Emerging Issues Series

A Peek at the Examiners Playbook
Phase III

Paul A. Decker
And
Paul E. Kellogg

Emerging Issues Series
Supervision and Regulation Department
Federal Reserve Bank of Chicago
May 1999 (S&R-99-2)

A Peek at the Examiners Playbook
Phase III

Paul A. Decker

Paul E. Kellogg

May 1999

Address correspondence to Paul Decker, Supervision and Regulation, Federal Reserve Bank of Chicago, 230 South LaSalle Street, Chicago, IL 60604-1413. Phone 312-322-2165, Fax 312-322-5894, E-mail: Paul.A.Decker@Chi.Frb.Org. Requests for additional copies should be directed to the Public Information Center, Federal Reserve bank of Chicago, P.O. Box 834, Chicago, Illinois 60690-0834, or telephone (312) 322-5111. The Emerging Series Working Papers are located on the Federal Reserve Bank of Chicago's Web site at: http://www.chicagofed.org/publications/workingpapers/emergingissues.cfm

A Peek at the Examiners Playbook
Phase III

By

Paul A. Decker and Paul E. Kellogg[1]

Banking supervisors are intensifying their efforts to ensure Y2K compliance in the banks they supervise. The examiners of all five federal regulatory bodies embarked upon Phase III of the millennium supervision effort (not all the regulatory agencies will identify it as a separate phase) on April 1st. During Phase III, examiners will continue to review banking organizations' compliance with the FFIEC critical milestone dates for internal and third-party testing and validation. They also will assess how well banks are implementing the remediated systems and the completeness of the contingency planning process.

In addition to the assessment and ratings processes, an enhanced program of Century Date Change monitoring is being implemented. In this program, the level of review work depends on institution size and/or risk.

Common Weaknesses and Performance Ratings

During Phase I of the Y2K supervision effort, the objective was to assess bank Year 2000 plans and their progress in achieving those plans. The most common weaknesses examiners found among less-than-satisfactory banks were:

- Inadequate audit reviews.
- Inadequate assessment of mission-critical and critical applications.

[1] Paul A. Decker and Paul E. Kellogg are Senior Examiners in bank supervision at the Federal Reserve Bank of Chicago. The opinions expressed in this paper are those of the authors and do not represent the opinion of the Federal Reserve Bank of Chicago or the Federal Reserve System

- Lack of an adequate project management plan.
- Lack of knowledge as to the scope and depth of the Y2K problem.
- Perception of Y2K as an IS problem and not an enterprise-wide problem.
- Lack of contingency planning.
- Lack of oversight by executive management and the directorate.

On the positive side, Phase I reviews found that 93.2% of all FFIEC-regulated financial institutions were making satisfactory progress in their Y2K renovation efforts.

The banking supervisors themselves faced many challenges in performing the Century Date Change reviews, including:

- The need to train examiners.
- Coordination efforts with other regulatory agencies.
- Institutions tended to view examiners as "consultants" in renovation efforts, which jeopardized their ability to render independent judgements.

During Phase II the banking supervisors focused on assessing bank remediation progress on program renovation, validation, implementation, and remediation contingency planning. In addition, an assessment of Year 2000 risk management practices relating to credit/counterparty, liquidity, fiduciary, legal, business interruption, and customer awareness risks were made and rated. While our expectation was that banks would have more difficulty in complying with the Phase II requirements, the actual results were better as 97 percent were making satisfactory progress..

Despite the impressive results weaknesses were uncovered that needed attention. The most common Phase II weaknesses found were:

- Failure to evaluate customers' Y2K exposure to the institution.

- Failure to identify customers that present a risk to the institution.
- Failure to implement adequate testing strategies.
- Inadequate communication with directors/management.
- Falling behind schedule.
- Lack of contingency planning for a prompt business resumption.
- Inadequate review by an independent third party of the Y2K renovation project.
- Failure to draft a written remediation contingency plan.
- Failure to appoint staff to manage Y2K program.
- Lack of a formal Y2K project plan.

Phase II reviews also uncovered two somewhat surprising deficiencies that are directly linked: lackluster customer risk assessments and the heightened need for customer outreach.

Customer Risk Assessments

The customer risk assessments proved to be the most consistent weakness examiners found during Phase II. Customer risk assessments of funds takers (loan customers) and funds providers (depositors) have been lackluster at best. Initially, some banks did not fully appreciate the level of risk posed by their customer base and, thus, **were** reluctant to approach their customers for fear of disrupting the account relationship. The use of questionnaires to assess customer risk (without follow-up) failed to provide the depth of information necessary for an adequate risk assessment. The most successful risk assessments were found in banks that utilized relationship managers to collect the information needed through on-site visits with their customers. These visits have yielded superior information for use in assessing risk as well as

providing a positive marketing opportunity. Banks that have utilized this technique have been able to alleviate customer concerns about the bank's efforts in dealing with the Year 2000 problem. In addition, the banks have been able to get their customers' perspectives on the Year 2000 problem. These visits have also been successful in assessing the liquidity risk associated with the millennium problem. Loan commitments are frequently several times loan outstandings**,** and many companies are unsure of what will happen at the rollover date and may plan to have additional liquidity available to meet unforeseen contingencies. To achieve this goal, borrowers may plan to draw down their lines of credit while simultaneously drawing down their deposit balances. These visits have proven very helpful in allowing banks to assess the impact of customer borrowing and transaction plans on their funding strategy. Perhaps William McDonough, President of the New York Federal Reserve Bank, best captured the importance of outreach during a recent speech before the Financial Regulators of the Asia/Pacific Region when he said, "…financial organizations need to provide information on their Year 2000 efforts to their customers and counterparties, their investors, and others. In the case of banks, for example, it is important for correspondent and custodial customers to develop comfort that the bank will be able to function normally in the new century."[2]

Outreach

In addition to their other functions, banks have a unique ability to inform the public of issues and, thus, mitigate the risks related to misinformation. Presently, there appears to be a millennium polarization underway that is creating two camps: those that feel that the rollover will cause an economic Armageddon and those that feel that the event will be inconsequential. This is creating misinformation and unnecessary stress on people and business in general, since

[2] Regional Y2K Meeting for Financial Regulators in Asia/Pacific Region, Remarks by William J. McDonough, October 19, 1998.

each camp's arguments seem to be fueling the fears of the other camp. As a result, many people do not know what to believe anymore.

As we near the millenium rollover date, there are some things regarding the success of the Federal Reserve and the banking system's Year 2000 renovation efforts that people can believe in:

- No one can say there won't be glitches, but we are confident that our nation's financial system will be prepared for the century rollover.
- The Federal Reserve is committed to doing all it can to safeguard the operations of the U.S. financial system.
- As a country, we all share the responsibility for meeting the Y2K challenge. The Federal Reserve and the banking system are doing their parts and we believe the public will do its part as well.
- Public understanding of the banking industry's Year 2000 preparations will help maintain public confidence.

To maintain public confidence, banks have been encouraged by their banking supervisors to conduct outreach to their customers not only as a good marketing tool but also as a stabilizing force to the community. While there have been some banks with very active outreach programs, the outreach efforts of the banking community needs further emphasis. The opportunities to correct customer misconceptions are plentiful. For example, every staff member of the bank should be trained to provide accurate information in their daily contacts and interactions with the community. Those banks that have made little or no attempt to discuss Y2K with their customers are encouraged to do so. Banks that have made outreach part of their daily business are to be commended and other banks are encouraged to follow their example.

Another Peek at the Examiners' Playbook

As examiners execute Phase III**,** they will continue to review internal and third party testing and validation just as they did in Phase II. However, they will emphasize two additional aspects: how well banks are implementing the remediated systems and the completeness of the bank's contingency planning process. From the results of the review, an assessment will be made of each bank's aggregate vulnerability to Y2K-related interruptions and that assessment will be rated utilizing the standard three ratings of "satisfactory," "needs improvement," or :unsatisfactory." Because some financial institutions may pose a greater systemic risk to the banking system than others, these institutions will receive greater scrutiny.

Internal and Third Party Testing

Testing of internal mission-critical systems should have been substantially completed by December 31, 1998, and testing with service providers should have been substantially completed by March 31, 1999.[3] During Second Quarter 1999, the way an examiner will look at testing will fundamentally change. To date, examiners have been assessing whether or not the bank's testing plan appeared reasonable for the upcoming testing phase. Now, examiners will be looking at what has actually occurred during the testing phase to see if the testing plan was adequately carried out. Each examiner's assessment will look at the following areas:

Testing Plan

- Was the testing methodology implemented as planned?
- Were the testing schedules followed?

[3] FFIEC Interagency Statement, Guidance Concerning Testing for Year 2000 Readiness, dated April 10, 1998.

- Were the critical test dates met?
- Were the test results properly documented?

Management Oversight and Control

- Was the board of directors kept informed of the progress of the testing phase on a regular basis?
- Were metrics used to measure progress?
- Were sound internal controls followed during testing?

Implementation of Remediated Systems

Implementation of remediated systems is one of the two areas that examiners will emphasize during Phase III, in an effort to gauge how well the implementation phase is progressing. Is it going smoothly or are there problems developing? In smaller banks, the implementation issue is not great, since most Year 2000 compliant software is moved as a complete package very quickly from the test system to the production system. In larger banks the issue can be more significant, since the implementation process is incremental and, thus, less straightforward. Here it is common to see Year 2000-compliant software running in production alongside non-compliant programs. Examiners will evaluate two areas:

1. Implementation Progress

- Is the bank making satisfactory progress in implementing the Year 2000-compliant software?
- Are there production problems impeding implementation?
- Are these problems serious enough to miss testing date guidelines?

2. Clean Management

Clean management is ensuring that tested and compliant software is not inadvertently corrupted through post-testing enhancements to the program. The examiner will focus on change control to verify that clean management practices were followed on any post changes made to previously tested compliant software.

Contingency Planning

The second area of heightened review in Phase III, and one receiving major emphasis, is contingency planning. The FFIEC guidance on contingency planning involves four phases:[4]

1. Organizational planning. Guidelines - establish guidelines that define the bank's business continuity planning strategy.
2. Business impact analysis - assess the potential impact of mission-critical system failures on the bank's core business processes.
3. Business resumption contingency plan - develop a plan to deal with mission-critical system failures.
4. Validation - the resulting business resumption contingency plan must be tested for effectiveness and viability.

Banks are now required to have two contingency plans in place: a remediation plan and a business resumption plan.

[4] FFIEC Interagency Guidance, Guidance Concerning Contingency Planning in Connection with Year 2000 Readiness, dated May 13, 1998.

Remediation Contingency Plan

During Phase II, banks were required to have a remediation contingency plan in place that mitigates the Year 2000 risks associated with the failure to successfully complete renovation, testing, and implement mission-critical systems. Many bankers have asked whether or not they still need a remediation contingency plan. Here is the guideline. If all mission-critical systems have been remediated, tested and implemented, then no remediation contingency plan is required. If remediation, testing and implementation are not complete, then a written remediation plan should still be in place. This plan must cover four areas:

1. Offer alternatives in the event remediation efforts fail (for banks with proprietary systems).
2. Assess the likelihood that the service provider will be able to provide remediated service for banks using a service provider.
3. Provide alternative service providers in the event the primary service provider is not fully remediated.
4. Establish trigger dates for activation of the remediation plan.

As the milestone date for the final testing of mission critical systems is June 30, 1999, the general expectation would be that trigger points for activation of remediation plans would have been triggered for systems that are not ready.

Business Resumption Contingency Plan

The business resumption contingency plan outlines what steps the bank will take to mitigate operational risk if the remediated mission-critical systems fail. Unfortunately, despite all the time, money, and effort expended on Y2K renovation efforts, the risk of a millennium

related disruption remains. Risk may arise either from an outside system that the bank interfaces and that may not be completely Y2K-compliant or from one or more internal systems that do not function as expected.

Many banks have questioned the need for such a plan since they already have a disaster recovery plan. The answer is yes, a business resumption contingency plan is needed. The contingency plan should be viewed as a disaster recovery plan supplement that pertains exclusively to the millennium problem. A business resumption contingency plan must be in writing and well documented to support its conclusions and procedures. It should have four parts:

1. Organizational Planning

The bank's business continuity planning strategy is created by establishing organizational planning guidelines. Since the directorate and senior management are ultimately responsible for the adequacy of the plan, it is vital that they ensure that adequate resources are devoted to its development. The examiners will be looking for evidence of the following steps in the planning process:

- Assignment of an individual or appointment of a group to develop the continuity plan and to monitor its relevance. These plans are expected to be periodically updated.
- Properly identified MIS-related and non-MIS-related core business processes. Core businesses may involve multiple mission-critical computer systems. The examiners are looking for evidence that the bank has identified the mission-critical systems and other systems that make up its core business processes and that these systems interface correctly.
- A set of event timelines for testing the plan that incorporate both the existing renovation and testing schedule should be established. As a suggestion, this timeline should broken down

between pre-millennium events (a pre-millennium date is entered into the system which causes a system failure) and post-millennium events (a year 2000 date causes a system failure).

- A risk management system should be developed along with a reporting system. Examiners want to verify that the bank is focusing the bulk of its contingency planning efforts on those core business processes that pose the greatest risk. A business impact analysis, which will be discussed shortly, provides a good mechanism for addressing the hierarchy of risk. For example, if the bank being reviewed has a high-impact core business process (such as the demand deposit processing system) but has purchased a renovated and tested processing package and has cooperated closely with the vendor during renovation, the examiner will conclude that this mission-critical system poses only a moderate risk to the bank. The portion of the contingency plan pertaining to the demand deposit processing system would not be expected to be very extensive. In this example, if the bank purchased a processing package with a low-level of coordination with the vendor during renovation, then the examiner will conclude that the system poses a high risk to the bank. In this case it would be expected that the demand deposit processing portion of the contingency plan would be extensive and well detailed.
- Existing business continuity, contingency plans, and disaster recovery programs should be reviewed to ensure that they are complementary with all redundancies eliminated. Finally, examiners will verify that the management reporting process will adequately measure progress.

Business Impact Analysis

The business impact analysis looks at the impact of a failure of the mission-critical systems on each core business process. These analyses should consider the types of risk likely to be found, the likelihood of their occurrence, their estimated cost, and the probable timing of the event. The results of this assessment will provide the underlying support for the contingency plan. This analysis should have three parts:

1. Undertake a series of risk scenarios for each core business process (deposit-taking, check payment, and so forth). Determine the impact of the loss of one or more processes on the institution in light of existing regulatory requirements.
2. Develop Year 2000 failure scenarios. These scenarios should consider the risk of internal and infrastructure failures on each core business segment.
3. Determine the minimum acceptable levels of performance that the bank is willing to accept.

Business Resumption Contingency Planning Development

Once the core business processes have been identified, a risk management process and reporting system developed, and an assessment of the potential impact of mission-critical system failures made, a contingency plan can be developed. In general, the plan should be designed to minimize the impact of service disruptions to the bank and its customers, minimize financial losses, and ensure a timely resumption of operations should a Year 2000 disruption occur. These business resumption plans vary in length depending on the complexity of the institution. At a minimum, the plan must provide an adequate process for enabling the bank to achieve acceptable operational levels in the event of a Year 2000-related problem and a clear blueprint for resuming full operations as soon as possible. When the plan is developed, it should be designed in a way that can be easily altered. As modifications are made to the bank's Year 2000 readiness plan, it

is expected that the contingency plan will simultaneously be modified to incorporate those changes. Examiners will review the plan for reasonableness. Each bank is left to determine exactly what path it will take to achieve its plan. There are six aspects of the plan that examiners will review for completeness:

1. Selection of the most reasonable contingency strategy after an assessment of available options. The central goal of the document should be to maximize speed of recovery consistent with cost and functionality. If your bank utilizes a service provider, its strategy should embody the various alternatives built into the service provider's contingency plan.
2. Evaluation of contingency plans and implementation modes. The central point here is to look at the bank's options and determine if manual systems or outsourcing could be used to support core business activities in the event of a systems disruption. The analysis should contain documentation on which mission-critical reports management needs to recover from a disruption, such as master files, trial balances, and machine readable data files. Other areas of focus should include:
    - Legal counsel review of data processing and service providers' contracts to determine the responsibilities of each party in the event of a disruption.
    - Legal review of data processing insurance coverage.
    - Review and testing of the bank's disaster recovery plan to ensure that Y2K compliant equipment would be available to meet a non-millennium related emergency.
    - Testing of any manual back-ups to mission-critical systems to ensure that they will function as intended.
3. Establish trigger dates to activate the business resumption contingency plans. Banks are responsible for continuously evaluating the progress of their Y2K preparedness and reporting

any significant deviation to management. Trigger dates should be established for implementing the contingency plan that are keyed to critical milestone dates. It is important to allow adequate lead time to obtain alternative sources of servicing when establishing trigger dates.

4. Responsibility for business resumption. The bank should establish a coordinated crisis management process that assigns overall responsibility to an individual or group that is responsible for implementing the contingency plan. Examiners will be looking for a document that clearly assigns responsibility for implementation of the various parts of the contingency plan as well as an outline of the strategy for responding to customer and media reaction to Year 2000 disruptions.

5. Contingency plan independent review. There should be an independent review performed on the feasibility of the contingency plan. This may be performed by a qualified individual in-house, a consultant, a CPA firm with expertise in the area, or other qualified party, depending on the size of the bank. The key is to ensure that a qualified individual/firm has done an independent and objective review of the contingency plan.

6. Implementation strategy for the Millennium rollover and other applicable key event dates.[5] Bank management should ensure that there is adequate staffing in place for the period between December 30, 1999, and January 3, 2000 to meet the demands outlined in the contingency plan. Several bankers have indicated their displeasure at what they perceive as a needless expense. The expense is relative to need and use; it is a lot easier to send people home if no adverse events occur than to try to recall them if problems develop.

[5] FFIEC Interagency Guidance, Guidance Concerning Testing for Year 2000 Readiness, dated April 10, 1998.

Validation

1. Once the business resumption contingency plan has been developed, it must be tested. On May 6, 1999, the FFIEC issued a statement clarifying what were regulatory expectations for the validation phase of business resumption contingency planning. Specifically, it reemphasizes the requirement for institutions to design a validation process by the milestone date of June 30, 1999, but allows them to execute these tests after the June 30th deadline designated for contingency planning. While the tests may occur after June 30th, they still must be completed in sufficient time to modify any contingency plan which may fail a test, and then retest the modified plans. Remember, any changes or modifications to the contingency plan itself should automatically prompt a review of the test plan to insure that the portions covering the area modified are still valid. To ensure that the test program is effective, a qualified individual or firm should perform an independent review.

Risk Based Monitoring and Classes of Risk

During Phase III, the banking supervisory agencies will continue to rely on a risk-based approach to determine the necessary frequency and scope of supervision reviews of banks' Year 2000 renovation activities. Based on experience, banks appear to fall into three risk classes.

1. The low-risk class is banks that have a well-managed Year 2000 renovation program and a sound contingency plan in place.
2. The moderate-risk class belongs to large banks posing greater than average risk due to the size of their activities in key markets. These banks generally have well-managed Year 2000 renovation programs but may lack control over these key market segments.

3. In the high-risk class can be found banks that have not managed their renovation programs well and/or failed to develop a sound contingency plan.

The highest priority for these reviews will be assigned to those institutions which have been identified as possessing the largest potential risk to the banking system and banks that have either not effectively managed their Year 2000 renovation effort or have failed to develop adequate contingency plans. Any bank that has been identified as belonging in one of the two higher classes of risk can expect much greater supervisory scrutiny of its Year 2000 renovation efforts, along with a much higher probability of being subject to a supervisory action and increased FDIC insurance premiums. Banks with normal risk levels will be reviewed using the schedule in Appendix A, which is derived from the Board of Governors Phase III Examination program.[6]

Supervisory Actions

Phase III will be characterized by an increase in regulatory supervisory actions. Those banks not meeting the standards set out in the FFIEC guidance papers can expect to be subjected to supervisory action more rapidly and possibly receive a more severe action than in the past. There are indications that regulators are going to initiate supervisory action much more quickly when banks miss milestone dates than in the past. The levels and the general conditions for qualifying for supervisory action are as follows. These guidelines should serve as a guide only. There will be variations in qualifying conditions between regulators:[7]

- Deficiency Notifications. Banks rated as less-than-satisfactory during Phase III will receive a deficiency letter. The deficiency letter option will generally be used only if the deficiencies are considered minor and easily correctable. Any severe deficiencies will likely subject the

[6] SR 99-2 (SUP), Phase III of the Federal Reserve's Year 2000 Supervision Program and Guidance Concerning Follow-up Enforcement Actions and Applications, dated January 29, 1999.

bank to additional supervisory action, since noncompliance with FFIEC guidelines this late in the renovation process is serious and likely to have an adverse impact on the bank's readiness for the millennium rollover.

- Written Agreement or Cease and Desist Orders. More serious supervisory action will be taken against banks in the following situations:
- Rated as "needs to improve" after Phase I and II reviews and still in noncompliance.
- Rated "needs improvement" after a Phase III review.
- Failed to respond to a Year 2000 deficiency letter.
- Failed to fully comply with the provisions of a previously approved corrective plan.
- Section 39 Orders. On October 15, 1998, the regulators issued guidelines establishing regulatory Year 2000 safety and soundness standards for depository institutions under Section 39 of the Federal Deposit Insurance Act (FDI Act).[8] These guidelines require insured depository institutions to implement appropriate due diligence processes and risk controls as well as mandate board and management involvement in Year 2000 readiness efforts. In addition, it enables the regulators to use streamlined compliance and enforcement mechanisms to address Year 2000 readiness-related safety and soundness concerns for situations in which prompt corrective action is necessary.
- Other Supervisory Actions. If there is a history of substantial noncompliance with a written agreement or a cease-and-desist order addressing Year 2000-related problems, it's highly probable civil money penalties will be assessed or a removal or prohibition action instituted.

[7] Ibid.
[8] FFIEC Guidelines, Interagency Guidelines Establishing Year 2000 Standards for Safety and Soundness, October 15, 1998.

- Insurance Premiums. The FDIC will take action to raise the insurance premiums for banks rated less than satisfactory. Even though the assessments are made on a case by case basis, institutions falling into this category will likely be paying a higher premium for a minimum of 180 days.

International Situation

Banking supervisors worldwide are aware of the dangers posed by the Year 2000 problem and are working together through the Basle Committee on Banking Supervision and the Joint Year 2000 Council to increase awareness and promote greater understanding. The majority of the foreign central banks are confident that the payment and settlement applications under their management will be Year 2000 compliant. However, there are indications that at least some foreign banks which are tied to these foreign central banks may be falling behind. Markets and payments systems and the private firms that are dependent on these institutions for funding may experience what Federal Reserve Governor Roger W. Ferguson, Chairman of the Joint Year 2000 Council, calls the "Year 2000 shadow."[9] Governor Ferguson explains this phenomenon and its potential repercussions this way: "The uncertainty surrounding preparedness for Year 2000 may make markets less liquid as institutions seek to insulate themselves from risk with counterparties who are thought to be unprepared. The financial cost of this is not clear, and I am not one of those forecasting recession as a result of a Year 2000 slowing, but we know from recent events that a flight of liquidity can have severe repercussions in the real economy."[10] Awareness of the seriousness of the situation and cooperative efforts among the different central banks and private financial institutions have increased and are starting to yield results.

[9] Global Year 2000 Summit, "The Challenge of Preparing for the Year 2000", Remarks by Governor Roger W. Ferguson, October 16, 1998.

Conclusion

William McDonough, president of the Federal Reserve Bank of New York, perhaps sums up the situation best: "The failure to get it right will affect the integrity of the payment system, financial markets, and the performance of the domestic and global economies."[11] The time grows ever shorter for banks to achieve Year 2000 compliance. Banking supervisors will continue to intensify their efforts to ensure that the banks they supervise will be ready for the millennium rollover. Regulatory emphasis during Phase III will continue on third party testing and validation but will be expanded to include implementation and the adequacy of contingency planning. Results from Phase II regulatory reviews suggest that these efforts are beginning to pay off; however, a need for greater effort in customer risk assessments and greater emphasis on outreach to customers and the public are indicated. Despite the shift in emphasis from internal and third- party testing and validation in Phase II to implementation and contingency plan adequacy in Phase III, supervision's goal in dealing with the Year 2000 problem remains the same: foster a strong economy and stable financial system while encouraging banks to manage the Year 2000 risks at their institutions. As William McDonough has said, " I am convinced that through the aggressive efforts of the global supervisory community and the firms that we supervise, we can build confidence that the financial sector will rise to the occasion long before January 1, 2000…"[12]

---

[10] Ibid.
[11] Michael J. Mandel, "Zap! How the Year 2000 Bug Will Hurt the Economy", Business Week, (March 1998), p. 96.
[12] Regional Y2K Meeting for Financial Regulators in Asia/Pacific Region, Remarks by William J. McDonough, October 19, 1998.

Phase III Supervisory Program			Appendix A
	2nd Quarter	**3rd Quarter**	**4th Quarter/Rollover**
High systemic risk institutions	On-site targeted exam	Monthly contacts	Monthly contacts/Some continuous monitoring (during weeks preceding rollover)
Community banks	Contact if needed	Risk based contact/ On-site review	Event management
Top 50 bank holding companies	Quarterly contact	Quarterly contact	Quarterly contact/ Event management
Bank holding companies	Contact as needed	Monitor through lead bank/Risk based contact/ On-site review	Event management
Shell bank holding companies	None	If lead bank not satisfactory then on-site review	None
Foreign branch offices/FCMs	Contact as needed	Risk based contact/On-site review of consolidated organization	Event management
Financial institution rated < satisfactory	Monitor monthly/ Corrective action as appropriate	On-site review/Monthly monitoring/Corrective action as appropriate	Event management
Service Providers/ Software Vendors	Quarterly contact (on-site if <satisfactory)	Quarterly contact (on-site if < satisfactory)	Quarterly contact/ Event management/ (on-site if < satisfactory)

Emerging Issues Series

A series of studies on emerging issues affecting the banking industry. Topics include bank supervisory and regulatory concerns, fair lending issues, potential risks to financial institutions and payment system risk issues.

These papers may also be obtained from the Internet at:
http://www.chicagofed.org/publications/workingpapers/emergingissues.cfm

The Impact of New Bank Powers (Securities and Insurance Activities) on Bank Holding Companies' Risk *Linda Allen and Julapa Jagtiani*	**S&R-99-1R**
A Peek at the Examiners Playbook Phase III *Paul A. Decker and Paul E. Kellogg*	**S&R-99-2**
Do Markets Discipline Banks and Bank Holding Companies? Evidence From Debt Pricing *Julapa Jagtiani, George Kaufman and Catharine Lemieux*	**S&R-99-3R**
A Regulatory Perspective on Roll-Ups: Big Business For Small Formerly Private Companies *Michael Atz*	**S&R-99-4**