Verba

SOLUTION GUIDE

Compliance and risk management

Mitigate risk and manage compliance with Verba Recording System

Introduction

Companies are focusing on compliance concerns because of their impact on all aspects of business operations. Efforts to comply with regulatory requirements must be supported by appropriate systems. Continuously growing regulatory burdens and increasing use of standards to improve processes are leading many organizations to formalize compliance programs, raising questions on organization, competencies, controls rationalization and alignment with risk management and business performance.

The following table lists some regulatory examples by industry (mostly for EU and USA):

Finance **Insurance**	▪ Basel II Accord ▪ MiFID (Markets in Financial Instruments Directive) ▪ PCI DSS (Payment Card Industry Data Security Standards) ▪ USA Patriot Act ▪ AML (Anti-Money Laundering) ▪ SEC 17-a-4/NASD 3010 (Securities Exchange Act 1934) ▪ GLBA (Gramm-Leach-Bliley Act) ▪ ECOA (Equal Credit Opportunity Act) ▪ TILA (Truth in Lending Act) ▪ FDCPA (Fair Debt Collection Practices Act)
Electronic **Automotive**	▪ Trade Act ▪ European Block Exemption ▪ End of Life (AP) ▪ RosettaNet

verba

Mitigate risk and manage compliance with Verba Recording System

	▪ WEEE (Waste for Electronics and Electronics Equipment) ▪ Wassenaar Agreement
Healthcare	▪ HIPAA (Health Insurance Portability and Accountability Act)
Multiple Industries	▪ SOX (Sarbanes-Oxley Act) ▪ DCGK (Deutsche Corporate Governance Kodex) ▪ CLERP 9 (Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure) Act)

Compliance Recording

Call centers, trading floors and businesses that regularly communicate with customers, clients, and partners, must be aware of the risk associated with every interaction. Many businesses are legally required to monitor these interactions as a means of managing risk and liability. Businesses must adhere to standards set by private companies and self-regulatory groups that monitor the protection of personal data. Monitoring the high volume of interactions that take place on a daily basis is a challenge, especially for businesses that operate large or multi-site contact centers. In order to maintain compliance with the numerous legal and internal requirements, these businesses must implement total call recording solutions that can effectively capture, store, monitor, and find their most critical interactions.

Using Verba Recording System, the award winning call recording suite, can help companies easily and effectively comply with regulations. The chapters below briefly describe the essential features of a reliable call recording platform.

Comprehensive set of recording methods

In order to support the various telephony environments and network topologies, the recording system must provide various methods for capturing the interactions. The Verba Recording System supports all major recording methods for Cisco, Avaya, BroadSoft, IP Trade and other communication environments, which allows centralized recording of all phones in the company or if required, locally installed recording devices with store and forward functionality at each branch office. In addition to the phone conversations, Verba Recording System is able to provide screen capturing capabilities in order to record the entire customer interaction. Finally, not only does Verba Rrecording System record voice conversations, it is also able to record video and telepresence calls and conferences.

Sophisticated access control

Verba Recording System's user authorization concept controls activities within the web application and the phone service application on the IP phone. User authorization is based on two key concepts: segregation of duties and activity level control. In the Verba Recording

Mitigate risk and manage compliance with Verba Recording System

System, groups can be defined in order to control user access to various contents, using one or many.

Privilege levels are used to define superior-subordinate relationships in the system, which allows superiors to access their subordinates' calls. There are many user types in Verba Recording System in order to adapt to a corporate hierarchy easily. The relationships between users can be vertically or horizontally defined.

In order to properly segregate the duties and ensure secured and safe operation, the security policies and privilege level assignments to user accounts need to be planned and enforced. Activity types allow access control in a more granular manner and further segregating roles and responsibilities. These optional rights can be granted to each user (and will be in effect for their authority privilege levels and below). These include: playback, download, deleting, e-mail, commenting, marking as private, silent monitoring, share calls, reporting, etc.

Every user has to be associated with at least one group, because certain functions and features like comment templates are configured through the associated groups.

User accounts have a validity period (start and end date) and can be also locked to suspend access. Multiple unsuccessful login attempts can also result in a locked user account according to the rules set by the system administrator.

Password expiration can be set system wide or on a per user basis. Password strength rules can be configured globally with many options (expiration length in days, password history check with length, minimum password length, must include capital letter, must include special character, and must include numeric character).

Audit trails

Verba Recording System provides detailed activity logging with easy search capabilities for administrators in two major areas: configuration changes (adding or changing user accounts, groups, extensions, server settings etc.) and user activity (login/logout) and business data changes (adding/removing markers, playback, download, delete etc.).

Every change record captures the activity, the user ID, the event date/time, the object ID and field(s) with old and new values. This feature cannot be deactivated. Verba Recording System provides a maintenance function to purge old, outdated records as a scheduled job.
A third area of logging is system component activities. The types and levels of logging are configurable and the information stored in log files assist the administrators with system management and monitoring activities. These files do not capture any business content related information, only include technology related data. Verba Recording System also provides many system and user activity monitoring features that help companies with system support and compliance monitoring as well.

Mitigate risk and manage compliance with Verba Recording System

Easy and quick access to recordings

Utilizing the unique and feature-rich web based user interface of the system, auditors or other users can easily find and retrieve the recordings. The standard SQL database in Verba Recording System provides numerous features for searching back, even archived interactions. The built-in player module provides an easy-to-use, but sophisticated playback experience using industry standards without the need of installing any proprietary application.

Encrypted storage and data protection

In order to prevent unauthorized access to recording on file system level, Verba Recording System can apply optional encryption for each recorded audio file. Without using the built-in user interface with proper authorization and full audit trail, nobody can play back any recording from the recording server. Verba Recording System uses the industry standard 1024 bit RSA (Rivest, Shamir and Adleman) and 256 bit AES (Advanced Encryption Standard) technology.

In addition to the multi-level access control protection of the recordings, any type of manipulation either on the media file or either with the call detail records can be easily identified with the built-in integrity protection feature of the system applying industry standard 1024 bit PKCS v1.5 (Public-Key Cryptography Standards) digital signatures.

Policy based data retention

As the amount of stored calls increases, it becomes more important to be able to set retention periods by certain parameters of calls, rather than saving all calls for the maximum required by the longest need. The built-in storage policy module in Verba Recording System allows for the creation of rules specifying how long a particular call is retained based on the business requirement for the specific call type. This approach not only helps control overall storage costs, but also ensures that calls are retained only as long as required.

Mitigate risk and manage compliance with Verba Recording System

Appendix

This appendix provides a brief description of the most common regulations and the various tools and features available in VERBA supporting the compliance regarding the given policies.

PCI DSS

PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The PCI security standards are technical and operational requirements that were created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. A company processing, storing, or transmitting cardholder data must be PCI DSS compliant. The PCI SSC (Council) is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Non-compliant companies who maintain a relationship with one or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined. All in-scope companies must validate their compliance annually. The current version of the standard specifies 12 requirements for compliance, organized into 6 logically related groups, which are called control objectives.

Cardholder data protection – Access to audio and screen recordings is managed at the user level with the enhanced multi-level access control module in Verba.
File encryption – Video and audio files can be optionally encrypted using the industry standard AES technology. This ensures that no encrypted data can be read (decrypted) on file system level.
Network encryption – Verba security features include SSL encryption for all client-server communications in playback.
Controlling recording – The standard requires that card security codes (CID, CAV2, CVC2, CVV2) are not stored. Verba is able to receive start and stop triggers via its standard API to define the beginning and end of a period within a call that contains this information, effectively pausing the recording of both voice and screen. Note: modern call recording systems are recording at the extension side, instead of the trunk side, so the sensitive card security codes are not recorded at all.
Audits – Verba includes an extensive activity audit system, providing a database of all activity in the system. You will be able to conduct full trace audits to determine who has accessed any recording in the system for playback, export, or any other critical functions.

More information:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
http://en.wikipedia.org/wiki/PCI_DSS

Mitigate risk and manage compliance with Verba Recording System

MiFID

The Markets in Financial Instruments Directive (MiFID) as subsequently amended is a European Union law which provides a harmonised regulatory regime for investment services across the 30 member states of the European Economic Area (the 27 Member States of the European Union plus Iceland, Norway and Liechtenstein). The main objectives of the Directive are to increase competition and consumer protection in investment services. As of the effective date, 1 November 2007, it replaced the Investment Services Directive. MiFID is the cornerstone of the European Commission's Financial Services Action Plan whose 42 measures will significantly change how EU financial service markets operate. MiFID is the most significant piece of legislation introduced under the Lamfalussy procedure designed to accelerate the adopting of legislation based on a four-level approach. The Financial Services Authority (FSA) in the UK has issued various policies based on the MiFID directive. One of these policies provides information for recording voice conversations and electronic communications.

Call recordings are a prime medium for customer interactions. A purpose built call recording system will ensure that relevant data can be maintained for the desired retention period and maintain the security and the integrity of the records through tamper-proof mechanisms. Furthermore, the system will provide easy search access to recover data if required by an external auditor.

More information:
http://europa.eu/scadplus/leg/en/lvb/l24036e.htm
http://www.fsa.gov.uk/pubs/policy/ps08_01.pdf
http://en.wikipedia.org/wiki/Mifid

USA Patriot Act

The USA PATRIOT Act (commonly known as the "Patriot Act") is an Act of the U.S. Congress and signed into law by President George W. Bush on October 26, 2001. The title of the Act is a contrived acronym, which stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. The Act dramatically reduced restrictions on law enforcement agencies' ability to search telephone, e-mail communications, medical, financial, and other records; eased restrictions on foreign intelligence gathering within the United States; expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and broadened the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. Besides extending law enforcement's surveillance and investigative powers and easing restrictions on foreign intelligence gathering within the US, the USA PATRIOT Act also expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities.

Mitigate risk and manage compliance with Verba Recording System

One provision of the USA PATRIOT Act requires financial services companies to develop improved capabilities to identify customers and flag suspicious transactions, making businesses responsible for seeking, detecting, and reporting computer trespasses. Banks in particular are expected to identify, discover, gather, amass, investigate, and report on financial activity to a far greater degree and depth than was previously expected of them.
Call recordings are a prime medium for customer interactions. A purpose built call recording system will ensure that relevant data can be maintained for the desired retention period and maintain integrity of the records through tamper-proof mechanisms. Furthermore, the system will provide easy search access to recover data if required by an external auditor. Verba Recording System also allows users to easily flag certain interactions for quick retrieval later.

More information:
http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html
http://en.wikipedia.org/wiki/USA_PATRIOT_Act

GLBA (Gramm-Leach-Bliley Act)

The Gramm-Leach-Bliley Act (commonly called GLB or GLBA) is also known as the Financial Modernization Act of 1999. The GLB Act includes provisions to protect all consumers' personal financial information held by financial institutions. Today, the vast majority of organizations use phone calls to communicate internally. Since personal financial information can be transmitted by and retained in electronic formats, it is critical to ensure that the management of such records complies with GLB. The GLB Act applies to "financial institutions" - businesses that offer financial products or services to individuals to be used primarily for their personal, family, or household purposes. Financial institutions include, for example, banks, securities firms and insurance companies; such entities are covered by the SEC (Securities and Exchange Commission). Businesses that provide many other types of financial products and services to consumers fall under jurisdiction of the FTC (Federal Trade Commission) for the purposes of enforcing GLBA. These non-traditional "financial institutions" include, but are not limited to, state-registered investment advisors, professional tax preparers, auto dealers engaged in financing or leasing, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies, retailers that issue credit cards to consumers, consumer debt-collecting firms, payday lenders and check-cashing businesses. The financial institution must take all precautions necessary to protect and defend the consumer and associated nonpublic information.

Call recordings are a prime medium for customer interactions. A purpose built call recording system will ensure that relevant data can be maintained for the desired

Mitigate risk and manage compliance with Verba Recording System

retention period and maintain integrity of the records through tamper-proof mechanisms. Furthermore, the system will provide easy search access to recover data if required by an external auditor.

More information:
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html
http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act

SOX

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called Sarbanes-Oxley or SOX, is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals. Thousands of companies face the task of ensuring their accounting operations are in compliance with the Sarbanes-Oxley Act. This Act instructs executive management of publicly held companies to evaluate and report on the effectiveness of their internal controls over financial reporting, and have independent auditors substantiate the effectiveness of these controls. These controls include the application software and information technology (IT) processes that sustain a company's day-to-day operations. Fundamentally, compliance is focused on the integrity of financial statements. Compliance is more than documentation; it also includes the controlled testing of systems, the tighter management of critical third party services, and the near real-time ability to report on all events that materially affect the business. Companies incorporating best practices to meet regulatory requirements are also creating the basis for a solid business continuity strategy.

Specifically all relevant audit-related documentation must be retained for a period of at least seven years. This includes contracts, policies, authorizations, verifications, recommendations, performance reviews and financial data. SOX also addresses the need for companies to effectively manage risk in all its forms—including ensuring that data residing on corporate computers is adequately archived and protected from damage or tampering. To comply with these needs, an effective storing system is required that can scale to meet the needs of storing large amounts of call recordings in a secure manner for long periods of time.

More information:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf
http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Mitigate risk and manage compliance with Verba Recording System

HIPAA

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule standards address the use and disclosure of individuals' health information – called protected health information by organizations subject to the Privacy Rule – called covered entities, as well as standards for individuals' privacy rights to understand and control how their health information is used. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

All patient information, authorizations, policies, procedures and contracts with business associate must be retained for at least 6 years. Call recordings are a prime medium for customer interactions. A purpose built call recording system will ensure that relevant data can be maintained for the desired retention period and maintain the security and integrity of the records through tamper-proof mechanisms.

More information:
http://www.hhs.gov/ocr/privacy/index.html
http://en.wikipedia.org/wiki/Hipaa

Basel II Accord

The Basel II Framework describes a more comprehensive measure and minimum standard for capital adequacy that national supervisory authorities are now working to implement through domestic rule-making and adoption procedures. It seeks to improve on the existing rules by aligning regulatory capital requirements more closely to the underlying risks that banks face. In addition, the Basel II Framework is intended to promote a more forward-looking approach to capital supervision, one that encourages banks to identify the risks they may face, today and in the future, and to develop or improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices.

Given that the emphasis is in the main risk assessment, the impact on phone calls is likely to be the requirement to retain all phone calls relating to a trade for a period of not less than 5 years, starting from January 2003. Financial institutions must ensure that data

Mitigate risk and manage compliance with Verba Recording System

and communication is secure, accessible and accurate.

More information:
http://www.bis.org/publ/bcbsca.htm
http://en.wikipedia.org/wiki/Basel_ii

Mitigate risk and manage compliance with Verba Recording System

verba technologies

Contact us to learn more about how the Verba recording solution can help you enhance your business to gain a competitive edge: www.verba.com

Available through Geomant:

www.geomant.com
products@geomant.com

Americas: +1 512 222 32 06
Europe: +44 1789 387900
APAC: +61 409 99 78 39

geomant™

Please consider the environment before printing this document.