



Governance & Strategy Services

HALOCK Security Labs

Building Strategic Security Programs

Building a Security Program using ISO 27001

CASE STUDY: American Imaging Management



“As part of AIM’s commitment to securing the protected health information that we receive from our clients, we strive to set the industry benchmark in information security.”

- Rich Bergman, CISO American Imaging Management



“The infosec space has certainly matured in recent years. Organizations have realized the need to actively patrol security as a part of their governance framework,” says **Terry Kurzynski**, CEO of Halock Security Labs, a Schaumburg, IL based information security consultancy. Halock refined its service offerings and identified healthcare as one of the major verticals to serve. “With heavy new regulations hitting healthcare, we developed solutions tailored for the industry and trained our teams.” says **Jeremy Simon**, Halock’s CTO.

Kurzynski says the message is simple, “use ISO 27001 to govern your security program.” Since 2005, organizations in the U.S. are able to register their Information Security Management Systems commonly referred to as the Security Program to the ISO standard. “We see 2008/2009 as the **tipping point** year. The year when a critical mass of companies has completed registration and awareness begins to spread virally. Like many in manufacturing worked to obtain the ISO 9001 registration in the early 90s, so too will information-centric organizations strive to obtain ISO 27001 registration to demonstrate they have a mature information security program,” says **Kurzynski**.

“Halock helped us identify threats and gaps to ISO 27001, and also helped us remediate our vulnerabilities”

- Inna Berkovich, CIO, AIM

A great example of Halock’s services in action is its recent work with American Imaging Management (AIM). AIM is a leading technology company in its segment and was in the process of redefining its information security program to meet its evolving business demands. AIM was searching for the right partner to help it harmonize and centralize the management of security controls. Enter Halock Security Labs.

Why Halock....

During an internal review of its security needs, American Imaging Management (AIM) identified the need to perform due diligence with an outside security expert. AIM spent a month interviewing security firms and selected **Halock Security Labs** because of Halock’s ability to not only assess vulnerabilities, but to assist in remediation efforts including application security solutions.



Why ISO 27001?

Model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS); often referred to as the Security Program

- IT Security Controls
- Recognized Internationally
- Formal Registration Available
- Harmonizes security requirements from regulation, legislation, and the business
- Often identified as a vendor requirement
- Demonstrates the existence of a mature security program
- Flexible to adopt to changing threats and security requirements
- Integral part to any enterprise IT Governance Strategy



“AIM differentiates itself through innovation, technology and service; security is a pre-requisite for all of those values.”

-Brandon Cady, President, AIM

Solution Approach

AIM concluded that it needed to invest and expand its current corporate security posture to enhance security for itself, its clients and the lives covered under its programs. Halock’s first task was to perform a risk assessment on AIM’s current security program.

Part I

Halock performed an ISO 27001 gap assessment to quantify AIM's overall security posture, and delivered a detailed recommended course of action to address and remediate areas both under and over controlled

Halock provided guidance during various remediation efforts and an independent audit to ensure that AIM’s scheduled client deployments were uninterrupted.

Subsequently, Halock provided a roadmap for building a Security Program that could be registered to the ISO 27001 standard. **Inna Berkovich**, AIM’s CIO stated *“Our applications are consistently evolving to meet client needs. We need a security program that provides the flexibility to address new threats and security requirements; ISO’s framework offers us that ability.”*





Part II

As a first step to implementing the new Security Program, Halock championed ISO's Plan-Do-Check-Act cycle to deploy a comprehensive set of security controls and initiatives. Through the following months, Halock worked as a member of AIM's Security Governance Committee and the following efforts were completed:

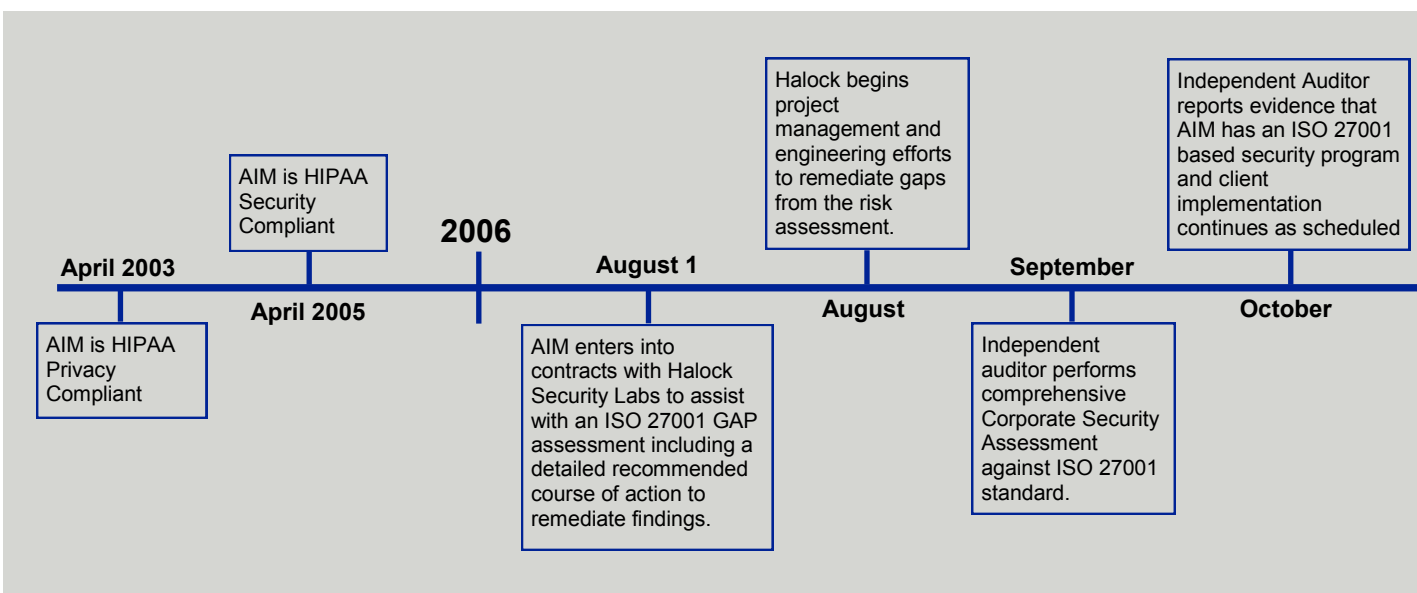
- Defined granular roles and responsibilities
- Specifically indentified security requirements (legislative, regulatory, and contractual)
- Defined supporting policies, standards and procedures
- Defined and established security awareness program
- Expanded vulnerability management program
- Collaborated with BC/DR to integrate Security Program objectives
- More clearly defined incident response program
- Implemented internal security control audit program
- Conformed Security Program to existing AIM Compliance, Privacy and Standards initiatives

Plan-Do-Check-Act Cycle

- Plan - Establish the Security Program
- Do - Implement and Operate the Security Program
- Check - Monitor and Review the Security Program
- Act - Maintain and Improve the Security Program

"As we continue to expand relationships with new and existing clients, our security program offers an important and tangible area of differentiation that is increasingly required by our customers."

- Brandon Cady, President, AIM





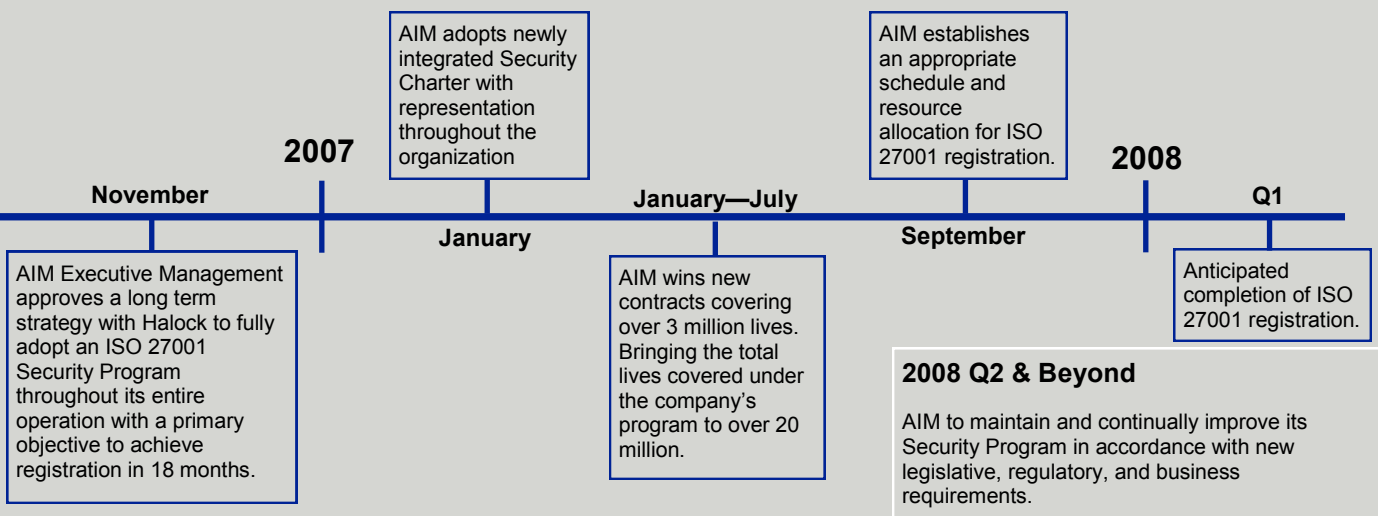
Part III

As AIM prepares for its annual Corporate Security Assessment in late Q3 and as Halock continues to refine and improve components of the operational Security Program, AIM is confident that it is fully compliant with the expectations of the ISO 27001 Standard and is ready to begin preparations for formal registration. AIM has set a target of Q1 2008 for completion of the registration process. **Inna Berkovich**, the CIO of AIM stated “Halock helped us to get Senior Management buy in early in the process, which was key to successful implementation of the new Security Program.”



“AIM’s partnership with Halock to implement the ISO 27001 standard only serves to strengthen our HIPAA privacy and security programs to protect the confidentiality and integrity of the information entrusted to us by our clients.”

- Kristine Tomzik, VP and Chief Compliance Officer, AIM





American Imaging Management ..

Founded in 1989, Deerfield, Ill.—based AIM is a leading manager of outpatient diagnostic imaging services. Since its inception, AIM has developed a spectrum of programs and services that ensure the right test is ordered at the right time, that patients are directed to the best imaging location for the service, and that proper payment is made by the health plan for the service. AIM’s programs manage diagnostic imaging services for more than 20 million people on behalf of health insurers across the United States. For more information about AIM, please visit

www.americanimaging.net.



HALOCKSecurityLabs

Halock Security Labs, is a full service Security Risk Management consulting firm focused on leveraging the ISO 27001 standard for information security best practices. Founded in 1996 Halock Security Labs (formerly Remington Associates), has assisted clients in securing their networks and applications while meeting their security requirements in confidentiality, integrity, availability, and compliance. Halock service teams include Governance & Strategy, Assessment & Compliance, PCI Compliance & Validation, Network & Systems Security, as well as Application Security. Halock’s client base is centered around healthcare, retail, and finance. www.halock.com

About ISO 27000 (27001/27002):

As security breaches intensify and regulations multiple, the need for a framework to manage vulnerabilities is eminent. ISO 27000 provides the guidance to initiate, build, and manage, and assess information security within any organization. Some of its features include:

- **Security Policy** – Documented management support for information security.
- **Security Organization** – a management framework for information security.
- **Asset Classification and Control** – assigned responsibility for inventory of assets.
- **Personnel Security** – well defined security roles and responsibilities.
- **Environmental Security** – security requirements for people and premises.
- **Communications and Operations Management** – operational optimization of communications of your ISMS.
- **Access Control** – ensure appropriate access to information and network assets.
- **Systems Development and Maintenance** – appropriate systems life cycles that minimize vulnerabilities and encrypt when necessary.

About Halock Governance & Strategy Services:

Governance & Strategy starts with identification and publication of security requirements and the security organization. Halock’s Governance specialists will assist in identifying the regulatory, legislative, contractual and business mission related security requirements and harmonize them. These requirements are gathered from the business leadership, many of which will be a part of the security organization.

Development of the Security Program Roadmap is a key deliverable from the Governance & Strategy team. Organizations can then build and deploy the controls and solutions that help meet their security requirements. Halock’s Governance & Strategy Services include:

- InfoSec Program Development
- Virtual CISO/Security Council
- ISO-27001 Registration Preparedness
- Policy & Procedure Development
- Security Governance Planning
- Incident Response Planning
- DR/BC Planning & Strategy



HALOCKSecurityLabs

1834 Walden Office Square Suite 150 * Schaumburg, IL 60173 * 847.221.0200 * www.halock.com