WHITE PAPER

Improving the Compliance Management Process

sagiss
smart. simple. managed IT.™

EXECUTIVE SUMMARY

All organizations must deal with compliance obligations. These range from relatively minimal obligations that focus only on protection of certain types of records; to very strict obligations to monitor and sample employee communications, retain a wide range of record types for long periods of time, and to protect the confidentiality of highly sensitive customer information. Consequently, all organizations must satisfy varying levels of compliance obligations – the only difference between a "heavily" regulated vs. a "lightly" regulated one is in the number and invasiveness of the regulations that they must satisfy.

Organizations in some of the more regulated industries – for example, financial services, insurance, healthcare, energy, government, education and life sciences – must deal with a large and growing number of compliance obligations. A failure to satisfy these obligations can result in serious consequences, including fines, sanctions or even business closure.

Complicating the problem is the fact that there are regulations at the federal, state and local level; not to mention the variety of industry-focused and international regulations that organizations must satisfy. Moreover, many of these regulations are in a continual state of flux as regulators modify and add to the body of regulations to which organizations are subject.

Many organizations satisfy their compliance obligations using manual processes focused on maintaining spreadsheets or using out-of-date software to help compliance managers keep the organization as close to full compliance as possible. Moreover, compliance obligations are managed with a significant amount of labor, which drives up costs beyond where they would be if a more automated and holistic approach for compliance management were available.

To understand the high cost of conventional compliance management processes, Osterman Research conducted a survey with organizations in a variety of industries. Using a subset of our survey sample to eliminate outliers, we discovered that organizations spend $524 per employee annually managing their compliance processes – in a organization of just 500 employees, this translates to a cost in excess of $261,000 annually. Moreover, we found that only 13% of the organizations we surveyed are "very satisfied" with the way that they manage regulatory compliance issues, despite the fact that 67% consider regulatory compliance to be "very important" to their organization.

Only 13% of the organizations we surveyed are "very satisfied" with the way that they manage regulatory compliance issues, despite the fact that 63% consider regulatory compliance to be "very important".

KEY TAKEAWAYS

The key takeaways from this paper:

- Compliance management is difficult because it requires a significant amount of labor caused by the manual nature of the compliance work that is required, and it is expensive to manage.
- Organizations need a more automated and less expensive approach to managing their compliance processes.

ABOUT THIS WHITE PAPER

This white paper discusses the variety of compliance obligations that organizations are obligated to satisfy, provides some high level recommendations about what organizations can do to address these issues, and offers a brief overview of KnowBe4 and the company's relevant solutions.

sagiss
smart. simple. managed IT.™

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

THE NEED TO MANAGE COMPLIANCE WELL

THERE IS NO "UNREGULATED" INDUSTRY

There is a mindset held by many that there are "regulated" industries like financial services and healthcare, and "unregulated" industries like manufacturers, retailers and virtually every other industry type. The truth of the matter, however, is that all industries and organizations are regulated – the difference is simply in the degree to which regulation applies. In other words, every organization, regardless of its size or the industry that it serves, faces some level of compliance obligation that it must satisfy, whether these are fairly basic regulations like those focused on employment records management, or difficult and onerous obligations like those in the financial services industry.

What follows is an overview of some key regulations in various industries, many of which are focused on the retention of records, although regulations cover a wide range of business activities. Please keep in mind that these are only highlights and barely scratch the surface of the many thousands of regulations of which compliance officers, senior managers, legal counsel and others must be aware.

HEALTHCARE

- The Privacy Rule in the Health Insurance Portability and Accountability Act (HIPAA) requires organizations to put in place appropriate safeguards to protect patient data so that it cannot be disclosed without permission of the patient[i]. HIPAA permits patients to request of healthcare providers an accounting of who has accessed their records over the past six years in accordance with 45 CFR 164.316.

- 45 CFR 164.530(C)(c)(1) states that "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." This is an essential component of any healthcare-related organization's data security and protection plan, whether on-premises or in the cloud.

- As specified in 45 CFR 164.308(7), covered entities and business associates must "establish…policies and procedures for responding to an emergency or other occurrence…that damages systems that contain electronic protected health information (PHI)", "establish…procedures to restore any loss of data", and "establish…procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode".[ii]

- 42 CFR 491.10 specifies that rural health clinics maintain "a clinical record system in accordance with written policies and procedures", that they provide "safeguards against loss, destruction or unauthorized use" of clinical records..." Compliance with this statute also include a provision that "A designated member of the professional staff is responsible for maintaining the records and for insuring that they are completely and accurately documented, readily accessible, and systematically organized."

- 45 CFR 164.306 states that covered entities must "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits"; "protect against any reasonably anticipated threats or hazards to the security or integrity of such information"; and "protect against any reasonably anticipated uses or disclosures of such information that are not permitted…"

- 45 CFR 164.308 includes a requirement for organizations to "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR 164.306(a)", and to "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

Covered entities must "ensure the confidentiality, integrity, and availability of all electronic protected health information…"

sagiss
smart. simple. managed IT.™

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

FINANCIAL SERVICES

- The Payment Card Industry's Data Security Standard (PCI DSS) requires any organization that processes cardholder data to protect that data from hacking, data loss and other types of breaches. Protected content includes cardholders' primary account numbers (PANs), names and credit card expiration dates. The minimum PCI DSS standard requires that PANs be unreadable on any storage media, including backups, and that strong cryptography be used for all sensitive data[iii].

- The Gramm-Leach-Bliley Act (the Financial Modernization Act of 1999, or GLBA) includes the Financial Privacy Rule and the Safeguards Rule that imposes strict requirements on any organization that maintains customer financial data. Affected organizations include merchants, mortgage brokers and any other organization in possession of credit card information, personal financial information or similar types of sensitive or confidential content. GLBA also includes "Pretexting Protection" that is designed to protect sensitive financial data from access using phishing or other social engineering attacks, and includes implied provisions for employee compliance training.

- The Bank Secrecy Act "requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities."

- The Financial Industry Regulatory Authority (FINRA) Regulatory Notice 07-59 indicates that FINRA "expects members to prohibit, through policies and procedures, communications with the public for business purposes from employees' own electronic devices unless the member is capable of supervising, receiving and retaining such communications." Moreover, this Notice requires "members using lexicon-based reviews of correspondence [to] utilize an appropriate lexicon, take reasonable security measures to keep the list confidential and periodically evaluate the efficacy of the lexicon."

PUBLIC COMPANIES

The Sarbanes-Oxley Act contains a number of requirements:

- Section 302 requires review and confirmation of the financial condition of the company "in all material respects". Moreover, officers who sign off on the financial condition of the company are responsible for the internal controls that have been established.

- Section 404 of the Act requires publication of information in annual reports regard the adequacy and scope of the issuers' internal control structure and financial reporting procedures.

- Section 409 requires issuers to inform the public rapidly about material changes in their financial operations or conditions.

GOVERNMENT

There is an enormous amount of regulation focused on government agencies' responsibility to protect sensitive information. Here are a few sample regulations focused on US federal government agency responsibilities in this regard:

- The Federal Information Security Management of 2002 (FISMA) mandates that the head of each federal agency will "be responsible for providing information about security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency…"

The Gramm-Leach-Bliley Act…imposes strict requirements on any organization that maintains customer financial data.

sagiss
smart. simple. managed IT.™

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

Among many other provisions, FISMA mandates that data backups exist in a separate facility from the primary data center, that content is encrypted during transit and when at rest, and that any facilities achieve SSAE 16 Certification, which is discussed later in this white paper.

- 49 CFR Part 15 requires that anyone subject to it must "take reasonable steps to safeguard Sensitive Security Information (SSI) in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room."

- Section 147 of the Atomic Energy Act governs handling of Safeguards Information (SGI), information that is unclassified, but nonetheless must be treated as sensitive because it focuses on the physical protection of nuclear material, physical protection of nuclear reactors and related information. Specific requirements are spelled out in 10 CFR 73.21.

LIFE SCIENCES

- The United States Department of Agriculture (USDA) departmental regulation 3440-002, Part 16 (Protection of Information Technology Assets) states:

    - "Security and the need to encrypt or otherwise protect SSI are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by an agency operate effectively and provides appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

    - Information that is considered sensitive by a responsible authority, or determined to have a high value or information that represents a high risk should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.

    - The use of personal home computers to store or transmit SSI is prohibited due to the high security risks in protecting sensitive information on non-government owned systems. Government-owned equipment will be issued and configured to maintain strong security protection appropriate to the highest level of information contained on the computer."

- 21 CFR 821.1(e) requires that "A manufacturer or distributor that goes out of business is required to notify FDA at the time that it notifies any government agency, court, or supplier and must provide FDA with a complete set of its tracking records and information."

- 21 CFR 11.10 mandates that "Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."

ENERGY

NERC Cyber Security Standards (CIP-002 through CIP-009) include a range of compliance obligations, including identification of critical cyber assets (CIP-002), the implementation of security management controls (CIP-003), appropriate training of staff members (CIP-004), creation of a cybersecurity perimeter and identification of all points of access to assets within it (CIP-005), a physical security plan for cyber assets (CIP-006), and appropriate security management plan (CIP-007), a system for

49 CFR Part 15 requires that anyone subject to it must "take reasonable steps to safeguard Sensitive Security Information…"

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

reporting and responding to security-related incidents (CIP-008), and recovery plans for compromised cyber assets (CIP-009).

EDUCATION

The Family Educational Rights and Privacy Act of 1974, which is focused on protecting the privacy of students' education records, includes provisions for how states can transmit data to Federal entities, requirements for institutions to notify students about their rights under FERPA on an annual basis, and provide access to education records to both parents and students.

OTHER COMPLIANCE OBLIGATIONS

- The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is a fairly new standard for attestation of service organizations established by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). SSAE 16 replaces Statement on Auditing Standards (SAS) 70 auditing that was formerly a key standard for service providers.

  SSAE 16 requires organizations to provide a detailed description of its systems, including "the services provided, along with the supporting processes, policies, procedures, personnel and operational activities that constitute the service organization's core activities that are relevant to user entities[iv]." SSAE 16 also requires the management of organizations seeking SSAE 16 attestation to "assert" several things, including verification that the system has been established as of a specific date or has been in operation for a particular period of time, along with other requirements[v].

- ISO certification establishes standards for a variety of processes and disciplines, including risk management (ISO 31000), information security management (ISO 27001), quality management (ISO 9000), environmental management (ISO 14000) and food safety management (ISO 22000). ISO Conformity Assessment – i.e., compliance with ISO standards – including a variety of compliance-related activities, including certification by an independent organization that a process, product or system is in compliance with ISO standards; testing of the processes that are in place; and regular inspection to ensure that the processes, products or systems remain in compliance.

MANAGING COMPLIANCE IS CUMBERSOME AND EXPENSIVE

One of the fundamental problems of compliance management is the fact that much of it is focused on manual processes – maintenance of spreadsheets, compliance manuals, other documents and software-based tools that help an organization to stay current with its compliance obligations, but that require significant effort to maintain. Add to this the significant amount of time that is required simply to search for the right information to populate these documents and tools. One source has estimated that up to 80% of the time spent by compliance risk professionals is focused on the search for relevant data[vi].

Moreover, there can be significant duplicate effort on the part of compliance management staff, particularly in large and distributed organizations because several people may be working on the same compliance issues unbeknownst to others in the organization. In conjunction with the manual nature of the compliance process in most organizations, this duplicate effort results in compliance management that is relatively inefficient and may actually be contradictory in some cases as different groups develop their own interpretation of how best to satisfy compliance issues.

One of the fundamental problems of compliance management is the fact that much of it is focused on manual processes.

sagiss
smart. simple. managed IT.™

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

COMPLIANCE UPDATES COMPLICATE THE PROBLEM

The documents and tools used for compliance management are often out-of-date because of frequent updates to regulations. As just one example, Environmental Protection Agency regulations with regard to chemicals used in the forestry industry change every five to six months, requiring significant manpower just to keep up with changes and to modify corporate practices.

Underscoring the difficulty of compliance management in the context of just US federal rulemaking – not to mention rules published by state, local and other governments and organizations – is the growth of the US *Federal Register*. This document, a daily publication that contains proposed and final regulations of US federal agencies, published an average of 3,827 final rules and 2,445 proposed rules each year between 2002 and 2012[vii]. That represents an average of 14.7 final rules and 9.4 proposed rules each workday. Managing this level of change using manual processes can be very difficult, if not impossible.

COMPLIANCE MANAGEMENT CAN BE EXPENSIVE

The research that we conducted for this white paper found that compliance management is expensive. Using a subset (to eliminate outliers) of the 104 organizations we surveyed in a variety of industries, we found that the median annual expenditure per employee on compliance-related products and services is $96.21.

However, our research also discovered that there is a median of 234 employees supported by each full-time equivalent compliance-focused employee (CFE). If we assume that the fully burdened annual salary of each CFE is a rather conservative $100,000, this results in an annual expenditure for compliance-related labor of $427.72 per employee:

$$\frac{\$100{,}000 \text{ salary for a CFE}}{234 \text{ employees per CFE}} = \$427.72$$

The combination of labor and expenditures on tools and services totals $523.93 ($96.21 + $427.72) per employee per year translates to a cost of $43.66 per month. Moreover, our research found that organizations typically spend 19% of their compliance and audit time each year on tracking requirements and another 31% on gathering and maintaining audit evidence. Because these two activities alone consume one-half of the typical organization's compliance efforts, addressing just these two requirements can save significantly on overall compliance costs.

The combination of labor and expenditures on tools and services totals $523.93 per employee per year translates to a cost of $43.66 per month.

NEXT STEPS

Osterman Research recommends that any organization that must satisfy compliance obligations take a multi-step approach toward reducing their compliance costs and improving their ability to satisfy its compliance obligations.

UNDERSTAND YOUR COMPLIANCE OBLIGATIONS

First and foremost is the need to understand the full range of compliance obligations that organizations must satisfy. While most compliance managers, risk managers, senior managers and other decision makers probably know the majority of the obligations that they must satisfy, the growing number of compliance obligations makes it difficult for most organizations to know all of the requirements.

As just one example, consider that 46 of the 50 US states today have a data breach notification requirement of some sort. These requirements generally obligate companies to notify their customers in those states if their personal or other confidential information has been breached by a hacker or lost. This means that if there is even a single customer in a particular state, a compliance mechanism must be established for that state.

sagiss
smart. simple. managed IT.™

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

DEVELOP THE APPROPRIATE POLICIES

Next is to develop the appropriate policies that will help the organization to satisfy its compliance obligations. Obviously, these will vary by the specific compliance requirements that the organization must satisfy, but these policies should be thorough and sufficiently granular so as to allow the organization to establish, maintain and modify them on an ongoing basis.

One way to do this is through the use of templates that can be continually updated as existing compliance obligations change or as new regulations become established. Osterman Research recommends the use of third-party capabilities for policy and template management because of the economies of scale that are possible when using a third party. The argument for using a third party for compliance management is the same one we offer for using cloud providers where it is practical to do so: third parties can manage services for a large group of customers more efficiently and at lower cost than if organizations were to manage these capabilities themselves.

AUTOMATE AS MUCH AS POSSIBLE

As noted earlier, one of the fundamental problems with current compliance practices is their reliance on manual processes. Because a manual approach lends itself to inefficiency and duplication of effort, costs are higher than they need to be. Moreover, compliance-focused employees that could be doing other, more efficient work if an automated compliance environment existed, create an opportunity cost for the organization – in other words, they could be contributing more value by doing more valuable work, but instead are focused on managing the minutiae of compliance management.

KEY ISSUES TO CONSIDER

Compliance-focused organizations should take a holistic view toward compliance management so that they can manage all of their obligations together instead of as separate siloes. This will not only reduce the cost of compliance management, but will make change management for policies much easier.

Moreover, decision makers should implement capabilities that will provide robust auditing, tracking and reporting capabilities to ensure that compliance policies can be satisfied and the likelihood that an organization will be out of compliance is minimized.

Compliance-focused organizations should take a holistic view toward compliance management.

- Fast setup using Self Assessment Questionnaires with templates for PCI-DSS, HIPAA, and other compliance obligations.
- Consolidation of multiple regulatory requirements into one list with KnowBe4's proprietary Controls Reduction Engine (CRE)™
- Elimination of duplicate efforts to save time on compliance tasks and reduce compliance costs.

sagiss
smart. simple. managed IT.℠

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

- An integrated Compliance Calendar keeps staff members on the path to maintaining compliance through automated alerts.
- A single, centralized interface for managing multiple areas.
- Adherence to the DRI (Directly Responsible Individual) methodology of assigning specific individuals to audit tasks.
- The Audit Evidence Vault™ provides a safe and secure way of storing and accessing policy/procedure documentation and audit evidence files.

Organizations can create custom compliance templates that allow staff members to track compliance with any standard or regulation, including ISO 27000, OSHA, SSAE-16 SOC, FISMA, and state-specific requirements, among many others.

For more information:

Sagiss, LLC

1616 Corporate Court, Suite 140

Irving, TX 76039

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com

REFERENCES

[i] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
[ii] http://www.ecfr.gov/cgi-bin/text-idx?SID=2be4a0a55e9b9ba398969b96a31b99ae&node=45:1.0.1.3.78.3.27.4&rgn=div8
[iii] https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf
[iv] http://www.ssae16.org/important-elements-ssae16/description-of-the-service-organiations-qsystemq.html
[v] http://www.ssae16.org/important-elements-ssae16/written-assertion-by-management.html
[vi] http://compliance-risk.com/the-compliance-problem
[vii] Source: *Ten Thousand Commandments 2013*, Competitive Enterprise Institute

Sagiss, LLC
1616 Corporate Court Suite 140
Irving, TX 76039
sales@sagiss.com