



Risk Oversight

The Newest Mantra for ALL Board Members

November 13, 2009
San Francisco, CA

Ken Proctor
Brintech, Inc.
(800) 929-2746
KProctor@Brintech.com
<http://www.brintech.com>

Atlanta * Austin * Orlando * Los Angeles



Example - “ABC” National Bank

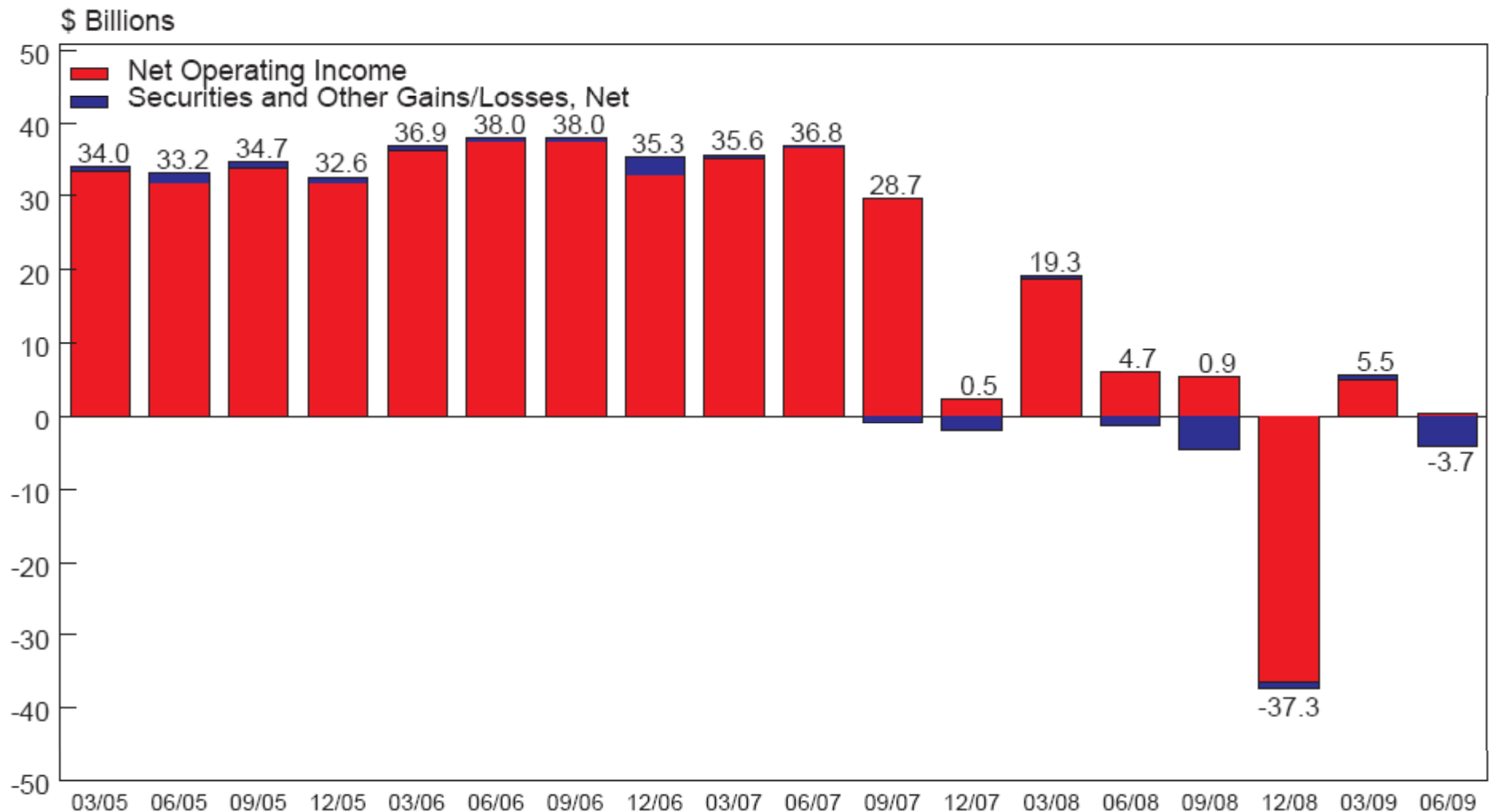
- 1 Rated Bank after OCC exam
- 21 months later - 4 Rated Bank by OCC
- 8 months later - Operating under an MOU with the OCC
- Next month - New Senior Lender
- 5 months after that - New President...and
- 2 months later - Directors paid Civil Money Penalties

***What
Happened??***

Agenda

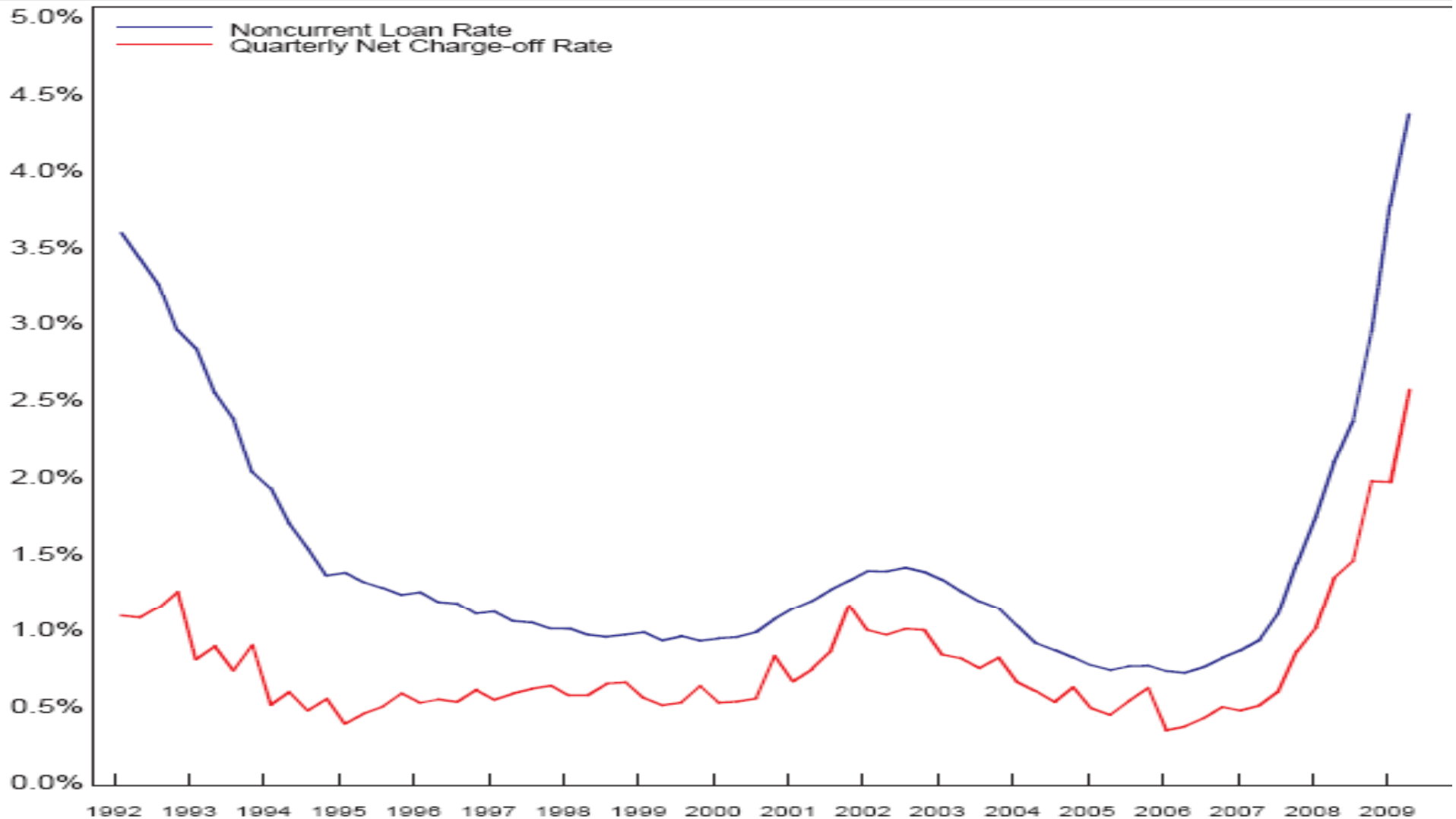
- Review current risk issues
- Cover risk management basics
- Discuss enterprise risk management approach

Earnings Decimated by Loss Provisions



Source: FDIC Quarterly Banking Report, 2nd Quarter 2009

Credit Cycle Turned In 2007




Source: FDIC Quarterly
Banking Report, 2nd
Quarter 2009

2005 OCC Underwriting Survey

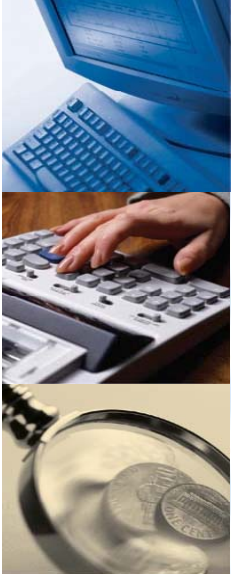
- Pronounced trend toward easing commercial credit standards in 2005, with significantly more banks easing underwriting standards than tightening standards.
- OCC reported **34 percent of banks eased**, 12 percent tightened, and 54 percent made no change to commercial underwriting standards.
- Easing trend **began modestly in 2004**
- Last time examiners reported more banks easing credit standards than tightening standards was in **1998, when 44 percent of the banks eased commercial standards** (and problems resulted 2 ½ years later)

Credit Risk Increased

- On average, community banks have over 200% of risk based capital in commercial real estate loans
- Core deposits in community banks have declined from 82% of average total assets in 1984 to 65% in 2008
- Wholesale funding increased from 5.5% of average total assets to 10% at community banks with 300% of risk based capital in CRE

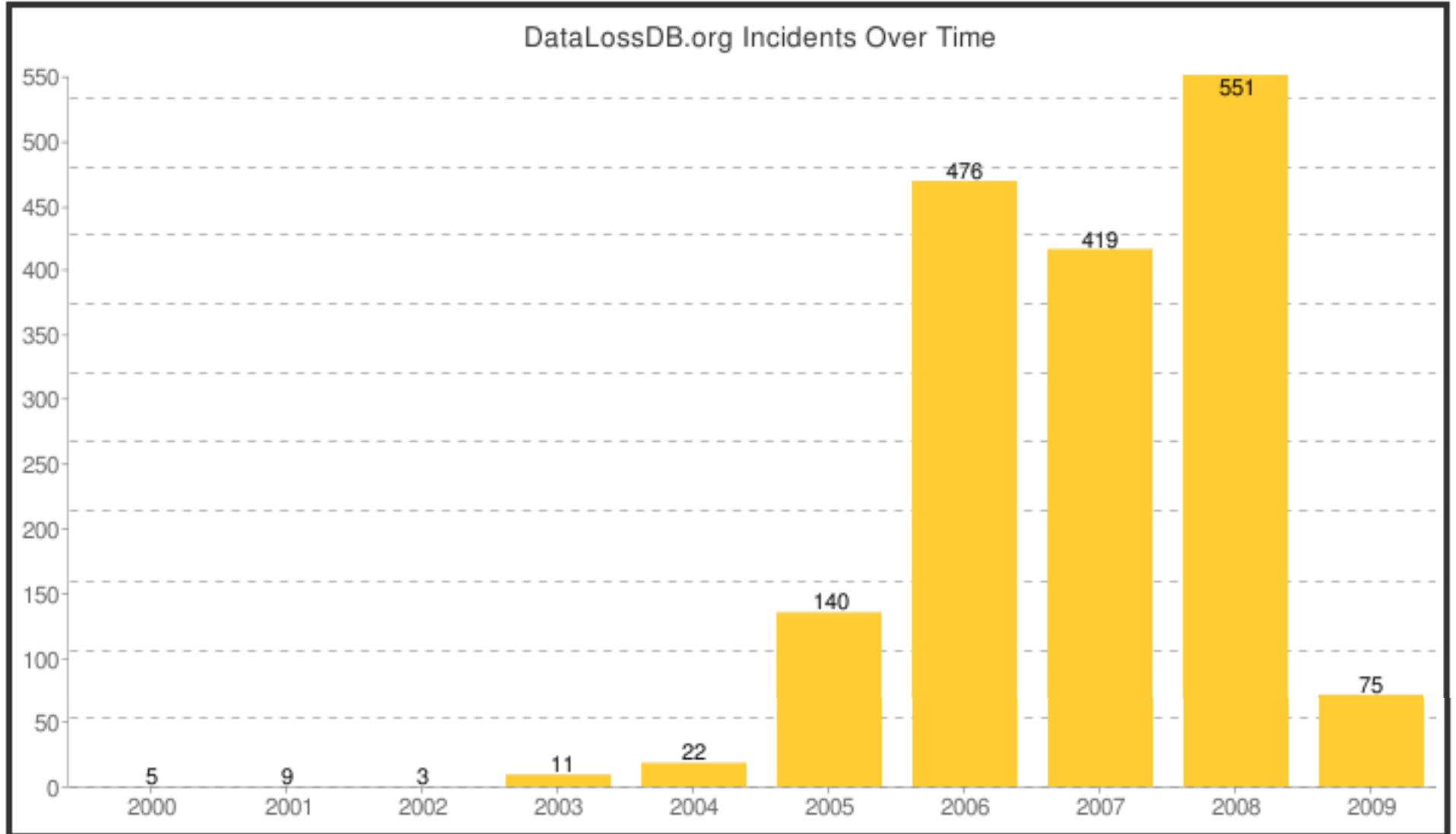


And Credit Risk is not the
only category of
increasing risk



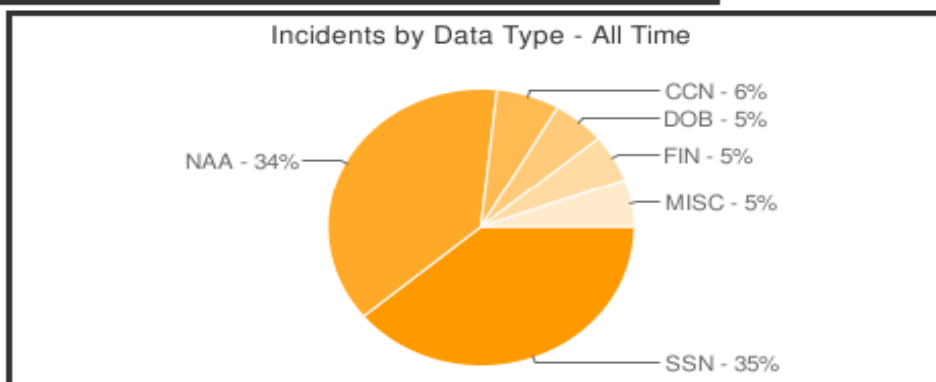
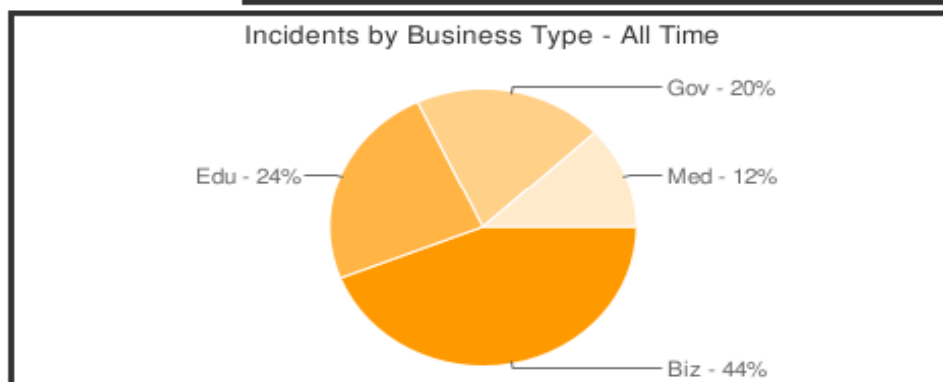
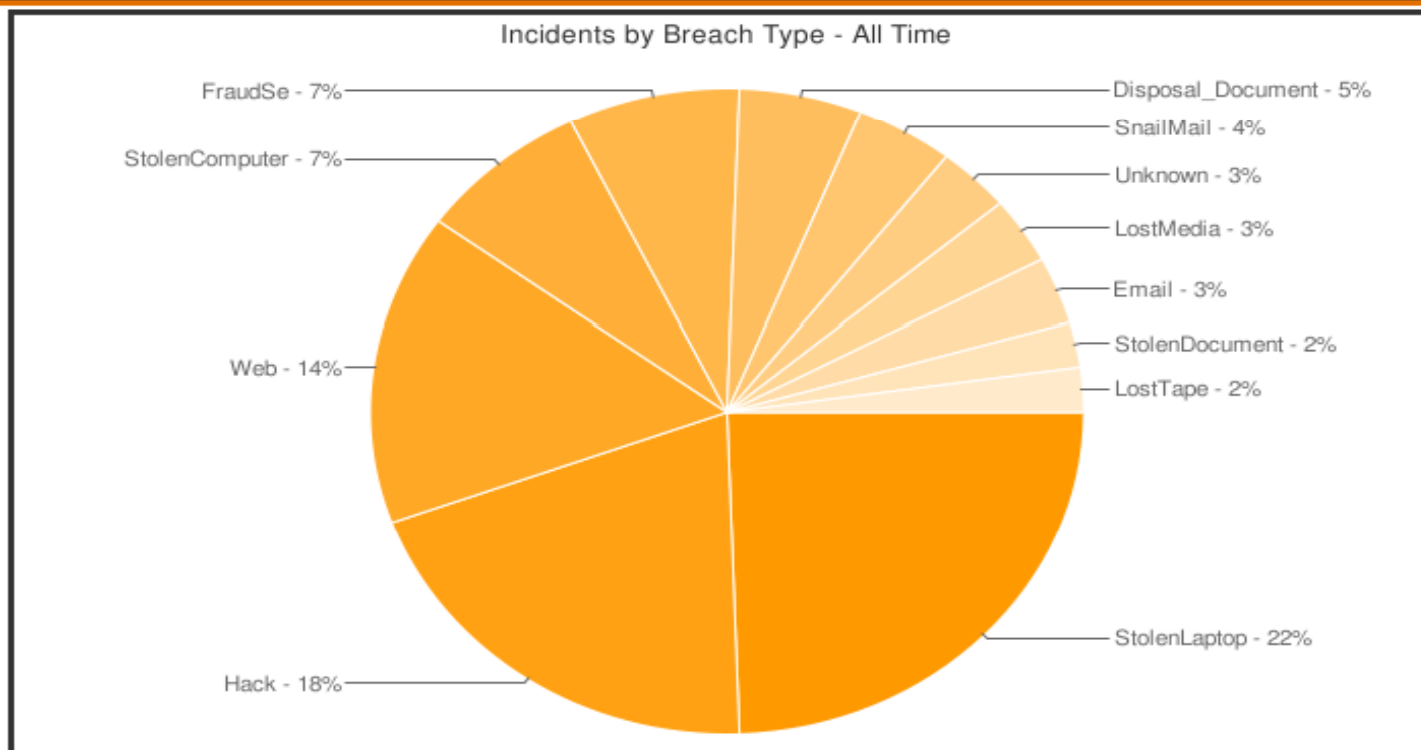
Incidents of Data Loss

NUMBER OF INCIDENTS



DataLossdb.org Stats

TYPES OF INCIDENTS

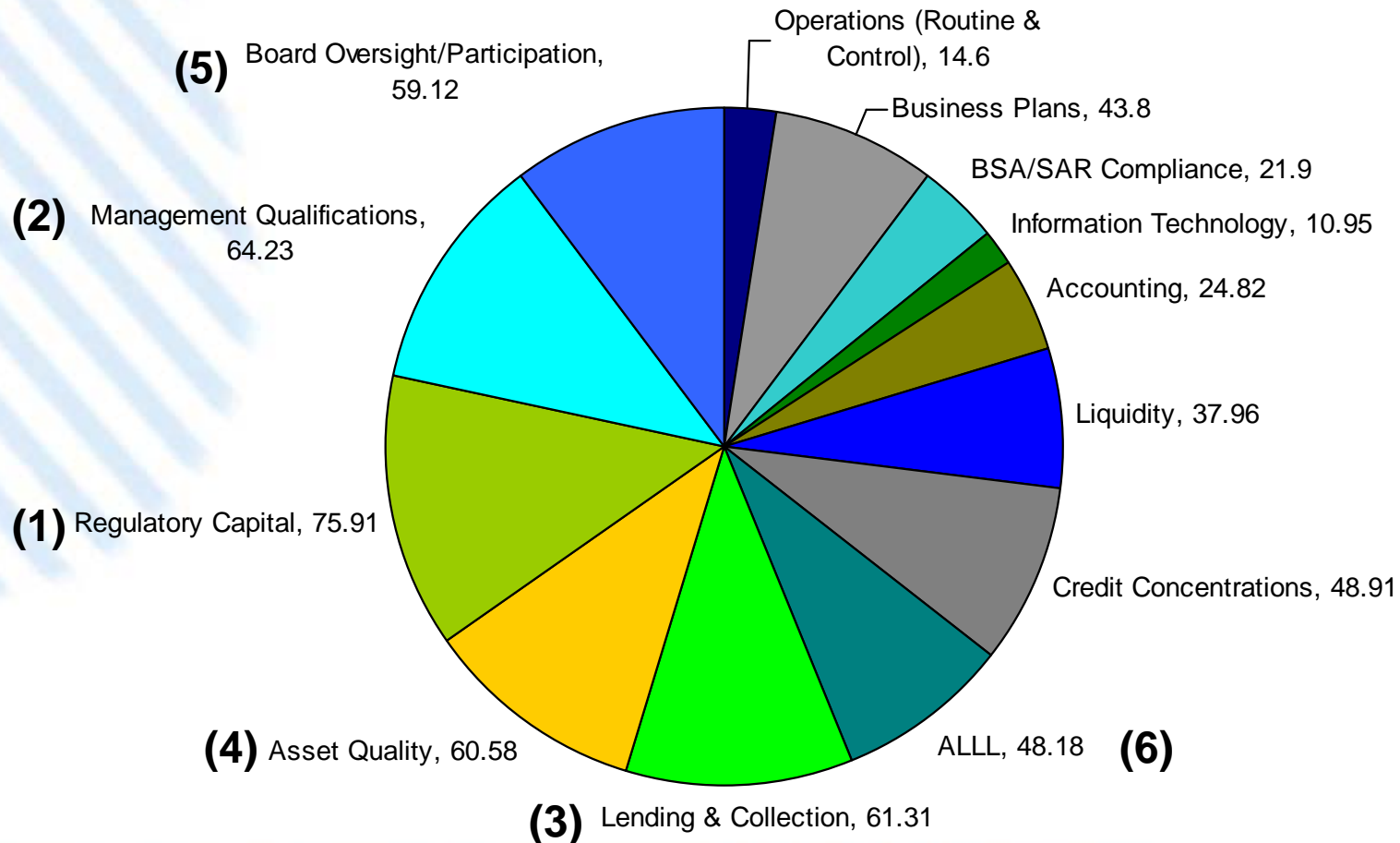




Compliance Risks

- Regulators continue to focus on BSA, HMDA, Flood and Compliance in general
- SOX now applying to non-SOX banks??
- Management concerned about compliance risk and costs

Total Formal Regulatory Orders Frequency of Matters



Regulatory Risk Management Requirements

- Financial institutions should implement a comprehensive program designed to:
 - Identify
 - Measure
 - Monitor and
 - Control risk Across a spectrum of risks

COSO II Enterprise Risk Management

A process, effected by an entity's Board of Directors, management and other personnel, that is ***applied in strategy setting*** and ***across the enterprise***.

Its goal is provide ***reasonable assurance regarding the achievement of organizational objectives*** by identifying events that may affect the entity and managing risk to be within the entity's risk appetite.

Brintech Enterprise Risk Solution

Company Goals/Objectives:

- Strategic Plan
- Technology Plan
- Operating Budget
- Regulatory Requirements

Risk Identification & Measurement:

- Inherent Risk Assessment
- FDICIA Risk Assessment
- Product Risk Assessment
- Vendor Risk Assessment
- Economic Studies
- Examinations/Audits
- Loan Review
- Compliance Audits/Exams
- In-House and Outside Legal Review of contracts & product documents

Risk Monitoring:

- Board/Committee Reports tied to Policy limit guidelines (Financial/Loan, etc.)
- EVE(Rate Shock) Analyses
- GAP Analyses
- Investment Market Value Reports
- Management reports highlighting exceptions (Budget to Actual, Period-to-Period, other)
- Examination & Audit Reports
- Loan Review Report
- Classifieds & Watchlist
- KRI and KPI

Risk Control:

- Documented Procedures
- Separation of duty controls
- Accounting Procedures - Counts, Reconcilements,
- Credit Analysis Methods/Tools
- Transaction Limits
- Disbursement Limits
- Documentation Review, File and Follow-up
- Contractual Warranties & Indemnification
- Insurance Coverage

General Control Environment:

- Board Structure/Experience
- Board Policies
- Management Structure/Experience/Philosophy
- Organization Structure, Adequacy of Staff
- Segregation of Functional Responsibilities
- Personnel Experience
- Physical/Information Security Programs

* Program based on the COSO model of control

** See FDICIA Risk Assessment and Controls Evaluation for more detail



Implementing ERM – Five Steps

1. Assess inherent risk and the risk trend
2. Review management policies and ensure that they incorporate appropriate risk exposure limits
3. Prepare an inventory of specific risk and exposures
4. Evaluate risk management strategies and controls and develop a Plan, incorporating risk management into business processes
5. Develop a risk management information reporting system

Step 1 – Assess Inherent Risk

- Inherent risk results from business choices (e.g. buying mobile home loans)
- Inherent risk exists in each line of business, regardless of the level or management control in place
- Inherent risk level may change with changes in the economy and other non-controllable factors
- Having a high degree of inherent risk is not necessarily negative, nor is having a low level of inherent risk necessarily positive
- The Bank's strategic business objectives help determine what is an acceptable level of inherent risk
- The level of inherent risk implies the risk strategies to be employed, and controls and monitoring procedures to be used (e.g., riskier approaches/more monitoring/more control)

Assessing Inherent Risk/Trends

- What has the Banking industry's loss experience been in each category of risk over the last 3-5 years? (5- High, 3-Moderate, 1-Low)
- Have losses been increasing or decreasing over the past five years? (5-Increasing, 1-Decreasing)
- Can exposure to potential individual losses be predicted with reasonable accuracy? (5-Low, 1-High)
- What would be the impact of a significant change in the economy? (5=Significant impact, 1=Limited impact, 0=No impact)
- Does the Bank have the ability to insure, transfer or otherwise mitigate risk? (5=Limited ability, 1=Significant ability)
- Is there significant regulatory scrutiny given to each risk category? (5=Significant, 1=Limited)

Step 2 - Review Management Policies

- Key policies prepared, current and approved by the Board
- Include risk tolerances appropriate to the inherent level of risk and strategic objectives of the Bank
- Contain contingency plans or call for remedial actions when risk tolerances are exceeded

Step 3 - Inventory Risks & Exposures

- Risk mapping:
 - Business process mapping
 - Interviews/questionnaires
 - Self assessment teams
 - Risk Control Self Assessments
- Begin tracking “event” and “result” data - transaction volumes, losses, other measurable information that can be correlated

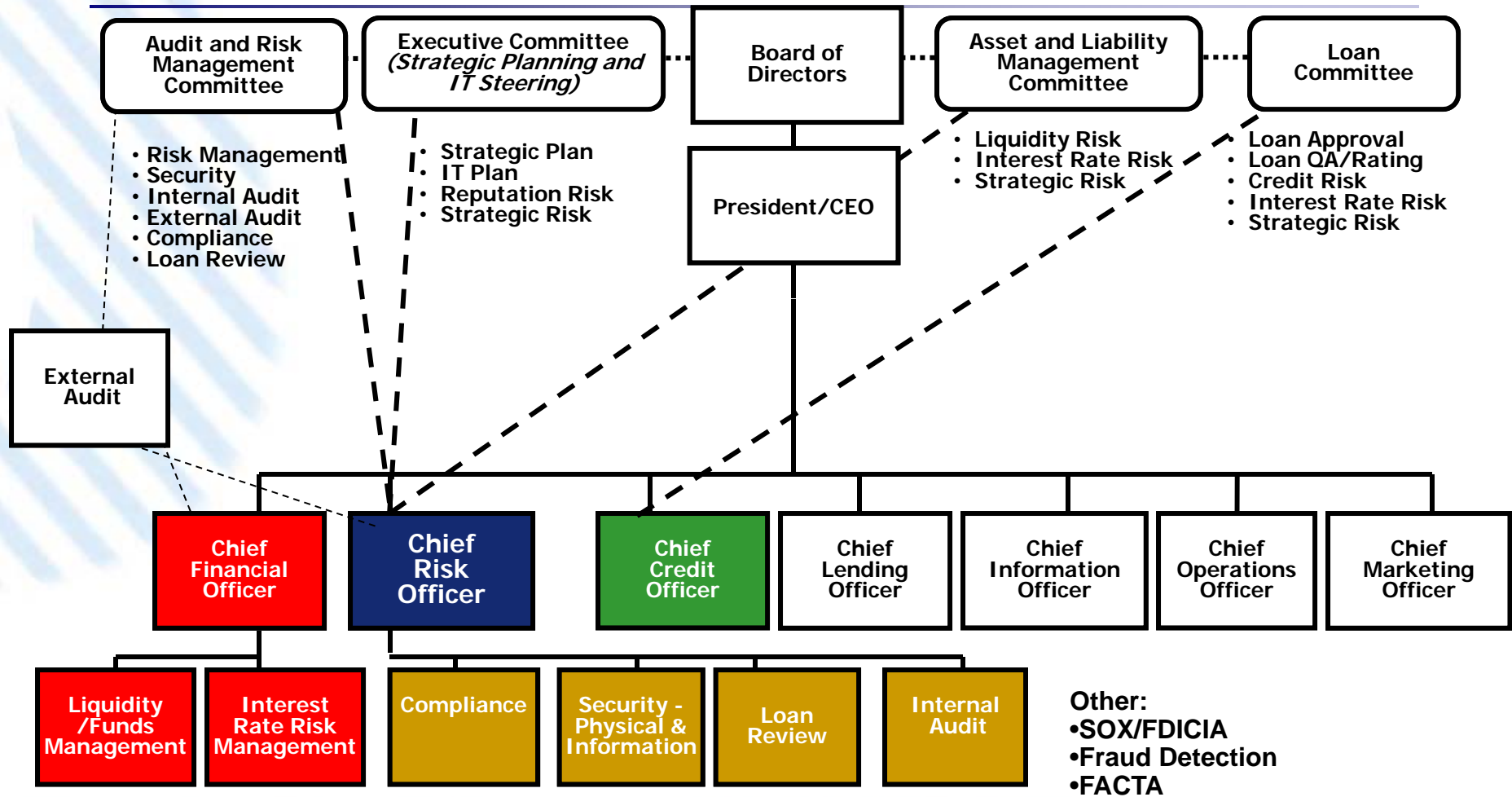
Step 4 - Develop Risk Management Program

- Prepare Action plans to address weaknesses in policy, process & control
- Develop risk tolerances and guidelines (revise policies)
- Create risk management organization:
 - Assign responsibility
 - Charter committees
 - Develop tools and information

Risk Management Organization

- Create risk management organization:
 - Assign organizational responsibility
 - Charter committees (remember....Committees do not do actual work)
- Complexity and Structure often driven by size of organization.....but keep it simple:
 - Not necessary to charter committees that duplicate other committees
 - Not always necessary to create new stand-alone business units
- Key is to incorporate risk management into business processes

Risk Management Organizational Alternative



Step 5 - Develop Information Systems

- Board and Management reports should be linked to Risk guidelines in policies
- Key indicators of performance, or potential problems and trends, should be monitored:
 - Reports of new business, compared to Loan Policy
 - Loans made as exceptions to Loan Policy (appraisal, limits, etc.)
 - Concentrations of credit tied to policy
 - Credit quality (e.g., delinquencies, classifieds, watch list) tied to policy
 - Credit grades by loan review compared to officer grades (percentages/trends)
 - Percentage of loan reviews completed
 - Levels of documentation loan exceptions

Risk Information Systems

- Measure / Track:
 - Inherent Risk
 - Risk Events
 - Control Effectiveness (RCSA)
 - Residual Risk
- Several Methods to do this:
 - Surveys
 - Assessments
 - Indices
 - Dashboards.....

Risk Indices

- Targeted to specific issue of concern
- Data to feed Dashboards
- Internal (Operational):
 - Process quality index (cycle time, volumes, errors);
 - Technology stability /control index (COBIT);
 - Client satisfaction index;
 - Control Effectiveness index
 - Physical Security index
- External (Operational):
 - Crime Incident / Loss index
 - Weather events index
 - Vendor SLA / Controls index

Sample Bank
GLBA Section 501b Data Classification Matrix

| Information Systems | | | | | | Data Classification | | | | | Ranking | |
|-------------------------|----------------------------|-----------------------|--|-----------|--------------|------------------------------|--------------------------|-----------------------------|-------------------------------------|--------------------------------|----------------------------------|---|
| Information System | Name and Provider / Vendor | In-House / Outsourced | Nature of System Information and General Access | Platform | Bank Contact | Sensitivity of Data Elements | Volume of Sensitive Data | Impact of Loss of Integrity | Impact from Loss of Confidentiality | Impact of Loss of Availability | Weighted Score High - 5, Low - 1 | Data Criticality Ranking, High > 3.6, Low < 2.3 |
| CIS / CIF | Jack Henry 20/20 | In-house | <p>Confidential customer data for controlled use within the company.</p> <p>This system contains confidential customer information for all bank customers, including address, taxpayer identification numbers, bank account numbers, etc.</p> | IBM AS400 | | H | H | H | H | M | 4.9 | HIGH |
| Loan Accounting Systems | Jack Henry 20/20 | In-house | <p>Confidential customer data for controlled use within the company.</p> <p>These systems contain confidential information regarding consumer, installment, and mortgage loan</p> | IBM AS400 | | H | H | H | H | L | 4.8 | HIGH |

SAMPLE BANK
GLBA Section 501b Risk/Threat Matrix

| SAMPLE BANK GLBA Section 501b Risk/Threat Matrix | | | | | | | | | | | |
|---|---|---|--------------------------|--|--|-------------------------------------|--|--|---|--|-------------------------------------|
| Information Systems | | | Ranking | Inherent Risk Rating | | | Mitigating Controls and Practices | | | Managed Risk Rating | |
| Information System | Name and Provider / Vendor | Nature of System Information and General Access | Data Criticality Ranking | Threats | Probability of Occurrence (High, Mod, Low) | Potential Severity (High, Mod, Low) | Administrative | Technical | Physical Security | Probability of Occurrence (High, Mod, Low) | Potential Severity (High, Mod, Low) |
| CIS / CIF | Altamira CLCS - Developed for BBYA by Accenture | Confidential customer data for controlled use within the company. This system contains confidential customer information for all bank customers, including address, taxpayer identification numbers, bank account numbers, etc. | HIGH | Hacking/ Unauthorized computer access, denial of service | High | High | Bank and servicer have adopted appropriate Information Security Policies to: <ul style="list-style-type: none"> Specify various categories of Information Systems, data, equipment, and processes subject to a comprehensive Information Systems practices and procedures Define Information Systems security responsibilities/roles within organization. Indicate appropriate levels of security through standards, guidelines, practice and procedure for the relevant confidentiality, integrity and accessibility requirements for each information system Staffing roles/responsibilities have been clearly defined for monitoring the network and related intrusion detection systems. Policy requires testing of intrusion detection systems | Servicer maintains firewalls network interfaces to application systems through all external/Internet connections. Intrusion monitoring systems have been installed and are monitored by service provider personnel on 24/7 basis. Servicer has developed incident response plans and has resources available 24/7 to execute such plans. Maintenance of these controls is outlined in Service Level Agreement with service provider. Bank maintains firewalls on network interfaces to core applications through all external/Internet connections. Intrusion monitoring systems have been installed and incident response guidelines prepared. Firewalls/IDS monitored by Bank personnel and maintained by third-party. Bank employs "smart view" software to manage and view firewall reports on a daily basis. This function performed by | Physical access to servers and telecommunications equipment in the Bank's principal data centers is secured through key/combination or card key locks and monitored by digital surveillance cameras transmitted over the network and monitored by Security. Workstation equipment is somewhat less physically secure during the day as some are located in high customer traffic areas. The Johnson center has a guard posted, camera surveilled man-trap at the entrance. Access between departments within the center is restricted through card key locks. Access to non-customer contact areas is secured through the use of card-key locks and restricted access areas (i.e., cards only permit access to selected areas). Appropriate after-hours security (e.g., alarms, digital/networked surveillance cameras, locks, etc.) has been implemented over this | Low-to-Moderate | Low-to-Moderate |
| | | | | Corruption of Data Due to malicious code (worm, virus, etc.) | High | High | The Bank is in process of completing Business Continuity Plans on a business unit-by-Business unit basis. Appropriate IT Disaster recovery plans have been | The Bank maintains anti-virus software on all servers and workstations. This software is automatically updated as updates are provided by/available from vendors. | Physical access to servers and telecommunications equipment in the Bank's principal data centers is secured. Workstation equipment is somewhat less physically secure during the day as some are located | Moderate | Moderate |

| | B | C | D | E | F | G | H | I | J | K | L | M |
|----|--|-----------------------|--|---|---|---|---|---|--|---|-------------------|--------------------------|
| 1 | Sample National Bank | | | | | | | | | | | |
| 2 | Information Security Program | | | | | | | | | | | |
| | Third-Party Vendor Risk Ranking | | | | | | | | | | | |
| 5 | Vendor Information | | | Vendor Classification | | | | | | | | |
| 6 | Third-Party Vendor | Type / Service | Description | Processes or Has Access to or Custody of Sensitive Customer or Proprietary Bank Data 25% | Volume of Sensitive Customer or Bank Data in Custody or Accessible by Vendor 25% | Potential for Loss of Integrity (Accuracy) of Information Processed by or in Custody of Vendor 20% | Potential for Breach of Security of Information Processed by or in Custody of Vendor 20% | Potential for Loss of Availability (Accessibility) of Vendor Service and of Information Processed by or in Custody of Vendor 10% | Weighted Score High - 5 Low - 1 | Info Security Ranking High > 3.7 Low < 2.3 | RESPONDENT | APPLICATION OWNER |
| 7 | BankAmerica- Check Inclearings | Service Provider | Inclearing checks | H | H | H | H | M | 4.8 | H | Bobby Bowdon | Bobby Bowdon |
| 8 | Wachovia- Check Inclearings | Service Provider | Inclearing checks | H | H | H | H | M | 4.8 | H | Bobby Bowdon | Bobby Bowdon |
| 9 | SunTrust Processing | Service Provider | Depository for checks | H | H | H | H | M | 4.8 | H | Kathy Baker | Kathy Baker |
| 10 | Vanguard Routers | Hardware | Routing services | H | H | H | H | M | 4.8 | H | John McGinnes | |
| 11 | Verizon | Service Provider | Local service, frame & ISDN | H | H | H | M | M | 4.4 | H | Ray Ammons | |
| 12 | Sungard | Service Provider | Trust processing services | H | H | H | M | M | 4.4 | H | David Keim | |
| 13 | Sprint | Service Provider | Local service, frame & ISDN | H | H | H | M | M | 4.4 | H | John McGinnes | |
| 14 | US Postal | Process | Mail pickup and delivery | H | H | M | M | M | 4 | H | Kathy Baker | Kathy Baker |
| 15 | ATT Communication Services | Service Provider | 1) Data circuits 2) local & long distance 3) | H | H | M | M | M | 4 | H | John McGinnes | |
| 16 | Bell South | Service Provider | Local service & ISDN | H | H | M | M | M | 4 | H | John McGinnes | |
| 17 | JHA_Synapsis | Software | CRM | H | H | M | M | M | 4 | H | Julie Story | |
| 18 | Credit Bureaus | Service Provider | Equifax is main Vendor via Internet | H | H | M | M | L | 3.8 | H | Craig Robinson | |
| 19 | Jack Henry- Passport (Silverlink) | Software | ATM/debit card online authorization | H | H | M | M | L | 3.8 | H | Ray Ammons | |

BSA/AML Geographic Risk Ranking

| | | Risk Criteria (Indicate H, M, L in each category, E through M) | | | | | | | | | | | |
|--------------------|-------------------|--|--------------------------|---|--|--|---|--|--|---|-------|---|----------------------------|
| Region/Branch City | Risk Weightings | Located in or near HIFCA | Located in or near HIDTA | Rural (<20,000), Suburban(20,000 to 50,000), Metro Area (50,000+) | Proximity to High Risk Businesses or High Crime Area | Fraud / Crime Loss or Suspicious Activity Experience | Open 5+ Years, 2-5 Years, Less than 2 Years | Turnover of Platform Staff (Tellers, CSRS) | Volume of High Risk / Cash Intensive Customers | Adquacy of Controls - Based on Audits and Exams | Score | Weighted Score High > 70 Moderate 30<or<70 Low < 30 | Comment |
| | | 5.0% | 5.0% | 15.0% | 15.0% | 10.0% | 10.0% | 12.5% | 15.0% | 12.5% | 100% | | |
| 1 | Cataño | H | H | M | H | L | L | M | L | M | 48 | MEDIUM | |
| 3 | Río Hondo | H | H | H | H | M | L | H | M | H | 79 | HIGH | |
| 4 | Urb. Caribe | H | H | H | H | M | L | H | M | L | 67 | HIGH | |
| 5 | Puerto Nuevo | H | H | H | H | H | L | H | L | L | 66 | HIGH | |
| 6 | 65 de Infantería | H | H | H | L | L | L | M | M | L | 43 | MEDIUM | |
| 7 | Villa Blanca | H | H | M | L | L | L | H | M | L | 42 | MEDIUM | |
| 8 | Plaza Bairoa | H | H | M | L | L | L | M | M | M | 41 | MEDIUM | |
| 9 | Hermanos Meléndez | H | H | H | M | L | L | L | L | L | 38 | LOW | |
| 12 | Ponce | H | H | M | H | L | L | L | L | L | 38 | LOW | Proximity to significant c |
| 13 | Mayaguez | H | H | M | M | L | L | L | M | M | 42 | MEDIUM | Proximity to significant c |
| 14 | Santa Rosa | H | H | H | M | L | L | H | M | L | 56 | MEDIUM | |
| 16 | Galería Suchville | H | H | H | L | L | L | L | M | M | 43 | MEDIUM | |
| 17 | Cataño – Alcaldía | H | H | H | M | L | L | M | L | L | 43 | MEDIUM | |
| 18 | Galería Paseos | H | H | H | L | M | L | H | L | L | 47 | MEDIUM | |
| 19 | Cayey | H | H | M | L | L | L | L | H | L | 38 | LOW | |
| 20 | Vega Alta | H | H | L | L | L | L | L | H | M | 36 | LOW | |
| 21 | Las Piedras | H | H | L | L | L | L | M | L | L | 22 | LOW | |
| 22 | Manatí | H | H | L | L | M | M | L | M | L | 32 | LOW | |
| 23 | Carolina | H | H | H | H | L | L | L | H | H | 71 | HIGH | Proximity to casinos |
| 24 | Trujillo Alto | H | H | M | L | L | L | L | M | L | 30 | LOW | |
| 25 | Las Catalinas | H | H | M | L | M | L | L | H | H | 53 | MEDIUM | |
| 26 | Arecibo | H | H | M | L | L | L | H | M | H | 53 | MEDIUM | |
| 27 | Condado | H | H | H | H | H | L | M | H | L | 73 | HIGH | Proximity to casinos |
| 28 | Isla Verde | H | H | H | H | H | M | M | M | L | 70 | HIGH | Proximity to casinos |

Product Service Risk Ranking

| 2 | Product/Service | Risk Criteria | | | | | | Weighted Score High > 3.7 Moderate 2.2<or<3.8 Low < 2.3 | Risk Ranked Potential for Use in Money Laundering | Comments |
|----|--------------------------------|--|---|---|---|--|-----|--|---|----------|
| | | 3rd party funds may be freely received, or funds may be paid to 3rd parties, without evidence of identity of the 3rd parties being taken 25% | Volume of Transactions is regularly High, Moderate or Low 25% | Account may be remotely accessed or accessed by variety of methods (e.g., wire, internet, other electronic, Voice initiated transactions, non-electronic) 20% | Account/Product used by businesses, or set up or purchased in "business/nominee" name 20% | International Use, Access or Ownership 10% | | | | |
| 3 | | | | | | | | | | |
| 4 | Money Orders | L | M | L | H | M | 2.5 | MEDIUM | | |
| 5 | Teller Checks | L | M | L | H | M | 2.5 | MEDIUM | | |
| 6 | Travelers/Gift Checks | L | L | L | M | L | 1.4 | LOW | | |
| 7 | Wire Transfers - Domestic | H | M | M | H | L | 3.7 | MEDIUM | | |
| 8 | Wire Transfers - International | H | M | M | H | H | 4.1 | HIGH | | |
| 9 | Internet Banking - Personal | L | M | M | H | M | 2.9 | MEDIUM | | |
| 10 | Internet Banking - Commercial | L | M | M | H | L | 2.7 | MEDIUM | | |
| 11 | Deposit Accounts: | | | | | | | | | |
| 12 | Personal Checking | H | M | M | H | L | 3.7 | MEDIUM | | |
| 13 | Public Funds Other | L | L | L | M | L | 1.4 | LOW | | |
| 14 | Equity Checking | H | L | M | H | L | 3.2 | MEDIUM | | |
| 15 | Investment Checking | H | M | M | H | L | 3.7 | MEDIUM | | |
| 34 | Personal Savings | M | L | L | L | L | 1.5 | LOW | | |
| 35 | Bonus Savings | M | L | L | L | L | 1.5 | LOW | | |
| 36 | Public Funds Savings | M | M | L | L | L | 2 | LOW | | |
| 37 | Employee Savings | M | L | L | L | L | 1.5 | LOW | | |
| 38 | Private Banking | | | | | | | | | |
| 39 | Private Client Checking | M | M | M | M | L | 2.8 | MEDIUM | | |
| 40 | Private Client MMA | M | M | M | M | L | 2.8 | MEDIUM | | |
| 41 | Private Client Business MMA | H | L | L | L | L | 2 | LOW | | |
| 42 | Wealth Management | H | M | M | M | L | 3.3 | MEDIUM | | |
| 43 | Individual Trust | M | M | M | M | L | 2.8 | MEDIUM | | |
| 44 | Credit Card Cash Advance | L | L | L | M | L | 1.4 | LOW | | |

BSA/AML Control Assessment

| BSA Area | Risk / Threat / Issue | Mitigating Controls | Indicate Risk Low to High (Scale of 5 to 1) | | | | | Aggregate Risk Score | Comments |
|-----------------|---|--|---|-----------|------------------|------------------------------|------------------|----------------------|--|
| | | | Policy | Procedure | Staff Sufficient | Staff Experience / Knowledge | Control Evidence | | |
| | | | 10% | 15% | 20% | 25% | 30% | | |
| Risk Assessment | The Bank has not appropriately identified risk within its operations, including those associated with products, services, customers and geographic locations, resulting in failure to implement appropriate BSA/AML controls and procedures and violations of BSA/AML and USAPA regulations | Procedures and methodologies have been adopted for preparing risk assessments. Risk assessments have been prepared for Quantity and Residual BSA Risk (June 2007). Additionally, specific Product and Geographic Location Risk Assessments have been prepared. Customer Risk assessments have been prepared, focused on certain FFIEC "High" risk categories where Bank is aware it has customers in such categories. Similar focused assessments have been prepared to certain FFIEC "High" risk categories where Bank is aware it has products in such categories. | 1 | 4 | 4 | 4 | 4 | 3.7 | BSA Policy does not cover requirement for an annual assessment of risk. Risk assessments have not been reviewed by the Board of Directors. Methodologies for preparation of risk assessment and integration of results into BSA Program are not fully documented. Staff preparing risk assessments, while knowledgeable and perhaps experienced at other banks, have only recent, short-term experience at DoAL in view of turnover in BSA, Compliance and other operations areas, they may not be as |
| | The Bank has not appropriately identified CIP risk within its operations, including those associated with products, services, customers and geographic locations, and identifying the specific procedures to be followed by customer/product resulting in violations of CIP guidelines and potential risk of opening accounts that are improperly documented or vetted. | BSA Policy requires an annual assessment of risk. A risk assessment has been prepared for CIP Risk (June 2007), by product and customer type and manner of account opening. Additionally, Customer Risk assessments have been prepared, focused on certain FFIEC "High" risk categories where Bank is aware it has customers in such categories. | 5 | 3 | 4 | 3 | 3 | 3.4 | Risk assessments have not been reviewed by the Board of Directors. Methodologies for preparation of risk assessment and integration of results into BSA Program are not fully documented. CIP Risk Assessment could be expanded to include: 1) increased detail breakdown on Product Groups and the related Risk assignment from the specific Product Risk Assessment and specific requirements for that product. Similarly, it could be expanded for Geographic and Customer risk ratings. Additional guidance could be added for errors and omissions and resolving address discrepancies. Finally, required documentation descriptions should be more specific to not exact type or documentation |
| | The Bank has not appropriately identified OFAC risk within its operations, including those associated with products, services, customers and geographic locations, resulting in failure to implement appropriate BSA/AML controls and procedures and violations of OFAC guidelines | BSA Policy requires an annual assessment of risk. Risk assessments have been prepared for Quantity and Residual OFAC Risk (June 2007). | 5 | 5 | 4 | 3 | 5 | 4.3 | Risk assessments have not been reviewed by the Board of Directors. Methodologies for preparation of risk assessment and integration of results into BSA Program are not fully documented. Staff preparing risk assessments, while knowledgeable and perhaps experienced at other banks, have only recent, short-term experience at DoAL |

Regulatory Risk Assessment

Sample Bank
Regulatory Risk Assessment Matrix
FYE 12/31/2006

| Regulatory Requirement | Prior Exam Violations 25% | Prior Internal Exception 25% | Litigation & Penalties (H/M/L) 20% | Examiner Emphasis (H,M, L) 20% | New Area / Change 10% | Score | Ranking | Comments |
|---|------------------------------|---------------------------------|---------------------------------------|-----------------------------------|--------------------------|-------|---------|----------|
| Equal Credit Opportunity Act — Regulation B | | | | | | | | L |
| 202.4 General rule prohibiting discrimination | M | L | M | M | M | 2.5 | M | |
| 202.5 Rules concerning taking of applications | M | M | L | M | L | 2.4 | M | |
| 202.5a Rules on providing appraisal reports | M | M | L | H | L | 2.8 | M | |
| 202.6 Rules concerning evaluation of applications | M | L | L | M | L | 1.9 | L | |
| 202.7 Rules concerning extensions of credit | M | L | M | M | L | 2.3 | M | |
| 202.8 Special purpose credit programs | L | L | L | M | L | 1.4 | L | |
| 202.9 Notifications | L | M | L | M | M | 2.1 | L | |
| 202.10 Furnishing of credit information | L | M | M | L | L | 1.9 | L | |
| 202.12 Record retention | M | L | L | M | L | 1.9 | L | |
| 202.13 Information for monitoring purposes | M | L | L | H | M | 2.5 | M | |
| 202.15 Incentives for self-testing and self-correction | L | L | L | L | L | 1 | L | |
| Home Mortgage Disclosure Act — Regulation C | | | | | | | | H |
| 203.4 Compilation of loan data | M | H | M | H | H | 4.1 | H | |
| 203.5 Disclosure and reporting | M | H | M | H | H | 4.1 | H | |
| Reserve Requirements of Depository Institutions — Regulation D | | | | | | | | L |
| 12 USC 1832 NOW Account Eligibility | L | L | L | M | M | 1.6 | L | |
| 204.2(d)(1) Savings Account/MMDA Restrictions | L | L | L | M | M | 1.6 | L | |
| 204.2(c)(1) Time Deposit Restrictions | L | L | L | M | M | 1.6 | L | |
| Electronic Fund Transfers — Regulation E | | | | | | | | M |
| 205.5 Issuance of access devices | L | L | L | L | L | 1 | L | |

Sheet1 / Sheet2 / Sheet3 /

Risk Dashboards

- KRI are warning signs of change and potential problems....not the answer....just the warning
- Dashboards are basic tools.....like Gap Analysis in 80s to Rate Shock Analyses in 90s
- KRI do not estimate losses:
 - Lack historical operational loss data
 - Lack correlation of event and loss, and degree of loss
- Aggregate risk scores in categories (i.e., regulatory categories or BASEL) for dashboards
- Support with risk indexes

Credit Risk KRI – Leading Indicators

| 13 | Leading Risk Indicators | | | | | | | | | |
|----|-----------------------------------|---|--|-----------|--------------|------------------------------|------------------|---|--------|------|
| 14 | Pass & Watch Loans/Capital + ALLL | indicator but I think there may be more benefit to including in Leading | System (G/L and Loan) and Credit Administration Listings | Monthly | 10% or less | greater than 10% through 20% | greater than 20% | 3 | MEDIUM | 0.1 |
| 15 | Loan Growth | This measures the rate or growth in total loans and leases. Rapid growth, particularly as measured against local, regional and national economic conditions, has long been associated with subsequent credit quality problems. Growth can strain bank underwriting and risk selection standards, as well as the capacity of management, risk management and administration processes. All other factors held equal, as loan growth rates increase, so will credit risk. | Kirchman Bankway system | Monthly | 5% or less | greater than 5% through 15% | greater than 15% | 5 | HIGH | 0.15 |
| | Change in Portfolio Mix | The sum of positive changes in the domestic loan portfolio mix for Commercial Real Estate and Commercial/Industrial Loans. This ratio reflects changes in the structure of the loan portfolio, and considers that significant change reflects increased risk. A significant increase in this ratio may indicate that the bank is lending in areas in which it may not have sufficient expertise or | | Quarterly | Less than 3% | 3% to 7% | In excess of 7% | 1 | LOW | 0.2 |

CREDIT RISK MANAGEMENT
KEY RISK INDICATORS
September 30, 2006

Trend Indicators: Red - Threat, Amber - Caution, Green - OK
Risk Levels: Lower, Moderate, Higher

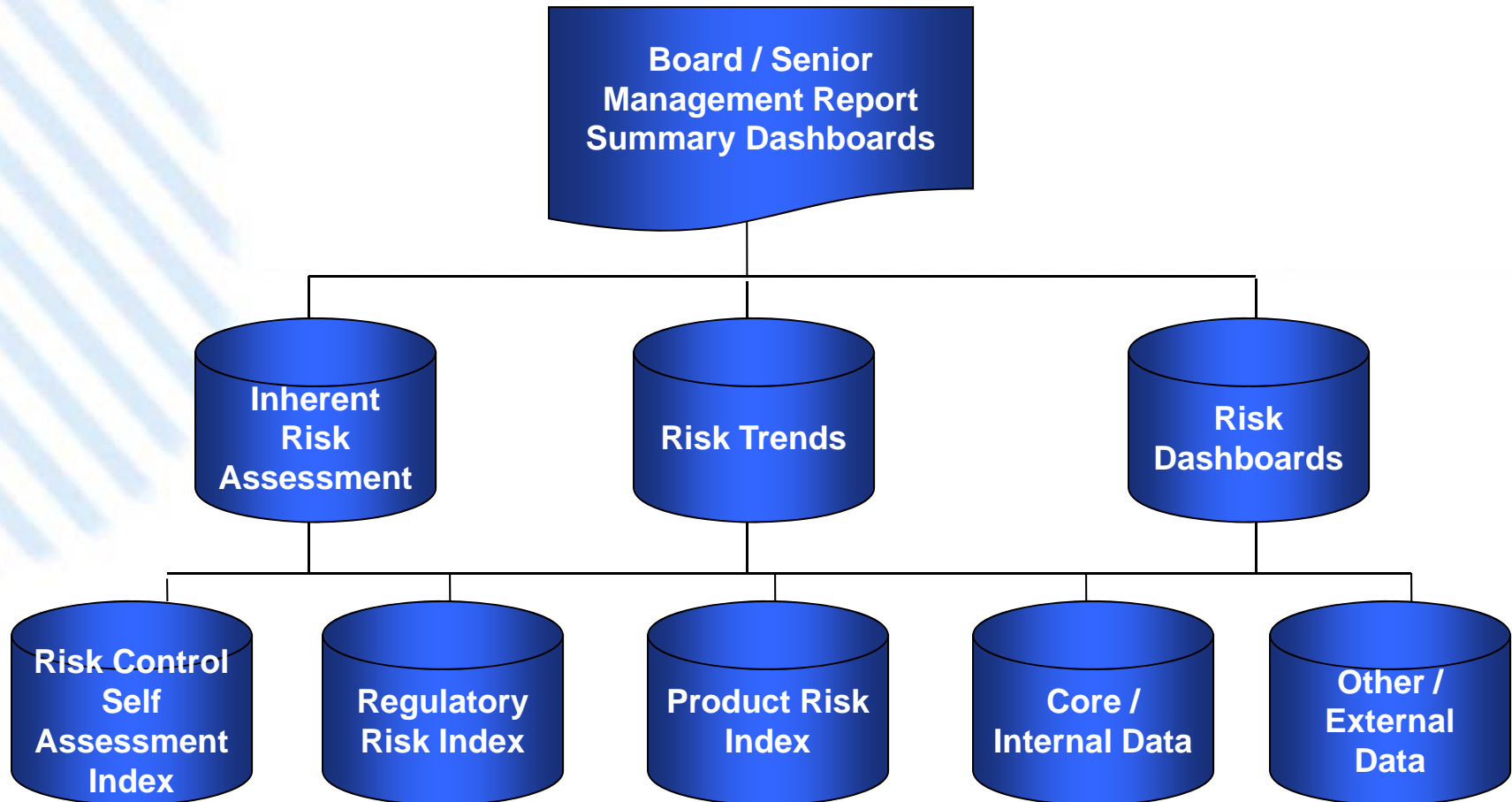
| | Prior Y1 12/31/2003 | Prior Y2 12/31/2004 | Prior Q3 12/31/2005 | Prior Q2 3/31/2006 | Prior Q1 6/30/2006 | Current Quarter 9/30/2006 | Target/Range | Current Peer Avg 9/30/2006 | Trend Indicator | Risk Level |
|--|------------------------|------------------------|------------------------|-----------------------|-----------------------|------------------------------|--------------|-------------------------------|-----------------|------------|
| STRATEGIC / CREDIT QUALITY | | | | | | | | | | |
| Growth Rate - Net Loans & Leases | 2.96% | 16.49% | 22.93% | 19.85% | 16.16% | 14.67% | 26.92% | 13.05% | | Moderate |
| Net Loss to Average Total Loans & Leases | 0.49% | 0.24% | 0.02% | 0.03% | 0.07% | 0.22% | 0.25% | 0.11% | | Lower |
| Past Due Loans / Total Loans | 2.44% | 1.00% | 0.78% | 1.17% | 1.29% | 1.17% | 15.0% | 1.02% | | Moderate |
| Gross Loans & Leases 90+ days plus Non-Accrual Loans Past Due 30-89 Days / Total Loans | 1.08% | 0.39% | 0.20% | 0.18% | 0.23% | 0.37% | 0.25% | 0.47% | | Moderate |
| ORE / Average Assets | 0.22% | 0.15% | 0.10% | 0.10% | 0.10% | 0.10% | .05 - .15% | 0.06% | | Higher |
| Adversely Classified Loans / Capital + Reserves | 8.81% | 10.71% | 8.11% | 8.90% | 8.56% | 8.93% | 15%-20% | n/a | | Lower |
| Special Mention Loans / Capital + Reserves | 6.71% | 11.23% | 7.10% | 12.85% | 12.72% | 12.56% | 10%-15% | n/a | | Moderate |
| Past & Watch Loans / Capital + Reserves | | | 10.50% | 7.27% | 6.52% | 7.78% | 7.5%-12.5% | n/a | | Moderate |
| Substandard Loans / Capital + Reserves | | | 8.62% | 8.31% | 7.36% | 7.58% | 10%-15% | n/a | | Lower |
| Doubtful Loans / Capital + Reserves | | | 0.77% | 0.75% | 1.19% | 1.59% | 2%-5.0% | n/a | | Higher |
| Off Balance Sheet Commitment to Total Loans | 8.53% | 10.00% | 11.13% | 14.21% | 13.42% | 13.78% | | | | |
| Credit Score - Low Override % (Active Loans as of period) | | | | | | 35.81% | 5-10% | n/a | | Higher |
| Personal Auto | | | | | | 30.77% | 5-10% | n/a | | Higher |
| HELOC SILVER | | | | | | 12.41% | 5-10% | n/a | | Higher |
| HELOC GOLD | | | | | | 20.26% | 5-10% | n/a | | Higher |
| HELOC PLATINUM | | | | | | 15.74% | 5-10% | n/a | | Higher |
| CONCENTRATIONS | | | | | | | | | | |
| Loan Concentration of Top 5 Categories by Volume/Total Loans | | | | | | | | | | |
| Non-Farm, Non-Residential Property | | | | | 23.33% | 22.73% | 25%-30% | n/a | | Lower |
| Residential Mortgage | | | | | 20.18% | 19.16% | 25%-30% | n/a | | Lower |
| Land Acquisition and Development | | | | | 12.67% | 12.92% | 5%-10% | n/a | | Higher |
| Residential Construction | | | | | 9.58% | 9.95% | 5%-10% | n/a | | Moderate |
| Agricultural Real Estate | | | | | 8.69% | 8.29% | 5%-10% | n/a | | Moderate |
| PAST DUE CONCERN RATION - Index > 1.0: | | | | | | | | | | |
| Auto's, RV's, Boats, Aircrafts & Other Personal Prop | | | | | 1.48 | 1.23 | 1.00 | n/a | | Moderate |
| Unsecured Loans | | | | | 0.96 | 1.28 | 1.00 | n/a | | Moderate |
| Residential Mortgage | | | | | 1.71 | 1.71 | 1.00 | n/a | | Higher |
| Equipment, Trucks, Trailers | | | | | 1.80 | 2.01 | 1.00 | n/a | | Higher |
| LOAN LOSS CONCENTRATIONS > Than .125% of Total Loans: | | | | | | | | | | |
| Non-Farm, Non-Residential Property | | | | | | | 0.12% | n/a | | Lower |
| PORTFOLIO MIX Growth Rate > 1% | | | | | | | | | | |
| SECURITIES PORTFOLIO | | | | | | | | | | |
| Non-Rated Securities / Total Capital | | | | | | | 0% | n/a | | |
| Classified or Below Investment Grade Securities / Total Capital | | | | | | | 0.00 - 33.9% | | | |
| ALCO Identified Securities of Concern / Total Capital | | | | | | | | | | |
| REGULATORY | | | | | | | | | | |
| Reserve for Loan Losses / Total Loans | 1.91% | 1.23% | 1.21% | 1.22% | 1.17% | 1.08% | | | | |
| Part 365 Measure #1 as a % of Tier II Capital (All R/E Loans) | 0.00% | 35.22% | 70.00% | 65.00% | 64.92% | 65.21% | 100.00% | n/a | | Lower |
| Measure #2 as a % of Tier II Capital (Land Develop, Improved Res Lohs, Commercial Construction, Improved Property) | 0.00% | 24.66% | 35.95% | 32.03% | 32.03% | 28.23% | 30.00% | n/a | | Moderate |
| ORE - % of Tier II Capital RC-C (a.l.) | n/a | n/a | 168.00% | 170.00% | 187.00% | 201.00% | 100.00% | 113.00% | | Higher |
| % of Tier II Capital RC-C (a.l.d., i.e.) | n/a | n/a | 391.00% | 409.00% | 416.00% | 427.00% | 300.00% | 338.00% | | Higher |
| Adversely Classified Loans to Total Loans (Exam 06/30/06) | | | | | | 13.6% | < 15.00% | | | Lower |

Dashboards and Reports

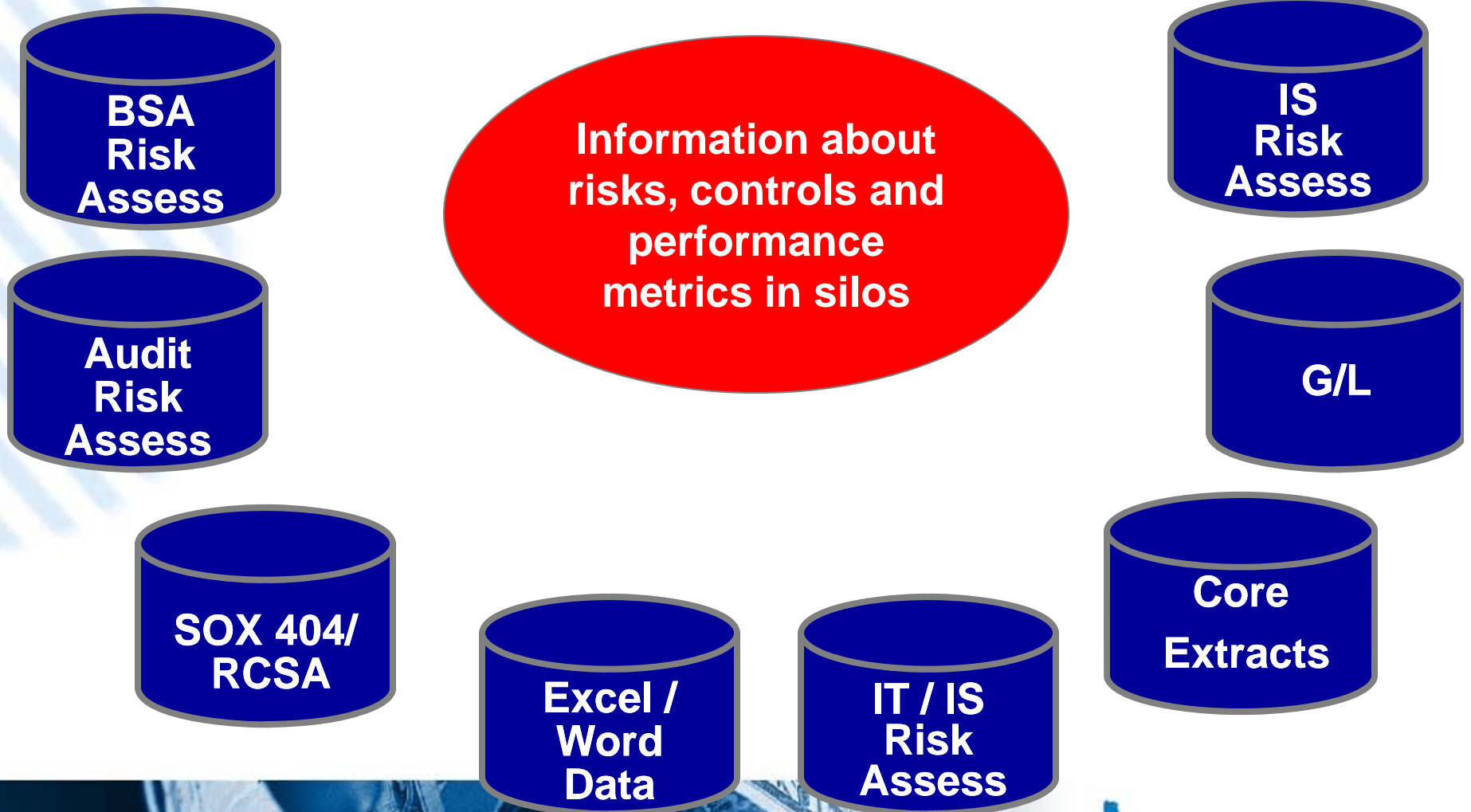
Reports to Audit & Risk Management Committee of Board

- **Annually:**
 - Assessments (Inherent and Residual Risk)
 - Control effectiveness (Design)
 - Recommendations and Plan
- **Quarterly:**
 - Brief narrative summaries supported by dashboards and graphs
 - Risk Dashboard
 - Control effectiveness
 - Risk / control remediation status
 - Quarterly and monthly trending analysis over annual periods
 - Drill-down to specific dashboards and indices to explore the detail
 - Consider product, process, business unit information
- **As needed:**
 - Product / Service Risk Assessments
 - Information Security Risk Assessments
 - BSA/AML

Risk Reporting



Leveraging Information



Summary

- Risk Management is key to effective management, profitability and enhancing shareholder value
- Processes need to be formalized in most bank, roles defined and tools improved
- Keep it simple....don't over complicate the “system” to the point the system only exists for itself
- Make it relevant



Risk Oversight

The Newest Mantra for ALL Board Members

November 13, 2009
San Francisco, CA

Ken Proctor
Brintech, Inc.
(800) 929-2746
KProctor@Brintech.com
<http://www.brintech.com>

Atlanta * Austin * Orlando * Los Angeles



© **b** **BRINTECH.**