ZERO NINES
ALWAYS AVAILABLE™

Compliance, Security and Continuity

the Value of ZeroNines®

ZERONINES: WHITEPAPER

www.zeronines.com

This document (“Brief”) was prepared by the management of ZeroNines Technology Incorporated (“ZeroNines”), and is being furnished by ZeroNines, subject to the prior execution of the Confidentiality Agreement, solely for use by a limited number of third parties potentially interested in exploring business continuity solutions. ZeroNines does not make any representations as to the future performance of ZeroNines. Additionally, ZeroNines believes that the sources of the information presented herein are reliable, but there can be no assurance that such information is accurate and ZeroNines expressly disclaims any and all liability for representations or warranties, expressed or implied, contained in, or for omissions from, this Guide or any other written or oral communication transmitted or made available, except such representations and warranties as may be specifically provided in definitive contracts to be executed and delivered. Except as otherwise indicated, this Guide speaks as of the date hereof. Neither the delivery of this Guide nor any ensuing discussions conducted hereunder shall, under any circumstances, create any implication that there has been no change in the affairs of ZeroNines after the date hereof, or other specified date. This Guide is being furnished for information purposes only with the understanding that recipients will use it only to decide whether to proceed with discussions with ZeroNines management involving ZeroNines solutions. The information contained in this Guide is confidential and proprietary to ZeroNines and is being submitted solely for recipients’ confidential use with the express understanding that, without the prior express permission of ZeroNines, such persons will not release this document or discuss the information contained herein or make reproductions or use it for any purpose other than potential discussions with ZeroNines management. By accepting this Guide, the recipient reaffirms its obligations set forth in the Confidentiality Agreement entered into in connection with the receipt of the Guide and agrees: (a) to maintain in strict confidence the contents of the Guide in accordance with such Confidentiality Agreement; (b) not to copy any portion of this Guide, and (c) if the recipient of the Guide does not enter into a transaction with ZeroNines to promptly return this Guide to ZeroNines at the address below. Inquiries regarding ZeroNines should be directed as follows:

For financial matters

Mr. Sean Myers, COO

ZeroNines Technology, Inc.

Corporate Headquarters

5445 DTC Parkway, Penthouse

Four Greenwood Village, CO 80111

+1.844.976.3696

Sean.Myers@ZeroNines.com

For all other matters

Mr. Alan Gin, President and CEO

ZeroNines Technology, Inc.

Corporate Headquarters

5445 DTC Parkway, Penthouse

Four Greenwood Village, CO 80111

+1.844.976.3696

Alan.Gin@ZeroNines.com

Contents

Intentionally blank

Introduction

Compliance, security and continuity

Audit standards for publicly held companies and the adjudication of Federal investigations of those companies have changed. These changes raise the bar and create demand for different mindsets, better processes and failsafe systems.

The Sarbanes–Oxley Act authorizes the Public Company Accounting Oversight Board to create audit standards for public companies. Beyond the GAAP standards with which you and your auditors are already familiar, there are now PCAOB audits.

Because of post-Enron developments, the PCAOB audit standards presume fraud. The firm has an opportunity to prove itself innocent of fraud. Assessment of a defendant's mental state includes both known and should-have-known; malice is no longer required to find fault. It could be argued that a negligence standard for criminal liability of officers and directors now exists, so that anything less than meticulous management has practically been criminalized. In the American legal tradition this is radical, but it must be addressed.

Operational audits that have been advisory in the past, such as information security or disaster recovery audits, now have teeth. A company that is "unable to locate" a required document or an email is automatically at fault in an investigation. If a health care provider does not comply with HIPAA's requirement for electronic personal health information to be accessible and secure in a disaster, their patient isn't the only person with a problem. And of course the "uptime" of the US banking industry has long been regulated.

Security and availability are flip sides of the information coin, and compliance requires them both. Deep in the process plumbing of your organization, audits and assessments performed as part of a *disaster recovery* strategy, such as Business Impact Assessments, have become the basis of modern *security* audits. In turn, these security audits support *compliance* audits.

Whether the cause is Katrina, al Qaeda or avian flu, operational crises destroy shareholder value. As Americans we prefer building the future to pondering these matters, but senior executives responsible for the whole picture have no prudent alternative. Continuity, security and compliance are essential design principles for your firm's processes, systems and the information technology that enables them. Customers are beginning to judge by the new standard of *business continuity*, virtually 100 percent accessibility.

ZeroNines is not the only firm to notice the natural synergy of IT investments to serve multiple regulatory and business objectives. In early 2004, principals of McKinsey & Company published advice to their banking clients interested in Basel II, to "consider combining

the IT programs they undertake for Basel II with those needed to comply with the US Sarbanes–Oxley corporate-governance legislation….[1]

ZeroNines enables compliance and security by enabling business continuity. Our licensees can do things that no one else can. Our patented intellectual property enables:

- Sox compliance
- HIPAA compliance if you're in health care
- Basel II and Federally expected resilience practices if you're in financial services, as well as
- business continuity needs that challenge the best COOs and CIOs.

We disaster-proof your business application software without massive overhauls. What we offer leverages your existing investments, works better than commercial alternatives, and diminishes the burden on your people during normal operations and during a disaster. We've tested this, it works, we've been using it internally for years, and it is now available to your organization.

This Brief addresses senior business executives, particularly those *without* a background in law, regulatory affairs, compliance or information technology. We summarize points of law and regulation, and introduce the value of ZeroNines' technology to enable compliance, security and continuity.

Senior IT architects and other readers who prefer a technical description are encouraged to complete this document and then to consult a related Technical Brief, *ZeroNines Technology Architecture Overview,* which illuminates one of our patents.

Sarbanes–Oxley Act

Introduction

The Sarbanes–Oxley Act requires that a publicly traded company's management regime include five primary components:

- control environment
- control activities
- risk assessment
- information and communication
- monitoring.

Sox includes control objectives for design of the firm's control environment and activities. These control objectives are:

- Confidentiality—private information is not disclosed
- Integrity—information is not altered or corrupted
- Availability—information is not lost, erased or stolen, but available to those within the company who need to know, outside the finance department.

(For ZeroNines' analysis of December 2006 regulatory proposals, see "December 2006 regulatory update" on page 17.)

Value of ZeroNines

ZeroNines enables all three of these control objectives with a *business continuity architecture* that disaster-proofs software without major rewrites, tracks every email, keeps at least two copies of every transaction, leverages existing investments—and is supplier-neutral.

Conventional disaster-proofing of application software is like fixing the Year 2000 bug, but managerially worse. The problem, albeit certain—a disaster *will* strike—has an unknown deadline.[2]

With the Y2K bug, two-digit year variables were going to "roll over" to zero, at least rendering incorrect year values for use in software. In more extreme cases the variables were denominators of fraction calculations, triggering divide-by-zero errors that halted part or all of the programs. References to year variables were spread throughout the computer program code. To fix the Y2K problem, each reference had to be identified, assessed, fixed and tested.

The conventional approach to disaster-proofing application software includes attention to its input/ouput (I/O) controls, the means by which programs read data to or write data from hard disks and other "peripherals" that serve the processors. *Most I/O controls have not been written to tolerate failures*, either by waiting a specified length of time or attempting the operation again. (Even those that do "limit their patience" by design.) As with the year references in the Y2K bug, each disaster-dumb I/O control must be identified, assessed, fixed and tested.

ZeroNines patented architecture includes adapters (the industry's technical term is "interfaces") that handle the input/output operations. The AlwaysAvailable architecture enables the application software to keep going.

HIPAA

Introduction

The Health Insurance Portability and Accountability Act of 1996 is best known as the law requiring that:

- health insurance continuance be available to a worker after employment termination
- doctors and dentists disclose privacy practices
- a patient's personally identifiable health information be kept secret.

HIPAA's reach is broader than this popular perception. Regulations from the Department of Health and Human Services project into the health care industry some principles from Sarbanes–Oxley and disaster recovery expectations from banking and other essential-infrastructure industries. HHS has defined "a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to individuals remains secure."[3] The health care industry is now viewed as essential infrastructure and is being regulated by the Federal government as such.

Required and Addressable provisions

Regulations to implement HIPAA include *Required* and *Addressable* provisions. Required provisions are uniformly mandatory. If a regulated entity's risk assessment identifies a threat or problem relevant to an Addressable provision, then the entity must develop and document a response. If the risk assessment has not identified a threat or problem relevant to the Addressable provision, the entity may choose not to act upon the rule, but must document that decision.[4]

HIPAA's Required provisions of Section 164.308(a) are that a regulated entity have each of the following:

- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan.

Provisions that are Addressable by each regulated entity are:[5]

- Applications and Data Criticality Analysis
- Testing and Revision Procedures.

Value of ZeroNines

ZeroNines enables all three of the Required provisions without obstructing either of the Addressable items. ZeroNines' patented technology enables organizations in most industries, not only health care, to surpass all current commercial data availability and disaster recovery designs by using our business continuity architecture.

Our AlwaysAvailable technology makes multiple copies of every transaction on-the-fly, obviating "recovery" by preventing software disaster in the first place.

Continuing to operate in both normal and emergency settings, the architecture respects criticality analyses by scaling. Applications that require 99.99999% availability ("seven nines") can be administered on the same platforms as applications that require only 99.9% ("three nines"). An application that requires 100% availability ("zero nines") can also be supported.[6]

Basel II

Introduction

If your company does business in the US and either Canada or Europe, chances are that at least one of your banks already uses or is preparing to use Basel II-compliant practices to serve you. If you are in the banking industry, you already know that Basel II is the recent regulatory standard from Basel Committee on Banking Supervision.[7]

Also known as the Capital Accord or simply the Accord, Basel II prescribes good banking and business practices. It aims to:

- ensure that banks' allocation of capital is more risk-sensitive
- separate operational risk from credit risk and provide separate capital charges for each
- bring about a convergence of economic and regulatory capital
- vary capital requirements between banks with differing types of business
- encourage banks to use internal systems to derive levels of regulatory capital.

Basel II addresses market, credit and operational risk, establishing a lowest common denominator of operational risk management practices. Operational risk is defined as an institution's exposure to losses from "inadequate or failed internal processes, people and systems, or external events."

Not surprisingly, consultancies such as McKinsey and Accenture urge their clients to embrace the Accord for competitive improvement and operational efficiency:

> Organizations that become Basel II-compliant early will gain real competitive advantages through superior capital efficiency, *data* and risk management *uniformity*, enhanced credit ratings, *reduced operational losses* and an improved credit risk/return profile (emphasis added).[8]

Using its own client work and benchmarks from other improvement efforts, McKinsey estimates *Basel II-style efficiencies can raise pretax earnings by 3 to 6 percent*. Mitigating operational losses alone, including conventional perparation for system breakdowns, can account for a third of the improvement.[9]

As with most business practice improvement, Basel II compliance is not confined to IT departments. The entire organization effects successful implementation, and risk management becomes a design principle of core business processes.[10]

A central role for IT in financial services, however, is unavoidable. Enhanced IT systems and data integration will account for more than 75 percent of the investment that the Accord requires of most banks. The cost categories are design and program management, prototyping and development of models, application development, hardware, systems integration, data migration, and organizational and business transformation.[11]

Adoption of a standard data set is one likely business and IT outcome. Even if first adopted as a result of the regulatory pressure, consistent data opens possibilities for streamlining business processes and creating new services. Operations that run on a single image of data—not only in banking as a result of Basel II compliance, but in other industries—are able to interact with customers with greater intelligence.[12]

Value of ZeroNines

ZeroNines' AlwaysAvailable architecture enables continuous availability of a single logical image of business data, even amid traumatic events such as natural disasters. We use our patented technology in our own business. The AlwaysAvailable technology also supports multiple logical images as required by different mission-critical software components of your enterprise. Single or multiple is your choice.

Federally expected resilience practices

Introduction

ZeroNines' belief in the value of business continuity exceeds our faith in disaster recovery strategy and commercially available products and services. Our founders have seen so many organizations go down because of the limitations of widely used single-vendor DR implementations. ZeroNines has developed the patented AlwaysAvailable method and architecture to enable real multivendor business continuity.

Data security and business continuity are valuable because operational failures are expensive in their direct and indirect costs. A vivid example of direct cost is lost revenue. An indirect cost is a drop in the company's stock price after an operational crisis.

These are examples of *private* value of business continuity, when the paychecks of one set of employees, or the wealth of one set of shareholders, is at risk.

Systemic risk is the value lost when the interaction of different companies or parts of the economy is disrupted. This is the conceptual space where economic damage grows exponentially and the complexity of recovery stupefies the imagination. It is the place where more and more companies now greet regulators who are interested in uptime. We believe regulators are beginning to view firms that cannot recover quickly as imposers of economic externalities, like polluters, only with a greater sense of urgency. Appropriately or not, what has long been a private matter of competition is becoming a public matter of regulation.

As part of the Federal regulatory response to 9/11, three Federal agencies solicited financial services industry comments on draft Resilience Practices for the US financial system. The thrust and intent of the draft was retained in the Interagency Paper issued in April 2003. The Paper now has Final Rule status.[13]

In interpreting the Interagency Paper, ZeroNines concurs with the Evaluator Group, a consultancy, to wit:

> Every CIO and Chief Legal Officer needs to read these documents. While they apply only to their industries in the short run…, they…. will define security standards for much of the IT industry by the end of this decade.[14]

Regulators now expect essential industry participants to affirm reasonable disaster recovery objectives, to implement sound practices for fulfilling those objectives, and we believe the regulators have asked firms—this is crucial—to exceed the capability of all commercial disaster recovery technologies known to exist at the time the rules were disseminated.

The disaster recovery objectives that the regulators sought to affirm are:

- Rapid recovery and timely resumption of critical (i.e. essential) operations following a wide-scale disruption
- Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location
- A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangement are effective and compatible.[15]

In general terms, the sound practices that the regulators require are:

- identify essential activities in support of the firm's stakeholders, especially its transaction counterparties
- determine appropriate recovery and resumption objectives for these activities
- maintain sufficient geographically dispersed resources to meet recovery and resumption objectives
- routinely use or test recovery and resumption arrangements.

Regulators expect essential firms to recover and resume with zero data loss within two hours of a disaster (the two-hour rule) using a distant secondary site (the dispersal rule). They state that "back-up sites should not rely on the same infrastructure components (e.g. transportation, telecommunications, water supply and electrical power) used by the primary site." Regulators clearly want a failover site hundreds of miles away from the primary site so the secondary site is not disrupted by the same weapon of mass destruction, earthquake or hurricane that disrupts or destroys the primary site. When the Interagency draft was circulated for comment in August 2002, all three of these trauma scenarios were plausible.

The two-hour rule and the dispersal rule cannot be satisified jointly by any commercial disaster recovery technology from any leading service provider or vendor today.

[A]ccelerated intra-day recovery/resumption with zero data loss, and a separation of 200-miles [sic] between primary and secondary sites, are technologically incompatible at this time….[C]yber-

attacks, which represent a clear and present danger … are not sufficiently addressed by the Draft Interagency White Paper.[16]

Value of ZeroNines

ZeroNines' patented AlwaysAvailable technology supports *continuous* service from your company's essential business application software *regardless of distance*. We have been operating a mission-critical application of our own across multiple server sites separated by thousands of miles across three regional electrical grids since July 2004. Our clients have experienced no downtime from the servers; client requests for transactions have always been served as they expect, even though service from one of the sites was interrupted by three local outages. Our technology also protects your firm from common cyber threats such as distributed denial of service attacks. Our architecture includes a Data Authorization Manager to resist hacker attacks and spam.

Value of ZeroNines

What's different about our intellectual property

ZeroNines' business continuity approach is superior to disaster recovery for one principal reason. This reason is so simple that merely stating it understates it.

Our transaction-based, supplier-agnostic MultiSynch technology does not rely on primary » secondary failover, which we believe is more fail-ready than fail-proof.[17] In the ZeroNines MultiSynch design, *all of your production servers are primary and can be thousands of miles apart*. With MultiSynch, essential application software does not experience a disaster; it prevails, enabling people to communicate and focus on the real concern in a crisis, your stakeholders.

Your organization does not recover data or processing because they are not lost. No disaster, no recovery. For commercial organizations, which don't have an endless supply of tax dollars, that's revolutionary—so much so that it's patented.[18]

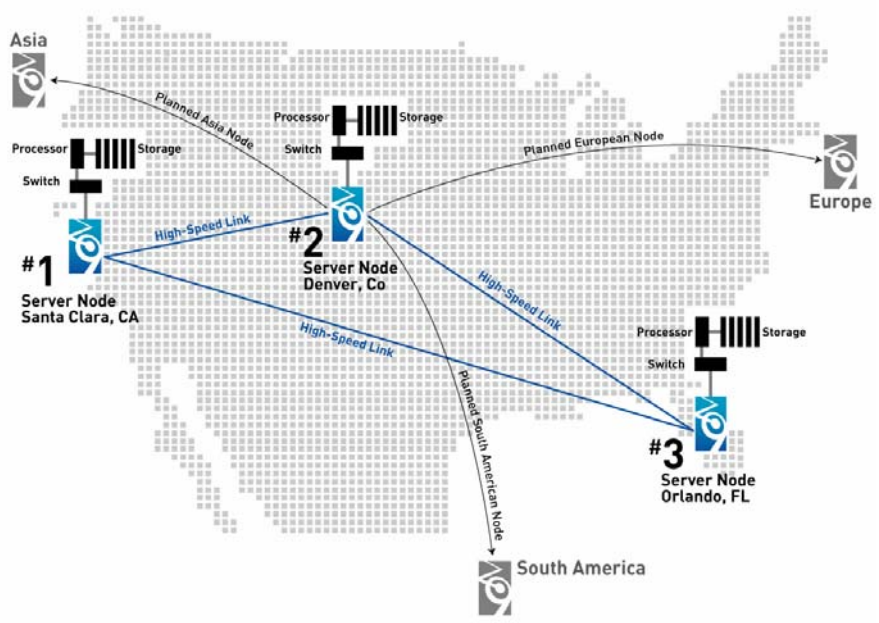

Figure 1
MyFailSafe.com topology, on continuously since 2Q2004

Why existing approaches are expensive and risky

ZeroNines believes that legacy disaster recovery methods are expensive, even recognizing that downtime costs US firms a visible fraction of annual revenue. Legacy recovery capability is expensive because hot sites from traditional service providers:

- must be too close to the primary site to avoid effects of the same earthquake, hurricane, utility-grid (or worse) man-made crisis, an indirect cost realized when recovery fails
- require duplicate hardware and operating system software from the same vendors, and the costs of this certain lock-in are passed to your company
- are available from a concentrated industry that historically has commanded high gross margins for oversubscribed recovery assets—a direct expense, oligopoly service pricing, and a clear and present danger of lack of access when a real disaster strikes.

Why ZeroNines is better

Using ZeroNines' patented MultiSynch architecture, your firm does not have to spend more for business continuity than for fail-ready disaster recovery—and you own something that you can trust.

- A MultiSynching configuration is more secure because the very design deflects distributed denial-of-service attacks, a notorious aspect of the Internet over the past decade.
- Supported distances are superior, so your indirect or opportunity cost is minimal or zero (no disaster, no recovery).
- Getting there is easier, too. Your CIO does not need duplicate hardware or operating systems, so vendors are denied lock-in and your fully depreciated assets can be utilized. Differing speeds can be patchworked with no functional detriment, so prototyping and testing are easier to start and produce realistic baseline results.

Case study of MyFailSafe.com

ZeroNines Technology, Inc., invented MultiSynch technology and has been using for years in our own business for our own operational continuity. We rely on it.

For us, email is a mission-critical business application, so we commenced a MultiSynch implementation with the MyFailSafe.com email service (Figure 1 on page 12).

The MyFailSafe service has run continuously since we started it in July 2004 across nodes in Florida, Colorado and California, even though service from the Florida node was lost three times to local outages.

MyFailSafe also includes a security feature with superior anti-spam benefits that we especially appreciate.

Intentionally blank

Conclusion

Compliance, security and continuity

Audit standards for publicly held companies and the adjudication of Federal investigations of those companies have changed. These changes raise the bar and create demand for different mindsets, better processes and failsafe systems.

Anything less than meticulous management of data, emails and other documents by officers and directors now seems practically criminalized. Whether it should be is a separate question. For compliance purposes now, prudent management requires efforts that are extraordinary in our tradition, more than merely asking your CIO to keep purchasing computer storage to back up your business data.

Information security and business continuity standards are changing and the trend is clear. Customers are beginning to judge by the new standard of *business continuity*, virtually 100 percent accessibility. The more important your firm is to the economy—the more successful it is or the more central its role in commerce—then the more likely you face the security and continuity requirements of regulated industries. We are not saying that this degree of government involvement is appropriate or not. We state that it is expanding.

ZeroNines enables compliance and security by enabling business continuity. Our licensees can do things that no one else can. Our patented intellectual property enables:

- Sox compliance
- HIPAA compliance if you're in health care
- Basel II and Federally expected resilience practices if you're in financial services, as well as
- business continuity needs that challenge the best COOs and CIOs.

We disaster-proof your business application software without massive overhauls. What we offer leverages your existing investments, works better than commercial alternatives, and diminishes the burden on your people during normal operations and during a disaster. We've tested this, it works, we've been using it internally for years, and it is now available to your organization.

Intentionally blank

December 2006 regulatory update

Introduction to the 12/22/2006 update

As part of its regular strategic intelligence program, ZeroNines scans for regulatory developments that are likely to affect our clients.

In December 2006, the Securities and Exchange Commission announced Interpretive Guidance for Section 404 of the Sarbanes–Oxley Act of 2002. The Commission also announced changes to the compliance schedule for the smallest publicly traded companies. The Public Company Accounting Oversight Board separately announced proposed changes to a related auditing standard.

What the Commission and PCAOB did *not* announce is at least as important to ZeroNines' clients as what they *did* announce. Our summary, analysis and conclusions are as follows.

Background of the announcements

The regulatory announcements can be understood only in the anxious compliance context since 2002, when the Act was passed by Congress, and June 2003, when the SEC implemented Section 404.

Corporate management has lacked guidance about how to comply with Section 404. Among other provisions, Section 404 orders that:

- management must attest to the existence and effectiveness of the firm's internal controls
- auditors must file two audit opinions, one on the effectiveness of the controls themselves and a separate opinion on management's assessment of those controls.

Lacking interpretive guidance and faced with rising E&O insurance premiums, corporate officers and Board members attempted to reduce career risk by purchasing audit services based on Federal Audit Standard 2 for internal controls (AS2). In effect, since management didn't have guidance, at least the external auditors seemed to have it; and even if the auditors didn't have it, they had to file the opinions anyway. These "compliance puts" purchased by management were expensive. A Finance Executives International survey of 217 public companies in March 2005 found average first-year Section 404 compliance expenses of $4.4 million for

approximately 27,000 hours of internal work and 8,000 hours of external work, including an increase of 57% in audit fees.[1]

Summary of the announcements

On December 13, 2006, the SEC announced that it was proposing Interpretive Guidance pertaining to Section 404 of the Act. Two days later the SEC announced proposals to change the compliance schedule for firms with a public float of less than $75 million. On December 19, the PCAOB announced proposals for change to related auditing standards. These proposals were to be published in the *Federal Register* for public comment.

Section 404 interpretive guidance[2]

The Commission proposed "risk-based" Interpretive Guidance for management pertaining to Rules 13a–15 and 15d–15 in place of an AS2-based approach. Crucially, the Commission also said that "[A] company choosing to perform an evaluation of internal control in accordance with the interpretive guidance would satisfy the annual evaluation required by those rules."

The SEC stated that:

- First, management should evaluate the *design* of the controls that it has implemented to determine whether there is a reasonable possibility that a material misstatement in the financial statements would not be prevented or detected in a timely manner….
- Second, management should gather and analyze *evidence about the operation* of the controls being evaluated based on its assessment of the risk associated with those control.

In its Interpretive Guidance announcement the SEC added the following:

- In the absence of guidance, management has looked to the … auditing standard [AS2] to conduct their evaluations, which is not what was intended. With this guidance, management will be able to scale and tailor their evaluation procedures to fit their facts and circumstances, and investors will benefit from reduced compliance costs.
- Our proposed guidance is based on risk and materiality…. It is also intended to rebalance control over the process by providing management with its own guidance—without the need to look to auditing standards—for evaluating internal control over financial reporting.

In a speech, Commissioner Campos added:

- [T]he removal of the requirement for an auditor to evaluate management's assessment process will effectively "de-couple" it from an auditor's attestation, such that management will now be able to exercise more flexibility in tailoring its approach.…[M]anagement's assessment is to be conducted without the need to consult the auditing standards.
- [T]o appropriately identify and assess risks, smaller, less complex companies may be able to rely on managements' daily involvement with the business. …[M]anagement's assessment must be supported by evidential matter that provides "reasonable support," but … management can exercise significant judgment and maximize efficiencies in determining what documentation is necessary.

Small companies announcement[3]

In its small-companies announcement on December 15, 2006, the Commission postponed compliance requirements for firms with a public float of less than $75 million.

- Newly public companies do not have to include auditor attestation or management reports on internal controls in the first annual reports that they file after going public.
- Management assessments of internal controls are now due in 2008, one year later than expected.
- External auditor assessments of controls are also postponed by one year to 2009.

PCAOB announcement[4]

On December 19, 2006, the PCAOB announced proposed changes to Audit Standard 2 and voted to extend the public comment to 70 days, 10 days more than the customary comment period. Highlights of the PCAOB announcement are as follows:

- make the external auditor's work risk-based along the lines of the SEC proposal, eliminate unnecessary procedures (such as evaluating management's process), and make the audit more scalable for smaller and less complex companies
- allow the auditor to use the work of others, and not just internal audit, for both the internal control audit and the financial statement audit, eliminating a barrier to integration of the two audits.
- focuses multi-location auditing on risk rather than coverage.

Analysis and conclusions

ZeroNines' analysis and conclusions of the announcements are as follows:

- Basel II logic is spreading
- Budget for a "Reporting Impact Assessment"
- Don't expect lower E&O premiums
- Size can help you but not hide you
- Multi-location risk analysis raises profile of recovery sites.

Basel II logic is spreading

The Commission's emphasis on risk-based regulation is informed by the Basel II approach, and this is good news for shareholders. U.S. regulation now seems tuned to the British model. It cannot have escaped the SEC's attention that stock exchanges in London and Hong Kong recently caught up to New York in the quantity of new public listings after many companies decided the Section 404 regime wasn't worth the headaches. So the SEC has responded both to international competition and domestic business lobby pressure, particularly from small business.

The benefit from diffusion of Basel II's risk-based logic outside the banking industry is that efficiencies identified in McKinsey's estimates are now more broadly applicable, with tangible benefits to pre-tax earnings in multiple industries. (Revisit "Basel II" on page 7 for a refresher.) We expect the incremental benefit to be most dramatic in firms that have not recently updated their Total Quality Management or Six Sigma efforts. We believe that a portfolio approach to risk is a winning management practice and we encourage our clients to take the plunge.

Budget for a "Reporting Impact Assessment"

Some ZeroNines clients will want to retain external audit services to develop risk-based designs of reporting controls so that the out-year monitoring is less expensive. As part of our view on a portfolio-based approach, ZeroNines has long believed that Business Impact Assessments are essential to rationalizing business continuity investments. Parallel reasoning and an inference from the SEC's Interpretive Guidance suggest that a "Reporting Impact Assessment" is a wise investment of consulting dollars and management time.

Not all material control risks will be large and discrete. As the SEC mentioned in its announcement, "an aggregate of significant deficiencies could constitute a material weakness."[5] The concept of systemic risk that we introduced at the macro scale in this paper can also operate at the micro scale, within a given firm (see "Federally expected resilience practices" on page 9).

After paying auditors so much in recent years, many of our clients are certain to find the thought of commissioning another external auditing study to be overkill. Yet auditors will be unable to assess future controls without understanding the risk assessment. Building auditor understanding by involving them early conveys a better benefit:cost ratio for shareholders.

Don't expect lower E&O premiums

All that said, clearly the compliance puts have expired and the auditors' three-year revenue windfall is over. Attempts to deflect career risk to external auditors through the purchase of AS2 services in lieu of interpretive guidance is not tenable. The SEC has placed responsibility for design and assessment of internal controls squarely in the lap of senior management. The Commission also notes that utilization of the Interpretive Guidance can be flexible and on its own constitutes compliance with the annual evaluation required by the Rules cited.[6]

Although this change will likely reduce senior management frustration with the regulatory regime to what it was prior to the Enron meltdown, the exercise of judgment by management that is now explicitly expected for compliance is likely to increase upward pressure on E&O insurance premiums for officers and directors. Future shareholder lawsuits may be more numerous, and auditors may be less likely to be dragged into paying judgments. Plan to move out-year budget from "external audit" to "officer and director insurance" while keeping some of the front-year external audit budget for the Reporting Impact Assessment.

Size can help you but not hide you

ZeroNines' smaller public clients who were hoping for an exemption from the Act need to prepare. No more publicly held companies are exempt from Section 404 now than were before the announcements.

It is obvious, however, that the regulators have listened to the concerns of these firms and responded, with both the delay in filing requirements and the guidance about management's daily involvement in the business. An example of such involvement is monitoring email traffic.

Multi-location risk analysis raises profile of recovery sites

By changing the focus of multi-location audit planning from coverage to risk, the PCAOB increases the chances that auditors will understand the exposures of the "failover" disaster recovery strategy. ZeroNines believes the SAS 55 / SAS 76 audit regime leaves audit committees and Boards relatively uninformed about the systemic risk of oversubscribed mitigation assets.

Notes

1 "The Business Case for Basel II," Buehler, D'Silva and Pritsch, *The McKinsey Quarterly*, 2004 Number 1.

2 As with other initiatives, this uncertainty affects the budgeting process in many large firms: something that is important never seems urgent, but when it becomes urgent, it's too late.

3 Federal Register, August 12, 1998, p. 43249.

4 Healthcare Information and Management Systems Society, himss.org.

5 From our experience with Business Impact Analyses in large, complex organizations, we would be surprised if a Criticality Analysis is irrelevant in any large hospital.

6 The name ZeroNines was coined in 2000 when one of our founders briefed an analyst from GartnerGroup, a consultancy with its heritage in information technology. As we concluded our presentation the analyst noted, "What you've developed in this architecture offers customers more than five nines availability…. You essentially take information technology availability to zero nines."

7 Unless otherwise noted, what follow is based upon "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," Basel Committee on Banking Supervision, Bank for International Settlements, November 2005.

8 "The Point: Wake-up Call," 11/1/2005, accenture.com.

9 "The Business Case for Basel II," Buehler, D'Silva and Pritsch, *The McKinsey Quarterly*, 2004 Number 1.

10 "Early to Basel II, Early to Rewards," Armstrong and Fink, 2/10/2005, accenture.com.

11 "The Business Case for Basel II," Buehler, D'Silva and Pritsch, *The McKinsey Quarterly*, 2004 Number 1.

12 "The Basel II Accord—How it may benefit banks that comply," Ayman Abouseif, 1/18/2004, ameinfo.com. At the time of publication, the author was a senior marketing director at Oracle Corporation.

13 Unless otherwise noted, what follows is based on ZeroNines analysis and "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System." Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Securities and Exchange Commission. April 2003.

14 "All aboard the new federal security rules super train," Jack Scott, TechTarget.com, 6/11/2003.

15 The new focus on "external continuity arrangements are effective and compatible" addresses a concern that ZeroNines articulated in a *Brief* to our clients in 2002. Prior to the Resilience rules, the challenge of interpreting SAS audit requirements led us to conclude that interaction between a DRSP and its client was not an auditable matter. We believed that audit committees and boards were, therefore, relatively uniformed about the systemic risk of oversubscribed assets. The Resilience rules suggest that DRSP–client interaction is now auditable. This is a step in the right direction. Oversubscription of DRSP assets, however, appears to pose systemic risk.

16 "SunGard Offers Comments on Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System." Press release, 12/18/2002. http://www.sungard.com.

17 We don't say this lightly. ZeroNines has developed and patented separate technology in failover, but we don't use it in our business because we don't trust failover to enable business continuity.

18 US Patent 6,760,861, July 6, 2004.

19 "Economic Consequences of the Sarbanes–Oxley Act of 2002," Ivy Xiying Zhang, AEI–Brookings Joint Center for Regulatory Studies, 2.

20 sec.gov.

21 sec.gov.

22 PCAOB Rulemaking Docket 021.

23 "Trouble Ahead for the SEC's 404 Plan," David M. Katz, CFO.com, 12/14/2006.

24 sec.gov.

ZERO NINES
ALWAYS AVAILABLE™

www.zeronines.com

For more information: **info@zeronines.com**

ZERONINES: **USE CASE**

ZERO NINES
ALWAYS AVAILABLE™

Corporate HQ
5445 DTC Parkway
Penthouse Four
Greenwood Village, CO 80111

T: (303) 814-8121
F: (303) 814-1495

ZeroNines® Technology, Inc. provides a new standard in network disaster recovery, shifting the paradigm from reactive recovery to proactive business continuity. Our Always Available™ information security and availability technology pushes application uptime beyond five nines (99.999%) to virtually 100% anytime, all the time – zero nines. This enables uninterrupted access to business data, applications, and transactions despite disasters or network disruptions that would otherwise cripple the enterprise. Always Available™ processes all transactions in parallel on geographically dispersed servers that are all hot and all active, eliminating single points of failure. It operates agnostically across multiple platforms, leveraging existing processing and storage infrastructure. We also offer enterprise infrastructure assessment, program management and project implementations. Founded in 2000 and based in Denver, Colorado, ZeroNines' primary target customer base includes Global 2000 companies.

Contact ZeroNines today to find out how your business can be Always Available!

info@zeronines.com
www.zeronines.com