Integrating ISO/IEC 27001 to Increase Efficiency, Eliminate Redundancy, and Demonstrate Effectiveness

Never before have we witnessed the current pressure on businesses to protect their customers, employees, and proprietary business information. IT security is becoming increasingly threatened on all sides as businesses struggle to protect this information, including computer data, marketing strategies, tax and personnel records, financial data, communications, and business plans. This white paper discusses an integrated approach to information security and how it can manage real risks associated with internal security and validity, complying with regulatory requirements, and e-Discovery[1], or providing a legal proceeding with litigation-ready records[2]. According to an online article from LAW.com, more than 90 percent of new business records are created electronically, and 40 percent of them are never converted to paper.

What is an integrated approach?

From a business perspective, an integrated approach creates value for customers and shareholders by improving capability, reducing cost, improving efficiency, and delivering a Return on Investment (ROI). An integrated approach also provides a pathway for developing people into business and process leaders, and for enhancing their knowledge, skills and value to the business. The aim of the integrated approach is based on the conviction that every process can and should be repeatedly evaluated and significantly improved in terms of time required, resources used, cost, and other aspects relevant to the process.

How can an integrated approach manage risk?

Organizations of all sizes and from all sectors face an identical problem set. All face inherent vulnerability to a wide variety of threats. Likewise, they face the high cost of reducing risk by maintaining an appropriate level of preparedness based on customer requirements and multiple regulations and standards.

An integrated approach can create the basis for a safe and secure resiliency program or management system, resulting in the design and deployment of a comprehensive risk governance platform, both for compliance and assurance.

[1] Electronic discovery (also called eDiscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

[2] The capability of an organization to respond to legal discovery demands.

How is an integrated approach better than my current solution?

Organizations spend millions of dollars on firewalls, routers, segmentation, and compartmentalization of their security model, but most don't spend enough time on internal processes and people. A Ponemon Institute study showed that 80 percent of organizations suffer breaches. The study also found that 75 percent of organizations in the U.S., U.K., France, and Germany have suffered data breaches caused by accidental internal lapses, while 26 percent say that they have experienced breaches from malicious insiders. Malicious insiders are within the confines that the firewalls and routers are intended to protect. This type of security structure is referred to as the egg shell security model. Like an egg, the organization is hardened on the outside but soft in the center. This solution fails due to a lack of attentiveness to people and process, i.e. employee training and awareness, absence of formal policies and procedures, and an overall lack of a solid foundation. The result is that a lot of information supposedly protected under your IT infrastructure is not. This is where most breaches will and typically do occur. The root cause in many cases is due to documents being leaked purposely for gain or unintentionally due to lack of training and process.

Further, each individual component of information security is analyzed independently of the other security systems. This creates a "silo" effect, which is expensive to maintain due to numerous regulatory requirements that a company is expected to address individually within each business system. The integrated approach allows you to break down the silos that have been implemented and develop an information security policy on top of a solid foundation rather than an ad hoc approach of constructing a management system with no design.

Are your information security policies litigation-ready?

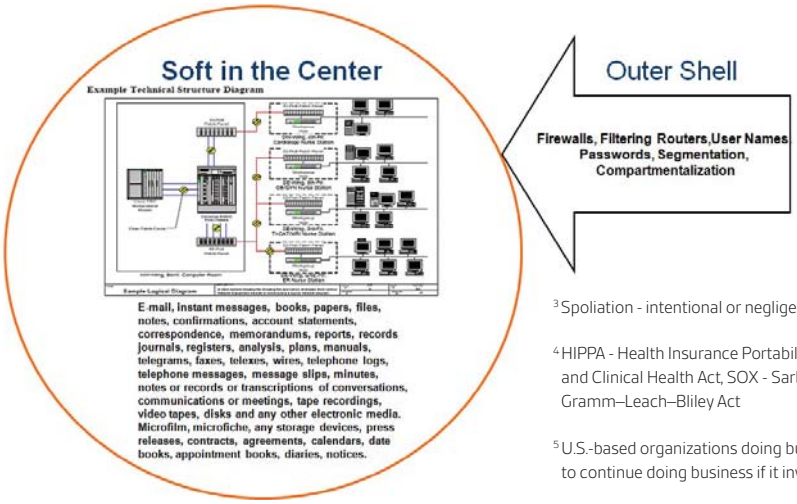
"The e-Generation" is one term that has been used to describe the current generation. Mail has given way to email. Commerce has given way to ecommerce and discovery; the process preceding a court trial where legal teams on each side gather evidence has given way to e-Discovery. Out of a necessity to bring the legal system into the 21st century and allow the admissibility of computer records into courtroom testimony, the rules and regulations concerning e-Discovery have been standardized in legal statutes across America.

As of December 1, 2006, U.S. companies and other parties involved with U.S. companies and in federal litigation are required to produce electronically stored information as part of discovery; the process by which both sides share evidence before a trial.

If your employees' personal policy is to delete emails that would be considered vital to litigation, then it could be deemed virtual shredding. The information the attorneys are looking for pertaining to the case isn't there, and the organization or employee will have to explain why. If the organization does not have formal policies and procedures in place, an organization could be accused of virtual shredding or spoliation[3]. These employee practices could get your organization sanctioned by the court and management could be fined or even incarcerated.

Litigation-hold is just one example of a regulatory requirement that could easily be ignored by the internal employees in an egg shell security model. There are numerous other regulatory requirements that your organization may have to consider as well, including but not limited to HIPAA/HITECH, SOX, FACT Act, GLBA,[4] individual state privacy laws, and EU Directive[5]. The soft center of the egg shell model simply makes enforcing all of these regulations piecemeal, an expensive and high risk, and a complicated task.

Egg Shell Security Model



[3] Spoliation - intentional or negligent withholding, hiding, altering, or destroying of evidence relevant to a legal proceeding.

[4] HIPPA - Health Insurance Portability and Accountability Act, HTECH - Health Information Technology for Economic and Clinical Health Act, SOX - Sarbanes–Oxley Act, FACT Act - Fair and Accurate Credit Transactions Act, GLBA - Gramm–Leach–Bliley Act

[5] U.S.-based organizations doing business in EU countries must meet the requirements of the EU Data Protection Directive to continue doing business if it involves sharing and/or processing data with these countries (which most do).

Develop a comprehensive risk governance platform

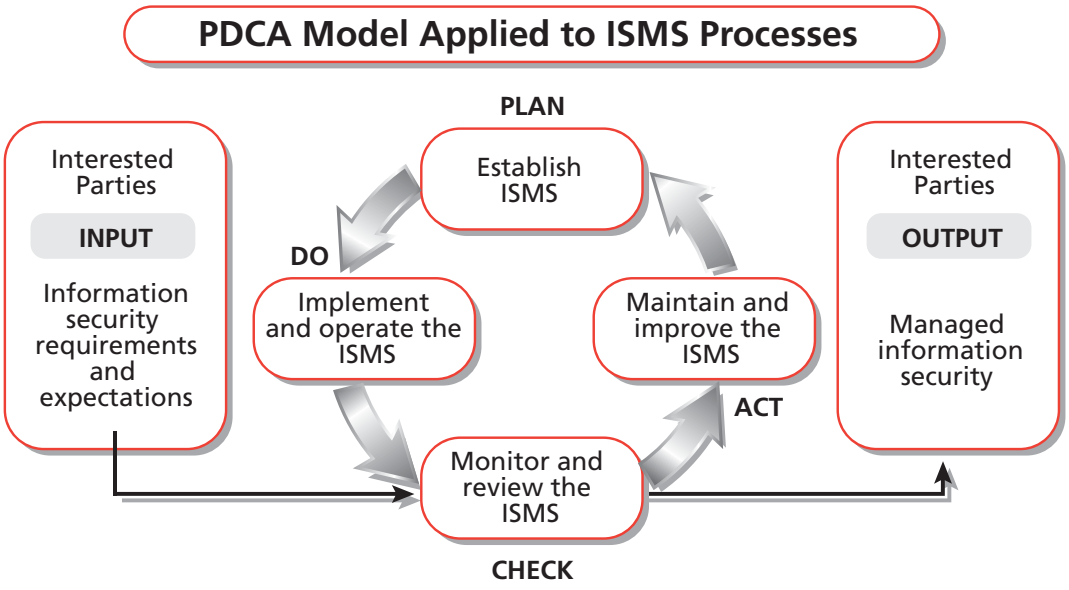
Using the ISO/IEC 27001 standard along the Six Sigma methodologies to manage your implementation, you can design and deploy a comprehensive risk governance platform that ensures both compliance and assurance with regulatory and internal requirements, while showing measureable savings over the more ad hoc approach.

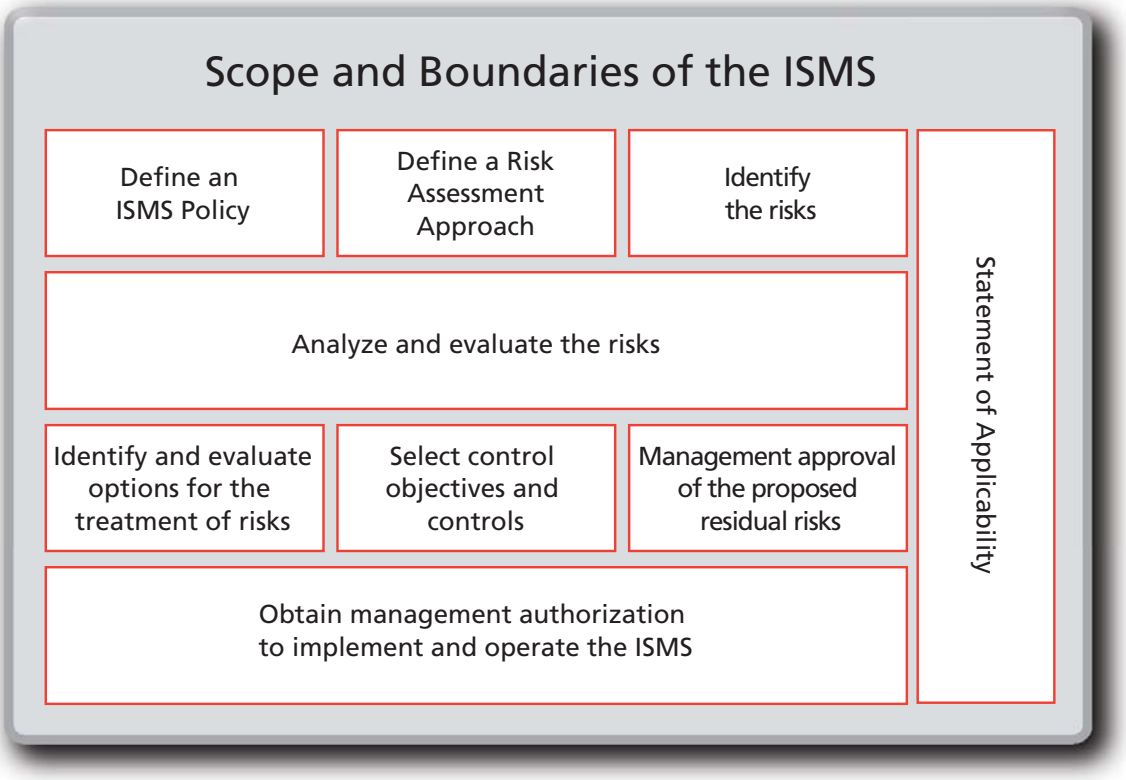
Step 1: Create a defined problem statement based on business priorities

- Identify poor performance and/or redundant areas of compliance.
- Understand sources of compliance requirements and business data to support performance and business objectives.
- Prioritize areas in terms of improvement value.
- Define and launch projects with well-articulated scope, problem, and objective statements that have a beneficial impact, either financial or strategic, to the business. The suggested project plan is designed.

Step 2: Identify ways to break down silos and begin to introduce effectiveness through collaboration

- Identify the true processes contributing to the observed undesirable performance, and determine the most likely contributors (e.g. business systems that contribute to the overall resilience, regulatory, and compliance program).
- Characterize the process thoroughly in terms of the input to and the output from the process, and measure the accuracy and repeatability of the method.
- Identify and analyze the data used to manage the process, and document value and non-value added activities (e.g. sources of variation by evaluating the inputs and outputs of the Information Security Management System (ISMS); e.g. The Plan, Do Check, Act (PDCA) process).
- Understand stakeholder risk management objectives and organizational risk tolerance.
- Capture organizational obligations specific to compliance and resiliency.
- Take inventory of related risk management processes.
- Establish targets (financial, operational, timing, and resources).





Step 3: Eliminate risk management redundancy

- Apply appropriate analytical tools to determine with statistical certainty which areas in the ISMS compliance and security processes are redundant and in need of improvement. Examples include process mapping, use case modeling, and maturity optimization analysis.
- Now that the true causes of the problems are known, along with their sensitivities and effects, accurate improvement solutions can be identified. Examples include redundant systems, silos, fragmented processes, and meaningless metrics.

Step 4: Continuous improvement process based on performance objectives

- Systematically review critical factors in the process to focus on the modifications and adjustments needed to achieve the desired level of performance output and to optimize specific processes.
- Begin the development of objective metrics.

Step 5: Measurement process driving long-term viability

- Incorporate the basic tools of process control and choose the critical process input to assure that the improved performance will be maintained and sustained.
- Implement a measurement process that provides management with the reporting mechanisms for tracking improvements, identifying opportunities, and documenting the ROI. Finalize the objective metrics.

Once completed, a new management system is now implemented, allowing continual improvement and increased measurable savings over time. At this point, it's appropriate to hand off the project from improvement specialist to the owners and workers within the process. This step involves knowledge transfer, development of consistent processes, and the determination of organizational resilience, resulting in one process that complies with many requirements.

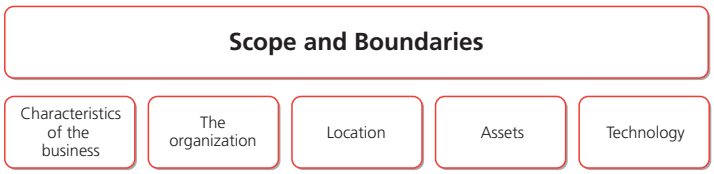
The ISO/IEC 27001 Solution: Implementing an Information Security Management System

ISO/IEC 27001 is an umbrella that organizations can use as a framework by which they can organize, monitor and control their regulatory and industry-standard requirements. A holistic ISO 27001 compliance solution means breaking down the silos and introducing effective information security policies.

The result of ISO 27001 is a continuous improvement cycle on the reliability and efficiency of internal security procedures. Implementing and maintaining an ISMS in accordance with ISO 27001 is a five-step process:

Step 1: Establish an ISMS

Define an ISMS policy and scope. Define the risk assessment approach. Identify the assets and risks. Analyze and evaluate risks. Identify and evaluate risk treatment options. Select control objectives and controls. Get management approval of the proposed residual risks. Get management authorization to implement and operate the ISMS.



Step 2: Implement and operate the ISMS

Risk treatment plan for managing information security risks. This is where top management must be involved in providing resources and setting responsibilities and priorities.

Step 3: Classify information

Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

7.2 Information classification

Objective: to ensure that information receives an appropriate level of protection.

7.2.1 Classification guidelines

Control

Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

7.2.2 Information labelling and handling

Control

An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.

- Implement training and awareness programs for employees, managers, human resources, legal, third party vendors, outsourced companies, auditors, compliance managers, and information technology professionals such as system administrators, network operators, and help desk staff.
- All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
- Manage operations and resources of the ISMS.
- Implement procedures and other controls for the detection of and response to security incidents.
  - Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room mail handling management, and safety.

Step 4: Monitor and review the ISMS

- Analyze the input and output of your processes and take action when you deviate from expected performance.
- Undertake regular reviews of the effectiveness of the ISMS, including meeting ISMS policy, objectives, and a review of security controls.
  - Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified.
- Measure the effectiveness of controls or group of controls through metrics to verify that security requirements have been met.
- Review risk assessments at planned intervals and review the level of residual risk and identified acceptable risk.

Step 5: Maintain and improve the ISMS

- Implement the identified improvements in the ISMS.
- Take appropriate corrective and preventative actions. Apply the lessons learned.
- Communicate the actions and improvements to all interested parties.

Ensure that the improvements achieve their intended objectives.

Structure of the Specification

1. Scope
2. Normative References
3. Terms and Definitions

Management System Requirements

4. Information Security Management System – Plan
5. Management Responsibility – Do
6. Internal ISMA Audits – Check
7. Management Review of the ISMS – Check
8. ISMS Improvement – Act

These are also controls!

The Eleven Control Clauses

(a.k.a. the Eleven "Domains")

A.5	Security Policy
A.6	Organization of Information Security
A.7	Asset Management
A.8	Human Resources Security
A.9	Physical and Environmental Security
A.10	Communications and Operations Management
A.11	Access Control
A.12	Information Systems Acquisition, Development, and Maintenance
A.13	Information Security Incident Management
A.14	Business Continuity Management
A.15	Compliance

Contains 39 Control Objectives and 133 controls in all

Case Study

A major IT service provider, the organization aims to be compliant with all applicable federal, state, provincial, county, and local laws, statutes, ordinances, and regulations concerning privacy and data protection and business continuity, including, but not limited to those applicable to the collection, storage, transfer, sharing and/or other processing of personal data made available to it by its customers.

The client performed a formal assessment using the techniques as described in this paper against the requirements of applicable international standards and regulatory requirements. The deliverable from the gap assessment was an integrated implementation project plan, including timescales and costs for achieving targets and milestones in the most cost-effective and efficient manner, while meeting the various legal, contractual and regulatory compliance requirements.

After the initial assessment was completed, the client executed the project plan and successfully achieved a holistic state. All regulatory, security and business continuity requirements now operate under one framework mapping to each other, eliminating past redundancies, system silos and cost overruns due to multiple audits, procedures and management systems.

A	B	C	D	E	F	G	H
Policy Areas	Federal and State Regulations						
	Sarbanes-Oxley	GLBA	HIPAA	State Banking	FCRA	USA Patriot	Canadian Info Privacy & Elec Doc
Security Organization							
Roles, Responsibilities, Process	x		x	x		x	x
Team Members						x	x
Incident Response	x	x	x			x	x
Escalation	x	x	x			x	x
Information and response communication	x	x	x	x		x	x
Asset Classification and Control							
Information values		x	x	x	x		x
Employee access	x	x	x	x	x		x
Security Zones	x	x	x				x
Information Flows: Data in motion		x	x		x		x
Information Flows: Data at rest		x	x		x		x
Personnel Security							
Employee obligations		x	x	x	x	x	x
Consequences		x	x	x	x	x	x
Physical and Environmental Security							
Security Zones	x	x	x	x			x
Fire Protection				x			
Power Failover				x			
Third Party Access Controls	x	x	x	x	x		x
Structural Security	x	x	x	x	x		x
Operations Management							
Separation of duties		x					x
Protection of Assets	x	x	x	x	x		x
Security Awareness Training	x	x	x		x		x
Usage and retention	x	x	x	x	x		x
Version and Patch Control		x					

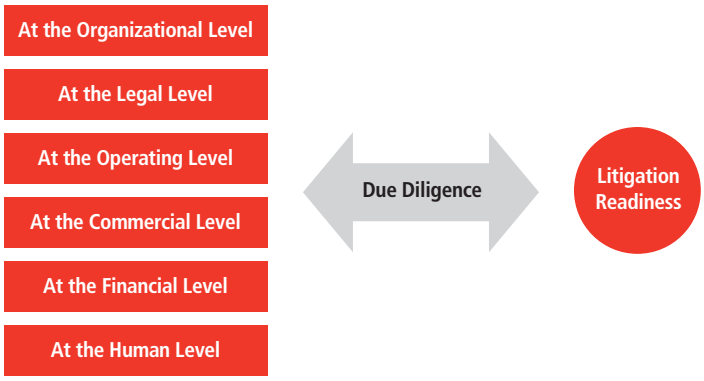
Example of integrated mapping

Conclusions

The result of implementing ISO 27001 as the managed risk architecture for your ISMS provides confidence at all levels of your organization. With proper due diligence performed, you can ensure that your organization is protected and litigation-ready in the event you are asked to produce records relating to regulatory requirements, or worse yet, court orders.

Implementing a fully robust ISMS that meets the requirements as outlined in ISO 27001 reduces the likelihood of control inefficiency and risk mitigation strategy overlap that results in overspending by the organization. Once you have the correct process and metrics in place, the integrated approach of ISO 27001 will deliver the means where you can show a measurable return on investment.

Confidence at all Levels



A recent survey of our customers has highlighted that BSI clients achieving ISO/IEC 27001 certification report major benefits from implementing the information security management standard. Among global businesses:

- 85 percent of businesses improved stakeholder confidence in their information security
- 79 percent of businesses improved their speed of recovery from incidents and disruptions
- 67 percent of businesses increased their sales revenue
- 58 percent of businesses achieved cost savings and revenue protection

BSI/USA/346/MS/0113/E

About BSI

BSI is a trusted partner to industry and government with a focus to support their business objectives through the transfer of knowledge of best practices, assurance services to identify and measure performance indicators, training services to aid the building of organizational competency and enable continual improvement, and the tools to monitor, enhance, and report on compliance against the organization's management system objectives.

BSI Solutions Package

BSI offers a comprehensive package to jumpstart your management system efforts, while allowing you to optimize control, maximize ROI, and drive operational performance to the next level. The BSI Solutions Package brings together assessment services, training, and a software tool that can provide your organization with the means to improve the effectiveness of your internal control systems.

- Assists in reducing costs
- Fosters continual improvement
- Manages risk
- Enhances organizational competency
- Protects your brand
- Improves internal control & processes

BSI provides comprehensive service offerings for a variety of sectors based on industry-specific standards. This approach allows us to provide you with an integrated approach to fit your needs.

As an additional benefit, our solutions package may be structured using an innovative monthly payment plan to reduce cost volatility and eliminate budget guess-work!

bsi.

For more information, call 888-429-6178
or visit www.bsiamerica.com

BSI Group America Inc.
12110 Sunset Hills Road, Suite 200
Reston, VA 20190-5902
USA
Tel: 1 888 429 6178
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada
Tel: 1 800 862 6752
Fax: 1 416 620 9911
inquiry.canada@bsigroup.com
www.bsigroup.ca
www.bsigroup.ca/fr

The BSI certification mark may be used on your stationery, literature and vehicles when you have successfully achieved certification and conform with applicable guidelines.

The mark shall never be applied directly on the product or service.

Copyright © 2013 The British Standards Institution. *All Rights Reserved.*