IRON MOUNTAIN®

LEVERAGING INFORMATION SECURITY STANDARDS IN LAW FIRMS: THE INCREASING POPULARITY OF ISO 27001 IN THE LEGAL INDUSTRY

2016 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

EXECUTIVE SUMMARY

As reports of data breaches, cybersecurity attacks and hacking continue to rise across the globe, many organizations (especially those in heavily regulated industries such as financial services and healthcare) are more closely reviewing how their data is managed, protected and stored – both internally and externally with third party vendors. Because law firms are in possession of highly confidential client data, they are identified by many – including the FBI — as prime targets for security incidents. Verizon's General Counsel Craig Silliman asserted his belief in their recently published 2015 Data Breach Investigations Report that law firms are prime targets for hackers, stating "Law firms hold a lot of sensitive documents about their clients. They are not just potential, but likely, targets for those looking to find sensitive information. We think it's very important that law firms look at the threat environment and make sure their systems are up to standard." (Edwards, 2016)

Clients from multiple industries are examining how their outside counsel protects information across their enterprise – not just within their technology, but also through their policies, procedures and the actions of their employees. As firms continue to be subject to security questionnaires and onsite audits, more consideration is being given (both by the client and by the law firm) to obtaining ISO 27001 certification as a means to validate their security profile. As an added benefit, some law firms leverage ISO 27001 certification as a competitive advantage. As of March, 2016, ILTA identified 30 firms (60 percent being AmLaw 100 firms) that are ISO 27001 certified and 55 more working towards or investigating certification. (Costello, 2016) Another survey performed in 2015 reflects that of the Global 100 firms, 30 firms reported ISO 27001 certification, 17 are actively pursuing certification during 2016 and 39 are investigating the process.

Set of standards to help organizations better secure information assets. ISO 27001 provides requirements for an information security management system (ISMS).

While certification is an increasing trend in law firms, such a decision is not being taken lightly, and certainly some are choosing not to become ISO 27001 certified. ISO 27001 certification can be a costly initiative to undertake and one that requires the attention and time of many individuals within the firm. Additionally, it can be challenging for a firm to measure the benefit of being certified, as not all clients demand the same level of security controls. It is also difficult to determine, at present, whether having ISO certification is a competitive advantage for a law firm over a firm that is not certified but has a very credible security program.

This paper defines ISO 27001 certification, illustrates various approaches to achieve certification, describes benefits and challenges with the certification process and identifies the direct linkage between ISO 27001 and Information Governance (IG) as a discipline. Information security must be a top priority whether or not a firm decides to pursue ISO certification. While ISO certification is not the only means to protect client and firm information, it is an approach worthy of very strong consideration.

SYMPOSIUM STEERING COMMITTEE

BRIANNE AUL, CRM
Firmwide Records
Senior Manager
Reed Smith LLP

BRIAN DONATO
CIO
Vorys, Sater, Seymour
and Pease LLP

LEIGH ISAACS, IGP, CIP
Director, Records &
Information Governance
White & Case LLP

RUDY MOLIERE
Director of Information
Governance
Morgan, Lewis & Bockius LLP

CHARLENE WACENSKE
Senior Manager Records and
Information Governance
Morrison & Foerster LLP

LEVERAGING INFORMATION SECURITY STANDARDS IN LAW FIRMS TASK FORCE

ANGELA AKPAPUNAM, IGP
Director, Information Governance
and Records
WilmerHale

BRIANNE AUL, CRM
Firmwide Records Senior
Manager
Reed Smith LLP

SCOTT CHRISTENSEN
Senior Associate
Olenick & Associates

BRIAN DONATO
CIO
Vorys, Sater, Seymour
and Pease
LLP

SAMANTHA LOFTON
Chief Risk and Information
Governance Officer
Ice Miller LLP

LISA MARKEY
Director, Information Security
Shearman and Sterling LLP

RANDY OPPENBORN*
Director, Information Governance
Foley & Lardner LLP

**Task Force Leader*

IRON MOUNTAIN WOULD LIKE TO THANK THE FOLLOWING INDIVIDUALS FOR PARTICIPATING IN THE PEER REVIEW SESSIONS OF THE 2016 SYMPOSIUM EVENT AND FOR SHARING THEIR PERSPECTIVES AND EXPERTISE DURING THE CREATION OF THIS TASK FORCE REPORT.

ANGELA AKPAPUNAM, IGP
Director, Information Governance and Records
WilmerHale

KAREN ALLEN
Manager, IG Technology
Morgan, Lewis & Bockius LLP

DERICK ARTHUR
Firmwide IG Operations Manager
Cooley LLP

BRIANNE AUL
Firmwide Records Senior Manager
Reed Smith LLP

MAUREEN BABCOCK
IT Business Operations Manager
Snell & Wilmer LLP

BRYN BOWEN
Director of Information Services
Schulte Roth & Zabel LLP

SCOTT CHRISTENSEN
Senior Associate
Olenick & Associates

TERRENCE COAN
Senior Director
HBR Consulting

GALINA DATSKOVSKY
CEO
Vaporstream, Inc.

BRIAN DONATO
CIO
Vorys, Sater Seymour and Pease LLP

BETH FAIRCLOTH
Director of Risk Management
Seyfarth Shaw LLP

STACEY FIORILLO
Managing Director
Information Governance Consulting Group

PATRICIA FITZPATRICK
Director of Information Governance & Compliance
Katten Muchin Rosenman LLP

LEIGH ISAACS
Director of Records and Information Governance
White & Case LLP

NORMA KNUDSON
Director of Compliance Support & Space Planning
Faegre Baker Daniels LLP

SAMANTHA LOFTON
Chief Risk and Information Governance Officer
Ice Miller LLP

FARON LYONS
Director of Enterprise Sales
Zia Consulting

LISA MARKEY
Director, Information Security
Shearman and Sterling LLP

RUDY MOLIERE
Director of Information Governance
Morgan, Lewis & Bockius LLP

RANDY OPPENBORN
Director, Information Governance
Foley Lardner LLP

ALEXANDRA PROPHETE
KM Operations Manager
Cleary Gottlieb Steen & Hamilton LLP

DEBORAH ROBBINS
Records and Conflicts Coordinator
Jones Walker, LLP

SUNNY SANGHANI
Associate Director
Robert Half Legal, eDiscovery, Managed Review and Consulting Services

JILL STERBAKOV
Manager of Information Governance Compliance
Morgan, Lewis & Bockius LLP

SUE TROMBLEY
Managing Director, Thought Leadership
Iron Mountain

CHARLENE WACENSKE
Senior Manager Records and Information Governance
Morrison & Foerster LLP

ROBERT WEAVER
Director of Information Security
Blank Rome LLP

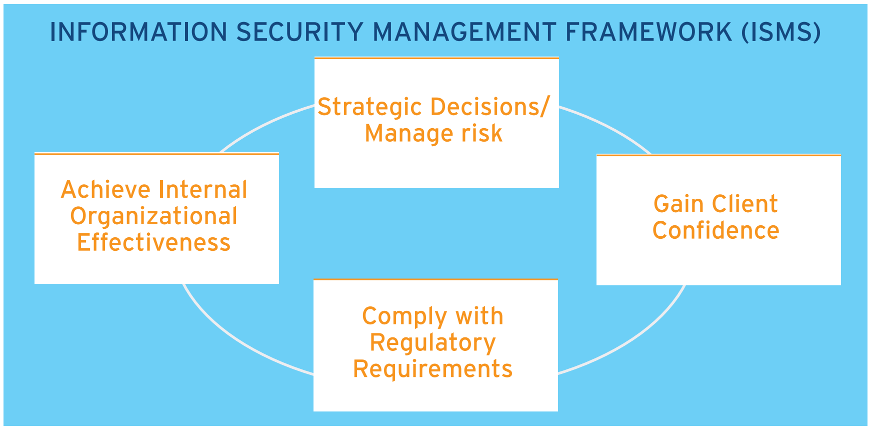
JOHAN WIDJAJA
Assistant Director Records and Information
Morgan, Lewis & Bockius LLP

JOEL WUESTHOFF
Senior Director
Robert Half Legal Consulting

INTRODUCTION

Many firms specify an individual or team dedicated to information security, and are often required to identify such a person(s) as part of a client audit. However, it is important to note that ISO 27001 addresses security in virtually all aspects of a firm: people, operations and technology, and as such, reinforces the motto that "security is everyone's responsibility." As many IG departments support a very similar motto for their own initiatives, this paper should resonate across many disciplines, including:

- Information Technology supports the firm's overall infrastructure and systems in which data is stored, accessed, exported, imported and more
- Information Security/ Operational ("Physical") Security identifies, implements and monitors cyber and physical activity which could create risks for data loss or exposure
- Information Governance and/ or Records Management ensures data is effectively identified, stored, accessed, secured, retained and disposed throughout its lifecycle
- Legal/Risk/Professional Responsibility/General Counsel identifies the firm's level of risk tolerance and the consequences the firm has faced or may face with past/ future data breaches
- Human Resources confirms personnel are background checked and educated regarding proper security controls, etc.
- Business Intake identifies which clients require stricter security controls on their data
- Marketing monitors client demand and industry trends regarding data security and its importance in outside counsel selection
- Procurement identifies resources and costs required to obtain certification as well as firm vendor's ability to comply
- Senior Management are key decision-makers and stakeholders for significant undertakings such as ISO certification


INFORMATION SECURITY MANAGEMENT FRAMEWORK (ISMS)
Strategic Decisions/ Manage risk
Achieve Internal Organizational Effectiveness
Gain Client Confidence
Comply with Regulatory Requirements

ISO 27001 CERTIFICATION

Many law firms have obtained, or are in the process of obtaining, the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) certification (referred to as ISO). ISO/IEC 27000 series standards incorporate continuous feedback and improvement activities, along with an iterative "plan-do-check-act" (PDCA) approach. ISO 27001 specifically provides an Information Security Management System (ISMS) set of standards that are high level yet applicable to all types and sizes of organizations. The ISO 27001 ISMS is one of the few security frameworks that mandate specific requirements for which an organization can be formally audited and certified compliant. Often referred to as the "Standard," ISO 27001 is both technology and vendor-neutral. The ISO ISMS includes recommendations for organizational structure, policies, planning activities, responsibilities and procedures for a structured approach to information security (Calder, 2010).

CHALLENGES AND OPPORTUNITIES TO BECOMING ISO 27001 CERTIFIED

CHALLENGES

Challenges in pursuing ISO certification include obtaining buy-in and engagement from stakeholders such as firm management, key practice groups and executive teams. This expands to engage the appropriate business partners in order to ensure a firm has the necessary support for a successful project implementation. Resources and time from key business partners become a significant challenge for any new initiative and ISO certification is no different. Attorneys may be resistant to new policies or procedures that must be implemented, especially those who do not have clients enforcing higher security measures from their law firms. In addition, staff members involved in the certification process may be overwhelmed by the corresponding time requirements, especially if they have conflicting projects and priorities. The initial investment in ISO certification requires dedicated executive and staff time, coupled with the right people to have on the internal and external consulting teams. Additionally, the firm must have a robust change management program to ensure those who are otherwise resistant or concerned about the impact thoroughly understand the intended benefit of becoming ISO 27001 certified.

A firm needs the following groups to take an active role in the ownership and success of the initiative:

Chief Operating Officer (COO)	• leads executive team support of major initiatives • owns security organization, sets roles and responsibilities • approves capital expenditures
Chief Marketing Officer (CMO)	• leads security-focused marketing efforts to clients through Request For Proposal (RFP) responses • brands security initiatives for the firm internally and externally
Chief Financial Officer (CFO)	• oversees financial support • leads analysis of claims cost and cyber-premiums
Chief Information Officer/ Chief Technology Officer (CIO/CTO) *(* CIGO/CISO functions could fall under the responsibility of the CIO/CTO. Separation of Duties in accordance with ISO should be considered.)*	• owns security tools, applications, network, help desk, IT training and access rights
General Counsel/Risk Partners	• review, approve and endorse necessary policy and procedures • sets example and endorses security awareness and compliance efforts
Chairman/Managing Partners/ Practice Group Leaders	• provides "top-down" management support of security programs, policies/procedures • requires all firm participation in security program

It should be noted that roles are dependent upon firm size and structure. Please refer to the LFIGS Report, "Evolving Role of Information Governance Professional" for additional information.

OPPORTUNITIES

For firms without current standards and governance, implementing ISMS and ISO processes will improve day-to-day business efficiencies, and the overall investment should ultimately lower operational cost. ISO 27001 creates value in that it enables a firm to measure the success of its ISMS and to manage service delivery and related risk. Other benefits of employing ISO 27001 standards are:

- provides a basis for comparison internally and externally
- focuses on securing information as an asset, as opposed to simply securing systems
- provides a roadmap which is internationally recognized and certifiable
- creates a global common language.

The risk assessment associated with ISO 27001 can help firms determine which security controls should be in place, and what exactly they are meant to protect. It allows firms to identify and close the gap between a current and desired state, monitor progress, improve its ISMS and create a repeatable process. A firm can also use ISO 27001 as a baseline to determine risks that are beyond the level of acceptability, and the probability of an occurrence.

WHERE TO BEGIN?

If a firm decides to pursue ISO 27001 certification, there are many ISO 27001 applicable options that do not require it to make a significant upfront investment. Low cost options can be an advantage, particularly for firms that are in the early stages of implementing security management or have budgetary or resource constraints. As a starting point, firms can use public resources, described below, to create an initial checklist and roadmap. The SANS Institute, Information Systems Audit and Control Association (known as ISACA), National Institute of Standards and Technology (NIST), Shared Assessments and HITRUST are some of the recommended resources, in addition to ISO, that earn notable mention and are generally applicable to law firms.

SANS INSTITUTE

Educating employees is a priority since most cyber threats are due to intentional or unintentional human action. The SANS Institute is a cross-industry, cooperative research and education exchange that shares lessons learned amongst professionals in a variety of organizations. SANS holds one of the largest collections of research and educational resources for both end-users and technical personnel.

COBIT

COBIT 4.124 and COBIT 5 (released in 2015) are internationally accepted sets of tools created by the Information Systems Audit and Control Association (ISACA.) COBIT provides a common language and methodologies that IT professionals can use to align with business objectives, deliver value and manage associated risks. COBIT's control model helps bridge the gaps between business requirements and IT governance. Within COBIT, the CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. The Controls provide a good opportunity to tackle a smaller number of actions with high payoff results. (Thompson, 2012)

NIST

The National Institute of Standards and Technology (NIST) provides a series of security guidelines for government information systems and contains guidance that can easily be applied to any organization. NIST guidelines provide several approaches, including developing security assessment plans (Publication 800-30) in all phases of the system development lifecycle. Publication 800-53A focuses on managing risks from near real-time information systems that can adversely affect operations, assets, individuals, other organizations or governmental functions. NIST assessment plans are flexible and lend emphasis on the process at every stage in the system development life cycle. A list of some of these guidelines, available online, are listed in Appendix A. (Computer Security Division: Computer Security Resource Center, 2015)

SHARED ASSESSMENTS

Shared Assessments is a member-driven organization summarizing good cyber security practices. There are a number of tools available to help an organization determine their strengths and potential gaps. The program leverages similar security controls across member organizations to better conduct security, privacy and business resiliency control assessments.

HITRUST

HIPAA-covered entities such as healthcare services providers, as well as financial services institutions, may require business associates to become certified as compliant with HITRUST's Common Security Framework (HITRUST). Results of a recent LFIGS member's survey showed that firms representing clients in these industries have implemented HITRUST in response to client requirements or as part of a hybrid security management approach. HITRUST is considered a cross-section of standards including HIPAA, HITECH, NIST, ISO and COBIT. HITECH's framework can be used by any organization managing personal health and financial information and allows healthcare industry clients to measure their business associates information security program beyond just HIPAA standards (McGee, 2015.)

Prioritizing budget and resource challenges to achieve a viable ISMS, whether through certifications or implementing defined frameworks, can seem insurmountable.   Law firms are certain of one thing: cyber threats can impact anyone and will continue to increase in frequency and sophistication. ISO 27001 processes provide the guided framework and opportunities to reduce risk and maintain client confidence. ISO 27001 certification can reduce the burden of complying with multiple security standards and client audits. The opportunity to improve a firm's overall security risk and organizational risk management outweighs the challenges.

APPROACH TO ACHIEVING ISO 27001 CERTIFICATION

REASONS FOR CERTIFICATION

Though the above security measures are approaches a firm may also take, there are multiple reasons why it may also desire to gain ISO 270001 certification. Typically, the reason drives the approach, such as client audits and RFPs. While having the certification is normally not enough to prevent an audit from occurring, the simple fact that a firm has passed the ISO audit means that they have their processes and their evidence lined up and ready to use for the audit itself. It also demonstrates clearly to an outside auditor that a standardized risk-based approach has been used and should lead to an enhanced level of confidence.

Another compelling reason is simply to ensure that a firm has covered all the bases in their security program. This does not necessarily mean that they are optimally secure, but it does mean they have addressed the key areas that lead to improved security and should have a good awareness of their gaps, which in turn leads to enhanced security. It is entirely feasible to harness the ISO program to design the firm's security program yet not pursue the actual certification. This is especially true for an organization with a less mature ISMS, or where the individuals responsible for security are on a steeper learning curve than in a fully mature security organization.

There may be a financial reason to utilize the framework. The risk assessment and gap analysis which form a major part of the certification process allows an organization to understand systems and processes of greater risk and therefore enable it to focus resources for maximum return on investment.

Global firms, specifically firms with a European presence or with European clientele, may find that the ISO 27001 certification is more readily known and accepted in regions outside of the U.S. and thus elect this approach as opposed to a more "domestic" standard.

Lastly, ISO 27001 has been recognized by several insurance carriers as the preferred model with which firms should align their security program.

DETERMINING THE SCOPE OF WHAT TO CERTIFY?

The certification scope is driven by the firm's objectives in achieving certification and the resources which are available both internally and externally. The "big bang" approach to certify the entire firm may be overwhelming and lead to a complex process that is difficult to sustain. Selecting just one critical service may be the simplest route to achieve certification, but may reduce the overall value to the organization.

Focusing on a number of key services is possibly the most strategic option. There is an "economies of scale" benefit in leveraging the work done on controls which can be applied across the services the firm has certified, e.g., physical security, user access or data center. The services to certify should relate to the business objectives and operational activities of the firm.

The following four functions are strong candidates for certification consideration because they represent areas of common use and potential security risks within a law firm environment.

Litigation Support – for firms that perform a significant amount of in-house eDiscovery work

Remote access service – for firms with attorneys who travel extensively and utilize remote access

Email systems – often the primary data exchange mechanism between attorneys and their clients

Document management system(s) – contains client and matter records

Geographical considerations should also be reviewed. Certification across jurisdictions may increase complexity considerably and may not be necessary based on the firm's objectives. Where there is large variation in the operational practices of different regional offices, it might be too great an undertaking for a firm to certify more than one jurisdiction. A more strategic approach would be to select one region to develop as a center of excellence by gaining certification, improving process, etc. This model can then be rolled out to the other regions and the scope of certification expanded to include these regions at a later date.

Appropriately scoping the certification is a critical decision. A cost/benefit analysis should be done before engaging in the process and revisited through the early stages to ensure that the right scope has been chosen for the specific organization. Factors to consider is determining scope are:

- maturity of the security function
- resource availability, both in the security team and the other key stakeholder areas
- business objectives
- geographical considerations

HOW TO GET BUY-IN AND BUILD THE TEAM

ISO certification does not happen in a vacuum within the Information Security or Information Governance team. As mentioned above, there are many teams and individuals within an organization who need to be involved, including IT, Human Resources and Compliance. There is an ongoing requirement for these teams to participate, therefore it is essential that they understand this at the start of the certification program development project. Depending upon services being certified, and the geographical scope, their level of involvement may be significant.

A firm should identify and document the core reasons and benefits for pursuing ISO certification. Successfully conveying those benefits to senior leadership and the various team members should ultimately drive participation and engagement. While it is important to explain how obtaining certification benefits the firm as whole, it is also advantageous to identify specific benefits that may resonate with various teams (e.g., leveraging certification as a way to market to clients, or the reduced risk of a potential data breach.) It can also facilitate operational efficiency by improving processes and increasing alignment with cross-functional teams.

HOW TO DEFINE REQUIRED RESOURCES

A significant certification requirement involves having the right management structure to support the program. There must be a team of identified subject matter experts (SMEs) for each area that is certified. These individuals are part of the external ISO audit and so it is crucial that they are the individuals who operate the controls on a day to day basis. They need to be able to explain quickly and clearly to the auditor how the controls work. If an individual is unable to readily direct the auditor to the evidence in support of a control then it may be reflected negatively in the firm evaluation. The key individual who manages the program, typically the senior security leader, and co-chair(s) should take responsibility for ensuring that SMEs are trained in how to handle an audit, how to respond to questions so that they answer the specific question being asked and to present the evidence in an efficient and concise manner.

A document repository should be considered to keep all certification-related information in a central location. It is essential that all of the evidence is collated in an organized fashion to provide the auditor with efficient access to information.

Another consideration is to grant appropriate auditor access to systems for testing purposes. Access should be set up and tested in advance.

There may be significant overhead in the implementation of controls and production of required evidence. When determining timelines for the project, consideration should be given to how much needs to be done based on the risks identified and the maturity of the security organization. Analysis of resource requirements should be continually reviewed and tracked against the project progress. There is a balance to achieve around the level of resource needed to fix everything that can possibly be fixed and ensuring that sufficient controls are in place to pass the audit. This should become apparent during the gap analysis stage.

POLICIES, PROCEDURES AND GUIDELINES

There are a significant number of deadlines to be met, and the firm needs to understand the process and dependencies. The external audit must be booked up to four months in advance and rescheduling is not simple. With multiple moving parts, and several key individuals with competing priorities, a careful project plan with documented dependencies, as well as communicated and managed due dates, is essential.

A firm must organize everything properly upfront so that the evidence is ready. They must set themselves up for success from the start, which means creating a plan for evidence collection. All team members must know what meetings need to happen and when. The "right" people, or their proxy, must be present and meeting minutes taken in order to demonstrate proper oversight. During the audit itself, the firm will be asked to take the auditor through these documents, so they need to start creating and storing them as early as possible as they will be expected to show the program has been in place for some time.

RESOURCES: INTERNAL AND EXTERNAL CONSIDERATIONS

A firm must identify the resources it currently has in-house that can be part of the certification process. In the same way that gaining certification from the IAPP (International Association of Privacy Professionals) or ISACA (Information Systems Audit and Control Association) requires a firm to understand the way questions are asked, they need to understand what the auditors will focus on and what they expect to see. For this reason, if a firm does not have resources in-house that are familiar with this process, it may make sense to hire an external consultant with extensive experience of certifying firms with a similar business model.

Engaging a consultant means additional cost to the firm, which can fluctuate depending upon the vendor used and scope covered. For example, a firm may pay approximately $100,000 to engage a vendor to assist with the certification process, which could be the same cost for both a small or large firm as the scope of work is relatively the same. A firm would then pay fees for the audit, as well as any work involved with the remediation process. Therefore, the cost could extend to $150,000 over a three year-period to maintain certification.

ISO AND INFORMATION GOVERNANCE

This section discusses the linkage that exists between ISO certification and IG in a law firm or department. As noted earlier, ISO 27001 specifies an Information Security Management System (ISMS) that is a management framework to identify and address information security risks.   Risks may be mitigated, transferred or accepted as a function of risk management by appropriate levels of firm management. ISO 27001 is focused on identifying assets that are at risk and finding ways to protect them.   It follows the perimeter "castle-wall" approach, focusing on prevention of important or sensitive data that a firm maintains, which is a key focus of a security program.   More recent views of the castle-wall approach suggest that it cannot be the only approach a firm pursues, with the assumption being that it is too difficult to "keep the bad guys out." There is increasing focus on taking steps to protect the data itself within a firm's walls. Encrypting the data at rest is one of the most common approaches to improving data protection because even if the data is accessed or leaves the organization, it cannot be decrypted or accessed in any way.

Information Governance is a framework supporting an "enterprise-wide approach to the management and protection of a law firm's client and business information assets." (LFIGS, Proposed IG Framework, August, 2012). It includes strategy, policy and process controls that support a broader set of goals. While both ISO and IG promote training and end-user awareness as cornerstones of their programs, they differ in approach. The security approach focuses on avoiding risky behaviors such as clicking on suspicious links as a function of security awareness training.

Information Governance, by contrast, attempts to educate management and the user population to think about the data they work with on a daily basis. It seeks to educate and ask users to make better choices about storing their data in authorized repositories and formats, and categorizing it in ways that allows retention and disposition of that data regardless of format.

The Records and Information Management (RIM) portion of an IG framework attempts to meaningfully address such issues as the disposition of data that is eligible for destruction in compliance with the firm policy. By reducing the amount of data stored, the security burden is reduced as there is less data to protect. In the same way that firms save money by employing tiered-storage solutions based on priority and performance need, firms can also save money and reduce risk by focusing categorization and protection of their most sensitive data.

While ISO 27001 and IG are different frameworks with differing focus and scope, they have a number of shared characteristics and goals:

SECURITY AND INFORMATION GOVERNANCE — SHARED CHARACTERISTICS & GOALS
Reduce risks to the organization
Respond to client demands (audit, etc.)
Identification and appropriate management of client data
Identification and appropriate management of firm data
Bridge the strengths of IT, Security, Records, Litigation Support and Risk Management to positively impact firm efforts towards reduction of risk
Joint staff effort on policy development, execution and compliance monitoring of policies such as Acceptable Use, BYOD, Data Breach, HIPAA, RIM, Confidentiality & Privacy, Written Information Security Policy, etc.
Seek to make security and data protection part of everyone's job
Engrain security and IG awareness and discipline into the organization's culture, from the executives down to the worker bee
Insert risk reduction steps into firm project management practices
Continuous improvement
Serves as a differentiator for law firms

Below are "real-life" examples within a law firm of how IG must be engrained into firm culture at all levels to avoid risk, which also resonate with the benefits of ISO certification:

- Ensuring proper security controls are in place for matter mobility events
- Documenting chain of custody of materials for incoming/ outgoing laterals
- Organizational understanding of information that is considered sensitive and confidential and should therefore be secured, as well as the procedures for securing the information, e.g., restrict access (inclusionary), ethical walls (exclusionary) and data monitoring for unauthorized access
- Policies and procedures around use of file sharing services either private or public (e.g. Google Drive, Drop Box, etc.)
- Limiting ongoing access to information when a matter concludes

SYMBIOTIC RELATIONSHIP

By working on teams to accomplish ISO certification project objectives for the firm, security and IG staff benefit from collaboration and seize opportunities for further improvement together.

IG professionals who learn more about security and technology are better equipped to improve projects and processes by recognizing the security implications of the projects they are involved in.   Security experts who learn more about IG are better equipped to identify IG issues as they get bombarded with technology or security requests throughout their day.

CURRENT STATE OF ISO CERTIFICATION

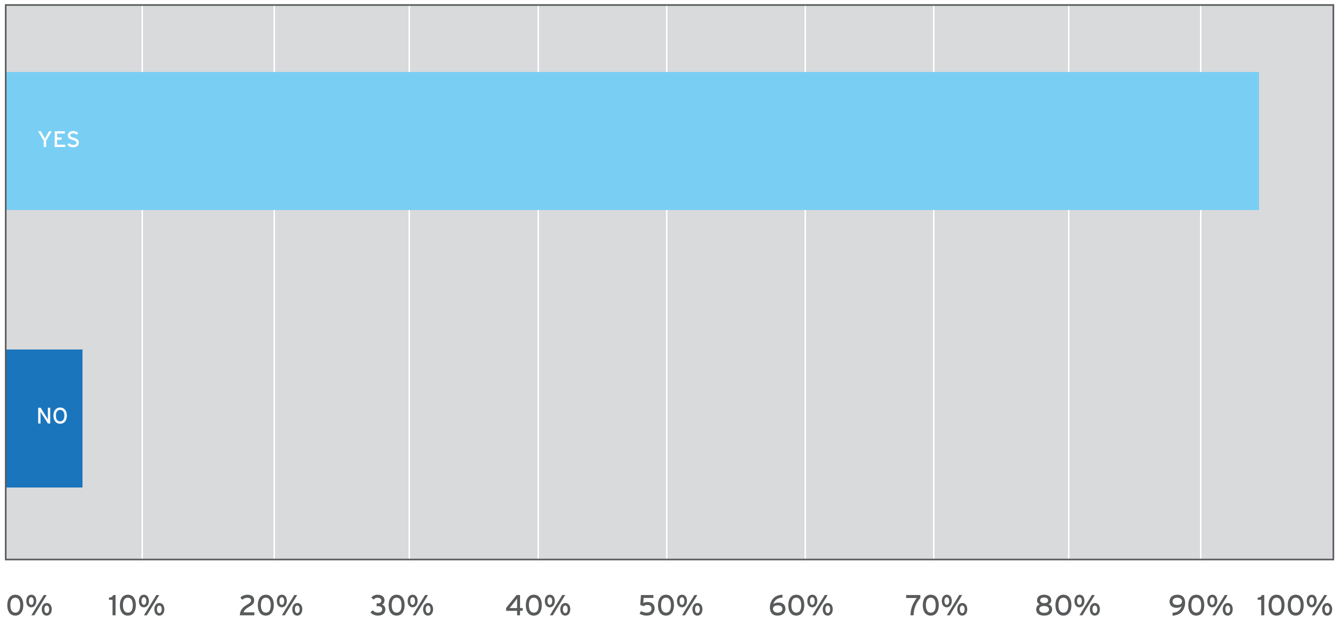
POLICIES, PROCEDURES AND GUIDELINES

As a means to gauge the current environment for law firms regarding ISO 27001 certification, this task force distributed a survey to members of ILTA LegalSec in early 2016. Thirty-five firms responded and the results provide some insight into what firms are thinking as they consider ISO 27001.

Thirty-three of 35 responding firms have considered aligning their security process with ISO 27001. These law firms tout its international application, the completeness of the framework, a potential competitive edge and the ability to compare controls against the rest of the industry.

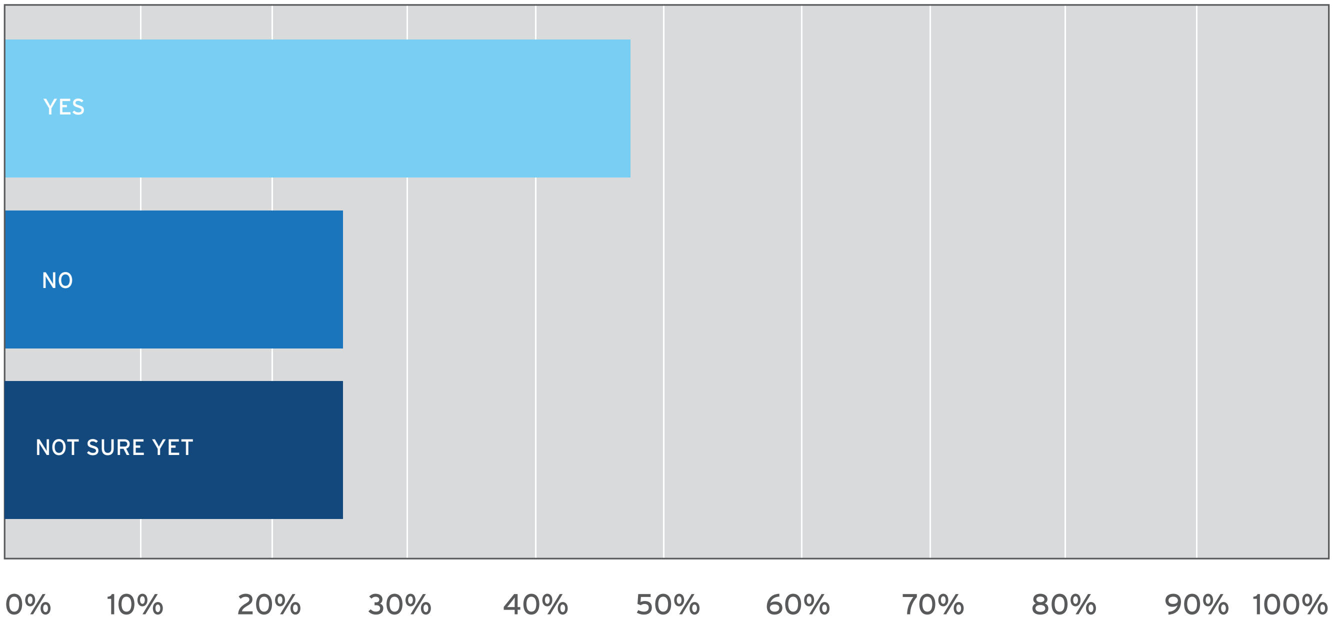
Q1: HAVE YOU CONSIDERED ALIGNING YOUR SECURITY PROCESS WITH ISO 27001? PLEASE TELL US WHY YOU DID OR DIDN'T PURSUE IN THE COMMENTS.

Answered: 35 Skipped: 0



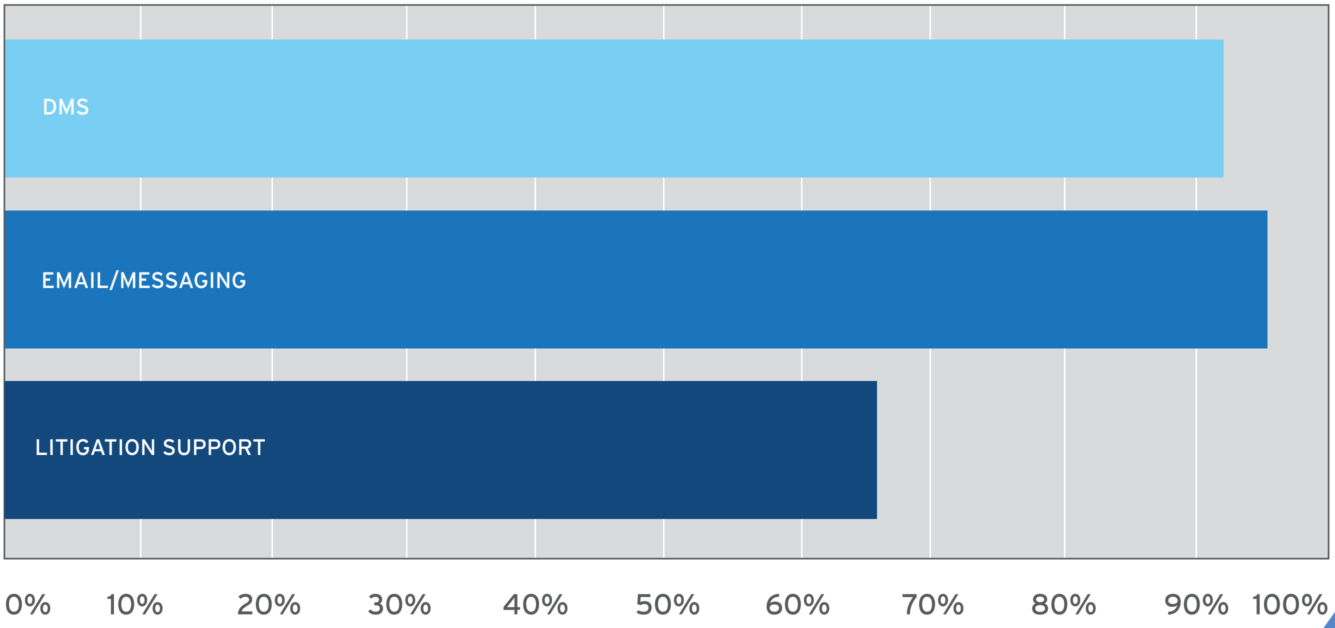
Q2: IS YOUR END GOAL CERTIFICATION? PLEASE EXPLAIN WHY OR WHY NOT IN THE COMMENTS.

Answered: 34 Skipped: 1



Q3: WHAT SYSTEMS WERE IN SCOPE FOR ISO PURPOSES?

Answered: 26 Skipped: 9



Firms have taken anywhere from six months to 3 years to complete the alignment and/or certification process, and multiple firms point out that the process never really ends, since maturing controls is part of alignment and certification. Law firms are split on whether ISO 27001 directly helps with client audits. Some clients have audits that are based on ISO controls, while others have specific questions about ISO certification. However, some law firms have not seen their clients ask about ISO 27001, nor provide "credit" in audits for ISO 27001 alignments or certification.

When a firm responded that they are not pursuing ISO certification, time and money are the biggest reasons. However, some firms report that lawyer resistance is still a significant obstacle. Several controls stood out as being difficult to implement including privilege access, separation of duties, a clean desk policy and cryptography. Firms also noted that the large amount of required documentation presented some challenges.

Firms had several insightful comments when asked, "What advice would you give firms about to undertake ISO 27001 alignment?" Many firms advised involving a qualified consultant with law firm experience if possible and allowing them to be involved in the policy/procedure creation. Firms also warned that this is a costly and time consuming process, so it is important to allocate appropriate resources and time. Other advice included:

- Start with an assessment and understand that all movement forward is positive change, regardless of size.
- Ensure that executive management understands that this is a big undertaking and that certification has their full support.
- If the effort seems daunting, start with a smaller scope.
- Set objectives and talk to other firms that have gone through the process to make sure you can achieve those objectives. For example, being certified will not get you out of client audits, but it will provide a more mature process that makes responding to those audits easier.
- Help your attorneys understand generally accepted recordkeeping principles, in particular the four responsibilities of a data owner (categorize data they ingest/create, determine who gets access, know its value and determine when it can be destroyed.)
- If you have already leveraged SANS top 20, NIST, COBIT or similar framework, mapping your controls to meet ISO 27001 may not be difficult. Assess what is already in place before tearing anything out.
- Be prepared to have more information security work after initial alignment/certification: the journey to security maturity never ends.

The firms in favor of ISO 27001 alignment/certification point out that it is a long process, but helps create the documentation on policy and processes that clients expect. It also allows a firm to spread the need for security amongst each SME.

"SNAPSHOTS" OF VARIOUS FIRM APPROACHES

An AmLaw 100 firm has recently begun the ISO-certification process and has engaged a third party vendor to assist them. Just as the documentation collected for the certification process can assist with client audits, this firm has been able to utilize documents they have collected for past audits to help prepare them for certification.

An international law firm with approximately 1,000 lawyers became fully compliant with ISO 27002 in 2012, and completed ISO 27001-certification of their e-Discovery systems in 2015. With a budget of $120,000, the firm is working toward enterprise-wide ISO 2700-certification by the end of 2016.

CONCLUSION

Information is the most valuable asset within a law firm and keeping this information secure is paramount to clients and firm leadership. ISO 27001 provides a framework to better protect information from an increasing variety of threats including fraud, cyber-attacks, inappropriate access and data leakage. Certification helps firms:

- Avoid penalties
- Protect their brand and reputation
- Ensure a secure exchange of information
- Foster stakeholder (client) loyalty and trust
- Achieve regulatory compliance, and
- Minimize the efforts of client security audits.

Certification also strengthens security as it requires firms to focus on continuous improvement and periodic assessment of compliance against policies, procedures and good security practices. Compliance with this standard provides law firms with a widely-recognized approach to information security that encompasses people, processes and technology.

TABLE 2: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

SP 800-137 Sep 2011	Information Security Continuous Monitoring for Federal Information Systems and Organizations
SP 800-122 Apr 2010	Guide to Protecting the Confidentiality of Personally Information (PII)
SP 800-115 Sep 2008	Technical Guide to Information Security Testing and Assessment
SP 800-100 Oct 2006	Information Security Handbook: A Guide for Managers
SP 800-84 Sep 2006	Guide to Test, Training and Exercise Programs for IT Plans and Capabilities
SP 800-83 Rev. 1 Jul 2013	Guide to Malware Incident Prevention and Handling for Desktops and Laptops
SP 800-70 Rev. 3 Dec 2015	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
SP 800-66 Rev 1 Oct 2008	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-64 Rev. 2 Oct 2008	Security Considerations in the System Development Life Cycle
SP 800-60 Rev. 1 Aug 2008	Guide for Mapping Types of Information and Information Systems
SP 800-59 Aug 2003	Guideline for Identifying an Information System as a National Security System
SP 800-53 A Rev.4 Dec 2014	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
SP 800-50 Oct 2003	Building an Information Technology Security Awareness and Training Program
SP 800-39 Mar 2011	Managing Information Security Risk: Organization, Mission and Information System View
SP 800-37 Rev. 1 Feb 2010	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
SP 800-18 Rev.1 Feb 2006	Guide for Developing Security Plans for Federal Information Systems

BIBLIOGRAPHY

Calder, A. (2010). Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing.

Computer Security Division: Computer Security Resource Center. (2015, October 16). Retrieved December 20, 2015, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/PubsSPs.html

Costello, K. (2016, March). ISO 27001 Certification - Momentum in the Legal Industry. Retrieved March 28, 2016, from ILTA: http://connect.iltanet.org/blogs/blogviewer?BlogKey=0ca7b43d-9846-47d9-9c66-4071014efc53&tab=recentcommunityblogsdashboard

Davis, A. E., & Downey, M. P. (2010, November 5). Protecting and Securing Client Information. Retrieved January 8, 2016, from New York Law Journal (Online): http://www.newyorklawjournal.com/id=1202474406608/Protecting-and-Securing-Client-Information

Edwards, B. (2016, February 4). Bloomberg BNA. Retrieved February 15, 2016, from Big Law Business Legal Communities: https://bol.bna.com/verizon-gc-law-firms-are-prime-targets-for-hackers/

McGee, M. K. (2015, June 3). "Should BAs be HITRUST Certified?". Retrieved February 15, 2016, from Government Info Security: http://www.govinfosecurity.com/should-bas-be-hitrust-certified-a-8366

Price, F. (2006, March 23). What is the Difference between ISO 27001 and ISO 27002? Retrieved February 16, 2016, from Pink Elephant: http://blogs.pinkelephant.com/index.php?/faq/comments/what_is_the_difference_between_iso_27001_and_iso_27002/

Security Awareness Training Product Overview. (n.d.). Retrieved January 08, 2016, from SANS: Securing the Human: https://securingthehuman.sans.org/

(2012). Security Best Practices: The Watchword is Proritize! In L. L. Thompson, Data Breach and Encryption Handbook (p. 328). American Bar Association.

IRON MOUNTAIN®

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.