Gary Berrigan has led many organizations in their SOX compliance needs since the passage of the Sarbanes Oxley Act 2004.

SOX and COVID-19

Today, companies are focused on rebuilding their customer base, reorganizing their corporate structure, and determining where the company will be when we are back to "normal". With that, public companies can not ignore their compliance with Sarbanes-Oxley 404 and their internal control environment.

To facilitate business continuity, employees were set up to work from home. IT departments across the globe enabled employees to VPN into their network so not to disrupt the business model. The decisions made were with a short-term fix until offices can be opened again. With now four months into the COVID-19 pandemic, companies have had to make difficult decisions to furlough employees and reassign work. Given this disruption with personnel and changes in the corporate environment, where do companies stand with their internal control environment and what should companies be doing to ensure they can effectively certify that their internal controls over financial reporting are working?

The IT environment

On at least an annual basis, internal audit determines if the access provisions in the network and the ERP systems are appropriate. Organizations are very practiced with provisioning new employees and are fairly effective when handling employee terminations. However, with the current employee disruptions, transferring employee access can be more difficult to handle because an employee's old access *should* be rescinded when their new accesses are provisioned. This can result in a growing number of employees who have a growing list of user access privileges. Assuming that any new access privileges are documented in the IT ticketing system, companies should determine which employees have additional access to the IT environment and determine if those privileges are still necessary.

It is important to consider potential segregation of duty implications and whether additional review procedures are also needed.

Working from home can also present additional cyber security risks. Employee's home Wi-Fi network should be configured with security features that protect the privacy as well as the availability of the Wi-Fi network.

Many companies are procuring additional circuits from telecoms and interconnection-focused colocation providers to improve network utilization to support remote workplace tools, including videoconferencing and virtual private networks (VPNs). Easing remote access runs counter to typical corporate security best practices, so companies should be engaging additional security protocols and professional assistance to prevent unauthorized access and data breaches. Audit and compliance processes are receiving extra attention given the newly distributed access to VPNs.

Malware threats can disrupt an organization's network or employees can be vulnerable to phishing attacks. With employees now not having immediate access to their colleagues or supervisors to determine if an email is impersonating another, training is essential to teach employees how to detect a fraudulent email.

According to the Global Technology Audit Guide (GTAG)[1], because cyber threats are designed to take down systems or capture data, the threats often occur wherever critical data is stored: data centers, internal networks, externally hosted environments, and even business continuity platforms.

To reduce the risk of such attacks reaching the firewall, the first line of defense takes preventive action at the perimeter of the network. This process involves restricting access and blocking unauthorized traffic. Detective controls, such as monitoring, should also be established to watch for known vulnerabilities based on intelligence gained about software products, organizations, and malicious websites.

When data is stored external to the organization, it is vital for the organization to ensure vendors are properly managing relevant risks. While employee and visitor access into both corporate and third-party colocation data centers has always been tightly controlled, with COVID-19, many facilities have further restricted access. When corporate IT staff can't readily visit their data center due to distance or access restrictions, they are increasing reliance on the colo provider for hardware and software installs, network optimization, IoT deployments, and managed security. A critical first step for the first line of defense is to establish strong contracts that require: service organization control (SOC) reports, right to audit clauses, service level agreements (SLAs), and/or cybersecurity examination engagements.

Internal Audit should scope for cybersecurity risk by understanding the following questions:

- What information is deemed critical and why?
- What is the value of the data (to fraudsters, competitors, etc.)?
- Where is the information accessed, processed, and stored?
- How is information transmitted?
- What is the extent of rigor followed to grant and revoke access?
- Have access levels been determined by role and what roles have administrative access?
- How is access assigned, approved, monitored, and removed?
- How well protected is the information to unauthorized access?
- What type of testing is performed (penetration, access, tracked changes, etc.)?
- How is cybersecurity risk monitored for those who have functional access to critical information?

SOX documentation

A company's Sox documentation, if not automated, likely includes narratives and control matrices that describe the processes and controls that companies have to ensure the proper internal controls over financial reporting, their IT controls and general corporate governance procedures following the COSO framework. Testing procedures are also developed to ensure the internal controls described are working.

Documentation is often updated when the internal or external auditor is performing the walkthrough of the controls.

[1] GTAG Supplemental Guidance: Assessing Cybersecurity Risk

During this walkthrough, observation of the process also takes place. In today's environment, these walkthroughs and observations may be on hold.

Companies should create a log of the process and control changes that have occurred since the COVID-19 outbreak. This log should be reviewed and approved by appropriate management. This will help in evaluating the changes and will be important later when performing testing of these controls.

The review and approval process has also most likely changed. Most smaller companies have manual controls that show documents have been reviewed. Email may have replaced a manual signature, but a more effective control would be an electronic signature. That will at least show that management has opened the document. Also, how are reviews being performed today? Management review controls should include the following criteria to ensure that controls are being performed properly:

- *Objective of the Review* – Is the review put in place to prevent or detect misstatements?
- *Level of aggregation* – Is the control being performed at an aggregated or disaggregated level?
- *Consistency of performance* – Is the control being performed routinely and consistently?
- *Correlation to relevant assertions* – Is the control specifically related to relevant assertions?
- *Predictability of expectations* – Is the control designed to detect misstatements by using key performance indicators?
- *Criteria for investigation* – What is the threshold for investigating differences from expectations?

Since uncertainty abounds today, there is a lot more focus on cash. More than likely, Corporate Controllers and CFOs are taking a closer look at their balance sheet. A review of the company's delegation of authority should be performed to ensure the process by which a manager divides and assigns work to his subordinates is still effective and potential changes in levels are approved.

According to KPMG[2], the following critical SOX control areas warrant additional attention:

Estimates and Reserves. *There continues to be a focus on estimates and reserve areas that are subjective in nature. Estimates need to be supported by data-driven assumptions. Given the speed with which the business environment is changing, there are many estimates that will need to be revisited, and the rationale for those decisions and assumptions should be well documented since facts and circumstances are changing so rapidly. For example, cash collections have slowed due to companies struggling to modify their payment processing activities to be virtual. At the same time, companies have struggled with the cash application process, and the collectability of receivables from certain vendors may have changed. All of these factors will require you to revisit the assumptions used in determining your receivable reserves. Reliance on prior assumptions and methodologies to calculate your reserves will likely not be sufficient. The same is true for many other asset valuations— inventory, goodwill and intangible assets, stock compensation, asset fair values, etc.—that are impacted by earnings and cash forecast modifications.*

Price and Quantity. *The revenue process, as a higher-risk process, continues to be a focal point for control testing, specifically with respect to the controls over price and quantity. As companies and their customers contemplate a sudden change in their economic outlook, we are seeing discussions around discounts, changes to payment terms, and other concessions. It is important to think through the governance and controls around making these types of*

[2] KPMG: COVID-19: The Impact on SOX 404 programs

modifications and how those are being communicated throughout the organization, specifically to the accounting and finance functions.

Significant and Unusual Transactions. *Consider the controls in place around any significant transactions, such as discontinuation of operations, sale/closure of business lines, renegotiation of debt covenants, lease renegotiations, reorganizations, and receipt of federal loans or aid. All of these actions and activities include a number of assumptions and estimates that need to be documented, and the decisions need to have the appropriate review and control processes in place.*

Risk Assessment

Auditors perform risk assessments and materiality calculations early in the engagement to see which accounts are being evaluated and which locations should be visited. Materiality levels for many companies have changed and the quantitative and qualitative factors in performing a risk assessment should be revisited. To determine materiality, auditors rely on projections that management provides. With the impact of COVID-19, these projections have changed, and the effectiveness of management setting projections will also be evaluated, as well as the lowering of the materiality dollar amount.

One of the challenges in performing entire off-site audits will be the loss of the observations of processes and the loss of the team environment. A lot of my own audit paths are created through dialog with control owners. They are the closest to see if a control is failing or not working in accordance with the described process and I am able to pick the sample that will show this weakness and start a conversation with management.

Corporate Governance

Sarbanes-Oxley §406 require a registrant to disclose whether it has adopted a code of ethics that applies to the company's principal executive officer, principal financial officer, principal accounting officer or controller, or persons performing similar functions. As best practice, a code of conduct should include all employees to ensure that any observed instances of misconduct or pressure to compromise ethics standards are reported. From an internal control's standpoint, the code of conduct should be reviewed and updated annually and distributed to all employees. With COVID-19, companies should include a work from home provision that state that employees that work from home, whether as a permanent or occasional location, have the same responsibilities regarding the use and protection of all Company assets at home as they do if and when working from the Company's offices.

According to Auditor's Dictionary: Terms, Concepts, Processes, and Regulations, the tone at the top is often considered to permeate an entire organization, and good tone at the top is considered a prerequisite for solid corporate governance.

Good organizational tone is set through policies, codes of ethics, a commitment to hiring competent employees, and the development of reward structures that promote good internal controls and effective governance and can be assessed through the 2013 COSO Framework. With COVID-19, additional fraud risks may be present.

Fraud risks have always been assessed in an audit, although COVID-19 may see an increase in these risks in the following areas:

- On-boarding third party advisors without proper due diligence due to the speed which they are needed;

- Accelerating revenue recognition due to the pressures of moving product to market or the need to perform to prior guidance;
- Companies are more focused on operational measures than compliance;
- Transfer of staff to a work at home model may lead to prevention and monitoring controls being understaffed;
- Delegation of Authority not being updated, and transactions being processed without proper approvals;
- Is any government aid being applied for and being used for correctly?
- Failure of timely reconciliations and misuse or theft of cash.

These are a few of the additional risks COVID-19 can increase.

Preparing for Quarter End and Analysis of Deficiencies

By now, the use of Zoom meeting and the like are being used to ensure effective communication for the teams, including internal audit. The use of secure file sharing software –applications, such as BOX, Accellion Kiteworks, OneDrive, and the like, can be used to securely transfer data between staff and the audit team and also allow for organization of files. The need to provide auditors remote access and determine who will need access to certain systems or information should be considered. In many cases, remote access can be provided directly to the auditor while in other situations audit staff will need access to run reports. If there is information maintained in paper only format or systems that can't be accessed remotely, assess the availability of an individual to access that information and any special timing restrictions.

Generally, companies need two consecutive quarters to remediate any control deficiencies found to ensure those deficiencies don't rise to a significant deficiency or material weakness. Now is the time to collaborate with your financial, IT, HR and other team members to ascertain where the biggest risks will be found.

Updating flowcharts and narratives will be important during this work from home model most companies are experiencing. This will help the internal and sox auditor to identify any key process changes and new key controls.

I want to hear from you.
Gary Berrigan, sideLook Consulting

Gary Berrigan
TEL: 917-306-2134
gary@sidelookllc.com

Function and Specialization

- Internal Audit
- SOX Compliance
- IT Controls
- Risk Management
- COSO Framework
- Corporate Governance
- Operational audits
- Project Management
- Financial Audits
- Forensic/Fraud Investigations
- Financial Reporting
- Technical Accounting
- Due Diligence
- Policies and Procedures
- ERP Implementation

Technical

- COSO
- CRMA
- GAAP
- GAIT
- CoBIT

Industries

- Technology
- Manufacturing
- Government
- Insurance
- Retail
- Media and Advertising
- Bio-pharma
- Start-ups

Education

Rutgers University, BS Accounting

Background

Gary brings progressive experience, including international experience, for start-up, mid-size and large companies, both public and private. A proven track record with significant management experience in the following:

- Process re-engineering and internal controls
- Internal auditing and regulatory matters, including SOX
- Enterprise risk management
- International operations
- Fraud investigations (including Whistleblower complaints and FCPA)
- Financial due diligence
- Business development
- SAP and NetSuite/Oracle implementation
- Board meetings and governance

Professional Accomplishments

- Designed, implemented and managed the internal audit department and developed its risk-based audit universe for public companies.
- Led SOX engagements for clients in sectors that included technology, media and entertainment, retail, and bio pharmaceutical. Gary has extensive international travel throughout Israel, Europe, Asia and South Africa, bringing SOX and internal control training to company's international financial directors.
- Developed a financial due diligence program and performed buy side financial due diligence on companies for venture capital firms and other private equity companies.
- Identified financial and ITGC controls for a technology Company's NetSuite and Great Plains implementations and Oracle enhancements and identified controls over a manufacturing Company's SAP implementation.
- Investigated internal fraud for financial improprieties misappropriation of funds, as well as whistle-blower complaints received through a company's confidential hotline.
- As a Financial Analyst with the FBI, Gary has supported FBI Special Agents in money laundering investigations that included organized crime, white-collar crime, public corruption, health care fraud, and other violations of federal statutes.

Professional Experience

Gary has significant experience in fraud investigation and audit with the Federal Bureau of Investigation, KPMG and New York Life Insurance Co; Internal Audit and SOX compliance and financial due diligence with Interpublic Group of Companies and Geller & Company and leading the audit function with Globe Specialty Metals, MRV, Inseego Corp. and SeaChange International.

Education/Certifications

Gary received his Bachelor of Science degree in Accounting from Rutgers University and has trained at the FBI Academy, Quantico, VA. for Anti-Money laundering initiatives and white-collar crime.