

A green chalkboard with two pieces of pink chalk and some faint white chalk markings. The chalk is positioned in the lower-left quadrant, and the board is covered with light, sketchy white lines. The text is overlaid on the right side of the board.

Compliance: What Every CU Needs to Know

Presented by Laura King and Jim Soenksen



Session Agenda

- Be Aware of Certain Regulations!
- Impact of the Regulations!
- What Does it Mean to be Compliant?
- Proper Incident Response Handling!
- Are You Ready for Multi-Factor?
- Questions and Answers

The Regulations to Know!

- Reg. 748 A and B
- GLB
- SOX
- BSA /ALM
- ISO 17799 / BS 7799



Understanding the Regs!

| | | | | | |
|---|---|--|--|--|--|
| 748 A&B | GLB | SOX | BSA/ AML | ISO 17799 BS7799 | FDIC FIL- 103- 2005 |
| CU's | Banks | Public & FI's > 500 mm | FI's | Any | FI's |
| Data Protection & Privacy | Data Protection & Privacy | Financial Reporting | SARS | Internal Control | ID Theft |
| Security Program & Incident Response | Security Program & Incident Response | Internal Control Processes, Procedures, Reporting, Auditing | Risk Based Monitoring & Reporting | Internal Control Processes, Procedures, Reporting, Auditing | Multi- Factor |





What is the Impact of the Regs?

- Security Program
- Risk Assessments
- Data Privacy & Protection
- Business Continuity & Disaster Recovery
- Access Controls
- Incident Response
- Vulnerability Management
- Monitoring & Reporting



Hot Audit Themes

- 3rd Party Risk Management
- Critical Data Risk Assessment
- Business Continuity/Disaster Recovery
- Multi-Factor
- Email Security
- Incident Response
- Vulnerability Management



What Does it Mean to be Compliant?

- Challenges: Theory vs. Reality
- “Testing Disaster Recovery”



Proper Incident Response Handling

- Assessment of Incident
- Prompt Notification to Feds
 - *Unauthorized Access*
 - *Use of Sensitive Member Information*
- Notify Law Enforcement & SARS
- Contain & Control & Preserve
- Notify Members-“When Warranted”



Are You Ready for Multi-Factor?

- What is it?
 - *More than a password/passphrase*
 - *Authentication*
 - *Layered Security*
 - *Controls*
- What are my options?
 - *Do Nothing!*
 - *Have a Plan!*
 - *Implement Solution!*



Are You Ready for Multi-Factor? (cont.)

- What is Compliance?
 - *Risk Assessment*
 - *Plan Based On Risk Assessment*
 - *Implementation Best Efforts*
- What are Best Practices?
 - *Policies*
 - *Training*
 - *Technology*
 - *Monitoring & Reporting*



Compliance Tips

- Set Up Framework
- Understand Requirements
- Create Policies
- Risk Assessment
- Processes, Controls, Training, Technology
- Monitoring, Reporting, & Enforcement
- Management Involvement
- Independent Review

Resources

- NCUA - www.ncua.gov
- FFEIC - www.ffeic.gov
- FDIC - www.fdic.gov
- Pivot Group - www.pivotgroup.net





Questions and Answers

Laura King

LauraK@LGEFCU.org

770-421-2612

Jim Soenksen

jsoenksen@pivotgroup.net

404-668-6734

THANK YOU!