FROST & SULLIVAN

GETTING STARTED WITH COMPLIANCE

A Frost & Sullivan White Paper

Sponsored by Google

"We Accelerate Growth"

TABLE OF CONTENTS

INTRODUCTION

The best way to stay clear of regulatory fines, lawsuits, and other penalties related to your company's electronic data is to create and consistently enforce a comprehensive set of data security, email retention, and web access polices. For most organizations, however, this is not an easy task. In fact, just figuring out where to start can be a tumultuous experience. Many compliance projects never get off the ground because IT personnel become paralyzed while educating themselves about relevant regulations and requirements. This period of getting up to speed prevents compliance systems from getting implemented in a timely manner.

Fears of substantial penalties from regulators along with internal risk mitigation efforts are driving the need to establish and enforce applicable compliance policies. As an IT manager, waiting to get started until you have it all figured out is not an option. Nevertheless, going into compliance projects blindly can turn seemingly small compliance projects into complex labyrinths, and leave managers with no means by which to measure progress or results.

So what is an IT manager to do? There are some basic actions an organization can take immediately to get started down the right path. This paper will cover some starting tips for communications security, message retention, and web security compliance. It will also present some factors to consider when selecting compliance solutions that are right for most organizations to help minimize initial investment risks and maximize flexibility. Once an organization gets started down the compliance path, projects will gain momentum in parallel with research efforts and it will become possible to demonstrate tangible progress and milestones to both auditors and management.

GETTING STARTED

Compliance is not about a one-time audit or reaching a single milestone, it is an ongoing effort with multiple phases. Becoming fully compliant can be a long process. It involves the creation and enforcement of policies, documented procedures, and the collection of data that can be measured and audited. Ideally, an organization will get to a state where most compliance efforts are automated.

A common concern for many IT managers is the possibility of being forced to start compliance initiatives over if they are not done exactly right the first time. Additional concerns revolve around the initial investment that will be required to get started – and whether the technology purchased today will be obsolete by the time the organization figures out how to implement it across different departments and divisions.

The fact is that many IT managers have the same concerns about purchasing systems that may not scale appropriately or have the flexibility to change if their compliance requirements change. These are all very real and common concerns, but the challenge is not impossible to surmount.

Given the need to balance thoughtful planning with getting started quickly, IT managers should begin by focusing on essential policies and systems they can rapidly implement that will provide the organization with the compliance basics. These basics are likely to align with long term regulatory and governance objectives for the enterprise and can help it steer clear of problems with regulatory, criminal, and civil action in the short term and give IT managers additional time to establish more comprehensive compliance requirements.

These basics are referred to as the "building blocks" for corporate compliance and are foundation-level policies and practices that address immediate requirements and will put an organization in a good position to implement and fine tune additional compliance policies moving forward. They are easily implemented and enforced and will help a business get its compliance projects underway.

Email Content Security

Email content security is extremely important. Much of the sensitive information for a business is shared via email. Email can be a source of sensitive data leakage including customer data records, credit card data, or personally identifiable information. This type of data is subject to privacy regulation and therefore must be protected. In addition, it is good business practice to protect sensitive data, regardless of whether it is subject to regulation because it is in the best interest of the company to protect.

Frost & Sullivan research has found that many organizations are subject to at least one industry or government regulation to protect data. The Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and various other data and privacy protection regulations require an enterprise to secure sensitive inbound and outbound data communications.

Most content security regulations do not actually specify details about what type of security is required (encryption algorithms, strength of encryption, authentication requirements, etc); however, when designing compliance policies, each organization should consider the "spirit" of the regulation. That requires a business to ask itself questions such as:

- Is the compliance approach in use or under consideration in alignment with the goal of the regulation?
- Does company policy provide an industry accepted best practice to secure sensitive customer information?

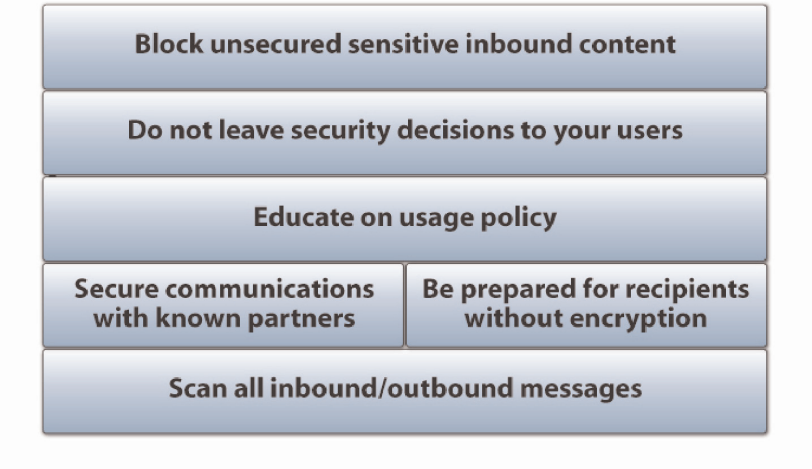
These are the types of considerations IT managers should keep in mind when implementing an email content security and compliance strategy.

In organizations that have already implemented an anti-spam and anti-virus solution, additional problems such as phishing and malware threats should be addressed while simultaneously reducing the amount of email to archive and increasing the scalability of existing email systems.

Some building blocks that can used to expand beyond basic filtering and address basic requirements for compliance are listed below.

Policy Building Blocks for Email Content Security

Policy Building Blocks for Email Content Security



1. **Scanning all messages –** Best practices dictate that an enterprise should ensure the scanning and filtering of messages for both inbound and outbound messages. Outbound message scanning is a very important component of corporate compliance efforts, so using a solution that can scan outbound messages will help an IT manager implement the proper policy building blocks. If an existing solution cannot scan outbound messages, it is time to consider replacing it with a solution that can.

2. **Secure email communications** – If there are a handful of partners that an enterprise regularly communicates with, encrypting the connection between the email servers using TLS is a practice that should be in place. For example, when a health care provider has several insurance companies that it communicates with on a regular basis, it is very easy to ensure the communications are always encrypted by policy.

3. **Secure email for recipients without encryption** – When an enterprise needs to send sensitive data to an infrequent business partner, there are several ways to do this using a simple message encryption solution. Google Message Encryption, powered by Postini, for example, enables an organization to send messages to a secure portal where the recipient can securely download the message using a browser without any additional software requirements.

4. **Education –** As with most corporate policies, it is a good practice to educate staff on corporate messaging policies and why they are in place. Remember, compliance is an ongoing process and the enterprise will need the help of everyone to make it work.

5. **Don't let individual users make security decisions** – Ideally, a content security system will enable IT managers to set policy and have it automatically and consistently enforced. Although employees may have good intentions, relying on them to consistently make security decisions on what should be secured is not practical. As a result, content security solutions should be able to automatically block or encrypt sensitive data, such as customer account data or records, credit card information, social security numbers, or other sensitive content such as product code names or company confidential content.

6. **Blocking unsecured sensitive inbound content –** When an unsecured email is sent to an organization with sensitive information included in it, the ability to block that unencrypted inbound content can be very important to corporate compliance efforts. For example, the retail and financial services industries are subject to PCI DSS requirements and do not want to accept any email that may contain regulated PCI data such as credit card numbers. In order to comply with PCI DSS requirements, IT managers must be able to assert control over the type of data that enters the network via email. The ability to inspect the data and block it before it enters an organization's network and is accepted by its email servers can significantly reduce the risk of compliance violations.

Web Security

Enforcing acceptable policies for corporate web usage can significantly reduce a company's risk of both criminal and civil penalties. Inappropriate web usage by employees can also subject a company to web borne threats that not only can be expensive to remedy but also exhaust IT budget. Implementing a web filtering and scanning solution can help a company quickly address concerns about web security and compliance.

Policy Building Blocks for Web Security

Policy Building Blocks for Web Security

Frost & Sullivan

1. **Web filtering and malware scanning –** Starting with a basic web security and filtering solution an enterprise can easily reduce most of the web content that could create liability risk. In general terms, content that should be filtered includes porn, gambling, hate, weapons, and hacking sites (filtering decisions should be based on legitimate needs of business users, i.e., gun manufacturers or emergency room physicians may have a legitimate need to access content discussing handguns). Malware and spyware protection will also help reduce risk of systems being compromised and doing things that could be regulatory violations.

2. **Web monitoring –** Any web security solution under consideration should include web monitoring capabilities. Whether an organization chooses to actively monitor web usage should be based on corporate culture and policy. Regardless of current policies, however, there could come a time when web monitoring is needed, therefore the solution an organization chooses should support it.

3. **Usage enforcement –** These policies are the easiest to implement, do not require user name resolution and are equitable since they apply to all users. Once the IT manager has policies in place for the organization, it is possible gather use data for several weeks. This provides a method of determining if rules should be adjusted for groups of users, categories visited, use times, bandwidth consumption, etc.

4. **HR and legal team inclusion** – Be sure to include the HR and legal teams when implementing filtering and monitoring policies so they can provide guidance on acceptable systems usage as well as communicate and enforce acceptable web usage policies to employees. It is important to ensure that employees understand they are using business infrastructure and that the company is responsible for all inappropriate usage of its systems. These measures help an enterprise to demonstrate good faith efforts aimed at reducing harassment or hostile workplace environments as well as protecting the systems from web-based threats. Preventing access to file sharing sites and downloading of copyrighted material such as music or other media should be part of these efforts since the company is responsible for the actions of its employees.

5. **Policy reviews** – Finally, plan and document regular reviews of the web security policies for the organization. This can be done quarterly, yearly, or as frequent as the IT manager and legal department feels is appropriate, but it must be a consistent process. Use the web monitoring reports to help fine tune existing policies and establish new ones if needed. Compliance is an on-going process and policy reviews are a critical.

Compliance is an ongoing process, thus, regular reviews of usage reports and periodic updated to policies based on recent data is a good practice to follow.

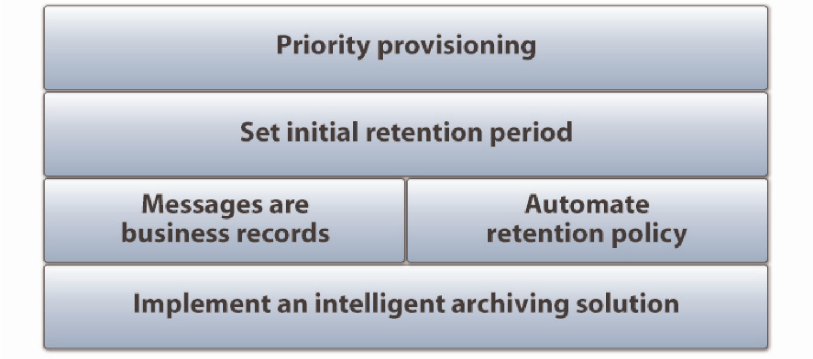
Message Retention and eDiscovery

Retention of email is usually a critical part of compliance efforts at countless organizations in the private and public sectors. There are multiple drivers behind email retention including regulations such as SOX, the Federal Rules of Civil Procedure (FRCP), and several SEC mandates that require messages be retained for several years. In addition, for court cases where there is a need for litigation holds, companies are required to preserve relevant data and make it readily accessible upon request, even if a retention period is about to expire.

Failure to properly retain and produce required email has cost companies millions of dollars in fines as well as lost court cases. However, an IT manager won't always know what email to keep and for how long due to complex regulations or instances where an enterprise is subject to more than one message retention regulation. As IT professionals know, however, keeping all messages received and sent on email servers is not a viable solution. Email servers, such as MS Exchange or Lotus Notes, were not designed for long term message retention or search capabilities, therefore relying on these to do so is not practical.

Policy Building Blocks for Message Retention and eDiscovery

Policy Building Blocks for Message Retention and eDiscovery



1. **Implementing an intelligent message archiving solution** – A solution implemented by an organization should have robust search capabilities and records should be stored in an accessible format that can be produced on-demand. Once the messages are offloaded from email servers to an archiving solution, IT managers will have more flexibility to apply organization policies at a later date. Any solution under consideration must support litigation hold requests. IT managers that implement an archiving solution with a litigation hold feature will simplify the eDiscovery process if the enterprise is ever involved in litigation or a regulatory investigation. A side benefit of offloading messages from email servers is that it significantly improves inbox quota management as well.

2. **Messages are business records** – All email messages should be treated as important business records. This means that any retention solution under consideration should be able to organize and store messages as though they were like other important business records in the organization.

3. **Automating retention policy** – Leaving decisions to users about which emails to keep or delete and when they should do it could come back to haunt a company if its retention policy is scrutinized by the courts or regulatory agencies. Although a company may have a written policy, business users may not always adhere to it, which can be as bad or worse as no policy at all. Automatic message retention for all inbound and outbound email is considered the best way to avoid legal liability.

4. **Setting retention periods –** An IT manager may not initially know how long to retain messages because in different industries or departments messages may need to be kept for three, five, or seven years – it really depends on the business and what regulations it is subject to. When an IT manager is unsure, it's best to establish an initial retention period of one year. This will provide the IT and legal departments with enough time to determine exactly what retention requirements the organization should follow.

5. **Priority provisioning** – When implementing an archiving solution, an organization may want to roll it out in phases. If this occurs, priority provisioning should be considered to ensure the most important needs are addressed first such as HR, legal, and finance departments.

Additional Considerations for Archiving and Retention Efforts

- Select an archiving solution that is easily searched and can provide on-demand access to message archives when needed. Failure to produce relevant email during the eDiscovery process for a lawsuit has been proven to be extremely damaging to defendants, some of whom have subject to millions of dollars in fines and punitive damages.

- Communicate to employees that corporate email is meant to be used for business-related activities and should not be used for personal reasons.

- Select a solution that enables messaging supervision for employees in departments or functions that may be involved in a policy violations or a lawsuit.

ARE WE COMPLIANT YET?

Ultimately in the event of an audit or lawsuit, it is the courts and regulators that must decide if an organization has met regulatory requirements for compliance. In situations where organizations are sanctioned for non-compliance, it is typically because an industry best practice was not implemented or properly adhered to. Failure to implement even the

most basic of controls, such as the building blocks previously discussed, could leave an organization at significant risk for liability in the event of an actual or alleged regulatory violation. IT managers should be ready to defend the compliance strategy of the organization they serve in the event that retention practices are questioned.

ASSESSING THE SOLUTIONS

When considering compliance solutions it is important for IT managers to remember that point solutions are not always the best option. Although a point solution may offer a best of breed solution for a single component of an overall project, managing a collection of point products tends to be more expensive and complex than using a single converged solution. The ease of use and management of converged solutions typically outweigh the advantages of point products. Most important of all is the ability of a solution to be flexible and scalable, something that point solutions cannot accomplish to the same extent as a converged solution.

Since bringing a messaging and web security solution in-house can be a considerable expense for most IT departments, most organizations are finding that outsourcing these needs to a third-party vendor is a sound business decision. This is due to the fact that outsourcing partners have the ability to achieve economies of scale that most companies will never be able to match in the messaging and web security compliance area.

ABOUT GOOGLE APPS SECURITY AND COMPLIANCE PRODUCTS

Google security and compliance products, powered by Postini, are available to businesses and organizations that want to make existing email and web infrastructures more secure, compliant, and productive. The message security products protect organizations from spam and messaging threats. The compliance products enable content-based policy enforcement, message archive and discovery features, secure web browsing, as well as encryption for sensitive email. All of these products leverage the "cloud computing" power of Google. As a result, there is never anything to install or maintain on-site. Organization can start small and implement additional services as requirements grow.

Google Message Encryption, powered by Postini, provides message encryption for organizations to securely communicate with business partners and customers according to security policy or on an "as needed" basis. Without the complexity and costs associated with legacy on-premises encryption technologies, Google Message Encryption makes encrypting email messages easy and affordable. The policy-based solution enables automatic encryption to any recipient based on message content or user initiated triggers.

Google Web Security for Enterprise, powered by Postini, blocks malware threats and unwanted content before they reach the network, helping to optimize both bandwidth and

user productivity. Because the solution is available using cloud computing, it eliminates the burdens of purchasing, maintaining and updating security infrastructure on-premise, freeing IT teams to focus on business critical projects.

Google message archiving, included in the Google Message Discovery, powered by Postini, , is a cost-effective, easy-to-deploy archiving solution that helps businesses implement data retention strategies for compliance and rapid e-discovery. The product captures and indexes all inbound and outbound messages into a centralized repository, enabling local mail servers to be optimized without sacrificing data. The solution is complete with flexible retention policies, role-based access controls, and extensive reporting capabilities.

Together, these products help businesses to be more secure, compliant, and productive using their existing messaging systems. They help to rapidly address some of complex compliance challenges with simple, easy to use, cloud-computing based products from Google. For more information, visit www.google.com/a/security.

CONTACT US

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Consulting Company, partners with clients to accelerate their growth. The company's Growth Partnership Services, Growth Consulting and Career Best Practices empower clients to create a growth focused culture that generates, evaluates and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 30 offices on six continents. For more information about Frost & Sullivan's Growth Partnerships, visit http://www.frost.com.