIPAA - What is it? Cont'd

- The "Security Rule" details what safeguards (controls) must be in place to ensure proper protection of electronic protected health information
  - Administrative **Safeguards**
    - Security Personnel – Designate Security Official
  - Technical Safeguards
    - Access, Audit & Integrity Controls
    - Transmission Security, etc.

HIPAA – How to Comply?

- The DHHS Office for Civil Rights created a HIPAA comprehensive audit program/checklist
  - Available online
  - Covers Privacy Rule requirements
  - Covers Security Rule requirements
  - Covers requirements for the Data Breach Notification Rule

HIPAA – Main Requirements

- Designate Information Security & Privacy Responsibility
- Establish an Information Security Program
- Establish Policies & Procedures
- Monitoring/Incident Handling/Compliance
- Establish Training and Awareness

Laws – GLBA - What is it?

- GLBA (Gramm-Leach-Bliley Act of 1999) – Revised 5/22/02
- A United States Federal Law
- Administered by the Federal Trade Commission (FTC)
- Set standards for Safeguarding Customer Information (non-public information (PII))
- Noncompliance can mean severe fines

GLBA - What is it? Cont'd

- GLBA (Gramm-Leach-Bliley Act)
- GLBA noncompliance can result in the following:
  - Institutions can be subject to civil penalties of up to $100,000 for each violation
  - The officers and directors of the financial institution can be subject to, and personally liable for, a civil penalty of up to $10,000
  - Imprisonment for up to five years is possible.

GLBA – How to Comply?

- The FTC created a Complying with the Safeguards Rule Checklist
  - How to Comply
  - Securing Information
  - Technical controls – Strong Passwords, etc.
- The FTC also created a How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act Checklist

GLBA – Main Requirements

- Designate Information Security Responsibility
- Establish an Information Security Program
- Establish Policies & Procedures
- Monitoring/Incident Handling/Compliance
- Establish Training and Awareness

Laws – RFR - What is it?

- The (Red Flags Rule) (RFR) – Revised 12/18/10
- Administered by FTC
- Requires developing and implementing a written Identity Theft Prevention Program
- Noncompliance can mean severe fines
  - **The FTC can seek both monetary civil penalties and injunctive relief for violations of the Red Flags Rule. Currently, $3,500/violation.**

RFR – How to Comply?

- The FTC created a Complying with the Red Flags Rule Checklist
  - Identify/inventory covered accounts (Accounts Receivables) – Recurring payments to pay-off debt
  - Identifying relevant red flags
  - Detecting red flags
  - Responding to red flags
  - Administering your Program – Designate Responsibility, Policy, etc.
- The FTC also created a website with tips on How to Fight Fraud with the Red Flags Rule

RFR – Main Requirements

- Designate Program Responsibility
- Establish a Red Flags Program
- Establish Policies & Procedures
- Monitoring/Incident Handling/Compliance
- Establish Training and Awareness

PCI DSS - What is it?

- PCI DSS (Payment Card Industry Data Security Standard) – Industry Regulation
- Compliance Administered by Individual payment brands (VISA, MasterCard, Discover, American Express, etc.)
- PCI Security Standards Council –
  - Open global forum, launched in 2006, responsible for the development, management, education, and awareness of PCI Security Standards. This is where you will find what you need to know about PCI and Governed by all five payment brands.

PCI DSS - What is it?

- PCI DSS -12 Requirements designed to ensure proper handling & protection of Credit Card Information
  - Technical IT Controls (Examples):
    - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
    - Requirement 2: Do not use vendor-supplied **defaults for system passwords** and other security parameters
    - Requirement 12: Maintain a policy that addresses information security for all personnel.

PCI DSS – How to Comply?

- The PCI Security Standards Council created a Requirements and Security Assessment Procedures Checklist
- Additionally they created a section on their website that details "How to Be Compliant"

PCI – Main Requirements

- Designate Information Management Security Responsibility
- Establish an Information Security Program
- Establish Policies & Procedures
- Monitoring/Incident Handling/Compliance
- Establish Training and Awareness

Development of Framework

- Re-inventing the wheel is not my way:
  - **Updated/Revalidated existing University-wide IT Risk Assessment**
    - Met and interviewed University Data Custodians (Registrar's, Research, etc.)
    - Interviewed other key personnel (University Auditor, Legal Counsel and IT Leadership Members, etc.)
  - **Laws&Regulation requirements Incorporated**

SUMMARY OF RESULTS

- Created a 5-Year IT Compliance Plan
- Created an **IT Security/Compliance Framework for Information Security in Higher Ed**
- **Ongoing Activities**
  - Implementing IT Compliance Framework Roadmap – 2 -5yrs
  - Compliance/Monitoring Never Ending

Q & A

Carlos S. Lobato, CISA, CIA

IT Compliance Officer

NMSU ICT – IT Compliance Function

clobato@nmsu.edu

www.ict.nmsu.edu/itcompliance

646-5902

Thank you for your time!

REFERENCES

- U.S. Dept. Ed
  - FERPA - http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
  - PTAC - http://ptac.ed.gov/
- U.S. Department of Health & Human Services (DHHS)
  - HIPAA - http://www.hhs.gov/ocr/privacy/index.html
- Federal Trade Commission (FTC)
  - GLBA - http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act
  - Red Flags Rule - http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml
- PCI Security Standards Council
  - PCI DSS - https://www.pcisecuritystandards.org/