

Determining your allowance for loan losses

by Steve Moore, Indianapolis

One of the most discussed topics recently has been the proper methodology for determining the allowance for loan and lease losses (ALLL).

Securities Exchange Commission (SEC) Staff Accounting Bulletin (SAB) Number 102 and the July 2001 Federal Financial Institutions Examination Council (FFIEC) policy statement collectively provide a framework for determining ALLL.

While Statement of Financial Accounting Standards (SFAS) 5 and 114 are still the definitive accounting principles for determining the adequacy of ALLL, the SEC and Federal Financial Institutions Examination Council were not satisfied with the industry's documentation and controls to support current ALLL levels. The SAB and policy statement:

- ▲ Clarify that the board of each institution is responsible for ensuring controls are in place to determine the appropriate level of ALLL
- ▲ Require the process to be thorough, disciplined and consistently applied
- ▲ Require documentation consistent with an institution's stated policies, generally accepted accounting principles and applicable supervisory guidance
- ▲ Provide guidance on maintaining and documenting policies and procedures

So what can you do to ensure your institution documents its ALLL in accordance with these guidelines?

Policies & Procedures

For your ALLL methodology to be effective, your written policies must:

- ▲ Assign responsibility for determining and approving ALLL
- ▲ Document internal controls to be relied on
- ▲ Outline a well-defined loan review process containing an effective loan-grading system
- ▲ Document how the loan portfolio will be segmented for determining the ALLL
- ▲ Provide a mechanism to validate assumptions utilized

Methodology

In calculating ALLL, segment the loan portfolio into two groups: loans evaluated individually and loans evaluated collectively. The evaluation of individual loans will follow SFAS 114.

Loans evaluated collectively will be homogeneous pools with similar risk characteristics. To evaluate loans in homogeneous pools start with an institution's historical loss experience for each group of loans. Determine and apply this loss ratio to each significant type of loan, *e.g.*, consumer loans, residential real estate, credit card, etc.

Methodology for determining ALLL also involves consideration of current environmental factors and their impact on the institution's loan quality. Management should consider:

- ▲ National and local economic trends
- ▲ Trends in delinquencies and charge-offs
- ▲ Trends in volume and terms of loans, including concentrations within industries
- ▲ Recent changes in underwriting standards
- ▲ Experience and depth of lending staff
- ▲ Industry conditions

These are subjective, and management should maintain adequate documentation to support amounts added to the ALLL for any of the above items. This may include documentation of situations that have an impact on the local economy.

Management should then aggregate losses identified in the individual loan reviews, through the application of historical loss ratios and for current environmental factors, and adjust ALLL to this amount. The board of directors should review and approve ALLL.

Validation

Management should build into its ALLL process a look-back approach to validate methodology. Management should periodically

compare actual losses to anticipated losses included in ALLL calculations. If actual results differ significantly from anticipated results, management should alter methodology to more accurately identify losses in the loan portfolio.

Conclusion

Determination of ALLL is highly subjective. The most important factor is to maintain adequate documentation to support the conclusions reached in determining ALLL. Contact your BKD Financial Institutions Group advisor for help in documenting and supporting your ALLL. □

In this issue

- ✓ Determining your allowance for loan losses
- ✓ ESOP, a successful option for banks
- ✓ Deleted data may be retrievable
- ✓ Compliance Corner: Bank Secrecy Act Reporting Update



by Bill Dickerson, Kansas City

Many banks have implemented or are considering an employee stock ownership plan (ESOP).

ESOPs have been successful in the banking industry for several reasons. Generally, ESOPs have been designed to fulfill specific board goals and objectives, including offering an alternative market for the stock of the company, providing tax incentives to selling shareholders, tax incentives to the bank and an incentive for retention and recruitment of employees.

Creating alternative market

Financial institutions generally have three opportunities to create a market of stock for a selling shareholder. Traditionally, these include the bank's officers and directors, individuals in the community and the bank's holding company. If a selling shareholder perceives little or no market for the stock, the bank is often faced with a negative community relations issue.

Formation of an ESOP provides the bank with another opportunity to provide liquidity to shareholders who desire to sell stock other than to the traditional markets. In addition, creating a fourth market through an ESOP will often provide an opportunity for the bank to remain independent rather than consolidating with a larger entity to provide liquidity to the shareholders.

Benefits of selling

The ESOP allows shareholders to sell stock to diversify their investment portfolios at fair market value

ESOPs & banks: a winning combination

(based on an independent, third-party appraiser) and receive capital gain treatment, assuming the holding period has been met. Also, if the ESOP owns at least 30% of the outstanding stock, the selling shareholder may elect (with bank's permission) to defer gain from the sale by investing in qualified replacement property (QRP) within 12 months from the closing date of the sale.

Therefore, by investing in equity or debt securities issued by a domestic operating company, the selling shareholder may not have to pay any current income tax on the sale of the stock.

If the selling shareholder holds the QRP until death, there is a step-up in basis, and the gain on the original sale of the stock is never taxed for income tax purposes (the value of the QRP is included in the value of the estate). The sale of the QRP before death would result in the gain being taxable.

Another alternative is reinvestment into long-term bonds specifically designed for ESOP transactions. These bonds are generally issued by investment grade companies with excellent credit ratings. They offer long maturity dates since gain on replacement property would be triggered when bonds mature.

The bonds are floating rate notes and may be leveraged. In most cases, the selling shareholder can borrow approximately 90% of the value of the bonds, providing the opportunity to buy and sell securities without incurring income tax on the gain from QRP.

Tax incentives

There are significant tax incentives to the institution with an ESOP. Contributions are deductible to the company, providing a significant deduction against current

income. If the ESOP were leveraged, the company would receive a deduction for not only interest paid but also principal reduction paid during the year.

Participants are not currently taxed on contributions or the increase in their account balances as a result of increased stock value or dividends. In certain situations, dividends paid by the company to the ESOP also may be deductible.

Participants benefit from act

In June, Congress passed the Economic Growth and Tax Relief Reconciliation Act of 2001, which provides significant incentives for retirement savings for participants. Beginning in 2002, 401(k) contributions deposited by employees no longer count against the employer deduction limit of 25% of covered compensation.

Therefore, the company would be able to deduct a full 25% of covered compensation, and employees may still defer significant pretax contributions into a 401(k) plan. Dividends paid on employer stock are generally deductible in addition to the 25% employer contribution limit, subject to alternative minimum tax.

S corp advantages

There are additional tax advantages to S corporations that sponsor ESOPs. Provisions of the Taxpayer Relief Act of 1997 made it possible for S corporations to sponsor an ESOP beginning January 1, 1998.

An S corporation's income is taxed to the shareholders rather than the corporation. Therefore, an ESOP-owned S corporation is essentially tax free since an ESOP is a tax-exempt entity because the plan is a qualified retirement plan.

For example, a BKD financial institution client 100% owned by an

ESOP paid approximately \$750,000 in taxes in the year before converting to an S corporation. In the year of conversion the bank paid \$0 in taxes.

In this instance, the institution paid an S corporation income distribution to the ESOP of \$750,000, which was allocated to plan participants. However, capital of the institution was virtually the same since the S distribution would have been paid to the Internal Revenue Service and state taxing authorities if the institution had not elected S status.

The result is to provide a significant cash-flow advantage that can be used for other purposes such as providing liquidity for terminating participants, outside selling shareholders or additional acquisitions. A 100%-owned ESOP financial institution is a strong competitor since it is not encumbered with taxes that burden its competitors.

Employee incentive

Unlike other employee benefit plans that typically diversify investments within the plan, ESOP is designed to invest in employer securities. Numerous studies show employees with ownership interest in the company are more motivated to improve corporate profits, which ultimately equates to greater retirement income.

ESOPs also have a proven track record as a tool for recruiting and retention since it is the only qualified plan vehicle providing significant stock incentives for employees.

BKD can help

Our ESOP consultants have in-depth experience and knowledge of rules relating to financial institutions. For specific information on how we can be an ESOP solution for you, contact your BKD Financial Institutions Group advisor. □

The missing data mystery

by Erica Garrison, Houston & Angela Morelock, Springfield,

You delete a computer file and empty the recycle bin. The file can't be found. Is it truly deleted?

The file is *not* deleted and could be recovered with the right technology. Deleting a file makes that

DataProbe is a computer forensics system designed to collect, preserve, analyze and prepare court presentation of computer-related evidence.

space available for other data to write over. That space may not be written over for months, years or ever. If so, your deleted file still exists on the hard drive even though you can't see it.

Much of the information on a hard drive could be recorded without the user's knowledge or consent. Footprints of Internet use, e-mail activity and files viewed or printed but never saved to the computer may be recoverable.

Visits to Internet sites typically download graphics, pictures and sometimes text to your computer. Knowing this, you reformat your hard drive. The data is still potentially recoverable. The information has not been deleted. Only the computer's pointer structure, indicating where the files and folders are, has been deleted.

Recovery technology

So how can these deleted, unseen, unknown files be recovered? Why is this technology useful, and how do you know it is accurate and reliable?

The fragile nature of electronic media necessitates appropriate handling and imaging to maintain forensic integrity of the information.

Hardware, software and a

forensic computer examiner's expertise are all crucial to recovering lost data. This recovery may be one of the most valuable resources in the internal investigation of an employee, former employee or soon to be former employee, since most workplace information is stored electronically.

Industrial espionage, employee misconduct, embezzlement, inappropriate use of company resources and theft of intellectual property are on the rise, costing businesses billions annually. No internal investigation should neglect computer evidence, especially as it pertains to litigation or potential litigation.

Hard copies aren't enough

Hard copies of files don't tell the whole story. Background information, or metadata, could prove vital to an investigation.

Electronic files also may provide passwords, other forms of protection, hidden data or other information a paper copy doesn't. Paper copies are not a substitute for electronic data.

Imaging electronic media such as hard drives, servers, backup tapes and discs can be thought of as taking an exact "snapshot" of that drive at that point in time. When imaged properly, deleted, temporary and swap files are preserved, as well as the integrity of the data. This process does not even turn the subject's computer on. It is noninvasive and leaves no evidence imaging has occurred.

Potential evidence

Since any imaged and analyzed data has the potential to become court evidence, an important feature of DataProbe is the verification process that establishes data was not

tampered with or altered in any way by examiners. This process employs a standard algorithm to generate what is known as a hash value.

This hash value can be thought of as an electronic fingerprint. The odds of two nonidentical pieces of electronic media having the same hash value are mathematically less likely than two people having the same physical fingerprint.

Once an image is taken, keyword searches, time stamps, file type or other file attributes can be used to cull relevant information. Timelines can be developed. Internet history and e-mail, sometimes even Internet-based e-mail, can be recovered. Data-mining techniques and data analysis can find files the user attempted to hide.

Data & internal investigations

Analyzing and recovering deleted electronic documents and e-mail can provide significant information in internal investigations that cannot be obtained from any other source. The following situations often necessitate review of deleted items and other electronic files:

- ▲ Internal fraud or embezzlement
- ▲ Intellectual property theft
- ▲ Improper or illegal use of a financial institution's computer resources
- ▲ Search for unlicensed or unauthorized software
- ▲ Sexual harassment allegations
- ▲ Potential wrongful discharge suits

Data & outside attacks

Financial institutions must contend with numerous risks to the integrity and security of computer systems.

When such incidents occur, it's critical the financial institution

respond appropriately to preserve electronic evidence. Obtaining a forensically sound copy of the computer media is the best way to preserve evidence of an intrusion, either internal or external.

Monitor for liability & compliance

Monitoring internal use of electronic resources is critical from both a liability and compliance perspective. All financial institutions should have written policies clearly prohibiting inappropriate use of computer resources. Such policies should establish:

- ▲ The financial institution's ownership of electronic information
- ▲ The institution's right to monitor daily activity, e-mail and Internet use
- ▲ That there is no employee personal expectation of privacy related to electronic information stored on the institution's computer systems

Obtaining an image copy of computer media is an excellent way to monitor compliance with corporate computer, e-mail or Internet policies. Such monitoring can be done at random on a periodic basis, or the financial institution can select specific employee computers to be image copied for review.

DataProbe™

BKD can help

Lost, damaged or accidentally deleted files can often be recovered using forensic technology such as DataProbe, saving you the cost of reconstructing the information.

DataProbe is just one of the solutions offered by BKD Forensics & Dispute Consulting, our national litigation services division. Contact your BKD Financial Institutions Group advisor to see how we can be a solution to your lost data problems. □

Bank Secrecy Act reporting updated

by Mark Dudley, Kansas City

September 11, 2001, triggered dramatic changes in our lives.

As a nation, we must do our part to ensure this type of tragedy never happens again. As an industry, bankers are doing their part by increasing efforts to assist law enforcement officials.

Nowhere is this more prevalent than with the Bank Secrecy Act. It seems daily there is something new on the money-laundering front. Legislation that, until recently, appeared dead has risen to the top of legislator's charts. What does this mean for you?

Office of Foreign Asset Control

If you didn't know about the Office of Foreign Asset Control (OFAC) before September 11, you do now. OFAC is not new. The banking industry has dealt with OFAC's requirements for years.

Banks have been required to maintain OFAC's listings of countries and individuals (SDNs) identified by the government as not allowed to conduct financial transactions within the banking system.

In addition, any accounts on record as belonging to anyone on the OFAC list were required by law

to be frozen or the assets "blocked" and reported to the government. While banks have been required to comply with OFAC for some time, it has only been in recent years regulators have started examining for OFAC compliance.

In the past, banks were considered ahead of the game if they verified new account openings against the OFAC list to ensure the person opening the account was not on the list and had a general understanding of OFAC.

The next step in OFAC vigilance was to compare your entire database of accounts to the OFAC list at least annually. This ensured that as the list changed, the database was checked against the updated list.

The evolution of OFAC was greatly accelerated following September 11. President Bush asked banks to check a new list of suspected terrorists. Today, the list is continually updated and should be monitored daily.

If you use Fedline in your processing, updates also appear on the daily Fedline reports. If you have a hit (an account that appears on the list) you must block those assets immediately and notify OFAC.

Suspicious activity reporting

In addition, banks have been

asked to increase efforts to file suspicious activity reports (SARs), especially if the bank has any reason to suspect a link to terrorism.

Again, while SAR reporting is not new, the events of September 11 have increased awareness of the value of SARs as a crime prevention tool and as a tool to help the government fight terrorism.

Banks have been reporting known or suspected violations of the Bank Secrecy Act (BSA) program and other criminal activity on SARs for years. This should be a part of every bank's BSA program. Staff at all levels should be aware of reporting requirements.

This is not just an East Coast or big city bank issue. Review your bank's training programs, and identify someone internally as the point person for coordinating SAR filings. If SAR reporting is not part of your BSA policy, consider adding it or creating a separate SAR policy.

Banks are now asked to go one step further. On October 5, 2001, at the request of the FBI, a joint regulatory agency letter was sent asking banks to name a senior-level person to receive and review a control list of individuals and entities whose records are to be reviewed.

Any hit from this list must be reported directly to the Federal



Reserve Board via e-mail at suspicious.accounts@nyfrb.org. It also must be reported on a paper SAR and through direct contact using the hotline number established by FinCEN, 866 556 3974.

Besides the increase in OFAC and SAR activity, Congress is working on new antimoney laundering legislation. Both Senate Bill S.1510 and House Bill H.R. 3004 are pending. Banks should review the requirements of each and contact their representative with any concerns regarding these issues.

On a final note, banks should verify that both OFAC and SAR reporting are included as part of their annual independent audit required by BSA.

BKD's Financial Institutions Group regulatory compliance consultants can answer your questions about OFAC, SAR or any part of your bank's BSA program. Contact your BKD advisor today to find out how we can be a solution for you. □

**How to Reach
BKD**

P.O. Box 1900
Springfield, MO 65801-1900

inFinet
RESOURCES
Independent Financial Institution Network

bkd.com

For a complete list of our offices and subsidiaries and their contact information, go to bkd.com or call Director of Communications at 417 831-7283.

PRSRT STD
US POSTAGE PAID
SPRINGFIELD MO
PERMIT #801

Address Service Requested