An Executive Brief

Getting Started with ISO 27000

A Global Information Security Standard

The ISO 27000 series is an important global information security framework that can be applied to address multiple regulations and standards and is applicable to organizations of all types, industries and sizes. Your organization may be impacted by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and possibly other regulations such as the Payment Card Industry's Data Security Standard (PCI DSS) or U.S. State requirements. An important reference and an excellent framework in the world of information security is the ISO 27000 standard. The ISO 27000 series is an important global information security framework that can be applied to address multiple regulations and standards.

The ISO 27000 standards are applicable to organizations of all types, across industries, and sizes.

The ISO 27000 family of information security standards includes:

- ISO 27001 (ISMS – Information Security Management System)
- ISO 27002 (Security Clauses, Categories & Controls)
- ISO 27003 (Guidance in implementing ISMS)
- ISO 27004 (ISMS measurement and metrics; effectiveness of ISMS)
- ISO 27005 (ISRM - Information Security Risk Management)

Why Adopt ISO 27000?

Organizations need to address several compliance mandates, both federal and States. Further, organizations also work with business associates, some may be in the United States, and others may be international firms. The ISO 27000 is the only global enterprise security standard that may be used as a framework for an organization's information security strategy. This increases efficiency and brings about consistency in the implementation of an enterprise security program. It also increases an organization's credibility about its security program.

ISO 27000 is a comprehensive security standard that may be used as a framework to address federal and state mandates. It enables an organization to ensure that its business associates are consistent in their approach to security. The ISO 27000 series provides best practice recommendations on information security management, risks and controls. So if your organization is required to comply with regulations such as the PCI DSS, HITECH Act, HIPAA or other national (federal) or stating requirement then you can seriously consider the ISO 27000 to provide an exceptional framework to address security related regulatory mandates.

The bottom-line is that adopting the ISO 27000 establishes *instant credibilit*y that the enterprise is basing its security strategy on the *most comprehensive*, global standard. It *delivers efficiency* by ensuring all compliance mandates are addressed with one standard. It *enables consistency* as all business associates address the organization's security requirements in the context of one global standard.

Benefits of ISO 27000

- **Compliance**. Selecting a control framework that not only complies with HIPAA and SOC2 but provides extra safeguards clearly demonstrates that gaps identified by the OIG audit are being seriously addressed.
- **Risk mitigation**. Provide the organization with a structured approach to information security management to enable them to secure their information assets. The management system considers risks to the confidentiality, integrity and availability of the data as well as business risks associated with non-compliance and data breaches.
- **Client retention**. Security questionnaires completed fully and appropriately; clients less likely to defect to a competitor that doesn't have the same certification.
- **Reputation**. Demonstrate compliance with an internationally recognized standard and the ability to satisfy customer security requirements. Become known for secure management of confidential and sensitive information.
- **Decreased costs**. Invest now to save later; consider the Information Security Management System to be an insurance policy. Help identify the true cost and ROI of risk mitigation.
- **Business alignment**. A Management System allows the information security initiative to be aligned perfectly with business strategic objectives and places information security as a high, visible priority in strategic thinking and project planning. This includes aligning security practices across all locations and subsidiaries.
- **Improved tools & procedures**. Enhance information security through adoption of best practices and implementation of best in class security products.
- **Marketing edge**. Demonstration of commitment to information security and provide a competitive differentiator when tendering for business and contracts. Demonstrate compliance with an internationally recognized standard and the ability to satisfy (and surpass) customer security requirements.
- **Resource utilization**. The formal procedural structure of a Management System helps optimize human resources, technical resources and financial resources.

A Phased Approach to Adopt ISO 27000

It should be noted that implementing and maintaining ISO 27001 is not a technology project, it is essentially about change management: changing the way staff approach data protection and the culture change that is required to improve the compliance maturity of the company.

The adoption of ISO 27000 as the framework for enterprise security should be a strategic decision for an organization.

Organizations should seriously consider a phased approach to adopt the ISO 27000, global information security standard, as its framework for protecting client and enterprise data.

Phase 1	Leadership commitment and communication
Phase 2	Planning & Gap Analysis
Phase 3	Implement the Management System processes
Phase 4	Complete “Statement of Applicability” and implement appropriate controls
Phase 5	Stage 1 Audit – compare Management System with ISO 27001 requirements
Phase 6	Stage 2 Audit – compare Management system with actual operations and controls
Phase 7	Certification Audit

Discuss with ecfirst how we can enable your organization to adopt the ISO 27000 global information security standard.

Perfecting the Art of Active Cyber Defense

Client Reference

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I continue to recommend ecfirst highly and often!"

BRG Berkeley Research Group — **Chip Goodman | Vice President of Information Technology**

"The ecfirst team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome COLLABORATIVE SYMPTOM MANAGEMENT — **DerShung Yang | Founder & President**

"Provant Health partnered with ecfirst to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were ***flexible, collaborative*** and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I'd recommend ecfirst to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification."

provant health life. changing. — **Tom Basiliere | Chief Information Officer**

Robert Acosta | Bob.Acosta@ecfirst.com | +1.949.793.5700

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

Kris Laidley

Inside Sales Support Coordinator

ecfirst/HIPAA Academy

Phone: +1.515.987.4044 ext 25

Email: Kristen.Laidley@ecfirst.com

Robert Acosta

National Sales Director

ecfirst/HIPAA Academy

Phone: +1.949.793.5700

Email: Bob.Acosta@ecfirst.com

www.ecfirst.com