A MICROMUSE WHITE PAPER

ASSURING SARBANES-OXLEY COMPLIANCE THROUGH EFFECTIVE IT GOVERNANCE

Micromuse Inc.
139 Townsend Street
San Francisco, CA 94107
(415) 538-9090
www.micromuse.com

INTRODUCTION

Regulatory Acts like the US Public Company Accounting and Investor Protection Act, also known as Sarbanes-Oxley (SOX), are driving greater accountability of the management and IT Operations in Public Companies. Implemented by the Securities and Exchange Commission in response to the fraudulent activity surrounding the Enron and Worlcom debacles, Sarbanes-Oxley aims to assure the accuracy of financial reporting and supporting process, through management assertion of financial reporting accuracy, as well as external auditor review of financial process, and implementation of enhanced financial and operational controls.

This whitepaper will provide executive and IT management with the necessary insight needed to not only address Sarbanes-Oxley and other regulatory compliance issues, but will also provide the recommendations on potential best practices, and methodologies that can support long-term business and operational objectives.

THE IMAPCT ON IT

While companies with well documented manual processes can achieve Sarbanes Oxley compliance, most companies are turning to technology to enhance IT controls, as a means of minimizing the risk of failures in process. With some deadlines past, and others looming, Sarbanes-Oxley has been described as "Y2K without an end date" – even those companies that find themselves with good controls, will need to continually enhance their operations to meet new regulation, and 'material changes', such as acquisitions or changes in key supporting systems that may impact reporting.

With audits nearing completion and in some cases extending past original deadlines, public companies are quickly realizing that the perceived loose requirements dictated by Sarbanes-Oxley legislation are broader in scope than previously anticipated and beyond the pure documentation of financial reporting process. Auditor recommendations for IT control enhancement are extending the need for documentation of IT process, with key areas of focus spanning change management, configuration management, and problem management processes. Compliance also requires greater retention of historical data such as access controls events for applications, systems, and supporting infrastructure to substantiate the existence of adequate controls.

In light of new documentation and control requirements, IT budgets are being stretched beyond capacity. Normal IT initiatives, funding and resources are giving way to Sarbanes-Oxley requirements. The big question for IT operations is how to quickly enhance SOX controls, while supporting the long term business objectives of the business.

Luckily, there is light at the end of the tunnel. For many organizations, industry best practices and standards can provide the flexible framework to not only support these types of initiatives, but also help align business and operational objectives to help address dynamic regulatory requirements, while driving 'Business Acceleration'.

THE ROLE OF STANDARDS IN ADAPTIVE COMPLIANCE ARCHITCTURES

COSO Framework for Financial Reporting

COSO (http://www.coso.orgi) is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance. It was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector organization often referred to as the Treadway Commission. Key sponsoring organizations include the American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA).

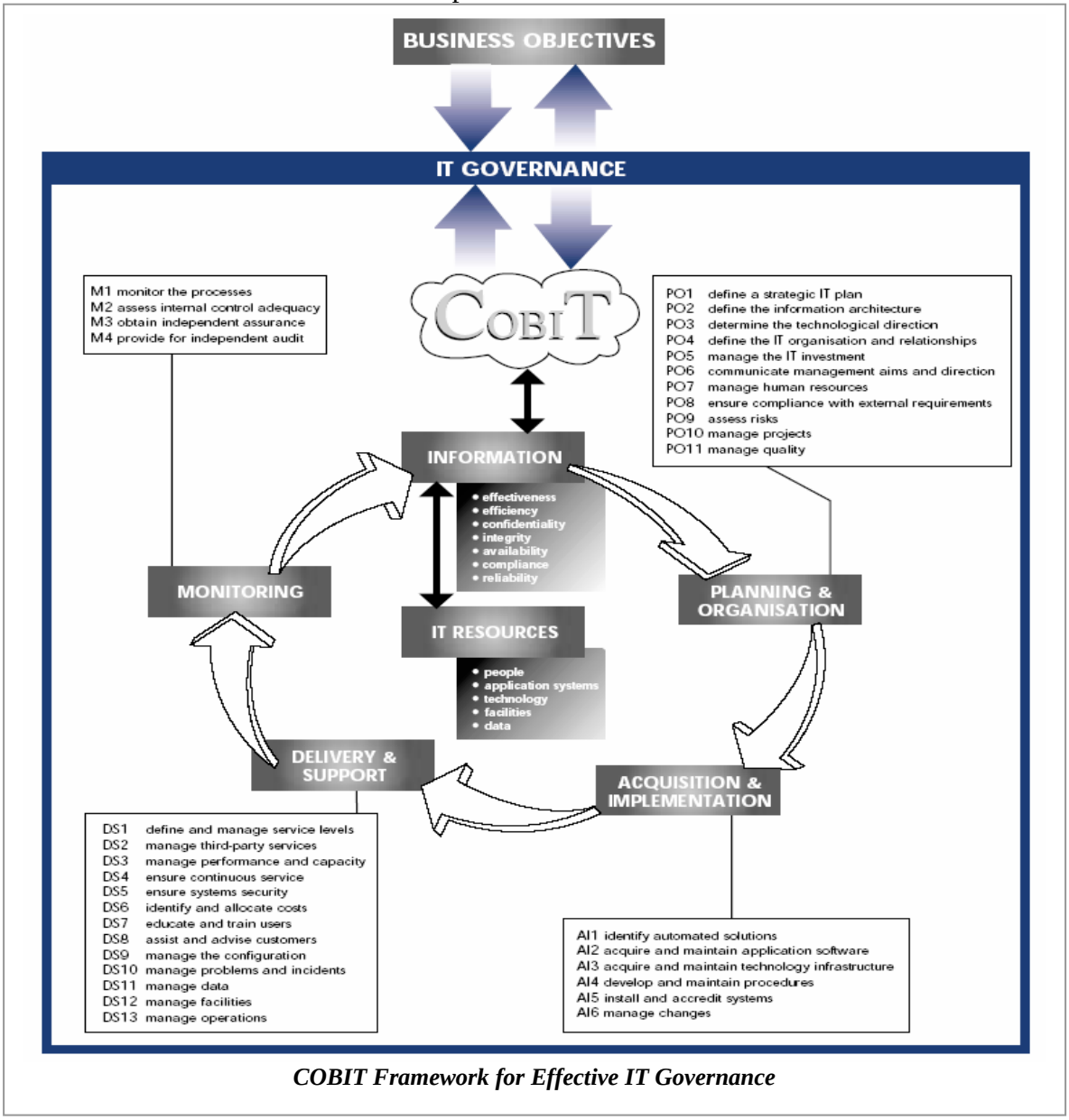
COSO identifies five essential components of effective internal control. They are:
• Control environment
• Risk assessment
• Control activities
• Information and communication
• Monitoring

While the importance of IT controls is embedded in the COSO internal control framework, IT management requires specific examples to help identify, document and evaluate IT controls. The COSO framework has been rapidly adopted by financial auditors as a means implanting controls for the financial reporting process. For the purpose of this document, however, we will focus primarily on popular IT control methodologies and frameworks and their role in achieving Sarbanes-Oxley compliance, as well as loosely, the value of these for assuring ingoing compliance as new regulatory measures are passed.

Several IT internal control frameworks exist. The IT control objectives known as COBIT are considered particularly useful and are an open framework, which aligns with the spirit of the Sarbanes-Oxley Act requirement that any framework used be open and generally acceptable.

COBIT (Control Objectives for Information and related Technology)

CIOs, CFOs, information security managers, auditors, and those involved in corporate and IT governance require a framework to compare international standards and guidance for managing the IT function. COBIT is an IT governance model that provides both company-level and activity-level objectives along with associated controls. In short, COBIT was originally designed as an IT process and control framework linking IT to business requirements. Initially used mainly by the assurance community in conjunction with business and IT process owners, it is now being rapidly adopted by auditors, systems integrators and public companies as a framework for IT governance, providing management tools such as metrics and maturity models to complement the control framework. The COBIT controls framework can be seen in the diagram that follows.



COBIT Framework for Effective IT Governance

The IT Governance Institute has published a document defining the specific areas of COBIT that support Sarbanes-Oxley audit preparation. Entitled *IT Control Objectives for Sarbanes-Oxley*, it highlights control objectives for thirty-two specific process areas. Using this document, an organization can design a system of IT controls to comply with section 404 of Sarbanes-Oxley. Micromuse's support for the specific subset of COBIT IT controls relating to Sarbanes-Oxley are defined in later sections of this whitepaper.

ITIL BEST PRACTICES – (Information Technology Infrastructure Library)

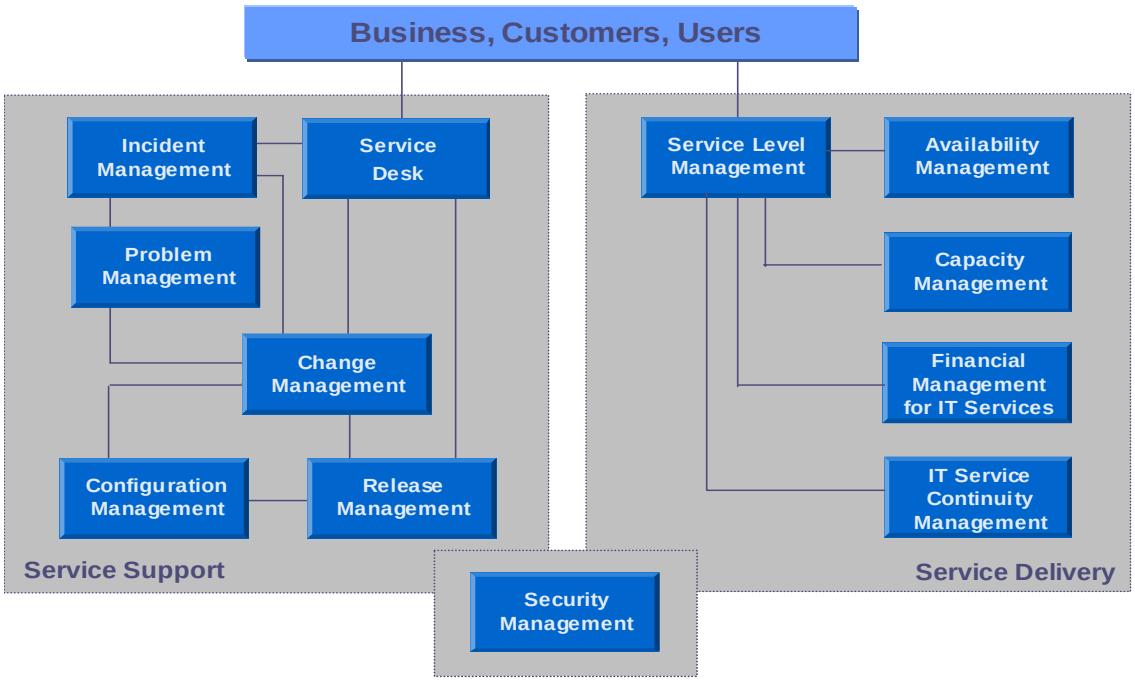
For many organizations, the adoption of ITIL best practices for Service Management provide the necessary future-proof course of action for implementation of process controls, and IT functions that enable regulatory compliance not only for Sarbanes-Oxley, but across regulatory legislation. In addition, because ITIL provides recommended guidelines for implementing checks and balances in IT process, ITIL offers the secondary benefit of driving Business Acceleration

through enhanced service visibility, preventative action, and automations that raise service and process availability and quality, and drive competitive advantage.

ITIL consists of a set of best practices to enable the delivery of IT services that are reliable, consistent, and of the highest levels of quality. IT provides a proven method for planning common processes, roles and activities with appropriate reference to each other and how the communication lines should exist between them. It is comprised of seven comprehensive publicly accessible specialist documents, namely:

- Service Support
- Service Delivery
- Application Management
- ICT Infrastructure Management
- Security Management
- The Business Perspective
- Planning to Implement Service Management

The core of ITIL are the Service Management best practices, namely, Service Delivery and Service Support, with both disciplines further broken down into several processes seen below. Micromuse's support of these disciplines, together with the Security Management discipline, is explained in later sections.



ITIL Service Management & Security Management Disciplines

ENABLING A STANDARDS-BASED COMPLIANCE ARCHITECTURE WITH MICROMUSE

For many companies, the tight timelines and requirements dictated by regulation measures have meant that Auditors and IT organizations have been forced to address the needs of SOX compliance through the application of targeted, SOX specific IT controls and point solutions. While this is an effective means of addressing short-term SOX compliance, the long term requirements of ongoing SOX compliance, as well as compliance with other regulatory measures imposes the need for more progressive and adaptive compliance measures, like those defined within the broader best practice guidelines of ITIL, COBIT and other methodologies.

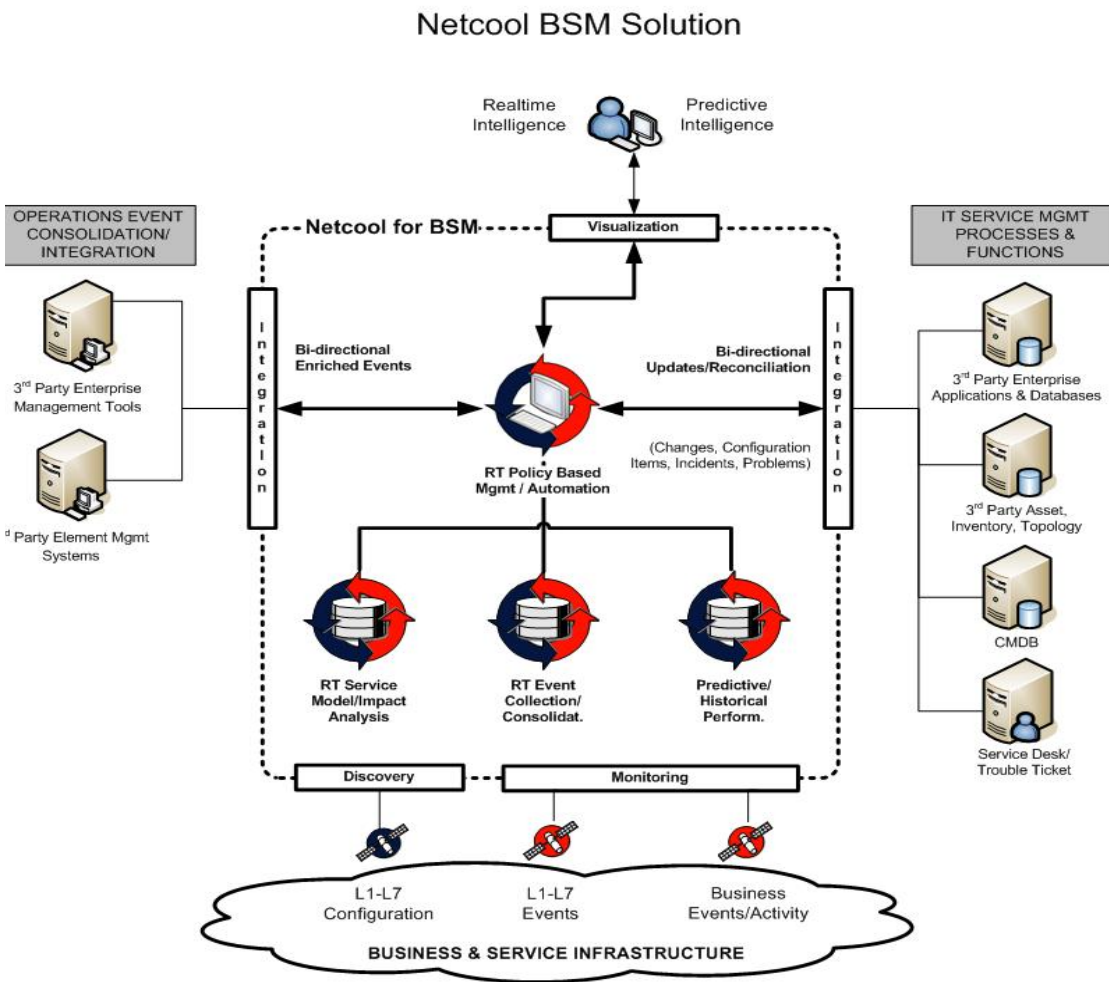
Many companies are proactively turning to these methodologies as the means to implement broader IT process restructuring, and compliance architectures that will allow them not only to address the needs of current and future regulatory action, but to more effectively align business and IT objectives, as a means to establish a world-class IT organization that can drives **'Business Acceleration'**, the ideal state achieved when business goals, operations, and infrastructure are optimally aligned to support significant improvements in:

- Revenue growth
- Competitive advantage
- Customer experience
- Return on OPEX and CAPEX
- Internal process efficiencies
- Risk management

While methodologies provide best practices for IT service management functions, processes and measurement, overall success requires effectively leveraging and integrating information technology to automate manual processes and reduce unnecessary incidents and problems.

MICROMUSE COMPLIANCE-ENABLING ARCHITECTURE

Micromuse plays a vital role in the overall success of IT best practices and methodologies, providing the necessary discovery, monitoring, and analysis of layer 1 to layer 7 configuration, status and performance information, as well as vital business data. This information can be shared in realtime with the service desk, as well as ITIL processes that support comprehensive Business Service Management (BSM) in the IT organization, including change, configuration, incident, problem, availability, capacity, and security management, to further streamline and automate IT workflow. In addition, Micromuse's policy management capabilities enable the implementation of COBIT IT controls and historical reporting for compliance with regulatory mandates.



Micromuse Logical Architecture for Standards and Regulatory Compliance

Micromuse is the first business & service assurance solution designed to provide executives and IT operations with the realtime intelligence needed to effectively assure the health and performance of critical, revenue driving business transactions, services and processes.

Many businesses are turning to realtime dashboards, as the means to deliver unprecedented intelligence across business and operational lines. Dashboards enable executive, line of business and IT management to quickly scan key indicators, from business transactions, revenue figures, and the number of new customers and orders, to the health indicators on critical business applications and processes.

Business Service Management Dashboards

Corporate, line of business and operations executives require realtime and predictive intelligence on the health and performance of the business to make effective short-term and long-term decisions that drive business revenue and assure corporate compliance with government regulations.

Patented technology for heterogeneous, realtime data access enables Micromuse dashboards to access and display data from virtually any business application, side by side, in realtime, across the gamut of ERP, CRM, Enterprise Management Systems and home grown applications in the distributed enterprise.

Unlike traditional Business Intelligence and Operations dashboard solutions, Micromuse BSM dashboards provide realtime and predictive information, side by side. Because BSM dashboards only collect relevant information, taken from across the business environment, users benefit from immediate access to the focused intelligence that matters most, regardless of the source.

Business and Operational Transaction Assurance

Micromuse BSM dashboards are further enhanced via advanced business transaction monitoring and assurance capabilities that are not limited to the application and infrastructure layer but extend well into the business layer for deeper intelligence and value to the business. Micromuse's patented, realtime data access capabilities enable the collection of business metrics across each step in a transaction or business process, allowing for advanced analysis and more decisive action. When combined with transaction simulation, and monitoring of the actual end-user experience, Micromuse dashboards provide the only truly integrated source of both business and operational KPIs, in a single comprehensive dashboard.

Automated Business Service Modeling and Impact Analysis

Unlike other business and operational dashboards available on the market, Micromuse's BSM solution is not just a dashboard solution for consolidation of business and operational metrics. To provide deeper value across the broader range of IT operational processes and initiatives including ITIL and Cobit, dashboards must allow for visibility beyond pure KPIs and transactions, and include valuable information linking individual business services and processes to the application and service components that support them, as well as the customers and users that rely on them.

Micromuse dashboards can leverage the dependency information stored in virtually any configuration management database (CMDB), third party or custom application or database or those provided by Micromuse's own discovery capabilities. Most importantly, patented, realtime data access capabilities assure service models are automatically populated, and maintained, making Micromuse's BSM solution the first and only automated solution on the market.

Further, the ability to leverage status and performance information provided by Micromuse's own end-to-end monitoring capabilities, and those of virtually any third party systems, means the Micromuse BSM solution can provide realtime insight into the health and performance of transactions, services and processes, and more importantly the impact of incidents on the business for more effective problem management across all IT domains.

Realtime Application Discovery and Modeling

Arguably, one of the fundamental challenges in achieving accurate, end-to-end service visibility is the lack of realtime information on application dependencies – this is due in large part to the mix of next-generation, legacy and custom applications that comprise a given service. Until recently, maintaining an accurate application dependency model was nearly impossible to do, and almost entirely a manual process.

Using our unique, agent-less technology, the Micromuse BSM solution automatically discovers and models application components and their dependencies, allowing clear visibility into how applications communicate. Because the dependencies are automatically updated via realtime discovery, application architects, business-line managers and IT organizations can now gain insight into the architecture of specific applications or use this realtime dependency model to feed dependency information into a complete service or process model, without the need for manual intervention.

Realtime Infrastructure Discovery and Monitoring

True end-to-end business service management requires an accurate understanding of the assets and dependencies of the underlying communication highway over which applications communicate. The Micromuse BSM solution provides the most advanced realtime discovery and modeling of this communication highway, identifying the complex heterogeneous mix of devices, including physical and logical dependencies that comprise the service infrastructure.

When changes to the infrastructure occur, the realtime discovery engine detects changes, including the addition of new devices, as well as any changes to device configuration and automatically updates the service topology accordingly.

Unlike most offerings from most BSM vendors, Micromuse's BSM solution is the only one to automatically update the service model in realtime, linking application, infrastructure and business dependencies, in a self maintaining model. As a result, the traditional inhibitors for BSM are removed – end-to-end transaction, service and process modeling and monitoring – resulting in substantial savings in both time and effort, and enabling more efficient and effective service management.

KEY REQUIREMENTS OF SARBANES-OXLEY

SARBANES-OXLEY: SUMMARY OF RELEVANT SECTIONS*			
Section	**Requirements**	**Relevance/Impact**	**Effective Date**
Section 302	CEOs and CFOs must certify financial and other information in their companies' quarterly and annual reports.	CEO, CFO, or any executive who executes signoff authority for financial statements.	August 27, 2002
Section 404	Requires an annual management report on and auditor attestation of a company's implemented internal controls over financial reporting.	CEO, CFO, any executive who executes signoff authority for financial statements, CIO and IT Operations.	May 27, 2003
Section 409	Requires disclosure on a rapid and current basis such additional information concerning material changes in its financial condition or operations.	CEO, CFO, any executive who executes signoff authority for financial statements, CIO and IT Operations.	Awaiting the adoption of implementing rules by the SEC.

Section 906	Establishes penalties for CEOs or CFOs who knowingly submit a wrong Sec. 906 certification. Violators are subject to a fine of up to $1 million and imprisonment for up to ten years. If the wrong certification was submitted "willfully," the fine can be increased to $5 million and the prison term can be increased to twenty years.	CEO, CFO, or any executive who executes signoff authority for financial statements.	August 27, 2002
* For additional information on the detailed excerpts of relevant Sarbanes-Oxley regulations, please see Appendix A-G at the end of this whitepaper			

ENABLING ITIL & COBIT CONTROLS FOR SOX-COMPLIANCE WITH MICROMUSE

ITIL Service Management Best Practices	COBIT Framework	Micromuse & Standards Enablement
Change Management Process The ITIL Change Management process provides a structured method for the management of all changes to both IT Services and infrastructure, enabling approved changes with minimum disruption to business.	**AI6 Manage Changes** Control over the IT process of managing changes that satisfies the business requirement to minimize the likelihood of disruption, unauthorized alterations and errors is enabled by a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure and takes into consideration • identification of changes • categorization, prioritization and emergency procedures • impact assessment • change authorization • release management • software distribution • use of automated tools • configuration management • business process re-design	**Direct Support** Micromuse provides realtime automated discovery for critical business applications, configuration items and dependencies. It provides an accurate, dependable and extensible record of all components across the application software, system and network tiers. It automatically creates and maintains detailed attribute values, dependencies and change history. This information is the basis for change management and provides a complete view of the runtime cross-tier structure and dependencies of applications and systems. It also provides IT operations staff with the ability to understand and predict the impact of proposed component and application level changes, minimizing unintended disruptions.

		Accurate records of any changes are available to 3rd party and custom CMDBs, as well as for use by the Micromuse impact analysis engine. Micromuse infrastructure discovery capabilities provide realtime automated discovery of the layer 1 to layer 3 infrastructure configuration items and dependencies. These combined application and infrastructure capabilities allow for automated modeling of business services and processes, including the financial reporting process. Further Micromuse's patented data access technology can monitor virtually any 3rd party application, database, CMDB, log file and flat file for changes and automatically pass this information to other systems, allowing for notification, reconciliation or other policy based management for workflow automation. Micromuse's advanced change detection capabilities can facilitate the verification of configuration records against true configuration in realtime, allowing correction of exceptions. This leads to higher efficiency and accuracy in the Change Management process. Dynamic detection of service dependencies and change provide visibility of end-to-end service and process dependencies, leveraging existing information on Configuration Items (network devices, server farms, applications, etc) to create a comprehensive model. This

		allows for quick assessment of the impact of infrastructure changes to the health of IT services, supporting other ITIL processes and functions.
	DS2 Manage Third-party Services Control over the IT process of managing third-party services that satisfies the business requirement to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements is enabled by control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organization policy and takes into consideration • third-party service agreements • contract management • non-disclosure agreements • legal and regulatory requirements • service delivery monitoring and reporting • enterprise and IT risk assessments • performance rewards and penalties • internal and external organizational accountability • analysis of cost and service level variances	**Direct Support** Micromuse provides monitoring and reporting of the availability, performance and security of third party services, including network, system, application, and end-to-end transaction monitoring and reporting. Micromuse models the business service and tracks service levels to assure vendors are meeting SLAs. This information can be used for evaluation of penalties. Micromuse impact analysis capabilities allows for proactive detection of developing problems and their potential impact on business services, providing early notification of developing problems for more effective mitigation of operational risk.
Capacity Management Capacity Management ensures that the capacity of the IT infrastructure matches the evolving demands of the business in the most cost-effective and timely manner.	**DS3 Manage performance and capacity** Control over the IT process of managing performance and capacity that satisfies the business requirement to ensure that adequate capacity is available and that best and	**Direct Support** Micromuse solutions for performance and capacity planning support proactive capacity analysis based on advanced trending of historical performance utilization metrics. They incorporate predefined

	optimal use is made of it to meet required performance needs is enabled by data collection, analysis and reporting on resource performance, application sizing and workload demand and takes into consideration • availability and performance requirements • automated monitoring and reporting • modeling tools • capacity management • resource availability • hardware and software price/performance changes	analytics and industry-standard process flows and have the ability to: > Analyze performance and utilization levels of any infrastructure resource > Utilize advanced analysis and statistical models to accurately determine future capacity requirements > Presents current capacity status and accurate Time to Capacity projections > Support business-prioritized IT investment decisions > Proactively identify performance problems and improve availability of IT resources and supported business services > Identify over utilized and underutilized assets > Facilitate planning for new capacity by automatically factoring in purchase cycles. Micromuse asset management solutions for applications and infrastructure offer asset discovery and reporting capabilities, providing detailed asset information coupled with highly accurate connectivity information. This arms users with essential asset visibility – detailing deployed assets, and specific configuration, including if the asset is under provisioned). Additional usage and performance monitoring capabilities provide detailed information on application, protocol, and bandwidth utilization. System monitoring provides a wide range of system usage information such as disk space, memory and CPU utilization. This information enables organization to

		effectively plan for additional or reduced IT infrastructure capacity to meet current and future business requirements.
Availability Management & IT Service Continuity Management Availability Management involves the design, implementation, measurement and management of IT Services to ensure that the stated business requirements for availability are consistently met. IT Service Continuity Management (ITSCM) supports the overall Business Continuity Management of the organization, ensuring it has the ability to continue to provide a pre-determined and agreed level of IT services to support the minimum business requirements after a problem has occurred.	**DS4 Ensure Continuous Service** Control over the IT process of ensuring continuous service that satisfies the business requirement to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption is enabled by having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements and takes into consideration • criticality classification • alternative procedures • back-up and recovery • systematic and regular testing and training • monitoring and escalation processes • internal and external organizational responsibilities • business continuity activation, fallback and resumption plans • risk management activities • assessment of single points of failure • problem management	**Direct Support** The Micromuse suite supports the Availability Management process by proactively monitoring applications, systems, mainframe, network and other supporting components of the IT infrastructure, tracking availability, performance and security in realtime and historically, to assure continuous uptime of business applications and services. Collected events from throughout the IT infrastructure are consolidated for, advanced correlation and analysis. 'Synthetic transactions' monitor service availability and performance from end-to-end– including critical Internet services, applications and systems, wireless, mainframe, network and custom service monitoring. Realtime active dashboards provide standard and custom views for managing the realtime status of the IT Services as well as historical reports. Advanced reporting of service infrastructure provides detailed information on availability and problem areas that must be addressed Micromuse supports continuity management by monitoring the availability of primary systems, core infrastructure, UPS, Storage applications and secondary systems, and detecting when backup and secondary systems have come online. The Micromuse suite

		also provides a wide range of monitoring, management, and troubleshooting functions descried throughout this document, that facilitate the many other disciplines and processes that the continuity management function interacts with. Furthermore, upon the detection of application and infrastructure affecting incidents and problems, automated impact analyses and custom correlation, for unique problem detection, isolate the realtime business impact of these service affecting incidents and problems and automatically trigger necessary actions (e.g. invoking the startup of secondary systems) to ensure the continuity of the IT services that support the business. When primary systems are back on line, realtime monitoring can detect primary system availability and trigger automated actions to assure smooth transition to primary systems. The Micromuse suite will also provide accurate reporting on the availability, performance and security of primary and secondary systems, as well as valuable information on the duration, cause and response to incidents and problems.
Security Management Process Security Management looks at security from a service provider standpoint, identifying how it provides the level of security necessary for the provision of the total service to the organization. The data and infrastructures are to be protected so that • Confidentiality is	**DS5 Ensure Systems Security** Control over the IT process of ensuring systems security that satisfies the business requirement to safeguard information against unauthorized use, disclosure or modification, damage or loss is enabled by logical access controls which ensure that access to systems, data	**Direct Support** Micromuse's solution for Security Management (provides the necessary, end-to-end management capabilities needed to assure adequate security for complete services. Acting as a manager of managers, and correlation engine for security events, the Micromuse solution consolidates potential service

appropriately preserved • Integrity of information is ensured • Availability is ensured • Conducting a transaction is not denied • Obligations imposed by law, contractual arrangements and supervisory bodies can be fulfilled	and programs is restricted to authorized users and takes into consideration • confidentiality and privacy requirements • authorization, authentication and access control • user identification and authorization profiles • need-to-have and need-to-know • cryptographic key management • incident handling, reporting and follow-up • virus prevention and detection • firewalls • centralized security administration • user training • tools for monitoring compliance, intrusion testing and reporting	affecting incidents and problems across a complex range security environments in a single management console. It improves the efficiency of security operations management by not only collecting, but also consolidating disparate IT security data across VPNs, firewalls, anti-virus programs, authorization programs, intrusion detection systems, environmental and physical security applications - it can correlate potential security events to known developing or known service outages, as well as to asset information, customer data and any other external data sources, allowing for proactive troubleshooting and even the prevention of service impacting problems. The Micromuse security solution can also rank business assets according to commercial need and perform an impact analysis to determine the financial and other costs associated with the loss of a specific business service. It has the intelligence to group events together, allocate them and track them as a single incident or problem. Advanced reporting can then be done to assure that the impact of security events are properly and addressed, while allowing compliance with increasing government regulations and contractual obligations.
Financial Management for IT Services Financial Management for IT Services focus on the justification of IT investment as well as the accountability for spending of IT services and attribute these costs to the	**DS6 Identify and Allocate Costs** Control over the IT process of identifying and allocating costs that satisfies the business requirement to ensure a correct awareness of the costs attributable to IT	**Direct Support** The Micromuse suite provides a wide range of realtime and historical reporting capabilities that support Financial Management for IT Services. Micromuse provides application and infrastructure

users of these services.	services is enabled by a cost accounting system which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering and takes into consideration • resources identifiable and measurable • charging policies and procedures • charge rates and charge-back process • linkage to service level agreement • automated reporting • verification of benefit realization • external benchmarking	usage and performance monitoring and reporting by service, customer, and department and other criteria. Detailed asset information is available to facilitate the accountability of IT services spending, providing a detailed up-to-date record of application and infrastructure assets, configuration and unused capacity. The realtime discovery and monitoring capabilities of the Micromuse suite can not only determine when services have been provisioned, but also track usage of applications and infrastructure that support each service, as well as the customer, business unit, application or user that consumes that service. This is accomplished through a variety of transaction, usage and performance monitoring techniques across application, system, mainframe, network and other infrastructure components. When combined with advanced service modeling and service level tracking, IT organization have the historical information needed for charge back and customer billing, linking asset and service utilization to the specific customer, user, etc. This information is available to external accounting and billing systems to support cost recovery, as well as future capacity planning. This further enables IT organizations to plan future IT spending, and directly bill users, customers or departments for needed enhancements to the service infrastructure, including supporting business applications and management

		tools. The Micromuse suite can combine information collected directly from customer and other chargeback databases and enrich, or tag these events (incidents and problems) with this charge back and billing related information. Service modeling capabilities further extend this competency, by linking applications and infrastructure with the services and customers they support. In combination, this information can be used for detailed reporting. Standard usage and performance monitoring records detailing usage of applications and devices and their performance history can then be used for effective capacity planning, and purchasing, according to the customer or service they support. Service level tracking and reporting can be leveraged for direct billing purposes. The Micromuse suite can send this data to a central database or directly to billing systems in realtime providing the records needed to accurately bill customer by infrastructure and service consumption. Leveraging information on the revenue impact of service downtime, the Micromuse suite can be configured to collect this data from a database and calculate financial and other costs associated with infrastructure and service failures.
Service Desk The Service Desk function provides a single point of contact within the IT organization for customers and/or users of IT services. It	**DS8 Assist and Advise Customers** Control over the IT process of assisting and advising customers that satisfies the business requirement to	**Direct Support** The Micromuse suite provides operators, internal users and external customers with the visibility of IT services they support or depend upon. A core

handles calls or queries on service-related issues, provides first line resolution and the necessary escalation, and provides timely feedback to users of all service events, actions and opportunities that may affect the IT services.	ensure that any problem experienced by the user is appropriately resolved is enabled by a help desk facility which provides first-line support and advice and takes into consideration • customer query and problem response • query monitoring and clearance • trend analysis and reporting • development of knowledge base • root cause analysis • problem tracking and escalation	function of the service desk is the central management of incidents. It also provides an efficient and effective means to collect and consolidate events across the service infrastructure, as well as disparate management tools, and normalizes those events into a subset of meaningful and manageable incidents. Through a combination of integrated event correlation techniques (de-duplication and filtering, application and device level correlation, topological root cause analysis, service and process modeling and impact analysis) the Micromuse Suite reduces the total number of redundant and symptomatic incidents and trouble tickets that must be managed.
Configuration Management Process The Configuration Management process involves identifying all relevant assets within the whole infrastructure (both hardware and software), recording and reporting the status of these assets, and verifying the completeness and correctness of the configuration management database. Configuration Management is an integral part of all other Service Management processes.	**DS9 Manage the Configuration** Control over the IT process of managing the configuration that satisfies the business requirement to account for all IT components, prevent unauthorized alterations, verify physical existence and provide a basis for sound change management is enabled by controls which identify and record all IT assets and their physical location, and a regular verification program which confirms their existence and takes into consideration. • asset tracking • configuration change management • checking for unauthorized software	**Direct Support** The Micromuse suite provides advanced realtime discovery of infrastructure assets as well as configuration. Micromuse solutions for Asset and Configuration Management can automatically discover the application and service infrastructure and update Configuration Management Databases (CMDB) with realtime asset information, including accurate application and infrastructure dependency and connectivity information. With the Micromuse suite, users have the essential asset visibility into asset usage, configuration and interdependencies. Micromuse reports on discovered application and infrastructure assets, configuration changes, interface details & status, IP addressing, and application, operating system and device

		software version, etc. It can detect changes in the application and infrastructure configuration and automatically update the records in the CMDB, facilitating the verification of configuration records against true application and infrastructure configuration in realtime, allowing correction of exceptions. This leads to higher efficiency and accuracy in the Change Management process. Micromuse application discovery and configuration management capabilities provide detailed application and systems discovery and reporting, as well as client side discovery, configuration and change information in realtime. Dynamic service modeling provides visibility of end-to-end service and process dependencies, leveraging existing information on Configuration Items (network devices, server farms, applications, etc) to create a comprehensive model. This allows quick assessment of the impact of infrastructure changes to the health of IT services, supporting other ITIL processes and functions.
Incident Management & Problem Management The ITIL Incident Management process handles service-affecting incidents. It aims to restore normal service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability	**DS10 Manage Problems and Incidents** Control over the IT process of managing problems and incidents that satisfies the business requirement to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence is enabled by a problem management system which records and progresses all	**Direct Support** The Micromuse suite provides a wide range of event collection (as well as normalization and enrichment with business data) capabilities as a means of gathering relevant incident information including device-level probes (layer 1 – layer 3 network devices), application and system monitors, including mainframe, and mid-range systems, end-to-end transaction

are maintained. The ITIL Problem Management process is comprised of both proactive Problem Management and reactive Problem Management. It aims to minimize the impact to the business caused by problems in the IT infrastructure and to prevent recurrence of incidents related to these problems. It involves problem detection, investigation, root cause identification, action initiation to improve or correct the situation, prevention of problem reoccurrences and problem reports generation.	incidents and takes into consideration • audit trails of problems and solutions • timely resolution of reported problems • escalation procedures • incident reports • accessibility of configuration information • supplier responsibilities • coordination with change management	monitoring and simulation, direct monitoring of business level data directly from business applications, databases, CMDBs, log files and flat files, and even probes for non-traditional management items such as card key systems, manufacturing equipment, refrigeration, ATM machines, airport ticket kiosks, and facilities management systems. Gateway integrations between the core Micromuse event processing engine and external trouble ticketing systems enable automatic creation of trouble tickets for service-affecting events. Through integration with common external databases and applications, collected events can be enriched with business-context information needed to accelerate incident resolution. Gateways act as bi-directional interfaces where status changes are synchronized between the trouble ticketing system and Micromuse event engine, enabling service desk personnel to proactively manage support operations and to be informed of all actions taken and real-time incident status. Micromuse correlation capabilities de-duplicate and filter events/incidents and provide information on the impact of specific events/incidents within the infrastructure. Built-in automations execute intelligent resolution scripts against recurring, predictable infrastructure problems without the need for manual intervention by operators, minimizing the impact to

		businesses. In addition Micromuse can escalate events to email, pagers and other systems - ensuring fast and efficient notification. The Micromuse suite supports the Problem Management process by proactively managing IT infrastructure and services for early detection of 'known problems' as well as rapid isolation of key incidents that are the root cause of new service-impacting problems. Micromuse event collection and monitoring capabilities gather realtime incident information from across complex IT infrastructures, as well as point management, element management, enterprise management systems and operational support systems – consolidating it for further analysis. First phase correlation capabilities minimize noise, using filtering, de-duplication, and suppression methods. Advanced correlation capabilities then provide rapid problem identification. Device-level correlation analyzes device and application information and provides real-time diagnosing of the underlying cause of hundreds of unique device-specific problems, providing an explanation for the condition, as well as the cause and recommended solution for problems. Topology based correlation and service modeling and impact analysis provide rapid isolation of the underlying cause of incident (event) storms, and pinpoint which component has caused a service affecting

		problem as well as the impact on services and customers. Detailed reports track the history of incidents and problems and provide valuable information about the behavior of devices, systems, infrastructure and services. They offer an intelligent window into incident and problem trends, revealing "hot spots". This information can then be used to proactively monitor for, detect, and resolve known problems, before they impact service availability and performance.
	DS11 Manage Data Control over the IT process of managing data that satisfies the business requirement to ensure that data remains complete, accurate and valid during its input, update and storage is enabled by an effective combination of application and general controls over the IT operations and takes into consideration • form design • source document controls • input, processing and output controls • media identification, movement and library management • data back-up and recovery • authentication and integrity • data ownership • data administration policies • data models and data representation standards • integration and consistency across platforms • legal and regulatory	**Direct Support** Through a combination of techniques Micromuse enables data the management of data integrity. Transaction monitoring simulates step-by-step user, application and, infrastructure transactions, from beginning to end. By tracking the ability of individual transactions to complete each step in a process, Micromuse can detect incidents and problems in the service or process that may impact the integrity of data. Additionally, the ability to dynamically access data from within applications, databases log files, and flat file, or from virtually any event source, as well as the ability to define specific criteria via Micromuse policy managements means the specific data can be collected and compared against a prior record or trusted source to ensure no changes to data integrity, file size, or other

	requirements	criteria have changed, thereby impacting data consistency or integrity. Micromuse monitoring of key access control systems, including, application and device log files, like those provided by operating systems firewalls or other source of security policy or access control information, mean incidents affecting data integrity can be quickly identified. Micromuse data and security monitoring and automated response capabilities, including those provided within Micromuse solutions for security management mean when potential threats to data integrity are detected, automated action can be taken to lock out unauthorized users, or other malicious and unauthorized activity. Operations or business users can be automatically notified to assure any material changes that may affect regulatory compliance or service quality are immediately known, for appropriate response.
	DS12 Manage Facilities Control over the IT process of managing facilities that satisfies the business requirement to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards is enabled by the installation of suit able environmental and physical controls which are regularly reviewed for their proper functioning and takes into	**Direct Support** Micromuse solutions provide the means to collect information from environmental items, including refrigeration and cooling systems, power supply equipment, access and surveillance equipment, and virtually any custom application that can generate an event, or from which Micromuse can collect information (databases, log files, flat files, etc) This information can be

	consideration • access to facilities • site identification • physical security • inspection and escalation policies • business continuity planning and crisis management • personnel health and safety • preventive maintenance policies • environmental threat protection • automated monitoring	automatically analyzed within the Micromuse service/process model, and correlated to determine the root cause, or business impact of an environmental event.
	DS13 Manage Operations Control over the IT process of managing operations that satisfies the business requirement to ensure that important IT support functions are performed regularly and in an orderly fashion is enabled by a schedule of support activities which is recorded and cleared for the accomplishment of all activities and takes into consideration • operations procedure manual • start-up process documentation • network services management • workload and personnel scheduling • shift hand-over process • system event logging • coordination with change, availability and business continuity management • preventive maintenance • service level agreements	**Enabler** Micromuse supports collection, analysis and reporting of realtime and historical data across a variety of operational areas including but not limited to: • Applications, infrastructure & services availability, performance & security • SLAs & OLAs tracking • Incident and problem logging for automation • Configuration change tracking • Change tracking between disparate data sources In addition, Micromuse enables IT workflow automation via integrations with existing enterprise management and point management systems, as well as through policy-based management for continual refinement of corrective action and data exchange between systems (additional information on automation available in prior sections on change, incident, problem, and

	• automated operations • incident logging, tracking and escalation	continuity management, among others).
	M1 Monitoring the Process Control over the IT process of monitoring the processes that satisfies the business requirement to ensure the achievement of the performance objectives set for the IT processes is enabled by the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations and takes into consideration • scorecards with performance drivers and outcome measures • customer satisfaction assessments • management reporting • knowledge base of historical performance • external benchmarking	**Direct Support** Micromuse dashboards for business and IT users deliver realtime intelligence needed to make effective decisions regarding IT services and processes, customers, financial reporting and transactions or other KPIs, IT metrics, and historical trend information. Further, Micromuse's unique capability to collect realtime and historical information from virtually any data source means organizations can create custom dashboards, scorecards, and views around compliance, service and process health, or any other unique requirement. This information can be distributed to other compliance applications or Business Intelligence dashboards, or can be displayed via any web browser, email, or other preferred method. The ability of Micromuse solutions to monitor themselves, other management or compliance applications, or any business critical application, service or process further mitigates operational risk.
	M2 Access Control Adequacy Control over the IT process of assessing internal control adequacy that satisfies the business requirement to ensure the achievement of the internal control	**Enabler** As defined in other sections of this whitepaper, Micromuse provides advanced monitoring, analysis, and realtime and historical reporting via a variety of mechanisms, including business and operations

	objectives set for the IT processes is enabled by the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis and takes into consideration • responsibilities for internal control • ongoing internal control monitoring • benchmarks • error and exception reporting • self-assessments • management reporting • compliance with legal and regulatory requirements	dashboards and historical reporting for improved intelligence on compliance issues and continued process improvement.
	M3 Obtaining Independent Assurance Control over the IT process of obtaining independent assurance that satisfies the business requirement to increase confidence and trust among the organization, customers, and third-party providers is enabled by independent assurance reviews carried out at regular intervals and takes into consideration • independent certifications and accreditation • independent effectiveness evaluations • independent assurance of compliance with laws and regulatory requirements • independent assurance of compliance with contractual commitments • third-party service provider reviews and benchmarking • performance of assurance	**Direct Support** The Micromuse suite provide complete historical reporting around availability, performance, security, and integrity of the data, applications, systems, and infrastructure that support businesses services and processes for the various processes and functions defined within the ITIL and COBIT frameworks. This information can be centrally stored using 3rd party data warehousing technology for long term auditing and compliance reporting. It can also can be displayed via realtime dashboards, or stored for historical trend analysis and reporting to support tactical or strategic decision making by IT or business users. Additional information is

	reviews by qualified personnel • proactive audit involvement	provided in several of the IT processes and control requirement sections earlier in this whitepaper.

ACHEIVING SARBANES-OXLEY COMPLIANCE

For many organizations, improving operational IT processes and controls are headline agenda items, made more critical through government regulatory actions, such as Sarbanes-Oxley, the need to do more with less, and increased competitive pressures. To support these goals IT organizations, systems integrators and auditors have turned to best practices, including ITIL to COBIT. While these initiatives provide best practices for IT service management functions, processes and measurement, overall success requires effectively leveraging and integrating information technology to automate manual processes and reduce unnecessary incidents and problems.

Micromuse' BSM solution architecture plays a vital role in the overall success of those initiatives, providing the necessary discovery, monitoring, and analysis of layer 1 to layer 7 configuration, status and performance information, as well as vital business data. This information can be shared in realtime with the service desk, as well as other processes that support comprehensive business service management in the IT organization, including change, configuration, incident, problem, availability, capacity, and security management, to further streamline and automate IT workflow. In addition, Micromuse policy management capabilities further enable the implementation of focused IT controls and historical reporting for compliance with regulatory mandates.

Sarbanes-Oxley imposes greater accountability for operational risk, requiring greater visibility, intelligence and assurance of critical financial reporting processes, and the applications and infrastructure that support the accurate and on time delivery of financial information. To assure compliance, Business and IT management must implement a compliance architecture that supports IT service management best practices and controls. Micromuse provides the means to align business and IT, facilitate compliance and achieve world class, service-oriented business and IT operations.

ppendix A: Sec. 302. Corporate Responsibility for Financial Reports

(a) REGULATIONS REQUIRED.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

(1) the signing officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

(4) the signing officers—

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

APPENDIX: SARBANES-OXLEY REGULATIONS IN DETAIL

H. R. 3763—34

(b) FOREIGN REINCORPORATIONS HAVE NO EFFECT.—Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.

(c) DEADLINE.—The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

Appendix B: Sec. 404. Management Assessment of Internal Controls

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board.

Any such attestation shall not be the subject of a separate engagement.

Appendix C: Sec. 409. Real Time Issuer Disclosures

Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m), as amended by this Act, is amended by adding at the end the following:

''(l) REAL TIME ISSUER DISCLOSURES.—Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the

public interest.''.

Appendix D: Sec. 802. Criminal Penalties for Altering Document.

(a) IN GENERAL.—Chapter 73 of title 18, United States Code, is amended by adding at the end the following:

''§ 1519. Destruction, alteration, or falsification of records in Federal investigations and bankruptcy

''Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

''§ 1520. Destruction of corporate audit records

''(a)(1) Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j–1(a)) applies, shall maintain all audit or review workpapers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.

''(2) The Securities and Exchange Commission shall promulgate, within 180 days, after adequate notice and an opportunity for comment, such rules and regulations, as are reasonably necessary, relating to the retention of relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review, which is conducted by any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j–1(a)) applies. The Commission may, from time to time, amend or supplement the rules and regulations that it is required to promulgate under this section, after adequate notice and an opportunity for comment, in order to ensure that such rules and regulations adequately comport with the purposes of this section.

''(b) Whoever knowingly and willfully violates subsection (a)(1), or any rule or regulation promulgated by the Securities and Exchange Commission under subsection (a)(2), shall be fined under this title, imprisoned not more than 10 years, or both.

''(c) Nothing in this section shall be deemed to diminish or relieve any person of any other duty or obligation imposed by Federal or State law or regulation to maintain, or refrain from destroying, any document.''.

H. R. 3763—57

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 73 of

title 18, United States Code, is amended by adding at the end the following new items:

''1519. Destruction, alteration, or falsification of records in Federal investigations and bankruptcy.

''1520. Destruction of corporate audit records.''.

Appendix E: Sec. 906. Corporate Responsibility for Financial Reports

(a) IN GENERAL.—Chapter 63 of title 18, United States Code, is amended by inserting after section 1349, as created by this Act, the following:

''§ 1350. Failure of corporate officers to certify financial reports

(a) CERTIFICATION OF PERIODIC FINANCIAL REPORTS.—Each periodic report containing financial statements filed by an issuer with the Securities Exchange Commission pursuant to section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a) or 78o(d)) shall be accompanied by a written statement by the chief executive officer and chief financial officer (or equivalent thereof) of the issuer.

''(b) CONTENT.—The statement required under subsection (a) shall certify that the periodic report containing the financial statements fully complies with the requirements of section 13(a) or 15(d) of the Securities Exchange Act pf 1934 (15 U.S.C. 78m or 78o(d)) and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.

''(c) CRIMINAL PENALTIES.—Whoever—

''(1) certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $1,000,000 or imprisoned not more than 10 years, or both; or

''(2) willfully certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $5,000,000, or imprisoned not more than 20 years, or both.''.

(d) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 63 of title 18, United States Code, is amended by adding at the end the following:

''1350. Failure of corporate officers to certify financial reports.''.

Appendix F: Securities Act of 1934, Sec. 13(a) & 15(d)

Section 13(a)-- Periodical and Other Reports

a. **Reports by issuer of security; contents**

Every issuer of a security registered pursuant to section 12 shall file with the Commission, in accordance with such rules and regulations as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security--

1. such information and documents (and such copies thereof) as the Commission shall require to keep reasonably current the information and documents required to be included in or filed with an application or registration statement filed pursuant to section 12, except that the Commission may not require the filing of any material contract wholly executed before July 1, 1962.
2. such annual reports (and such copies thereof), certified if required by the rules and regulations of the Commission by independent public accountants, and such quarterly reports (and such copies thereof), as the Commission may prescribe.

Every issuer of a security registered on a national securities exchange shall also file a duplicate original of such information, documents, and reports with the exchange.

Section 15(D) -- Securities Analysts And Research Reports

a. **Analyst protections**

The Commission, or upon the authorization and direction of the Commission, a registered securities association or national securities exchange, shall have adopted, not later than 1 year after the date of enactment of this section [enacted July 30, 2002], rules reasonably designed to address conflicts of interest that can arise when securities analysts recommend equity securities in research reports and public appearances, in order to improve the objectivity of research and provide investors with more useful and reliable information, including rules designed--

1. to foster greater public confidence in securities research, and to protect the objectivity and independence of securities analysts, by--
    A. restricting the prepublication clearance or approval of research reports by persons employed by the broker or dealer who are engaged in investment banking activities, or persons not directly responsible for investment research, other than legal or compliance staff;
    B. limiting the supervision and compensatory evaluation of securities analysts to officials employed by the broker or dealer who are not engaged in investment banking activities; and
    C. requiring that a broker or dealer and persons employed by a broker or dealer who are involved with investment banking activities may not, directly or indirectly, retaliate against or threaten to retaliate against any securities analyst employed by that broker or dealer or its affiliates as a result of an adverse, negative, or otherwise unfavorable research report that may adversely affect the present or prospective investment banking relationship of the broker or dealer with the issuer that is the subject of the research report, except that such rules may not limit the authority of a broker or dealer to discipline a securities analyst for causes other than such research report in accordance with the policies and procedures of the firm;
2. to define periods during which brokers or dealers who have participated, or

are to participate, in a public offering of securities as underwriters or dealers should not publish or otherwise distribute research reports relating to such securities or to the issuer of such securities;

3. to establish structural and institutional safeguards within registered brokers or dealers to assure that securities analysts are separated by appropriate informational partitions within the firm from the review, pressure, or oversight of those whose involvement in investment banking activities might potentially bias their judgment or supervision; and
4. to address such other issues as the Commission, or such association or exchange, determines appropriate.

b. **Disclosure**

The Commission, or upon the authorization and direction of the Commission, a registered securities association or national securities exchange, shall have adopted, not later than 1 year after the date of enactment of this section [enacted July 30, 2002], rules reasonably designed to require each securities analyst to disclose in public appearances, and each registered broker or dealer to disclose in each research report, as applicable, conflicts of interest that are known or should have been known by the securities analyst or the broker or dealer, to exist at the time of the appearance or the date of distribution of the report, including--

1. the extent to which the securities analyst has debt or equity investments in the issuer that is the subject of the appearance or research report;
2. whether any compensation has been received by the registered broker or dealer, or any affiliate thereof, including the securities analyst, from the issuer that is the subject of the appearance or research report, subject to such exemptions as the Commission may determine appropriate and necessary to prevent disclosure by virtue of this paragraph of material non-public information regarding specific potential future investment banking transactions of such issuer, as is appropriate in the public interest and consistent with the protection of investors;
3. whether an issuer, the securities of which are recommended in the appearance or research report, currently is, or during the 1-year period preceding the date of the appearance or date of distribution of the report has been, a client of the registered broker or dealer, and if so, stating the types of services provided to the issuer;
4. whether the securities analyst received compensation with respect to a research report, based upon (among any other factors) the investment banking revenues (either generally or specifically earned from the issuer being analyzed) of the registered broker or dealer; and
5. such other disclosures of conflicts of interest that are material to investors, research analysts, or the broker or dealer as the Commission, or such association or exchange, determines appropriate.

c. **Definitions**

In this section--

1. the term 'securities analyst' means any associated person of a registered broker or dealer that is principally responsible for, and any associated person who reports directly or indirectly to a securities analyst in connection with, the preparation of the substance of a research report, whether or not any such person has the job title of 'securities analyst'; and
2. the term 'research report' means a written or electronic communication that

includes an analysis of equity securities of individual companies or industries, and that provides information reasonably sufficient upon which to base an investment decision.