bsi.

...making excellence a habit.™

Managing security and compliance through an ISMS

Using an holistic approach to managing ISO/IEC 27001, data protection, privacy and PCI DSS

Introduction

The aim of this paper is to provide insight on how an Information Security Management System (ISMS) can be used to drive a holistic management approach for security standards and compliance obligations such as ISO 27001, PCI DSS and privacy.

By using a single system for the ongoing management of compliance, regulatory and legal information security obligations, overlapping requirements can be identified, efficiencies leveraged and greater visibility and assurance can be provided to the organization. To achieve this single point of management we advise adopting the internationally recognised ISO/IEC 27001 – Information Security Management System (ISMS) model.

ISO 27001

ISO 27001 as an ISMS

ISO 27001 is an internationally recognised management system for managing information security governance risk.

The standard provides a best-practice framework, describing key requirements necessary to implement an effective and compliant ISMS.

The requirements relate to the ongoing governance and good management of the system and intend to ensure:

- On-going awareness and understanding of the organization's operating environment and the needs of internal and external interested parties
- Leadership and support from senior management is in place to drive policy and allocate roles and responsibilities
- Planning is conducted to ensure ongoing alignment of the ISMS with the organization's objectives
- Support and resources are made available to run the system effectively
- Risk management is conducted to ensure that organizational risk appetite and control is appropriate to the external and internal risk factors
- Monitoring and continuous improvement of the system takes place

Annex A of the standard, contains 114 controls from which risk treatment options must be considered to address identified information security risk.

Leveraging the ISO 27001 ISMS to manage a broader set of regulatory, legal and industry driven requirements

In addition to the suggested controls, ISO/IEC 27001 also requires legal and regulatory obligations are understood and incorporated into the management system. In this example, data protection and PCI DSS are being considered. A high level analysis is presented in this paper to show where overlaps exist.

Privacy

The impending EU General Data Protection Regulation (GDPR) will become enforceable in May 2018. This new regulation builds on the existing data protection directive and although it's not vastly different from existing European data protection principles, it does introduce new concepts which have to be integrated into an organization's

compliance program. The regulation applies specifically in the following areas:

- Enhanced risk management processes to consider privacy as a primary concern
- Inventory and accountability
- Communications with customers and staff
- Personal privacy rights and supporting procedures
- Changes to access requests
- Consent and legal basis
- Processing children's data
- Breach reporting
- Privacy Impact Assessment (PIAs) and "Privacy by design"
- Data Protection Officer (DPOs)
- International data transfers

It's commonly accepted that EU GDPR is a complex instrument and is heavily weighted in its legal foundation. As such it is a non-trivial task to turn much of the EU GDPR into actionable tasks.

The approach being commonly adopted is to align with an international privacy management standard to ensure a defensible approach. Standards such as ISO 29001 and BS 10012 provide robust and defensible privacy management systems*. Again, leveraging the ISO 27001 management system and incorporating controls suggested by the above privacy standards, could deliver centralized efficiencies and a single view of compliance.

** It must be noted however that any outliers in legislation such as GDPR should also be considered, where specified very clearly, and certification to the standard in itself does not constitute compliance with the legislation. Consider breach reporting time frames, particular categorizations of sensitive PII, DPO roles and responsibilities, fines etc.*

Payment Card Industry Data Security Standard (PCI DSS v3.2)

The Payment Card Industry Data Security Standard, commonly referred to as PCI DSS provides a mandatory and detailed set of controls for protecting credit card information.

The controls align with ISO 27001 Annex A controls but are more prescriptive, mandating very detailed requirements that must be implemented, as opposed to using a risk based approach to select requirement applicability. Using the ISO 27001 management system to manage PCI DSS is a relatively seamless integration, due to the existing overlap of Annex A requirements.

Many PCI DSS compliant organizations, opt to certify to ISO 27001, as the additional requirements are relatively inexpensive to implement and manage when viewed in light of PCI DSS.

Scope is key

Scope is a key factor when it comes to certification to standards. In many cases, organizations will have a specific service, department or collection of systems certified to a standard, as opposed to the whole organization. This is often due to the costs and human resources associated with maintaining governance processes as well as costs associated with software and licensing of security systems.

We suggest that a minimum acceptable security baseline is defined and adopted across an entire organization. However, where valuable assets/systems/services reside, the level of security controls should increase so they retain their value.

Adopting this risk based approach drives appropriate spending to protect services that typically:

- Generate revenue
- Are subject to regulatory controls
- Interact with PII or credit card information
- Contain intellectual property
- Are internet facing

So when considering the scope of the management system, the organization should allocate resources wisely to give the most value. ISO 27001 drives this process through the "asset management" control domain, where information and system inventory and classification play a key role. By understanding what information you have, where and through what systems it flows, you can quickly identify and classify systems that play a key role in your organization.

The asset inventory becomes the single source of truth for managing system priority and the classification policy dictates how these systems must be protected. For example, you may state that all systems must have a minimum security baseline applied, however, where systems store credit card or Sensitive Personally Identifiable Information (SPII) your classification policy may stipulate that this information must be encrypted. This control alone crosses many (but not all) compliance requirements, including, but not limited to:

ISO 27001

- A 8.1.1 Inventory of Assets
- A 8.2.1 Classification of Information

PCI DSS v3.2

- Executive Summary Section 3, 4.3,
- (2.4) Maintain an inventory of system components that are in scope for PCI DSS.

GDPR

- Article 30

In the above scenario, the classification policy and inventory can be used for satisfying the inventory requirements across the three compliance areas. They would provide:

- A single source for system and information inventory
- A consistent approach to manage:
    - Information classification
    - Information handling
    - Information retention
    - Information destruction

- Information security
- Information labelling
- Access requests

As a result, the organization would be able to review and maintain one set of governance documents and drive assurance across an organization and be able to demonstrate that compliance obligations are being managed appropriately.

Classification and inventory management is not the only area where the three standards overlap. Consider:

- Governance, roles and responsibilities
- Risk assessment
- User awareness
- Access control
- Logging and monitoring
- Incident response and breach notification
- Change control (privacy by design and privacy impact assessments)
- Third party management

There are of course, many more areas that overlap between the three requirements, which must be managed on a control by control basis.

Conclusion

We believe that information security and compliance is best driven from the board and senior executive levels, where efforts can be managed from an aggregated view point, with clear delegation of roles and responsibilities. By including the senior management group in the risk and compliance conversation, informed strategic decisions can be made which further ensure support of the broader business agenda.

A centralized Information Security Management System facilitates you to identify opportunities for efficiencies and overlaps, appropriately allocate roles and responsibilities and provides assurance and visibility of the organization's governance, risk and compliance posture through a single looking glass.

- Make informed decisions about compliance and present a defensible front to compliance management
- Save time and resources by managing three separate compliance programs under one formal management system

References

- **Data Protection Commissioner:** https://www.dataprotection.ie/docs/Home/4.htm
- **Information Commisioner's Office:** https://ico.org.uk/
- **PCI Security Council:** https://www.pcisecuritystandards.org/
- **Cloud Security Alliance (CSA):** https://cloudsecurityalliance.org/
- **International Organization for Standardization:** https://www.iso.org/home.html
- **European Commission:** ec.europa.eu/

Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more

Call UK: +44 345 222 1711

Call IE: +353 1 210 1711

Visit: bsigroup.com