



Safe
Systems



Compliance Tips, Tricks and Trends for 2011

Presented By:
Tom Hinkel, Director of Compliance
Safe Systems, Inc.

Agenda

- Regulatory Hot Buttons
- Audit & Examination Trends
- Policy Updates

Lessons Learned

- Sources
 - Pre-audit, pre-examination assistance
 - Post-audit, post-exam support
 - Customer survey – 11/10
 - Auditor survey – 1/11
 - Compliance Advisory Committee
 - FFIEC, ISACA, IACPA, COBIT

Hot Buttons

DR/BCP - Compliant

1. Business Impact Analysis
 - Recovery Time Objective
 - Recovery Point Objective
 - Interdependencies
2. Risk Assessment
 - Impact
 - Probability
3. Process Recovery Procedures
4. Maintenance & Testing

Hot Buttons

DR/BCP - Recoverable

- Testable
 - Do test recovery objectives follow BIA?
 - Do test scenarios follow RA?
 - Process recovery NOT system recovery
- Tested
 - Increasingly complex scenarios
 - Gap analysis between RTO and actual recovery capability

Process Recovery NOT System Recovery

*“The business continuity planning process involves the recovery, resumption, and maintenance of the entire business, **not just the technology component**. While the restoration of IT systems and electronic data is important, recovery of these systems and data will not always be enough to restore business operations.”*

- FFIEC Business Continuity Planning Booklet - March 2008

Trends Dodd-Frank

- Enacted July 21, 2010
- Requires 243 rulemakings and 67 studies
- “Systemically important”
 - \$50 billion or more in consolidated assets
- Compliance may be required for non-systemically important financial companies
 - “Source of financial strength” doctrine for holding companies
 - Risk Committees
- OTS eliminated

Dodd-Frank – Risk Committees

Risk Committees at Public Companies (effective by October 21, 2012)

- The Act requires risk committees for systemically important, publicly traded nonbank financial companies, as well as any publicly traded bank holding companies with total consolidated assets of \$10 billion or more. The Federal Reserve may impose the requirement on publicly traded bank holding companies with less than \$10 billion in assets as necessary or appropriate to promote sound risk-management practices. **Risk committees must have the number of independent directors as determined by the Federal Reserve, and include 1 risk management expert having experience in risk management at large complex companies.***

Trends

Director Responsibilities

- Recent FDIC MOU

(b) Within 60 days from the effective date of this ORDER, the Board shall establish a compliance committee comprised of at least 3 directors who are not active officers of the Bank and at least 3 members of senior management, including the Compliance Officer (“Compliance Committee”).

(i) The Compliance Committee shall meet no less frequently than monthly at which, at a minimum, the following areas shall be reviewed and approved: minutes of the Compliance Committee, Compliance Officer

Trends

Regulatory Consolidation

- Memorandum of Understanding, July 2010 - FDIC, OCC, OTS, FRB

Interagency Memorandum of Understanding on Special Examinations

This Memorandum of Understanding (“MOU”), dated as of July __, 2010, is made and entered into by and among The Federal Deposit Insurance Corporation (“FDIC” or the “Corporation”), the Office of the Comptroller of the Currency (“OCC”), the Board of Governors of the Federal Reserve System (“FRB”), and the Office of Thrift Supervision (“OTS”) (the OCC, FRB and OTS collectively, the “Agencies;” and separately, the “BER”). This MOU concerns the implementation of Section 10(h)(3) of the Federal

Deposit Insurance Act that provides that examiners appointed by the Board of Directors of the Corporation “shall have power, on behalf of the Corporation, to make any special examination of any insured depository institution whenever the Board of Directors determines a special examination of any such depository institution is necessary to determine the condition of such depository institution for insurance purposes.”

Trends

Regulatory Consolidation

- Memorandum of Understanding, July 2010 - FDIC, OCC, OTS, FRB

V. CAMELS Rating Differences

Differences in CAMELS ratings between the FDIC and the appropriate PFR will be communicated by the FDIC Contact to the PFR Contact in writing, including an explanation of the basis for the FDIC's position. In the event those officials are unable to resolve the ratings disagreement, the matter shall be referred to the Director of the FDIC Division of Supervision and Consumer Protection (the "Director") (or other officer of the Corporation designated by the Chairman of the FDIC) and the appropriate senior-most supervision official of the PFR for resolution. Any decision by the FDIC to depart from the appropriate PFR's assigned rating will be made by the Director of the FDIC Division of Supervision and Consumer Protection (or other officer of the Corporation designated by the Chairman of the FDIC) after consultation with the Chairman of the FDIC.

Dodd-Frank

“Source of Financial Strength”

- “A company that directly or indirectly controls an intermediate holding company established under this section shall serve as a **source of strength** to its subsidiary intermediate holding company.”
- Separate provision limits the obligation for holding companies to serving as a “**source of financial strength**” to its depository institution subsidiaries.

Dodd-Frank OTS Eliminated

Elimination of the OTS

- Initially, the Treasury proposed consolidating all prudential regulatory authority over federally-chartered depository institutions under one agency, but the Act instead dissolves the OTS and redistributes the agency's powers among the Federal Reserve, the OCC and the FDIC.
- OTS Institutions will adopt the Safety & Soundness expectations of the new PFR.

Trends

- Across the board increase in overall scrutiny by examiners
 - State examiners adopting FDIC IT pre-examination questionnaire
 - OTS doubled the size of the PERK
 - CUNA soliciting examination complaints from NCUA members
 - FIL-13-2011 – Examination findings “overly harsh”



Trends Outsourcing

- Social Media
- Cloud Computing
- Hosted Services
- Mobile Banking
- Merchant Services
 - Merchant Capture
 - Remote ACH
 - Wire Transfer



Trends

Outsourcing

- FFIEC stated in their 2004 Outsourcing Handbook: ***“In many situations, outsourcing offers the institution a cost effective alternative to in-house capabilities.”***
- ***“Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the financial institution were conducting the activities in-house.”***

Trends Outsourcing

Must review:

- Key service level agreements (SLAs) and contract provisions **prior to and periodically;**
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and review of audit reports (SAS 70) and other internal control reviews.

Trends

Outsourcing

- **Bank Service Company Act** - Requires financial institutions to report all service provider relationships that directly support banking functions.
 - *Has the bank identified and reported its service provider relationships (both domestic and foreign-based) to the FDIC (Y/N)?*



Trends

Outsourcing

- **Bank Service Company Act** - services include *"check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution."*

Trends

Outsourcing

Don Saxinger, Senior Examination Specialist with the FDIC, 10/2010 interview:

- "business function" versus outsourcing an IT function?
 - "...we consider them both on our same risk ranking process. So, business function, IT processing, they sort of go hand in hand. In fact, we look at IT as simply one of the layers to support a business process."

Trends

Outsourcing

To Report or Not?

- “I would look at it from a banking function perspective. If this is a function of the bank, where somebody is performing some service for you that is a banking function or a decision-making function, including your operations and your technology and you have outsourced it, then yes, **that would be a technology service that is reportable.**”



Safe
Systems

“Notification of Performance of Bank Services”

OMB NUMBER: 3064-0029
EXPIRATION DATE: 11/30/2011

Federal Deposit Insurance Corporation
NOTIFICATION OF PERFORMANCE OF BANK SERVICES

Name and Address of Bank *(Include Street, City, State and ZIP Code)*

Name and Address of Regional Director *(Mail to the appropriate Regional Director (DSC) for your institution.)*

┌

┐

└

┘

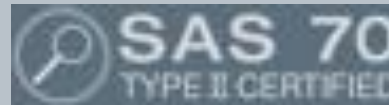
In compliance with the requirement of the Bank Service Company Act, we hereby notify the Federal Deposit Insurance Corporation of bank services provided by the servicer reported below.

Corporation Title of Servicer

Location of Premises Where Services Are Performed

Trends

SAS 70 Phase-out



Trends

SAS 70 Phase-out

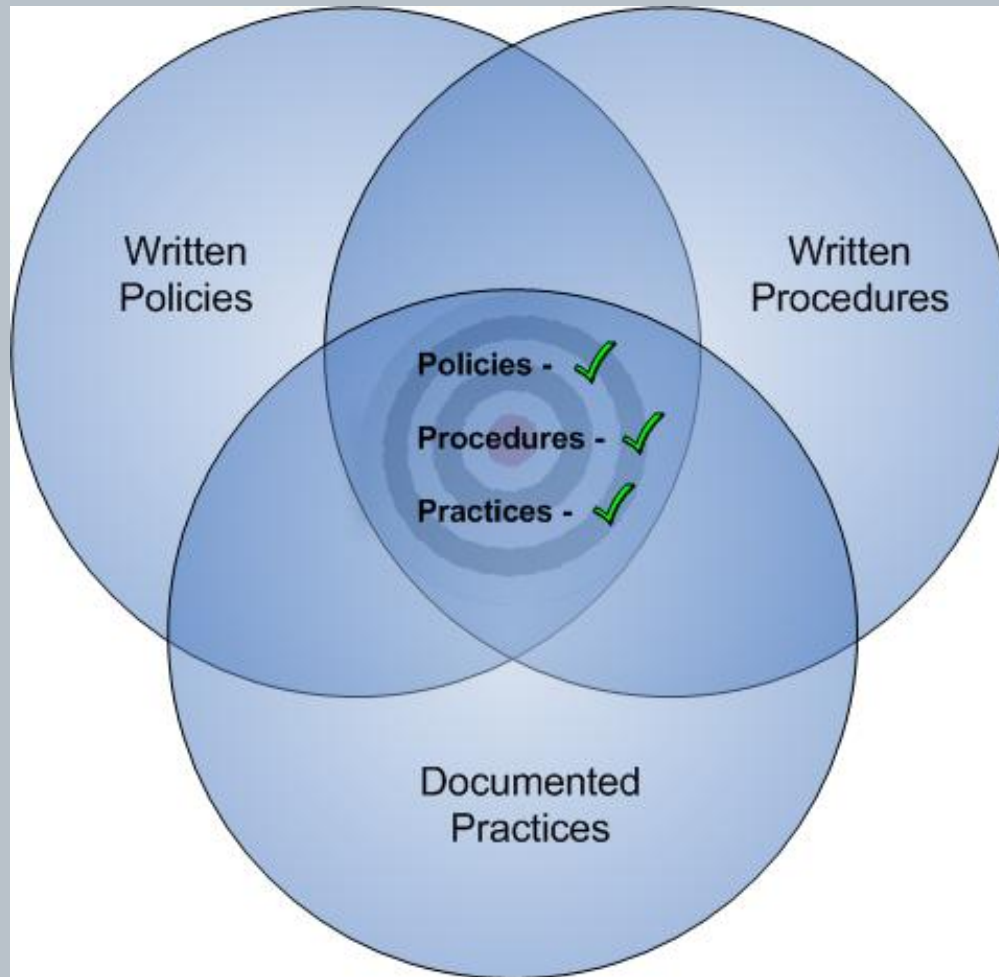
- IACPA - 6/2011 (early adoption encouraged)
- Replaced by SSAE 16
 - SOC 1 – SAS 70 functional replacement for ICFR reviews
 - SOC 2 – Servicing Institutions (non-ICFR)
 - Privacy
 - Security
 - Confidentiality
 - Availability
 - Integrity
 - SOC 3 – Management attestation

✓ Turn off auto pilot!

Lessons Learned in 2010

- Overwhelming emphasis is still on asset quality, but IT examination scrutiny increasing.
 - Shift from CAMELS “A” to “M”
- PFR’s are modifying their pre-examination questionnaires.
 - State regulators adopting FDIC questionnaire
 - OTS 10 page, 128 question questionnaire
- ✓ **Documentation is key**

Lessons Learned in 2010 - Documentation



Lessons Learned in 2010

- ✓ Tech Steering Committee
 - Involve all departments
 - Outside expertise
 - Use standard agenda
 - Track issues to resolution
 - Minutes

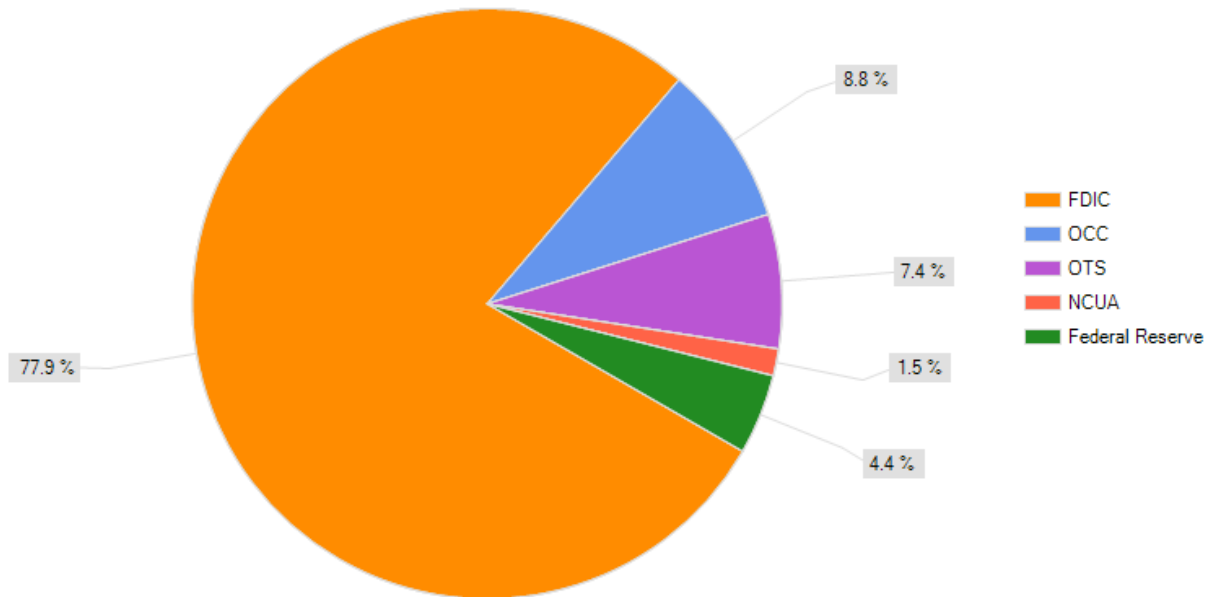
Customer Survey

2010 Customer IT Examination Questionnaire

- Q4 2010
- 12 questions, 68 responses
- Recent examination experience

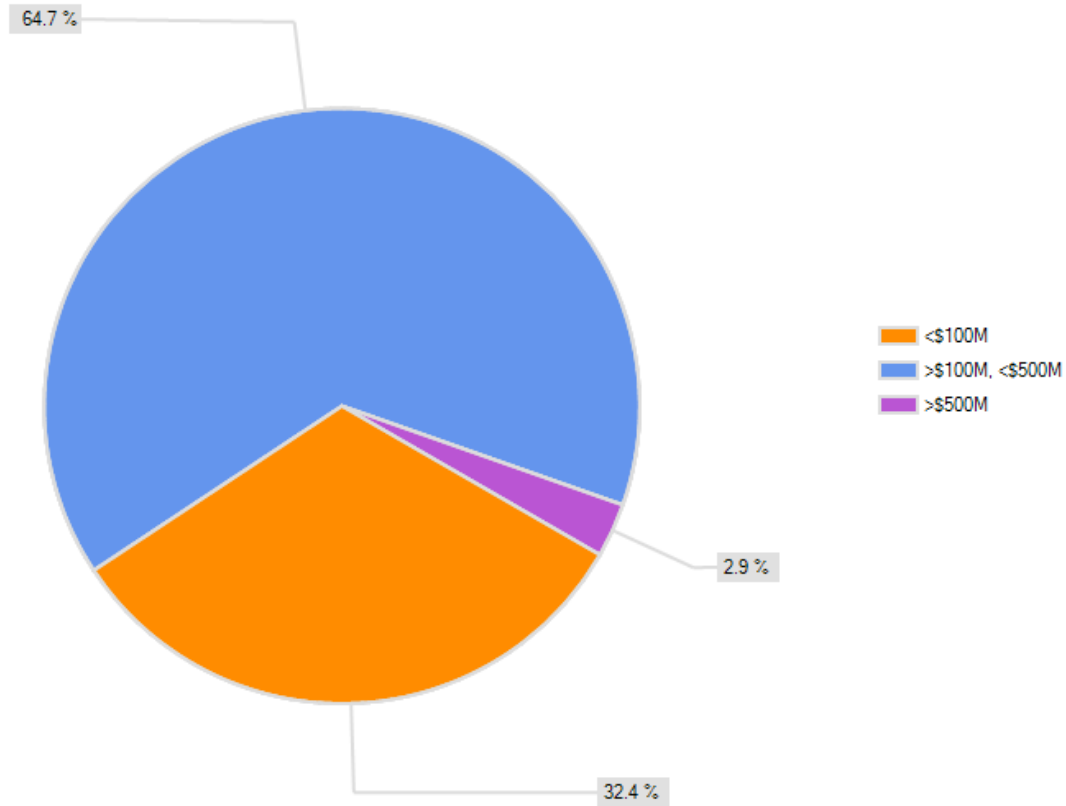
Customer Survey

Who is your primary federal regulator?



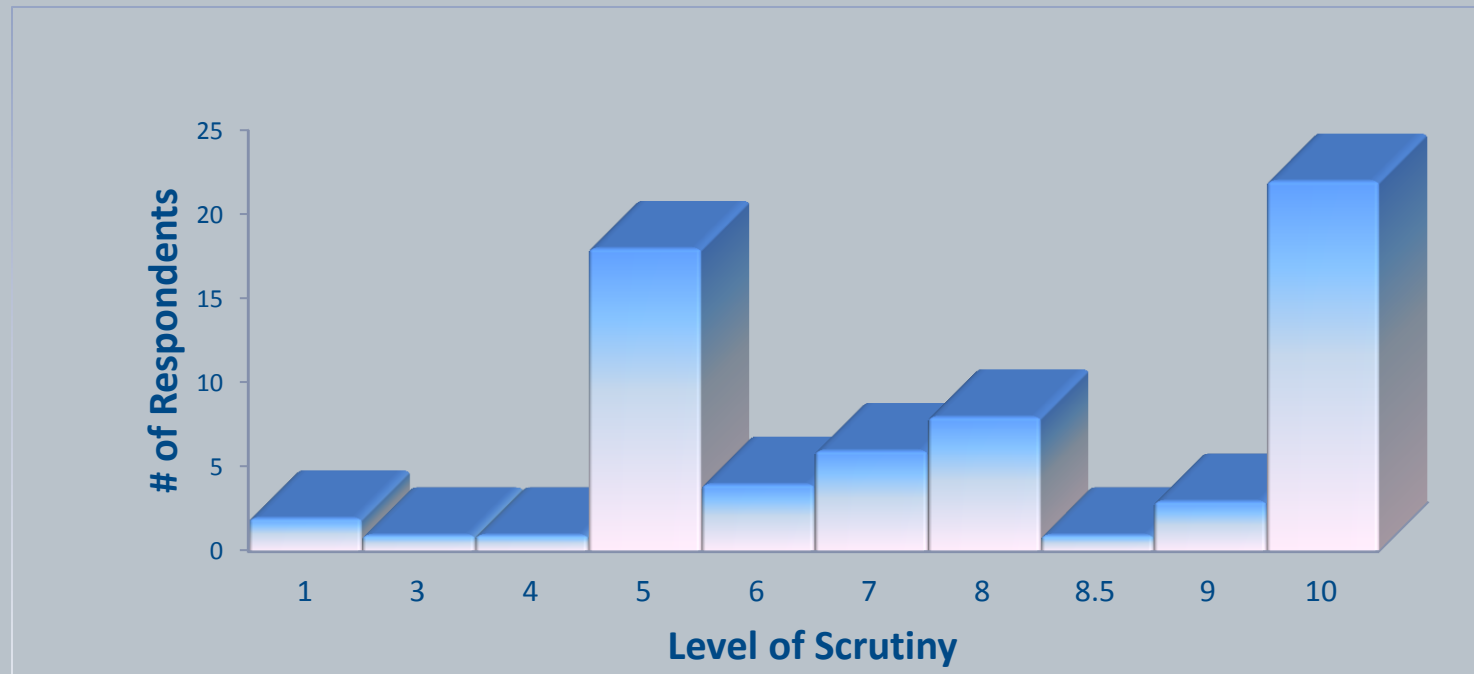
Customer Survey

What is your asset size?



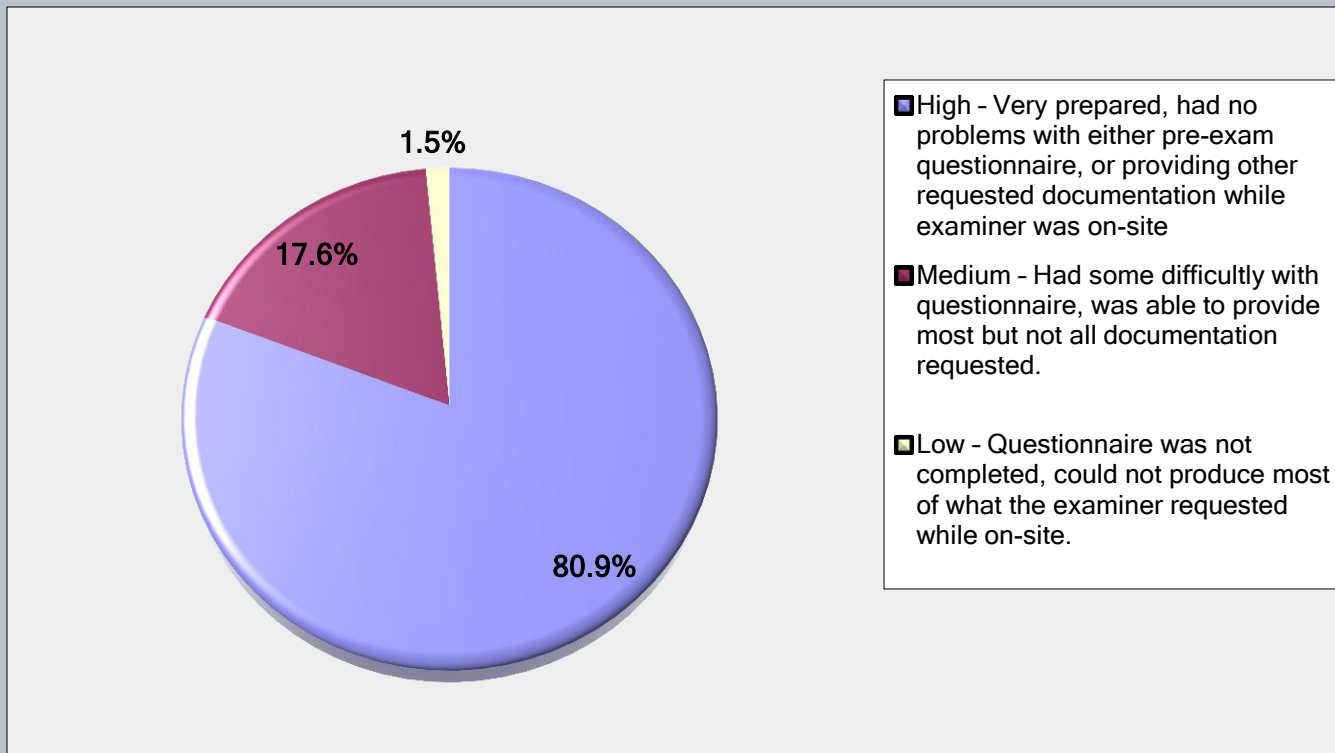
Customer Survey

- During your last examination, how would you describe the overall level of examiner scrutiny on a scale of 1 to 10?



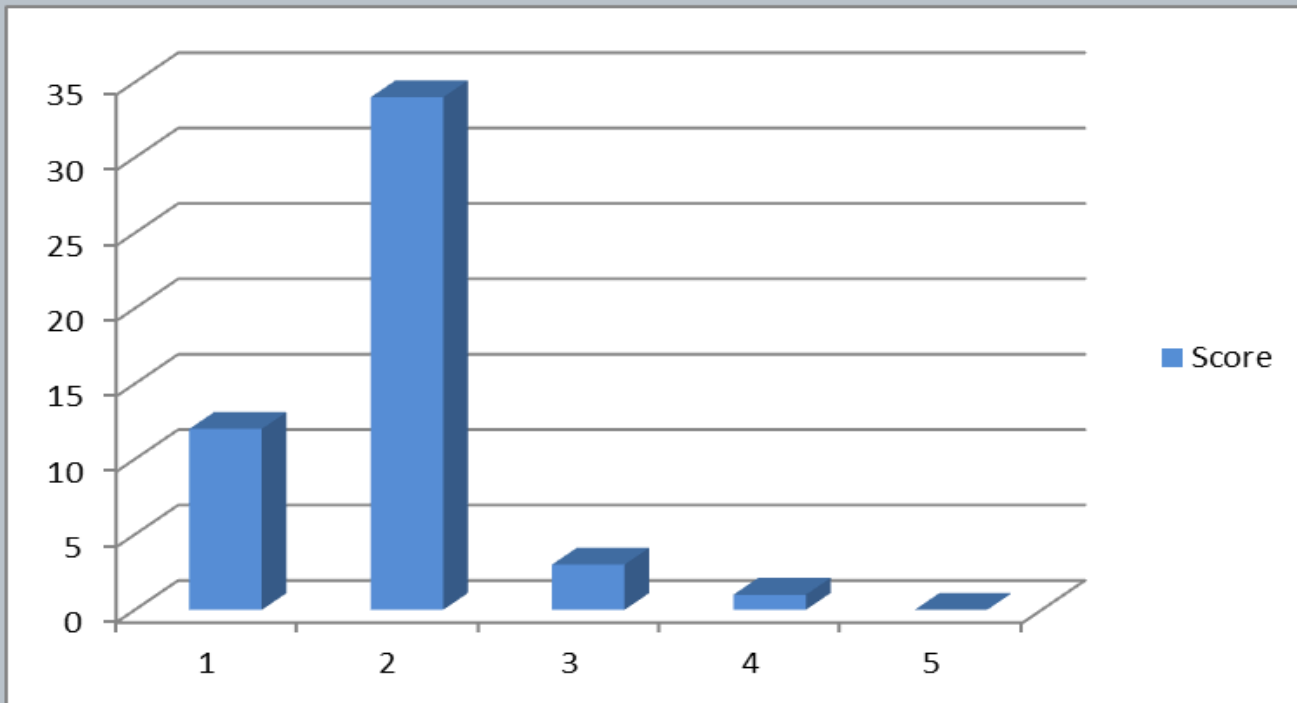
Customer Survey

- How would you describe your level of preparedness going into your last examination?



Customer Survey

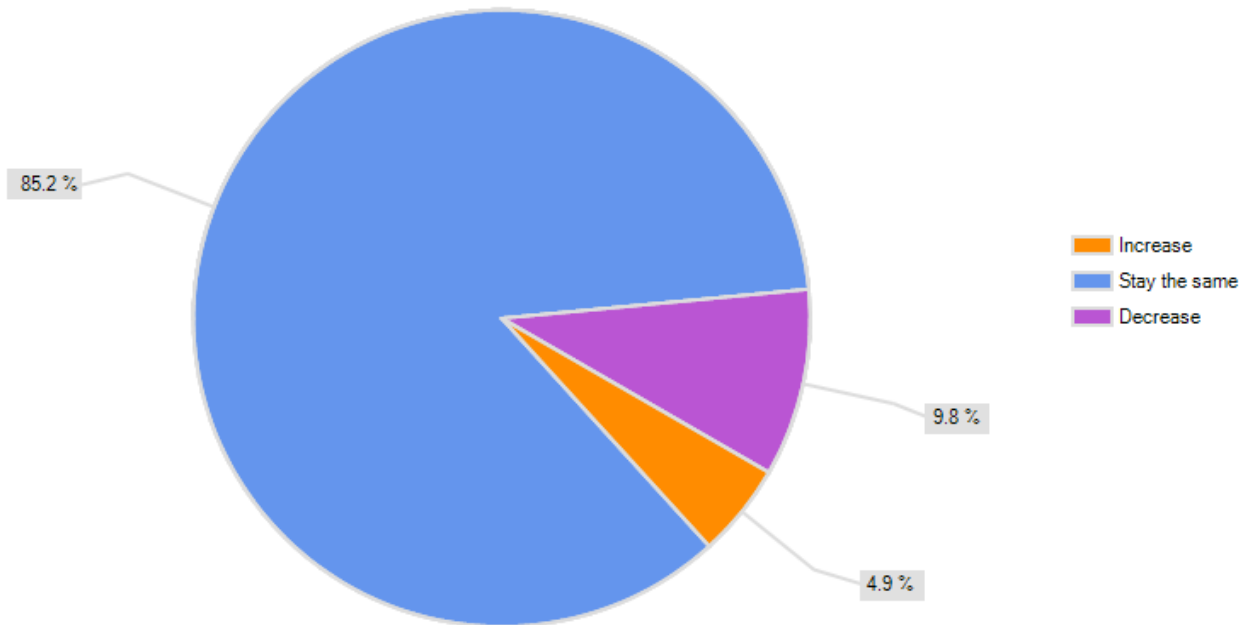
- What was your IT Composite rating? (1, 2, 3, 4, 5)



Average – 1.86

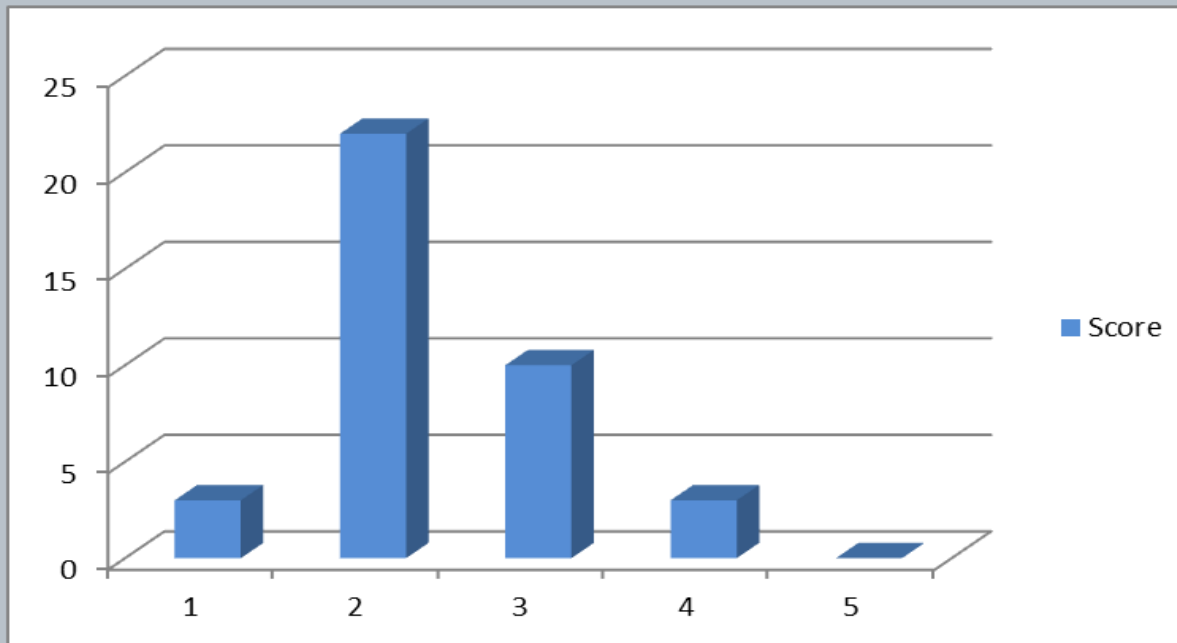
Customer Survey

Did your IT Composite rating:



Customer Survey

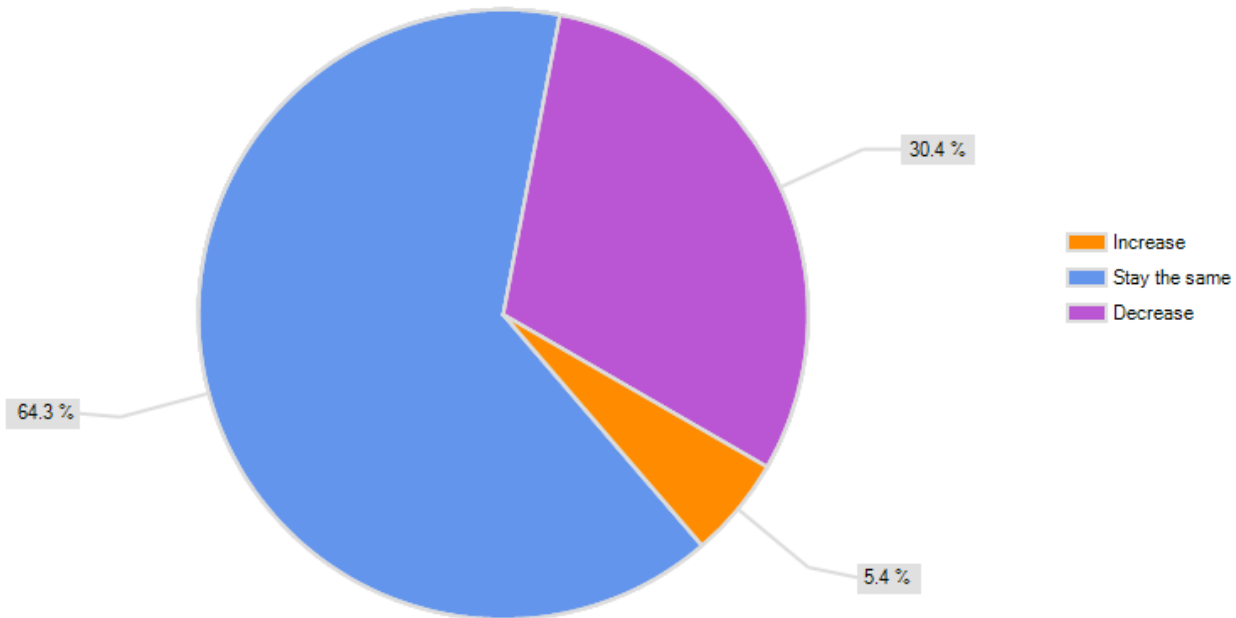
- What was your Safety and Soundness/Risk Management Composite rating? (1, 2, 3, 4, 5)



Average – 2.34

Customer Survey

Did your Safety and Soundness / Risk Management rating:



Auditor Survey

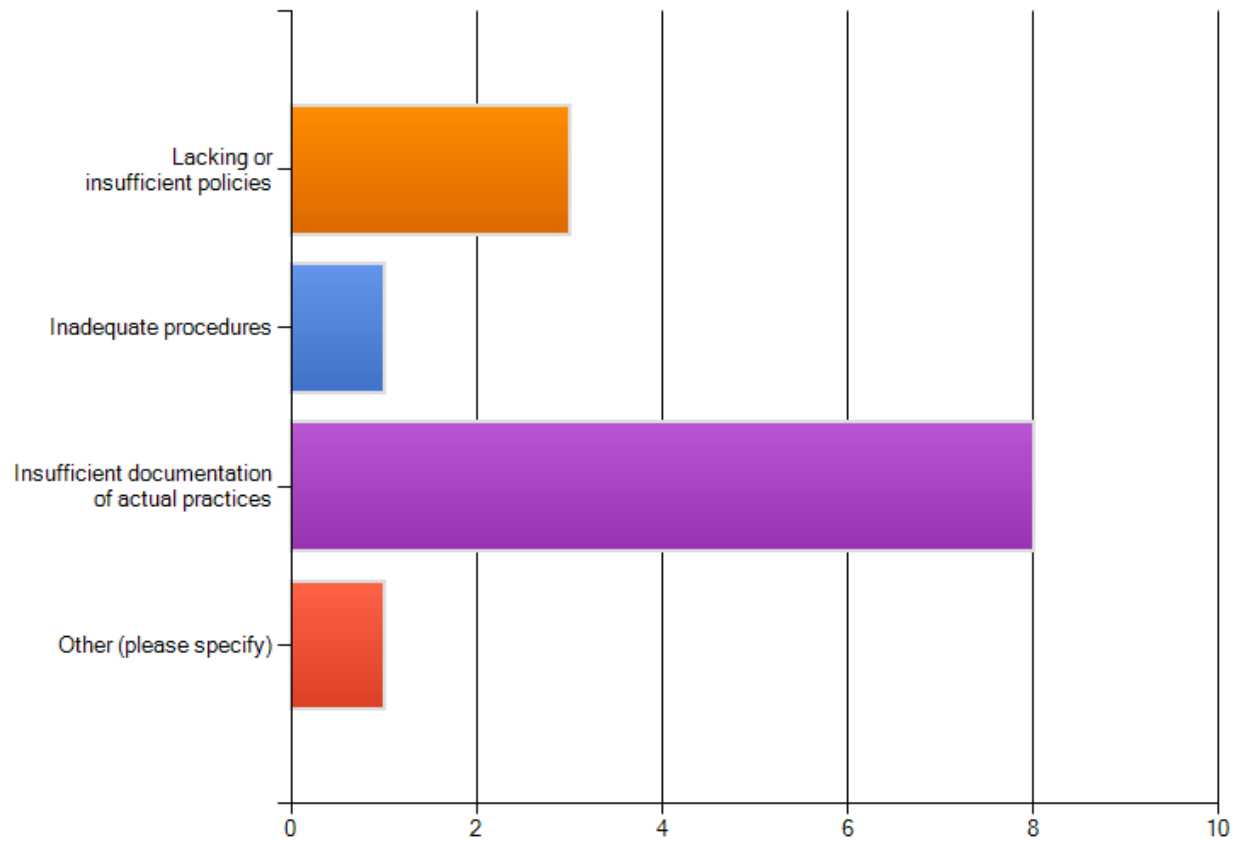
- Audit & Examination - 2010 Experience & 2011 Trends
 - January, 2011
 - 13 IT auditors and 1 examiner surveyed on 2010 experience and 2011 expectations.
 - 11 questions total.

Auditor Survey

- During the past year, in which category would you say MOST of your IT audit/exam findings occurred?
 - Lacking or insufficient policies
 - Inadequate procedures
 - Insufficient documentation of actual practices

Auditor Survey

During the past year, in which category would you say MOST of your IT audit/exam findings occurred?

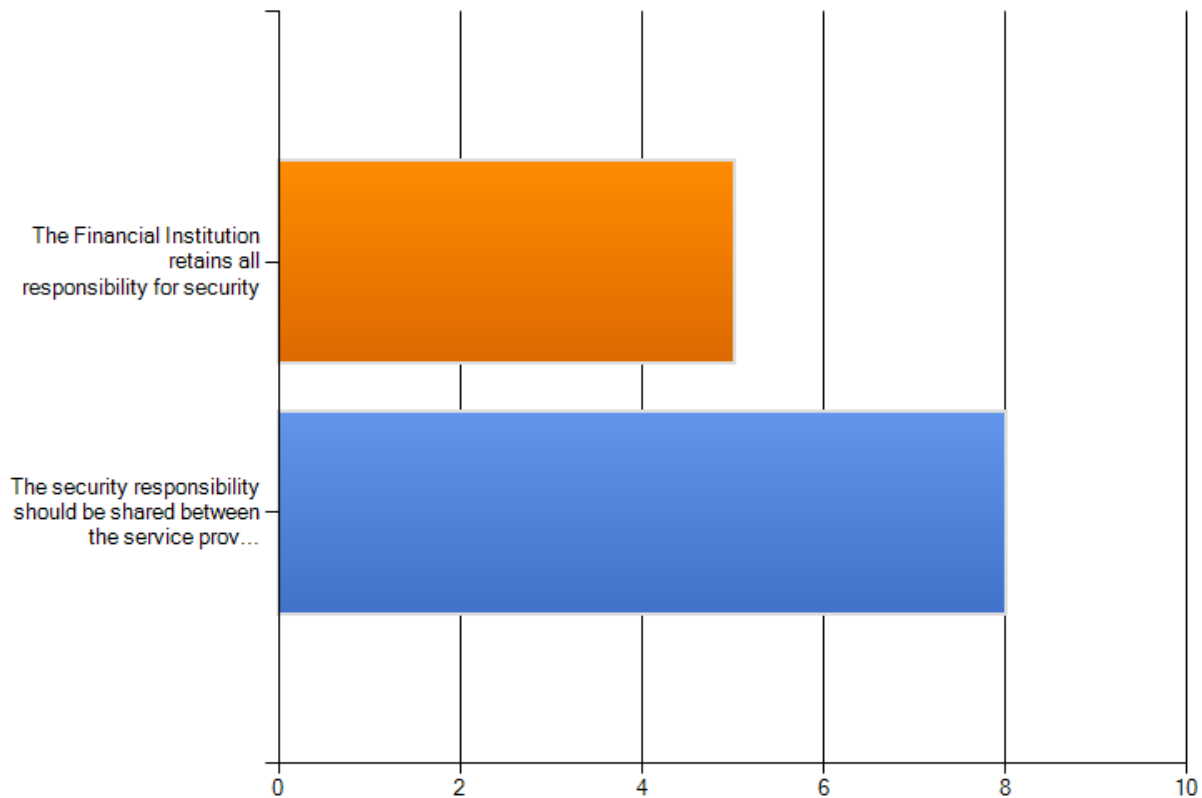


Auditor Survey

- With regard to electronic banking services provided by third parties, how do you draw the line between the security responsibilities of the third party and the security responsibilities of the Institution?
 - The Financial Institution retains all responsibility for security
 - The security responsibility should be shared between the service provider and the Institution

Auditor Survey

With regard to electronic banking services provided by third parties, how do you draw the line between the security responsibilities of the third party and the security responsibilities of the bank?

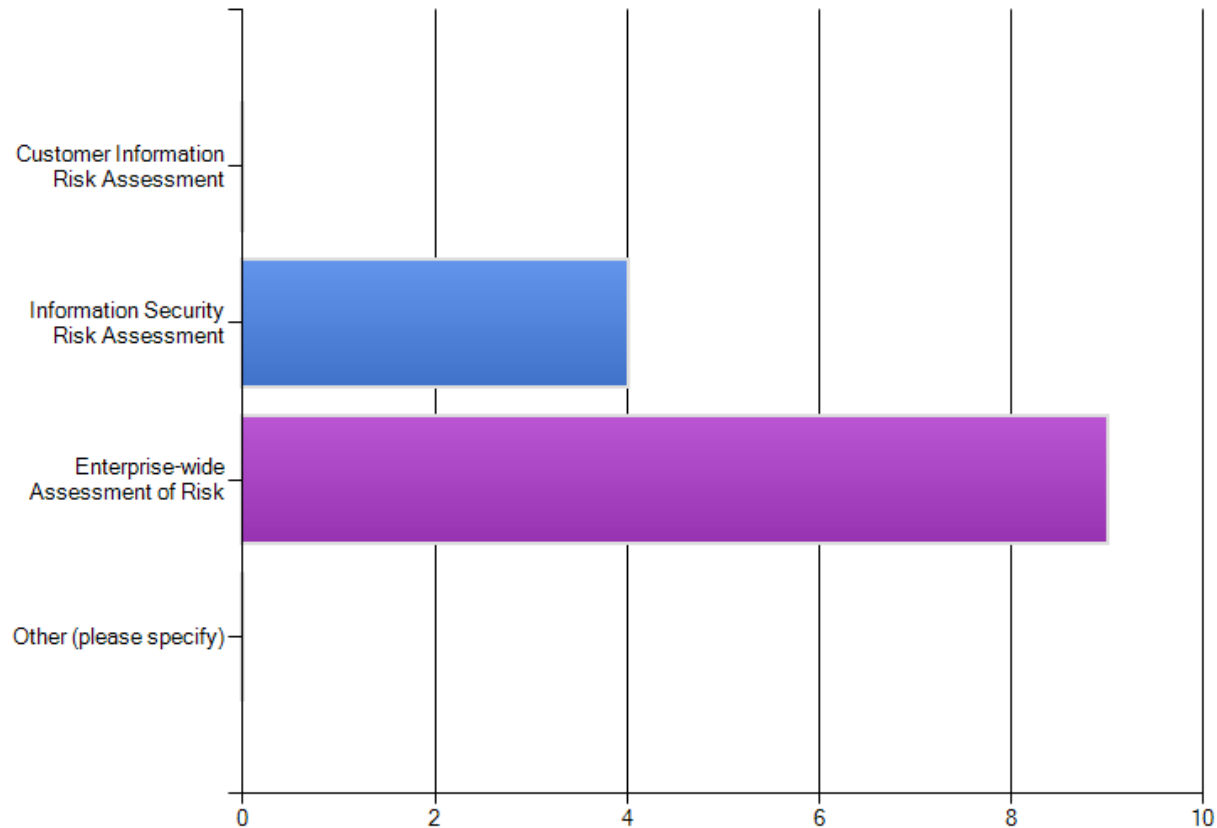


Auditor Survey

- What is the current regulatory expectation and standard for documenting the assessment of risk?
 - Customer Information Risk Assessment
 - Information Security Risk Assessment
 - Enterprise-wide Assessment of Risk

Auditor Survey

What is the current regulatory expectation and standard for documenting the assessment of risk?



Regulatory Changes in 2011 – Up Next...

- New FFIEC Authentication Guidance
 - Update to 2005 *“Authentication in an Internet Banking Environment”*
 - *OOB-MFA*
 - *“Out-of-Band” + Multi-Factor Authentication*

Questions?



www.FFIECguru.com
www.safesystems.com

Tom Hinkel, CISA, CRISC
Director of Compliance, Safe Systems, Inc.
tom@safesystems.com