

# ***“Serving the Servants” by Securing their Data***

Readout on Gramm-Leach-Bliley Act Assessment Project

June 14, 2007

**Rick Dent**

Messiah College – CIO

**Dick Morrison**

Messiah College – College Counsel

**Kathleen Roberts**

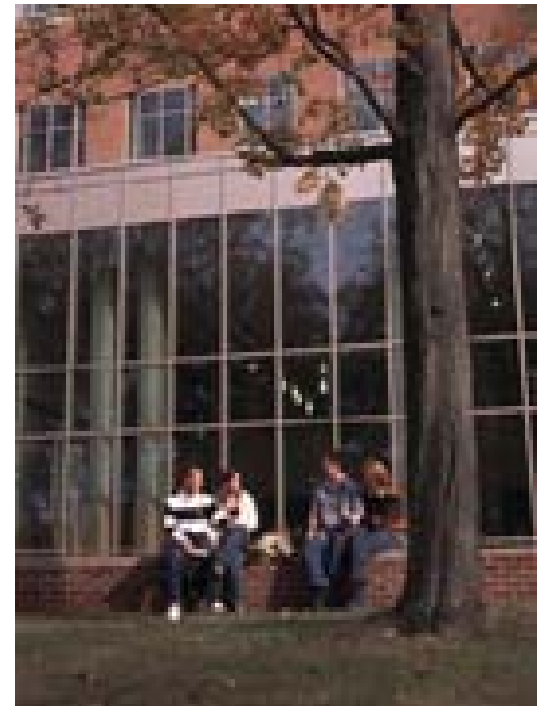
iSecure Solutions – Principal

1611 Arran Way

Dresher, PA 19025

215-641-1396 (Office)

[kathleen@isecuresolutions.com](mailto:kathleen@isecuresolutions.com)



Graphic – Messiah College



iSecure Solutions

# ***Objectives of Today's Session***

- **Understand Why GLBA Compliance Matters to Messiah College**
  - GLBA regulatory mandate
  - Significance of GLBA compliance to Messiah College
- **Share Resource Commitments Required to Engage in the Compliance Project**
  - Time and effort requirement by Messiah College
- **Discuss the GLBA Assessment Project**
  - Review project goals (What and Why)
  - Explain methodology (How and Why)
  - Share recommended remediation approach
- **How Your School Can Get Started**
  - Key requirements for GLBA compliance
  - How to Begin

# ***Introduction – About Us***

**Rick Dent, Messiah College – CIO**  
**BACKGROUND AND EXPERIENCE**



**Dick Morrison, Messiah College - Legal Counsel**  
**BACKGROUND AND EXPERIENCE**

**Kathleen Roberts, iSecure Solutions – Founder & Principal**  
**BACKGROUND AND EXPERIENCE**

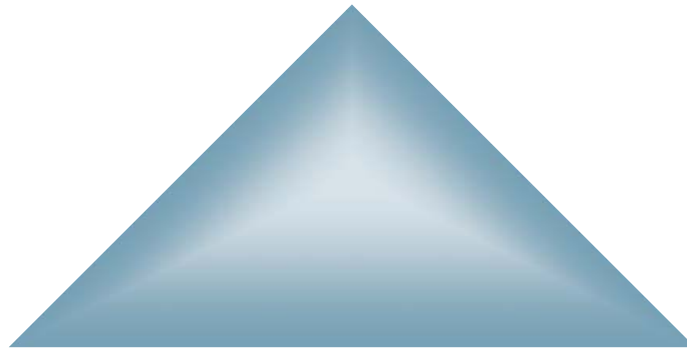
# ***About Kathleen***

- I am a Christian by grace
- I am an Information Security Professional by trade
- I am an MBA in Information Systems by education
- I am a Sansei by blood
- I am an Ice Cream Fanatic by choice

# ***Information Security Principles***

## ***Confidentiality***

*Protection from unauthorized or unintentional access or disclosure*



## ***Integrity***

*Assurance that information and systems are accurate, complete and reliable, safe from unauthorized or unintentional modifications*

## ***Availability***

*Ensuring reliable and timely access to systems and data resources by authorized users*

# Privacy vs. Security

# Privacy and Security are two different things!



- **Privacy** is the appropriate use of information as defined by:
  - Law
  - Public sensitivity
  - Context
- **Security** is the protection of information
  - Data Classification Categories
  - Define who has access - (Confidentiality)
  - Define who can manipulate the data - (Integrity)

**Security is a Pre-Requisite to Privacy !**

Original Content Source - [www.privacyassociation.org](http://www.privacyassociation.org) - URL - [www.ehcca.com/presentations/HIPAA10/grymes.ppt](http://www.ehcca.com/presentations/HIPAA10/grymes.ppt)

# Agenda



- **Introduction**
- **Compliance in Higher Education**
  - Evolution of Information Security Regulation
  - Key Components of the Gramm-Leach-Bliley Act (GLBA)
  - Significance of GLBA Compliance to Messiah College
- **GLBA Compliance Assessment Project**
  - Project Goals, Scope and Rationale
  - Messiah Personnel - Time and Effort Required
  - Methodology and Tools Used
  - Key Information Documented
- **Compliance Project Readout**
  - Selected Final Reports
  - Suggested Implementation Approach
  - Determine Next Steps
- **Conclusion**
  - Getting Started - GLBA Key Components
  - How to Begin

# Information Security Regulatory Environment



Graphic - Microsoft

- **Protection of Non Public Personal Information (NPPI)**

- **1980's and 1990's**

- » Self Regulation using “Good Security Practices”

- **2000 - 2007**

- » Security Breaches became Common Occurrence - 155 Million Records to date
    - » All Industries: ChoicePoint, U.S. Dept. of Veterans Affairs, Ohio State University, YMCA, DSW Retailer, UVa, etc.
    - » Type of Breaches: Hackers, Lost or Stolen Laptops, Lost or Stolen Back Up Tapes, Disgruntled or Dishonest Employees, Third Party Providers, etc.

- **Result:**

- » Federal and State Regulatory Agencies Stepped In and created HIPAA, GLBA, CA SB 1386, PCIDSS, FDA Rule 21, (32) additional state data breach laws, etc.
  - » Regulatory Environment Grows More Complex for Higher Education Institutions

# ***Information Security Regulatory Environment (Continued)***

The current regulatory environment requires higher educational institutions to protect student and employee financial and health information from improper disclosure.

- Financial Information – **GLBA, PCI-DSS**
- Health Information – **HIPAA**
- Educational Information - **FERPA**
- Data Breach Disclosures – **CA SB 1386, etc.**
- Research Information – **FDA Rule 21**



Graphic - Microsoft

# GLBA Six Key Elements



- Prepare a comprehensive, flexible, **written Information Security Program**
- Designate an employee or office to be **Information Security Program Coordinator**
- **Identify and assess the risks** involving the security of customer information (includes a risk assessment of computer information systems)
- **Develop appropriate safeguards** to control risks
  - Ensure that **administrative, technical and physical safeguards** are implemented to control the risks identified
- **Oversee service providers**
- **Evaluate** and **adjust** the information security program

# Agenda



- **Introduction**
- **Compliance in Higher Education**
  - Evolution of Information Security Regulation
  - Key Components of the Gramm-Leach-Bliley Act (GLBA)
  - Significance of GLBA Compliance to Messiah College
- **GLBA Compliance Assessment Project**
  - Project Goals, Scope and Rationale
  - Messiah Personnel - Time and Effort Required
  - Methodology and Tools Used
  - Key Information Documented
- **Compliance Project Readout**
  - Selected Final Reports
  - Suggested Implementation Approach
  - Determine Next Steps
- **Conclusion**
  - Getting Started - GLBA Key Components
  - How to Begin

# ***GLBA Compliance Assessment – Project Goals***



- Conduct an IT Risk Assessment to understand overall picture of IT risk and areas for improvement
- Conduct a GLBA Gap Analysis to determine areas for improvement
- Prioritize remediation recommendations and identify “low hanging fruit” areas of opportunity
- Assuming limited staff resources, create a remediation plan that is realistic and useable

# ***GLBA Compliance Assessment – Project Scope***



- **Inventory Critical Information Assets**
  - » Identify data, systems, hardware and people
  - » Determine Data Classification rules and prioritize data
  - » Determine risk factors and weightings
- **Inventory and Rate Current Level of Security Safeguards**
  - » Identify and rate current controls
- **Prepare for and Conduct IT Risk Assessment**
  - » Select key departments handling critical data
  - » Identify knowledgeable staff for interview participation and prep all parties
  - » Customize and administer IT risk survey that includes GLBA requirements
  - » Obtain information on department use of technical and administrative controls
- **Analyze Data and Perform GLBA Gap Analysis**
  - » Conduct comprehensive analysis of data collected
  - » Compare findings to GLBA requirements and determine gaps
- **Create Remediation Recommendations**
  - » Write Final Report including remediation steps necessary for compliance
  - » Provide Remediation Plan to begin the process to implement findings.

# ***GLBA Compliance Assessment - Messiah College Personnel Involvement***



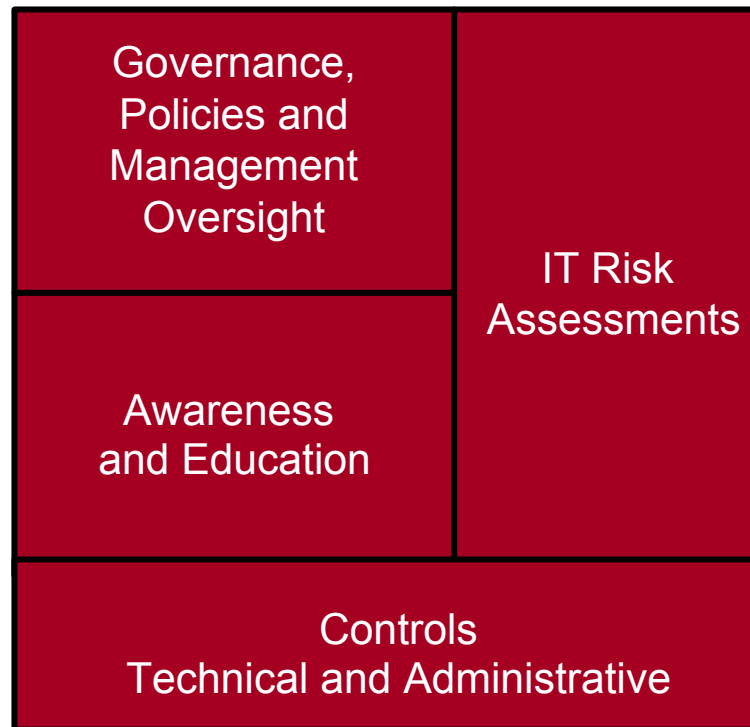
Graphic - Messiah College

<b>Department</b>	<b>Time and Effort</b>
<b>Project Team</b> (ITS and College Counsel)	Meetings Data Collection
<b>Departmental</b> Subject Matter Experts	Meeting Prepare/ Data Collection

# Information Security Program Framework



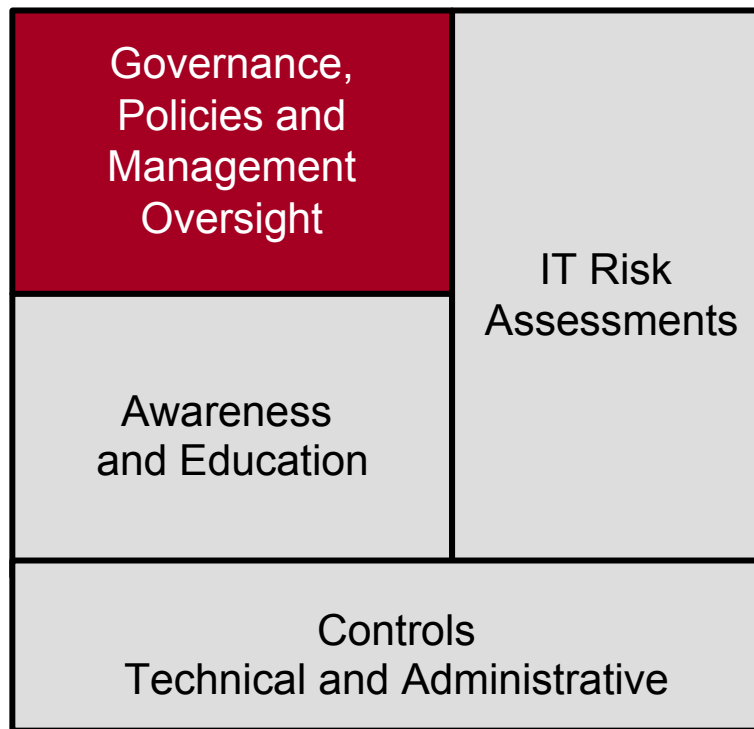
All four components within this framework are required by security standards, best practices and regulatory compliance.



# Information Security Program Framework – Governance, Policies and Management Oversight



## Establish and Oversee an Information Security Program

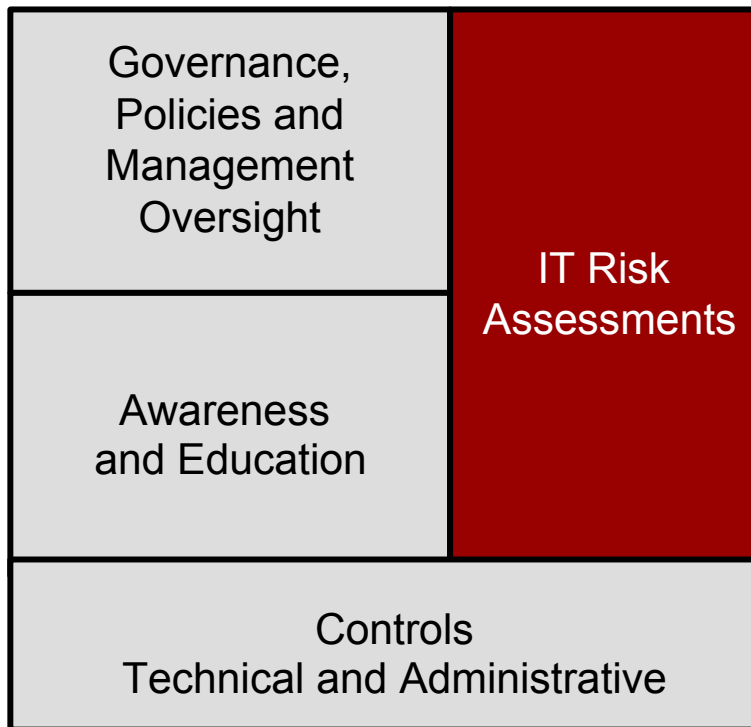


- Develop, Implement and Update the Information Security Program
- Report on the Status of the Information Security Program and Security Issues to the Audit Committee and the Institution's Board.
- Develop, Implement and Update Information Security Policies, Standards and Operating Procedures
- Develop, Implement and Update an Information Security Incident Response Program.

# Information Security Program Framework – IT Risk Assessments



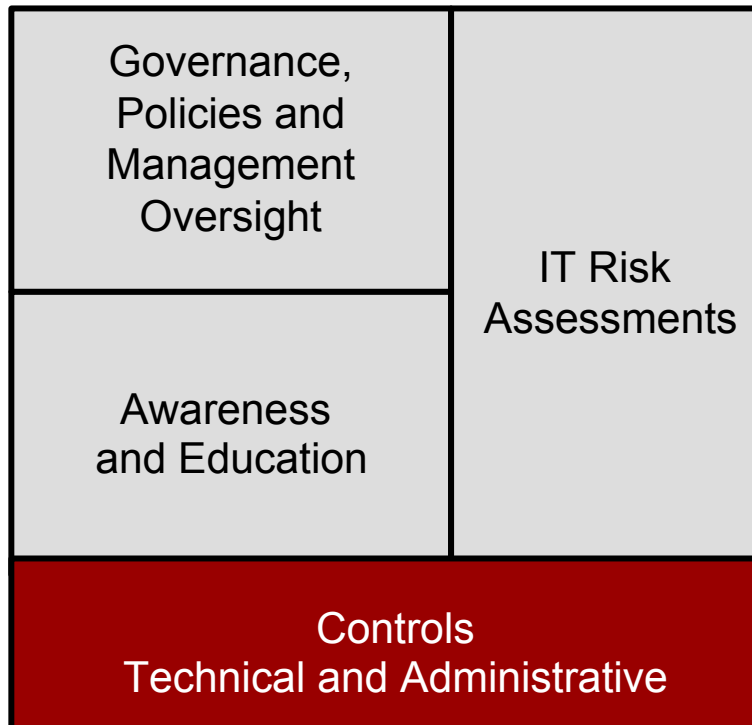
## Establish and Lead the IT Risk Assessment Process



- Develop IT Risk Assessment Methodologies and Model
- Assess IT Infrastructure and Departmental Application Risks
- Assess Technical and Administrative Operational Risks
- Assess Business Partner Risks

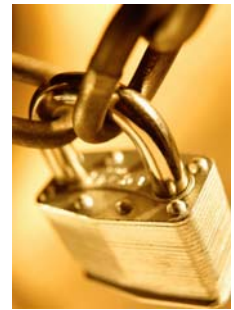
# Information Security Program Framework – Technical and Administrative Controls

## Implement new Technical and Administrative Security Controls based on the changing Environment

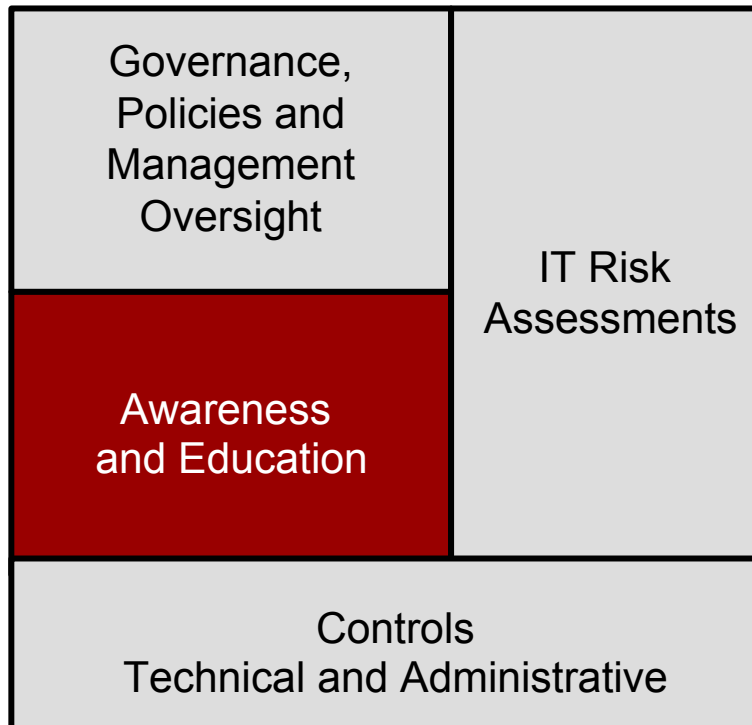


- Stay Aware of New Technology
- Determine Impact of Emerging Threats
- Assess System Vulnerabilities
- Monitor Environment Based Upon Changing Legal and Regulatory Requirements

# Information Security Program Framework - Awareness and Education



## Advocate Information Security Awareness among the entire Institution's Community



- Develop and Implement Security Awareness Campaigns
- Provide Targeted Presentations and Educational Seminars
- Enroll Key IT Staff in Targeted Security Education Classes
- Communicate the Requirements for Secure Computing among the Student and Staff Population.
- Educate Students regarding the Ethics of Computer Use and Security.

# GLBA Compliance Assessment Project



## iSecure Solutions Built Project Scope based upon this Framework



- Governance, Policies and Management Oversight
  - Policy Assessment Completed in Phase I
  - Governance, Mgmt Oversight Assessment Needed
- IT Risk Assessment
  - IT Infrastructure Network Review Completed in Phase I, Detailed Asset Info Needed
  - Dept. Applications Assessment Needed
- Controls
  - IT Infrastructure Assessment Needed
  - Dept. Applications Assessment Needed
- Awareness and Education
  - College Community Assessment Needed

# GLBA Compliance Assessment Project - Process Flow

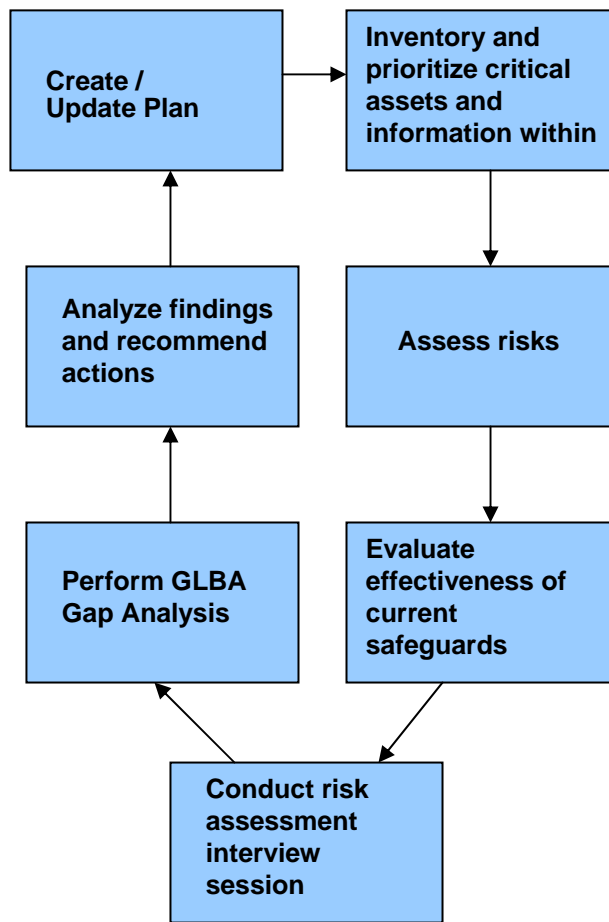
10. Monitor, test, evaluate and adjust program every 1-3 years.

9. Develop recommendations with corrective actions required for compliance and to mitigate risks.

8. Compare findings to regulatory and best practice standards. \*

\* iSecure Solutions has a Tool available to assist.

7. Conduct risk assessment interview session with selected individuals.\*



1. Inventory all critical assets. (data, systems, hardware and people)

2. Classify data in identified assets to prioritize, based upon data stored within \*

3. Assign initial risk factors. \*

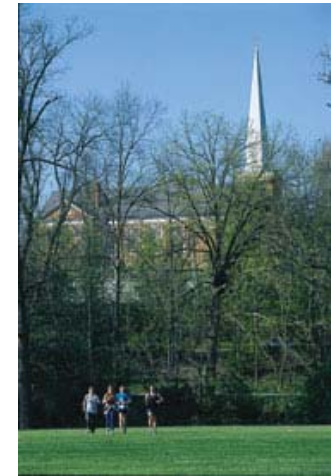
4. Prioritize risks using weightings. \*

5. Identify all safeguards or controls in use. \*

6. Determine adequacy of these safeguards based upon defined risk factors. \*

# GLBA Compliance Assessment – Project Tools Used

Tool Name	Process Step	Function
Critical Asset Inventory	1	Identify and document all mission critical assets - data, systems, hardware and people.
Data Classification Aid	2	Identify, locate and classify mission critical data.
Risk Factor Identification and Weighting	3 & 4	Identify vulnerabilities and threats to mission critical data and operations. Assign relative weight to prioritize.
Security Controls Rating Matrix	5	Identify current safeguards/controls and "maturity level."
Risk Assessment Interview Customized Survey	7	Customize to target specific areas and maximize overall understanding.
High Level IT Security Risk Matrix	6 & 8	Populate matrix. Analyze findings comparing to regulatory and best practice standards.
GLBA Assessment Final Report	9	Analyze findings, develop recommendations and write final report.
GLBA Remediation Project Tracker	10	Using final report findings, create remediation implementation plan.



Graphic – Messiah College

# Key Information Documented

- **Critical Asset Inventory**
  - Critical Data Listed and Sorted by Data Classification Category
  - Critical Systems, Hardware Listed
  - Critical Departmental People Listed
- **Security Control Matrix**
  - Inventory of Control Coverage at the College
  - View of Impact to Overall Environment
  - Control Scorecard
- **Risk Assessment Interview Survey Responses**
  - IT Infrastructure – NOT REQUIRED due to Phase I Security Assessment)
  - Departmental Practices – Risk Areas
  - Details of Inconsistencies for Follow Up
- **High Level IT Risk Matrix**
  - Consolidated View of Specific Information Asset, GLBA impact, Score across all Messiah College Risk Factors, Relative Risk and GLBA Risk.
  - Use to Prioritize Areas to Focus On
- **Final Report Document**
  - Official Scorecard from GLBA Gap Analysis
  - Detailed Explanation of Assessment.
- **GLBA Remediation Project Tracker**
  - Implementation Tool Allowing further Customization



Graphic - Microsoft

# Agenda

- **Introduction**
- **Compliance in Higher Education**
  - Evolution of Information Security Regulation
  - Key Components of the Gramm-Leach-Bliley Act (GLBA)
  - Significance of GLBA Compliance to Messiah College
- **GLBA Compliance Assessment Project**
  - Project Goals, Scope and Rationale
  - Messiah Personnel - Time and Effort Required
  - Methodology and Tools Used
  - Key Information Documented
- **Compliance Project Readout**
  - Selected Final Reports
  - Suggested Implementation Approach
  - Determine Next Steps
- **Conclusion**
  - Getting Started - GLBA Key Components
  - How to Begin



# High Level IT Risk Matrix

## ABC College High Level IT Security Risk Matrix

Information Security Governance & Infrastructure Components



Graphic – Messiah College

Level Of Risk - Numerical Values			
Description	Color	Value	Risk
relevant or the significance of a control failure is not minimal risk potential	White	0	N/A
or the significance of a control elevated risk potential	Green	1	LOW
or the significance of a control extensive risk potential	Yellow	2	MED
or the implications of a control	Red	3	HIGH

RISK FACTORS		Factor Weight
F1	Customer Information - Confidentiality	0.28
F2	Improper/incorrect Transactional Data - Integrity	0.18
F3	Infrastructure Stability/ Change Control/ Business Continuity/ Physical - (Availability)	0.11
F4	Alumni/Student Organizational Confidence - Reputation	0.28
F5	Regulatory Compliance - Legal	0.10
F6	Operational Systems Reliance	0.08
F7	Fraud / Data Breach - Financial Loss	0.06

ASSESSMENT AREA	RISK		CONTROL PROCESS	Regulatory Compliance Requirement		Risk Factors							Relative Risk Factor	Risk Factor Avg	High Risk Factor	GLBA Risk Factor	GLBA High Risk Factor
	CATEGORY	FUNCTION		GLBA - FTC Enforcement	State Data Breach Notification Laws	F1	F2	F3	F4	F5	F6	F7					
Management Oversight & Governance	Information Security Program / Information Security Plan	Development and Management	X		2	0	1	2	3	0	1	1.60	1.338	1.870	3.000	3.000	
		Implementation	X		3	0	1	2	3	1	2	1.87					
	Security Steering Committee	Implementation			2	0	0	2	2	1	0	1.30					
	Information Security Policies	Development and Management	X	X	1	2	2	2	2	1	2	1.88					
	Implementation	X	X	1	2	2	2	2	1	2	1.88						
Vendor Management	Implementation	X		0	0	0	0	0	0	0	0.00			0.000			
Information Security Incident Response Plan	Information Security Incident Response Plan	Development and Management	X	X	1	1	2	2	3	0	1	1.61			3.000		
		Implementation	X	X	2	1	3	3	3	0	2	2.19			3.000		
	Information Security Risk Assessment	Development and Management	X		0	0	0	0	1	0	0	0.10			1.000		
		Implementation	v												< .000		

# Sample GLBA Scorecard

Rule No.	Type	GLBA Safeguards Rules Required Controls	Rating
1	Governance	Information Security PlanS	Adequate
2		Security Program Monitoring and Adjustments	Not Adequate
3		Safeguards Coordinator	Adequate
4		Periodic Risk Assessments	Not Adequate
5		Information Security Training and Awareness	Adequate
7		Administrative, Technical and Physical Control Implementation	Not Adequate
8		Third Party Service Providers	Adequate
9		Third Party Service Provider Contract Enforcement of Objectives	Adequate
6	Administrative	Employee Training	Adequate
10		Periodic Update and Testing of Program's Key Controls	Not Adequate
11		Limit Access Using Segregation of Duties, Dual Controls, Background Checks	Not Adequate
12		Information Security Incident Response Program	Adequate
13		Records & Storage Media Destruction - Policies & Procedures	Not Adequate
14	Administrative & Technical	Access Controls to NPPI Systems	Not Adequate
17		Physical Access Controls to Business Records and Computer Systems with NPPI	Not Conclusive
15	Technical	Monitor Systems and Procedures to Detect Unauthorized Access	Adequate
16		Secure Data Transmission - Encryption	Adequate
9 out of 17 = 53 % Compliant			

# GLBA Detailed Report



iSecure Solutions

Information Security Consulting for Higher Ed and Small Business

## Requirement #1:

A Written Information Security Program

### Requirement Description:

An "Information Security Program" means the administrative, technical, or physical safeguards used by a financial institution to protect the access, collection, distribution, processes, protection, storage, use, transmission, disposal of, or otherwise handling of customer information.

**Control Type:** Governance

### Control Objective:

a) Review, Approval, And Authorization	b) Planning And Controlling	X
c) Safeguarding And Monitoring	d) Training And Development	
e) Analysis And Calculation	f) Verification And Quality Control	
g) Processing And Information Exchange	h) Reliability And Information Integrity	
i) Segregation Of Duties	j) Regulatory Compliance	X

### Analysis and Observations:

In discussions with ABC College management, it has been determined by the iSecure GLBA assessment team, that ABC College does not currently have a written Information Security Program that meets the GLBA compliance requirements as stipulated in 16 CFR §§ 314.3 (a) & (b) - Interagency Guidelines and standards for Safeguarding Customer Information. This finding was reaffirmed in the mid-level control compliance matrix that was completed by IT management.

# ***Suggested Implementation Approach***



Graphic – Messiah College

- **Unified, Institution-Wide Approach**
  - Most efficient use of scarce resources
  - Many similarities in the approaches required by regulation (HIPAA, GLBA, PCI DSS, CA SB 1386, etc.) so minimizes duplication of efforts
  - Able to comply with multiple regulations at once by implementing the minimal safeguards
  - If conflicting laws, implement the most stringent regulation
- **Embraced Autonomy Model**
  - Information Security Officer (ISO) “officially appointed” as lead – form committee of key stakeholders within the school community
  - Committee collaboratively identifies scope of projects and standards to be implemented
  - Implementation handled locally by departments

# Determine Next Steps – Remediation Implementation



Graphic – Messiah College

- Prioritize Recommendations
- Examine “Low Hanging Fruit”
- Balance a Bias for Taking Action with Realistic Expectations - consider starting with the following:
  - Information Security Officer (ISO) officially named
  - ISO forms Small Committee with Representation from Key Data Owners, Departments and Users
  - Committee Function and Responsibilities defined and approved
  - Remediation Plan developed and implemented
- Regularly Communicate Progress to Executive Leadership
- Monitor, Evaluate and Revise on an Ongoing Basis

# Agenda

- **Introduction**
- **Compliance in Higher Education**
  - Evolution of Information Security Regulation
  - Key Components of the Gramm-Leach-Bliley Act (GLBA)
  - Significance of GLBA Compliance to Messiah College
- **GLBA Compliance Assessment Project**
  - Project Goals, Scope and Rationale
  - Messiah Personnel - Time and Effort Required
  - Methodology and Tools Used
  - Key Information Documented
- **Compliance Project Readout**
  - Selected Final Reports
  - Suggested Implementation Approach
  - Determine Next Steps
- **Conclusion**
  - Getting Started - GLBA Key Components
  - How to Begin

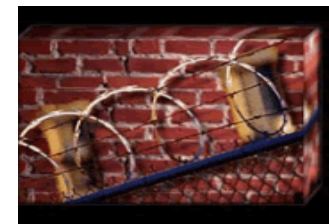


# Getting Started – GLBA Key Components Review



- Prepare a comprehensive, flexible, **written Information Security Program**
- Designate an employee or office to be **Information Security Program Coordinator**
- **Identify and assess the risks** involving the security of customer information (includes a risk assessment of computer information systems)
- **Develop appropriate safeguards** to control risks
  - Ensure that **administrative, technical and physical safeguards** are implemented to control the risks identified
- **Oversee service providers**
- **Evaluate** and **adjust** the information security program

# How to Begin



- **Inventory Critical Information Assets**
  - » Identify data, systems, hardware and people
  - » Determine Data Classification rules and prioritize data
  - » Determine risk factors and weightings
- **Inventory and Rate Current Level of Security Safeguards**
  - » Identify and rate current controls
- **Prepare for and Conduct IT Risk Assessment**
  - » Select key departments handling critical data
  - » Identify knowledgeable staff for interview participation and prep all parties
  - » Administer survey that focuses on GLBA requirements
  - » Obtain data on department use of technical and administrative controls
- **Analyze Data and Perform GLBA Gap Analysis**
  - » Conduct comprehensive analysis of data collected
  - » Compare findings to GLBA requirements and determine gaps
- **Create Remediation Recommendations**
  - » Create Final Report with findings and remediation steps necessary for compliance
  - » Provide Remediation Plan to begin the process to implement findings.

# *Questions?*

# *Thank You*



Please allow iSecure Solutions to  
*serve you ...*

stop by the **Larson Student Center** this evening  
between **7-9 pm** for some locally made ice cream,  
compliments of iSecure Solutions!

[www.iSecureSolutions.com](http://www.iSecureSolutions.com)



iSecure Solutions