A Beginner's Guide to Data Security and Information Security Compliance Audits

Latitude Software
7800 Belfort Parkway, Suite 100
Jacksonville, FL 32256
Telephone: 904.680.7100
Toll Free: 866.396.2599
www.Latitude-Software.com

Interactive Intelligence Group Inc.
7601 Interactive Way
Indianapolis, IN 46278
Telephone/Fax: 317.872.3000
www.ININ.com

insideARM, LLC
6010 Executive Blvd.
Suite 802
Rockville, MD 20852
Telephone: 240.499.3836
www.insideARM.com

Rev. 01.12, version 1

Table of Contents

Introduction 4
Data security 5
Goals for a comprehensive data security program 5
10 steps to data security 5
Information security compliance audits 8
Security frameworks 9
Implementation best practices 10
Now it's time for the audit 11
Remediation 11
Conclusion 12
One, and not done 12
Contributors 14

Introduction

If your company isn't focused on compliance, more than just your reputation is at risk.

ARM performance is no longer only measured in terms of liquidation, dollars collected, and right-party contacts per hour. Overall performance is now inclusive of the compliance and quality practices that your firm maintains and adheres to. Compliance is at once a legal requirement, a risk management strategy, an ethical imperative, and an unavoidable line item on most companies' balance sheets.

If you are a third-party collector for a creditor, you are going to be audited. This won't just be an audit of your recovery performance; it will be an audit of your compliance practices. Less than exemplary compliance, in appearance or actuality, can hurt creditors in the marketplace, and that's a risk more and more creditors are no longer willing to take. In this era of heightened consumer lawsuits, no debt collection company can be effective in this industry while also shirking the responsibility to be fully cognizant of compliance issues.

This Beginner's Guide should be seen as a primer for the accompanying webinar, presented by Interactive Intelligence, Latitude Software, and insideARM.com on February 2, 2012. The tips and talking points introduced here will be part of an expanded conversation in a workshop setting. Our thanks to Flavio Villanustre, VP of Data Security at Lexis Nexis, and Belinda Hickling, Director of Information Security at Latitude Software, for their input and participation.

Data security

Recent global trends indicate a proliferation of data originating from multiple sources and permeating throughout all business areas. Nowadays, thanks to the growth of the Internet and social networks, not only do organizations have a need to deal with internally generated data records, but also with a substantial amount of external data collected in the course of normal business activities. All this data can create a significant risk for the organization if leaked or misappropriated, and costs to recover from it can be as high as $214 per record, as reported in a study performed by Ponemon Institute and Symantec in May 2011.

In addition, different laws and regulations may require specific data retention schedules for particular data types – and the penalties for non-compliance can be steep. Ongoing litigation is another factor that can suddenly force data retention schedule changes – requiring adequate communication channels across the organization and an effective tracking and management system to ensure compliance.

Goals for a comprehensive data security program

When designing a comprehensive data security program, there are different aspects that need to be considered in order to adequately mitigate the risks. Identifying the different data types, and classifying them based on company needs and legal and regulatory frameworks, allows for a straightforward determination around data value, protective measures to implement, and retention requirements.

Data security cannot be implemented in a vacuum: it needs to be part of a coordinated comprehensive information security program and, as such, it will need adoption and support from the top of the organization. Executive buy-in and sponsorship are crucial for any respectable long term program.

10 steps to data security

1. **Inventory**: Know which data you have and where it resides. Label your data repositories and your data records, if at all possible. Use these labels to track the individual data records along their lifetimes, and maintain electronic logs.
2. Research the **laws and regulations** that could apply to this data and the controls that they require.
    a. Is encryption of data at rest required?
    b. For how long should this data be retained?
    c. Is there any ongoing litigation that would require retaining this data for a longer period of time?
    d. What is the value to the business?
    e. What is the risk level associated with the loss/exposure?
    f. Is some of this data subject to the credit card industry PCI compliance?
    g. Do I need an offsite backup of this data?

3. **Access controls**: Identify the groups that should have access to the data and compare with the list of people that should have access based on data sensitivity or regulatory requirements. Next step is to correct the gap. You'll also want to prevent unauthorized access to the data by implementing an adequate authorization process during access provisioning. Ensure an expedited access revocation process upon job role changes or terminations. Put in place a periodic access review process. Ensure that data is made available only on a need to know basis and exercise a "least privilege principle" when granting access to data repositories.

> The *principle of least privilege* requires that every module within a data environment (process, user or program), must be able to access only the information and resources that are necessary for legitimate work purposes.

4. **Application Security**: Review the security of the applications that have access to your data. If some of these applications are built in-house, implement a Secure Development Lifecycle process, providing defensive coding practices training, fostering code reviews, and performing periodic application security assessments. If there are commercial off-the-shelf applications, ensure that vendor notifications on security problems and vulnerabilities are promptly handled, and updates and patches are swiftly deployed. Identify the different data elements and utilize tokenization techniques to mask those sensitive elements that are not an absolute requirement for a particular process.

> Tokenization is the process of replacing some piece of sensitive date (for example, a credit card number), with a value that is replaced with a random value that is not sensitive, (for instance a "*" in place of the numbers themselves).

5. **Infrastructure Security**: There are several critical components in this area.
    1. Verify that any external access to data repositories is properly vetted, and that adequate isolation is in place across the network architecture.
    2. Physical access controls where applicable are paramount.
    3. Implement a data disposal program to ensure that magnetic and non-magnetic media is securely wiped before their removal from the secure environments.
    4. Deploy data encryption at rest and/or full disk encryption if any data repositories leave the secure perimeter (laptops, mobile devices, offsite backups).
    5. Ensure that transmission channels are encrypted for sensitive data.
    6. Implement two-factor authentication if external access is required to sensitive data.

6. **Data retention policies**: Define a consistent data retention policy and communicate it across the organization. Avoid complex classifications and keep the number of categories to the minimum required by law, regulations or company needs.

7. **Data loss prevention**: Implement a data loss prevention system to detect and block accidental and/or intentional data leaks.

8. **The human factor**: Require background screening as part of your hiring and contracting practices. Provide regular awareness campaigns and training around data security and cyber threats.

9. **Audit**: Assess regularly the effectiveness of all these measures, and apply corrective actions to improve these controls over time.

10. **Transfer your residual risk**: : If, after applying the steps above you determine that the residual risk is still not acceptable to the level of risk tolerance of the organization, you can transfer part of this risk by contracting an insurance policy to cover for some of it.

The importance of data security, as part of a comprehensive information security program, has increased significantly in recent years. Ignorance, when it comes to data risks, is certainly not bliss. Hiding your head in the sand will just increase chances for a disaster.

If at all possible, rely on a standard framework for your information security program (ISO 27001/2 is probably one of the most widespread ones), and assume that eventually, things could go wrong. In extreme cases, data breaches and their associated cleanup costs can cost companies hundreds of millions of dollars, as the incident with Sony PlayStation® Network proved in 2011.

Information security compliance audits

It may be best to start by sitting down to answer three high level questions with regards to information security compliance:

1. What are you trying to accomplish? Begin by clearly defining your requirements.
2. Which compliance framework are you trying to achieve? How familiar are you with the various compliances and certifications? Do your research to help determine those that most cleanly align with your requirements.
    a. PCI-DSS 2.0
    b. SSAE-16 (replaces SAS 70)
    c. ISO1799 27001 (compliance)
    d. ISO 17799 (certification)
    e. COBit
    f. COSO
3. Who or what is driving your compliance efforts? Be sure to include all stakeholders and influencers. Many times compliance efforts are driven by clients. When that's the case, it's also in ***your*** best interest – take the time to first ensure that their requirements are legitimate and appropriate for you organization.
    a. Predefined by client. Ask for clarification on the issues and pressures driving this compliance requirement.
    b. Ensure that the compliance requirements are legitimate and appropriate for your organization.
    c. Own choosing. You'll need to research the pros and cons of the various general security frameworks to determine which one(s) are best for your organization and clients.
4. Make sure you have senior level or executive support, as these efforts are typically time consuming and costly.

As a provider of collections desktop applications, Latitude Software was requested by a client to comply with Red Flags rule. After consulting with an external security partner we determined that Latitude was not within scope of this particular requirement and we were able to strike it from our agreement.

Security frameworks

A security or compliance framework maps to a set of compliance standards that perform a series of checks following broadly accepted best practices or controls, ensuring that IT infrastructure, applications, business services and processes are organized, configured, managed, and monitored correctly.

The below list is just a sample of the many security frameworks. This list is not meant to be exhaustive but merely provide a sample of common audits that are in use today.

Type of Certification	**Who is it for?**	**Additional information**	**Certification/Compliance**
ISO/IEC 27001:2005	Organizations who have implemented the ISO/IEC 27002: 2005 standard and want to validate their controls with a qualified IT certification body	Released in 2005 the ISO 27001 is the certification to the ISO 27002 controls	Certification
PCI DSS 2.0	Companies, that store, transmit or process credit card data	The Payment Card Industry Data Security Standard (PCI DSS) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures	Compliance/Certification
SSAE-16	Organizations that have implemented a security framework and want to attest to its validity	The SSAE-16 audit validates an organization's compliance to a series of trust, confidentiality and security controls	Attestation performed by a certified American Institute of Certified Public Accountants (AICPA) auditor. Available in SOC1, SOC2, or SOC 3 form
Sarbanes Oxley	Publicly traded companies	The Act requires improving and safeguarding the reliability and transparency of accounting statements and regulatory filings	Compliance

Implementation best practices

Once you have decided on a compliance framework, here are some best practices for implementation of your compliance initiative.

Gain management approval – You need to have an executive level or senior sponsor for your endeavor; otherwise it will most likely not succeed. The senior manager should communicate to the organization explaining that this is a high priority for your organization and that it requires their full support. You should provide sponsors with regular updates and advise them of any risks or issues with the project.

Know your business or allocate the appropriate resources – It is very difficult for one person to know everything about an organization. Ensure you have a good representation of your organization within your team. If you don't have the appropriate security resources internally then supplement them with outside resources.

Define your scope – It is extremely easy to get carried away. Make sure that you and your team understand specifically what you are trying to accomplish.

Identify a security auditor to assist you with your compliance goal – Look for referrals by others in your vertical. Make sure to obtain multiple quotes and get a good understanding of what their deliverables will look like and that you are comparing apples to apples.

Budget – Make sure to include soft costs for tools, resources as well as the cost of your audit.

Complete a gap assessment* –This step is imperative as it allows you to see what and where your gaps are – and it defines how much time you will need to ensure compliancy. Typically an auditor or auditors will come to your location and interview any applicable representatives within scope. It is imperative that the employees are upfront with the auditors regarding existing practices; otherwise you will not get a true representation of the risks to your organization.

[* I would not commit to a project completion date until you have completed this step, it's difficult to determine how long an audit is going to take until you have a good understanding what your gaps actually are.]

Assign Tasks –Once you have identified the gaps, identify the priority, owners and required time frame to remediate said gaps.

Now it's time for the audit

Once you have completed your application and initial remediation phase, you will need to compile evidence for the onsite audit of your existing controls. The extent of the audit will be based on the type of compliance (certification, accreditation or attestation) that you are completing.

> ***Note***: If you have questions or disagree with the auditor, do not hesitate to ask questions. Audits are subjective by nature, so make sure that you have a good understanding of why you are being required to do something, or why a control that you have implemented is not sufficient. If you have a good response as to why your control meets the requirement then let the auditor know; they will at least give you information as to why your control is deficient.

Once the audit has been completed, there is typically a final remediation period to compile any additional evidence or implement supplemental controls.

Remediation

The idea here is to reduce the risk to your business by implementing one of the following:

> **Risk transfer** – Whereby risk is transferred to another party by outsourcing services or purchasing insurance to cover said risk.
>
> **Risk mitigation** – Using tools, resources, or some other means to mitigate the risk to an acceptable level. Be careful here; you need to make sure that the cost of your countermeasure does not exceed the risk you are trying to mitigate. Perform a cost/benefit analysis on your proposed solution(s), including the probability that the remediation will in fact mitigate your risk.
>
> **Risk acceptance** – Typically only done when the item is a low risk and the cost to mitigate is not going to impede your business in a negative manner.

Once sufficient evidence has been provided the auditor will prepare a final report or deliver the required certification, etc.

Conclusion

One, and not done

Compliance is not a one-time checklist. Most compliance audits require that you undertake additional audits to confirm continued compliance on a regular basis. It is easy for management to get caught up in the fact that "We have this, so now let's move on to the next initiative." That simply will not work. Typically, follow-up audits are more stringent than the originals as they require that you show evidence from the time of the preceding audit –not just at a single point in time (as might have been required for the original audit).

Remember that an audit is simply an external review of your controls specific to a certification or compliance. An auditor may not find all of your issues; therefore, it is your responsibility to stay well versed and in-touch with any certification criteria changes and how it may impact your environment.

The ARM industry is a highly regulated and heavily scrutinized industry. As such, there is no one-stop compliance-shop or magic bullet that can address the complex challenges ARM service providers face every day as they strive to achieve compliance. Use this paper and the accompanying February 2, 2012 webinar as a launching pad to assess your own compliance-related business needs in order to grow your company and help safeguard the reputation of the ARM industry as a whole.

Kaulkin Media, publisher of insideARM.com, provides the most credible platform for service providers to reach potential clients, and is also uniquely qualified to help ARM businesses with their own websites, social media programs, and overall marketing strategies.

The mission of insideARM.com is to shift the public conversation about the ARM industry in order to help creditors and collection professionals reduce risk, lawsuits, and bad press; we'd like to change consumer perception that speaking with collectors should be avoided. With over 70,000 subscribers our website and newsletters reach collection agencies and law firms, debt buyers, credit grantors, suppliers of technology and services to these groups, regulators, industry investors, and many other interested parties. Visit www.insidearm.com

LATITUDE SOFTWARE
AN INTERACTIVE INTELLIGENCE COMPANY

Interactive Intelligence and its subsidiary, Latitude Software, provide on-premise and cloud-based dialer and debt collection software solutions for accounts receivable management. Interactive Intelligence outbound dialing software increases agent utilization and right-party contacts, eliminates workforce segmentation, and maintains compliance. Latitude debt collection software and services are easy to use and offer comprehensive functionality for faster, more effective debt collection and portfolio recovery. Visit inin.com or debtsoftware.com for more information.

INTERACTIVE INTELLIGENCE
Deliberately Innovative

Deliberately Innovative All-in-One Communications for Business. Interactive Intelligence Group Inc. is a global provider of unified business communications solutions for contact center automation, enterprise IP telephony, and business process automation. The company's standards-based all-in-one communications software suite was designed to eliminate the cost and complexity of multi-point systems. Founded in 1994 and backed by more than 4,000 customers worldwide, Interactive Intelligence is an experienced leader in delivering customer value through its on-premise or cloud-based Communications as a Service (CaaS) solutions, both of which include software, hardware, consulting, support, education and implementation.

At Interactive Intelligence, it's what we do.

Contributors

Flavio Villanustre is the Vice President of Information Security for LexisNexis Risk Solutions. In this position, Mr. Villanustre is responsible for information and physical security and overall infrastructure strategy. Previously, Flavio was Director of Infrastructure for Seisint, Inc. Prior to 2001, Flavio served in a variety of roles at different companies including infrastructure, information security and information technology.

Belinda Hickling is the Information Security Officer and Director of Hosted Services for Latitude Software. Belinda is an Information technology professional with 12+ years of progressive management responsibility in corporate security, and has experience in security strategic planning and management, auditing, project management, risk management strategies, compliance, security technologies, and developing security programs for both the financial and software sectors.

In addition to managing Latitude's security needs, Belinda also directs operations in the Latitude hosted environment. She was instrumental in Latitude obtaining the coveted ISO 17799 27001 certification for Latitude's Hosted/SaaS environment in 2011 and is currently heading up the Interactive Intelligence SSAE-16 initiative for their CaaS group.

Prior to Belinda's tenure with Latitude in 2007, she gained invaluable experience in the collections industry by assisting the tremendous growth of Focus Receivables Management over a period of seven years. During that time she held ever increasing management responsibilities culminating in her ultimate position as VP of Technology and Customer Support. As with Latitude, she was instrumental in obtaining ISO certification and earned the second highest compliance rating with limited budget and personnel.