

Identifying Compliance Risks in Your Company



Ten Questions to Identify Compliance Risks When Sharing Information

Corporate and regulatory compliance policies have forced companies to ensure that information flows are documented, auditable, and highly secure. Yet in order to conduct their business, companies must share sensitive information outside the firewall, introducing serious potential information risk. This white paper poses ten questions to help identify compliance risks and explores mitigation strategies and best practices suitable for each scenario.

SARBANES OXLEY

1. How does your company provide confidential or sensitive financial information to external auditors, compliance bodies, board members or other external users?

- We don't share confidential financial information offsite (skip to next question).
- File sharing technology such as VPN, SharePoint or other document sharing platform, FTP site.
- Send as email attachment.
- Mail hard copies or ship on physical media such as paper, CD-ROM or USB drives.

Analysis

b. With any file sharing technology, you need to consider the document's transparency. At the minimum, confidential or sensitive financial information should be encrypted on the

server while at rest and while it is being transmitted (uploaded and downloaded). Companies must develop policies addressing who can access and modify the information. If information must be restricted from IT personnel, the file sharing technology must be user friendly enough for business users to administer it, and efficient enough to ensure 100% user compliance in order



to prevent accidental financial information disclosure.

c. Email attachments pose several risks: the content can be intercepted, people using auto complete are at great risk of emailing information to the wrong person in their address book, the data is typically not encrypted and there is no way for remote users to know whether they have the most up-to-date information.

d. Shipping hard copies or physical media exposes your company to the risks of accidental loss or delivery to the wrong person or organization. Once the media are out of your hands, there is no way to track document accesses or changes. Additionally, both hard copies and electronic files on physical media can be copied, misplaced, or even inadvertently left behind in a public place such as a cab or airplane. Distribution of hard copy materials,



with watermarks, provides little to no control over reproduction and further distribution of sensitive material. Workflow is essentially non-existent.

Recommendation

A secure work space, onsite or cloud-based, offers an access-controlled Internet location where an organization can put documents to be shared and controlled. The best online work spaces take advantage of document compliance technologies such as secure presentation and watermarking to extend control beyond the workspace. Secure online work spaces protect documents from access by unauthorized users and capture an audit trail of all document accesses and changes.

2. How does your company track spreadsheet document approval such as approval of journal entries, asset listings, payment approvals, etc?

a. With an electronic signature and audit trail through an ERP system (skip to next question).

b. We don't track approvals of spreadsheet documents.

c. We track approvals on the hard copy document.

d. We track electronic signatures through a document sharing platform such as SharePoint.

Analysis

b. & c. In order for organizations to take credit for their review and approval of spreadsheet documents, the auditor must be able to prove that the document was approved. Trust but verify. To prove review and approval in a paper-based tracking system, the auditor must be able to see notations and a signature on the document itself. For reduced cost of compliance, workflow purposes and the strongest audit evidence, capturing approvals from verified users electronically in a tamper-proof audit trail is a much better choice.

d. Document sharing platforms such as SharePoint are a good tool to use as a document repository and they do provide some level of version control. Depending on the version and implementation, workflow may or may not be available. If some of the contributors and approvers are outside the network, managing security rights can be a challenge.

Recommendation

Controls need to be wrapped around spreadsheets so that they can only be accessed by authorized users and edited by only one authorized user at any given time. Any changes made are recorded. Previous versions of the spreadsheet are

saved, providing an audit trail of the changes. There are a number of file sharing technologies available such as SharePoint and other collaboration platforms, although these have shortcomings as previously described. A better approach is to use secure online work spaces that offer collaboration features, protect documents from access by unauthorized users and capture an audit trail of all document accesses and changes.

3. How does your company control changes over spreadsheets?

a. Through an automated change management system (skip to next question).

b. We don't track changes to spreadsheet documents.

c. We track changes manually by reviewing last modified date and notes in the spreadsheet.

Analysis

b. Spreadsheets may be the single most utilized financial reporting application in use by businesses today. To ensure accurate reporting, the spreadsheet data, formulas and logic must be tested and validated just as it would be for any financially significant application. The potential for errors and fraud in spreadsheets raises the risk of incomplete, inaccurate and invalid data and also leads to substantial time and effort in auditing or verifying the data contained within. In order for organizations to ensure that the spreadsheet formulas are accurate, each



critical formula must be painstakingly validated (tested) when it is first produced. Then from that point on, changes to the spreadsheet are strictly controlled with the goal of preventing errors from being introduced. Without such change controls in place, the organization cannot be sure of its reporting.

c. Using manual methods for change control and versioning of spreadsheets is a very labor intensive process and no matter how careful one might be, it is subject to error. What if the last version was saved in a different directory? What if a prior version was opened and resaved, providing a last modified date more recent than the current version?

Recommendation

One option for organizations that don't utilize any change control today is to identify which spreadsheets handle critical business functions, and then implement controls to ensure their integrity and accuracy, and especially to prevent fraud. Apply standard change management controls to spreadsheets, including sign-offs, a record of all changes and the rationale for every change, plus rollback capabilities. Each spreadsheet's business logic must also be thoroughly vetted, as with any application which handles complex business functions. Once the spreadsheets are validated then they can be retained in a document management system.

Another option is the use of a fully

automated change management tool to provide facilitated collaboration and sharing through automatic versions, change notification and alerts, workflow / task management, and document format conversion. This should also provide a traceable audit trail in which all events and actions in the system are captured in a time-stamped, tamper-proof audit trail. One such tool is Brainloop's document compliance platform, which also provides for secure central management, encapsulating user administration to prevent the administrator from viewing user data, access-controlled administration console and use of digital rights management.

4. How does your company lock down audit trails of accesses and changes to documents?

a. Microsoft SharePoint or similar tool manages access rights and maintains audit log of accesses and file changes. Operations management reports are reviewed regularly.

b. We don't track access to or changes at the file level.

Analysis

a. Although document management systems such as Documentum, Opentext LiveLink or Microsoft SharePoint have the capability to manage access rights (ACL's) at the file level, third-party add-ons or software are required for reporting or to ensure non-repudiation of documents.

b. Knowing who has access and what access they have to which files is critical to understand whether the file data, formulas or information have been changed or are the current version. Who has access to change or "improve" an Excel formula? Do only the right people have this access? Access at the folder level does not provide this security. When a file is changed, what was changed, by whom and when? This information is retained in an audit log but this has to be separately set up. Not knowing who has access to what files and an audit trail of what was done does not allow the organization to ensure that the data is correct, leading to increased costs to manually verify the file information over and over again.



Recommendation

Monitoring who has access, what access level they have, and documenting whether changes have been made clearly includes keeping a record of who has viewed, sent or changed a document and when the action took place. All events and actions in the system should be captured with a digital fingerprint in a time-stamped, tamper-proof audit trail, including all events on the application, directory and object levels. Access to audit trail information should be controllable via the permission system. Creating and securing audit logs are two separate activities and not all tools provide the same level of security, which can be an issue if documents are to be shared externally. Companies should evaluate their planned distribution of sensitive documents, and use a tool that's

designed to capture an audit trail for externally-shared documents when appropriate.

PERSONALLY IDENTIFIABLE INFORMATION**5. How does your company manage the degree to which individuals can access personally identifiable information (PII) and other sensitive information such as customer records, payment information, employee 401(k) information and payroll data?**

a. We use a company-wide policy of least required privilege, implemented automatically to ensure that individuals have only the level of access they require. This may include read-only access, as well as restrictions on printing, forwarding, downloading or saving (skip to next question).

b. We use rights management protection for some documents as requested by the business units.

c. Sensitive documents are protected by read-only access, combined with ongoing training on safe information practices.

d. In-house portal like SharePoint, an intranet, or file servers.

e. We don't have the capability to restrict access at the document level.

Analysis

b. Rights management is a good option but it needs to be driven by a central policy and consistently implemented to

ensure full protection. When individual document owners must actively decide who should be able to access each document, the result is unevenly and inadequately applied PII security.

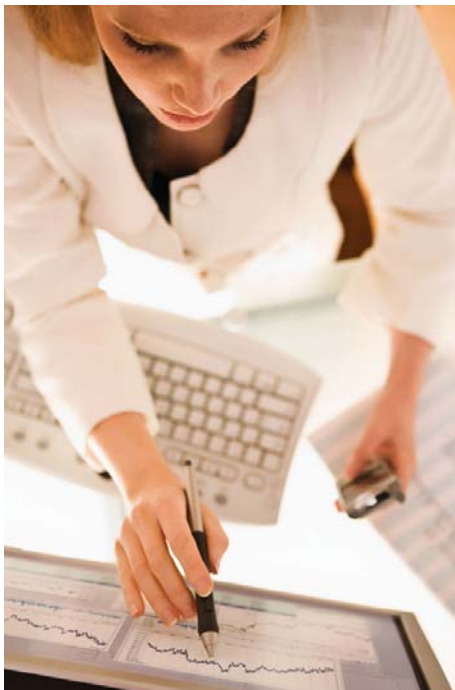
c. Even the best training programs can't prevent every instance of user error. Time-strapped users will do whatever it takes to get their work done, including sending unsecured email attachments and sharing PII more broadly than necessary. Regardless of whether documents are secured with read-only access, they can be saved under another name, emailed or printed and shared. Although read-only access is a step in the right direction for securing access, we are required by law to go further.

d. Although these options are easy and convenient, they fail to address collaboration outside the firewall. Even when used within the corporate network, you need to consider whether documents can be easily classified and access rights consistently granted at levels supporting a policy of least required privilege.

e. Restricting access at the server or directory level doesn't allow for any type of safe document sharing. Without the ability to share documents with colleagues inside and outside the corporate network, a company can't reap the benefits of collaboration that the competitive environment demands.

Recommendation

Despite the challenges that make email, VPN, file shares and in-house portals



unsatisfactory, organizations are going to share sensitive documents whether they have a safe platform to do so or not. That being said, it is critical that appropriate options are provided to allow users and organizations to perform their jobs.

b. Rights management needs to be driven by a central policy for the access and distribution of sensitive information and needs to be consistently implemented across all sensitive information with a single application. Rights management will effectively protect documents from unauthorized forwarding, saving or printing, but may be time-consuming for IT to implement, so there is a risk that it won't be used in all appropriate cases unless the company has an efficient way to allow business users to automatically apply the appropriate level of protection to documents for each type of recipient. A secure work space that enforces centrally defined policies while allowing business users to easily apply rights management when appropriate is an ideal solution.

c. Although training and awareness are key to safeguarding information, they can be time-consuming, expensive and not as thorough as an automated solution to prevent unsafe document handling. Training should be paired with an automated solution as described above, and not relied on as the primary control.

d. & e. A secure online work space will allow your company to share files outside the corporate network while

maintaining central control over the access levels applied to each document.

APPLICABLE TO ALL

6. How is confidential information such as PII, HIPAA, corporate strategy and financial information protected from access by IT staff or other administrators?

a. All confidential documents are encrypted on the server to protect them from access by the administrator. The keys are distributed so that only document owners are able to access documents or grant access to other individuals (skip to next question).

b. System and database configuration settings and segregation of duties restrict all access to confidential or sensitive data. (Skip to next question).

c. Confidential information is protected by NDA.

d. Administrators have full access to confidential information although password access is required.

Analysis

c. & d. The risk of accidental or intentional disclosure by current or former employees increases with the number of people who have access to sensitive information and / or the password to the data. Additionally, in the event of data leakage, all individuals with access must be viewed as potential sources of the leak, increasing the cost and complexity of investigation, and imposing a burden of suspicion on an unnecessary number of people.

Recommendation

Implement secure central management where encapsulated user administration prevents the administrator from accessing and viewing confidential data. Prevent unauthorized viewing of data through operator shielding which prevents the IT staff from viewing the contents of data. This involves encrypting stored data to prevent



EVEN THE BEST TRAINING PROGRAMS CAN'T PREVENT EVERY INSTANCE OF USER ERROR. TIME-STRAPPED USERS WILL DO WHATEVER IT TAKES TO GET THEIR WORK DONE, INCLUDING SENDING UNSECURED EMAIL ATTACHMENTS AND SHARING PII MORE BROADLY THAN NECESSARY.



unauthorized access by any individual, either internal or external. At a minimum, documents should be encrypted with 256-bit key based on the Advanced Encryption Standard. Key management should also be shielded from systems operations and administrative personnel.

Administrators must be able to monitor and manage the availability of the server and back up and restore data, but they should not be able to access encrypted confidential documents or the encryption keys.

Keep in mind that encryption secures data at rest and if the data is to be transmitted, secure transport options also need to be implemented.

7. How does your company control services, such as file sharing, that are used for external collaboration?

a. We have a single secure document sharing and collaboration platform with processes and document access privileges addressed in corporate compliance policy (skip to next question).

b. Our employees use secure document sharing platforms as needed. These are vetted for IT security and network compatibility but not addressed in a unified compliance policy.

c. Business users choose their own collaboration tools independently.

Analysis

b. Organizations cannot remain competitive without collaboration.

Sharing documents with external parties is inherently risky, yet in order for an organization to succeed, business cannot be conducted without exchanging information. Multiple secure document sharing platforms will protect information against intentional or accidental disclosure so long as access rights have been implemented correctly. However, use of multiple document stores will impede document discovery for litigation and audit support. Meeting subpoena and other deadlines may be difficult. IT support of multiple tools will create additional costs for the organization as well.

c. In addition to the document discovery risks stated above in b, tools chosen by business users may fail to meet corporate compliance and security requirements.

Recommendation

b. & c. Sensitive documents travel beyond the corporate firewall and it is critical that they remain accessible yet secure so organizations avoid compliance and data security breaches, corporate risk and exposure. Industry best practices favor a single secure collaboration platform to protect all sensitive documents that are used outside the enterprise, thus streamlining externally-imposed regulatory compliance.

A central document repository allows employees to share a single set of documents, facilitating eDiscovery and eliminating the need for multiple versions distributed among members.



ORGANIZATIONS CANNOT REMAIN COMPETITIVE WITHOUT COLLABORATION. SHARING DOCUMENTS WITH EXTERNAL PARTIES IS INHERENTLY RISKY, YET IN ORDER FOR AN ORGANIZATION TO SUCCEED, BUSINESS CANNOT BE CONDUCTED WITHOUT EXCHANGING INFORMATION.



8. How does your company address different levels of security required for specific types of information?

a. We have a policy that defines the types of information, the security classification of each type, requirements for handling each classification, and a mechanism that allows document owners to specify and automatically manage the appropriate security controls (skip to next question).

b. We have a policy regarding security requirements for each type of information, but compliance with the policy is managed by individual employees.

c. The business units determine the security level for documents they are responsible for.

d. We don't have a corporate data classification policy and we don't manage security at the data level.

Analysis

b. Having a formalized data classification policy in place is the first step in securing data and providing guidance on the appropriate level of security to the organization. Leaving compliance to data classification policies up to individual users is a subjective task and can be prone to error. Extensive training and annual re-training is required and even with this, errors will be made. As is the case with access control, training is crucial to ensuring the appropriate level of security for different types of documents. But because it is costly and doesn't guarantee consistent implementation,

training should be paired with an automated solution and not relied on as the primary control.

c. Different types of information require different levels of security. Some, for example, should be stored in the digital equivalent of a safe, whereas others require only a filing cabinet. By centrally defining security categories and providing a tool that automates their implementation and management, companies avoid the risk of providing some documents with inadequate security and the cost of providing others with too much security.

d. In addition to the above, the organization should first develop a data classification policy that identifies the key information assets of the organization and determines the appropriate category that each information asset should be placed in. For example: public, internal use only, sensitive, confidential, top secret. Second, determine the appropriate technology solution to automate the policy.



Recommendation

Organizations need to have in place a data classification policy that identifies the key information assets and determines the appropriate level of security for each of them. This policy must be communicated to the organization and be supported by an automated solution to ensure that it is consistently applied and easy to administer. Technology options should take into consideration ease of determining which classification applies to any single asset, and the ability to automatically apply a pre-defined set of protections to each document according to its security classification.

9. How does your company track receipt and ensure non-repudiation of documents sent to individuals outside the company?

a. Documents reside on a secure server where each access can be captured with a digital signature in an audit trail. Document integrity is verified using fingerprints to identify the active version at the time of access (skip to next question).

b. User tools such as email receipt and "protect document" option are used when sending documents outside of the organization.

c. Documents are password protected allowing only authorized users to access and / or change the content.

d. Verbal or email confirmation.



Analysis

b. Email receipt is a good option if used, but it can be ignored. So the absence of a receipt cannot prove that the email wasn't received, opened or read. The document protection feature built into business applications can help prevent unintentional editing, but document integrity cannot be guaranteed without a method, such as digital fingerprinting, to detect document changes.

c. Password protecting documents that will be shared is a convenient, but low-security way to control access to the documents. It is important to realize that password protection can be circumvented, particularly in cases where access is not protected by a second authentication factor, such as a one-time use PIN. You can also protect the document as read-only but the user can potentially make changes and save the information under another file name. The original is safeguarded but the data can still be shared.

d. Even the most conscientious employees can introduce serious breaches of security policy. People are human and confirming document access without using an audit trail or log means relying on memory, sorting through email messages, or other unstructured methods.

Recommendation

Electronic documents should be non-repudiable through documented access using a tamper-proof audit trail and time-stamps. Document fingerprints should be used to identify the version that was live at the time of the

documented access.

10. How does your company ensure that only authorized users can save, print, forward or change documents?

a. Documents are not allowed to leave the corporate network, they remain behind the firewall where they stay under direct control.

b. Documents are shared outside the company through a collaboration portal or password protected FTP site. Rights are set and managed through a collaboration tool.

c. Sensitive and confidential documents are not shared electronically; they are required to be shipped by overnight express. All hard copy documents retain a company watermark.

Analysis

In order to effectively communicate, organizations must allow sensitive documents to travel outside the firewall where they are no longer under the organization's direct control. Hard disk encryption only secures inactive documents, while email encryption is limited to data in transmission. This is not good enough for PCI, PII and HIPAA compliance purposes because the documents are no longer protected once they arrive at the desktop. Also, hard disk encryption cannot accurately record every document access and often requires the installation of client software.

b. In-house portals are relatively easy to establish and convenient, but such solutions fail to address collaboration



outside the firewall. Online collaborative space addresses this issue, is broadly available and inexpensive but typically unsecure and may create a false sense of security that contributes to even more risk. Password protected FTP sites are simple to set up but lack the convenience of workflow for document management and audit trails. None of these solutions address the problem of securing documents after they have been downloaded to the user's local PC; once out of the collaboration platform, you have no ability to prevent a user from forwarding, saving, printing or changing a document.

c. Shipping hard copies or physical media exposes your company to the risks of accidental loss or delivery to the wrong person or organization. As with electronic documents on unsecured collaboration platforms, once the files are out of your hands, there's no way to prevent unauthorized forwarding, printing, saving or editing. Distribution of hard copy materials, even with watermarks, provides little to no control over reproduction and distribution of sensitive material.



Recommendation

Rights management services (RMS) from Microsoft and Adobe provide end-to-end document encryption and are suitable for enterprise wide deployment, but they keep key management in the hands of IT, who then have access to the data. An ideal solution is to use a secure online workspace integrated with Microsoft RMS or Adobe LiveCycle RM. The online work space controls access to the documents within the document repository, and documents are protected after download by the rights management service. With this configuration, the RMS can be managed by the document owners, thus preventing IT from accessing the

information. The online work space security architecture ensures that only authorized employees are able to view or modify the documents, and versioning and an integrated audit trail inform users of changes to the materials and allow them to roll back to a previous version if necessary.



EVEN THE MOST CONSCIENTIOUS EMPLOYEES CAN INTRODUCE SERIOUS BREACHES OF SECURITY POLICY. PEOPLE ARE HUMAN AND CONFIRMING DOCUMENT ACCESS WITHOUT USING AN AUDIT TRAIL OR LOG MEANS RELYING ON MEMORY, SORTING THROUGH EMAIL MESSAGES, OR OTHER UNSTRUCTURED METHODS.



About the author

Cheryl Klein, CPA, CISA, CITP, is a governance, risk and compliance consultant and founder of GRC Consulting Services (<http://GRC-Consultingservices.com/>), a provider of IT compliance consulting services.

GRC Consulting Services specializes in IT Governance, Risk Assessment, audit and regulatory compliance with specific focus on NCUA, FDIC, FFIEC, GLBA, Sarbanes Oxley (SOX), Payment Card Industry (PCI), Personally Identifiable Information laws (PII) and Health Insurance Portability and Accountability Act (HIPAA) regulations.

About Brainloop

Brainloop provides a highly secure online work space that helps companies mitigate information risk, meet compliance objectives and increase process efficiencies when sharing confidential documents inside and outside the enterprise. Major organizations that use it include BMW, Deloitte, Eurocopter, Fujitsu Siemens, T-Mobile, and Zurich Financial Services.

Brainloop's secure online work space acts as a virtual safe where sensitive documents reside and can be viewed and edited by authorized users, whether inside or outside the network. The application protects documents against unauthorized access, forwarding, saving or printing, and provides a tamper-proof audit trail that ensures that every activity is recorded and traceable. Automatic versioning, change notification and alerts, workflow / task management and document format conversion support collaboration and process efficiency, thus promoting user acceptance.

**CONTACT**

Brainloop, with offices in Boston and Munich, is the leading provider of Document Compliance Management solutions that enable customers to share confidential documents in a highly secure and traceable environment.

Europe

Brainloop AG
 Franziskanerstr. 14
 81669 München · Germany
 T: +49 (89) 444 699 0
 info@brainloop.de
 www.brainloop.de

USA

Brainloop Inc.
 One Broadway, 14th floor
 Cambridge, MA 02142 · USA
 T: +1 (800) 517 3171
 info@brainloop.com
 www.brainloop.com

