Information Security Management with accordance to ISO27000 Standards: Characteristics, implementations, benefits in global Supply Chains

1. WHY INFORMATION SECURITY IN A SUPPLY CHAINS IS SO IMPORTANT?

Security in supply chains could be defined as “The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorized contraband, people or weapons of mass destruction into the supply chain”\(^2\). Looking at this definition one can notice two aspects of security of supply chains – “soft and hard”. Soft aspect refers to information security, while hard one refers to more tangible vulnerabilities such as theft of physical items (product, equipment and personnel) or any physical damages. It is important to understand that any occurring hard aspects will have direct impact on soft aspects, thus they are correlated. This paper focuses on soft aspects of security of supply chains from a perspective of ISO 27000 standards, thus hard aspects are not described herein.

In supply chain management the collaboration is the solution for almost every aspect except one: information security (aka “cyber security”). And then it becomes the problem. “The very nature of global supply chains demands that companies exchange sensitive information with multiple partners, some of them several tiers removed from the manufacturer. Their ability to protect data can be highly variable. Internet thieves and predators are looking to take advantage of the slightest weakness.”\(^3\)

The information communicated by a company with its supply chain partners is foremost critical of its assets, thus the goal of information security in supply chains is to reduce the risk of any potential losses that may be caused by any disturbance, systems misuse, abuse or tampering, as well as fraud, corruption or any other form of theft. Information (data) protection must be provided against any external threats and from any internal abuse, to ensure its security. The essential for supply chains’ sharing information increases the risk of the information being compromised and stolen, thus cyber security is the foremost a supply chain issue that must be instantly addressed. Many firms are not even aware of the extent of the issue. Thus they suffer from a lack of understanding and identifying the risks related to the potential information security breakage across their supplier’s network. As a matter of fact, many complex and extend supply chains have so many suppliers and partners that makes it impossible for them to evaluate the potential risk of cooperation with every single one of them and to manage the information security risks. Therefore they pay high price for the lack of knowledge. According to ISF\(^4\) chief executive officer Michael de Crespigny, 40% of information security breaches in organizations arise from attacks on their suppliers.

The threat comes from both private and governments offenders e.g. for purpose of stealing intellectual property, seeking the technology advancements, establishing dominance in global markets

\(^1\) e-mail: jgnowak@mail.com
\(^4\) Information Security Forum (ISF) www.securityforum.org
or undermining competition across the borders from foreign companies and bodies, to name a few. The most obvious sensitive information for supply chains that can be stolen is the personal information about clients, customers and their financial transactions. But the risks are higher, as security breach can cause the treats of acquisitions, or making fragile and sensitive information being made public just before closing the deal, or alerting competitors when a company is preparing for a big financial or logistic move – it all can have a serious impact on company’s stock price or credit score. In supply chains the treats can cause serious impacts including even business closure due to loosing long term contracts or new markets expansion deals.

To secure the information (sensitive data) a company should identify all suppliers that could potentially pose a risk, and not only among the main contracts, but also those most vulnerable ones. In order to do so, a formal process of auditing standards such ISO 27001 or formal implementation of Information Security Management systems should take place. But it is only a help for the companies to assess basic risks and to address formal procedures and policies, as each business should define and implement customized solutions ensuring that the information security is achieved in most sensitive areas, such customer and supplier relations.

2. INTRODUCTION TO THE ISO 27000 FAMILY OF STANDARDS

International Standards for management systems in accordance to the ISO 27000 provide a general model to follow in setting up and operating a management system, which incorporates certain features summarized in the official document marked as: ISO/IEC JTC 1/SC 27. The document is maintained by an international expert committee that is dedicated to the development of Information Security Management System (ISMS) standards (international management systems standards for information security).

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets including the following: financial information; intellectual property (including "know-how"), employee details, and of course information entrusted by their customers or third parties. These standards can also be used as a benchmark for preparation of an independent assessment of their existing ISMS applied to the protection of information.

While the ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). Other standards within ISMS family of standards include the following “International Standards, under the general title Information technology — Security techniques (given below in numerical order):
— ISO/IEC 27000, Information security management systems — Overview and vocabulary
— ISO/IEC 27001, Information security management systems — Requirements
— ISO/IEC 27002, Code of practice for information security controls
— ISO/IEC 27003, Information security management system implementation guidance
— ISO/IEC 27004, Information security management — Measurement
— ISO/IEC 27005, Information security risk management
— ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
— ISO/IEC 27007, Guidelines for information security management systems auditing
— ISO/IEC TR 27008, Guidelines for auditors on information security controls
— ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
— ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
— ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
— ISO/IEC 27014, Governance of information security
— ISO/IEC TR 27015, Information security management guidelines for financial services
— ISO/IEC TR 27016, Information security management — Organizational economics

(...)

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:
ISO 27000 Standard lays out what the ISMS family of standards stands that:
a) “define requirements for ISMS and for those certifying such systems;
b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain and improve ISMS;
c) address sector-specific guidelines for ISMS; and
d) address conformity assessment for ISMS.”

3. SHORT HISTORY OF INFORMATION SECURITY STANDARDS.

ISO 27000 standards (known then as BS 7799) provide the guidance for the organizations since 1980’s, and has several reviews of the standards, including the latest in 2014. The following diagram shows the time line of the ISO 27000 Series of Standards:

Figure 1. Timeline of ISO 27000 series of Standards
Source: www.ISO27001Security.com

The beginning of the idea of security standards starts in late 1980's when Royall Duch/Shell group donated to the public their internal Information Security Policy Manual known as BS 7799. First official issue was then published in 1995. Unfortunately, the document was outdated since it focused on mainframe security concepts, lacking the concepts and references to the Internet technologies. Meantime, in 1989, UK Department of Trade and Industry’s Commercial Computer Security Centre (CCSC) published their information security guide for its members – based all on the Shell's manual. They also published so-called “the Green Books”. The white paper was developed based on the cooperation with UK Government's Communications Electronics Security Group (CESG). It became the

---

5 ISO/IEC 27000:2014
6 ISO/IEC 27000:2014
UK ITSEC (IT Security Evaluation and Certification) scheme for certification of security products that was officially launched between 1990 and 1991.

In 1993, a new UK standard called **BSI-DISC PD003** (BSI - Delivering Information Solutions to Customers - Public Document 003) was released by the UK Department of Trade and Industry through the British Standards Institute as a free informational item, thanks to the cooperation between UK National Computing Centre⁷ (NCC), Shell, BOC Group, British Telecom, Marks and Spencer, Midland Bank, Nationwide, supported by “BP, British Aerospace, British Steel, Bull, Cadbury Schweppes, Cameron Markby Hewitt, Chelsea Building Society, Ciba Geigy, Digital Equipment Corporation, Reuters and TSB Bank”⁸. Then, in 1995 the British Standards Institute (BSI) issued an official **BS 7799**, which was based on the BSI-DISC PD003 standard.

In 1998 a new certification standard was developed as Part 2 to the original BS 7799 called Part 1. Then BS 7799 Part 1 was revised in 1999, to become finally **ISO/IEC 17799** in December 2000, after harsh and very frustrating international discussion. Thus, in 2005 the ISO/IEC 17799 was updated, adding a number of significant sections, including those on risk and incident management and implementation guides for each of the control sections. The standard was then finally renamed as **ISO/IEC 27002** leaving the body text of the standard unchanged.

The major “operational” standards in the ISO 27000 series are listed in the table below⁹:

<table>
<thead>
<tr>
<th>ISO 27001</th>
<th>ISO 27002</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the specification for an information security management system (an ISMS) which replaced the old BS7799-2 standard</td>
<td>This is the 27000 series standard number of what was originally the ISO 17799 standard (which itself was formerly known as BS7799-1).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO 27003</th>
<th>ISO 27004</th>
</tr>
</thead>
<tbody>
<tr>
<td>This will be the official number of a new standard intended to offer guidance for the implementation of an ISMS (IS Management System).</td>
<td>This standard covers information security system management measurement and metrics, including suggested ISO27002 aligned controls.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO 27005</th>
<th>ISO 27006</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the methodology independent ISO standard for information security risk management.</td>
<td>This standard provides guidelines for the accreditation of organizations offering ISMS certification.</td>
</tr>
</tbody>
</table>

Figure 2. Operational ISO 27000 standards

Source: [www.27000.org](http://www.27000.org)

Then a series of following revisions and alternations were made reflecting the need of updating the standards due to rapidly changing technology. Major revision of the ISO 27001 and ISO 27002 was in 2013, other standards from the family of ISO 27000 were also revised and developed. The ISO 27000 was just recently revised in 2014.

---

⁷ a group lead by Prof. Edward Humphreys from NCC
⁸ As listed on: [www.iso27001security.com](http://www.iso27001security.com)
⁹ Source: [www.27000.org](http://www.27000.org)

The standard provides an overview of information security management systems, defines related terms and outlines basis for all the standards within this family of standards. It is worth mentioning that the paper itself is laid out in “kind of” opposite sequence, as it introduces the definitions and terms, then benefits and procedures first, then lists all ISO 27000 standards with their description. This is the Vocabulary standard, while 27001 and 27006 are the Requirement standards, others are divided yet into another two groups: Guideline standards and Sector-specific guideline standards. There is also another separate group called Control-specific guideline standards denoted as 2703x and 2704x series. The table “ISMS Family of Standards and their Relationships” below shows all the standards divided in the described above groups:

![Figure 3. ISMS Family of Standards and their Relationships](source: ISO 27000:2014)

The standard covers most of the information security related terms and definitions used in all ISO 27000 series of standards. However, some of them have different meanings or interpretations within the context or typical perceptions. This makes the document to be quite detailed in the descriptive part of all well-known security related vocabulary, yet necessary to be defined precisely by authors in order to guide the rest of the ISO27k standards. In fact, provided definitions are quite helpful in situations when in professional life some clients are familiar with the ISO versions.

as such in the information security context. They are not necessarily used in the ISO27k standards in full accordance with the original definitions or intended meanings. However, as the definitions are gradually updated or superseded, the lexicon is evolving into a reasonably coherent and consistent state across the whole ISO27k suite - a remarkable achievement in its own right given the practical difficulties of coordinating the effort across a loose collection of separate committees, editing projects, editors and managers, developing the language and the concepts as we go.”

The ISO27k family of standards summarizes almost all aspects of information security in major fields of human activities, and are updated following changes in the technology and procedures.

The ISO27k Standards specifying requirements have the following purposes:

- “ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS.”
- “ISO/IEC 27006 supplements ISO/IEC 17021 in providing the requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against the requirements set forth in ISO/IEC 27001.”

The ISO27k Standards describing general guidelines outline the following purposes:

- ISO/IEC 27002 provides guidance on the implementation of information security controls, provide specific implementation advice and guidance on best practice in support of the controls specified in the standardization.
- “ISO/IEC 27003 provides a process oriented approach to the successful implementation of the ISMS in accordance with ISO/IEC 27001.”
- “ISO/IEC 27004 provides a measurement framework allowing an assessment of ISMS effectiveness to be measured in accordance with ISO/IEC 27001.”
- “ISO/IEC 27005 provides guidance on implementing a process oriented risk management approach to assist in satisfactorily implementing and fulfilling the information security risk management requirements of ISO/IEC 27001.”
- “ISO/IEC 27007 will provide guidance to organizations needing to conduct internal or external audits of an ISMS or to manage an ISMS audit programme against the requirements specified in ISO/IEC 27001.”
- ISO/IEC 27008 “provides a focus on reviews of information security controls, including checking of technical compliance, against an information security implementation standard, which is established by the organization. It does not intend to provide any specific guidance on compliance checking regarding measurement, risk assessment or audit of an ISMS as specified in ISO/IEC 27004, ISO/IEC 27005 or ISO/IEC 27007, respectively. This Technical Report is not intended for management systems audits”
- ISO/IEC 27013 provide “organizations with a better understanding of the characteristics, similarities and differences of ISO/IEC 27001 and ISO/IEC 20000-1 to assist in the planning of an integrated management system that conforms to both International Standards.”
- ISO/IEC 27013 provide general guidelines on principles and processes on information security governance for governing bodies who oversight information security to ensure the objectives are met.
- ISO/IEC TR 27016 purpose is to supplement ISMS family of standards. It overlays an economic perspective and guidelines how to apply organization’s economics in the field through use of examples and variety of models.

The last, but not least group of standards describing sector-specific guidelines provide key sector-specific guidelines with the following purpose:

- ISO/IEC TR 27010 “is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or
market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organization’s or nation state’s critical infrastructure.”

- **ISO/IEC 27011** provides telecommunications organizations with an adaptation of the ISO/IEC27002 guidelines unique to their industry sector which are additional to the guidance provided towards fulfilling the requirements of ISO/IEC 27001.”

- **ISO/IEC TR 27015** “is a specialist supplement to ISO/IEC 27001 and ISO/IEC 27002 International Standards for use by organizations providing financial services to support them in:
  b) Designing and implementing controls defined in the ISO/IEC 27002:2005 International Standard or within this International Standard.”

- **ISO 27799** provides health organizations with an adaptation of the ISO/IEC 27002 guidelines unique to their industry sector which are additional to the guidance provided towards fulfilling the requirements of ISO/IEC 27001”

5. **WHAT IS THE ISMS AND INFORMATION SECURITY, AND WHY IS IT SO IMPORTANT?**

Following an official definition as stated in the ISO 27000 documentation, “an **Information Security Management System (ISMS)** consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives. It is based upon a risk assessment and the organization’s risk acceptance levels designed to effectively treat and manage risks. Analyzing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

- a) awareness of the need for information security;
- b) assignment of responsibility for information security;
- c) incorporating management commitment and the interests of stakeholders;
- d) enhancing societal values;
- e) risk assessments determining appropriate controls to reach acceptable levels of risk;
- f) security incorporated as an essential element of information networks and systems;
- g) active prevention and detection of information security incidents;
- h) ensuring a comprehensive approach to information security management; and
- i) continual reassessment of information security and making of modifications as appropriate.”

In this sense, the terms “Information” and “information security” are defined in quite detailed way. Information is defined as an asset stored in many forms, but also as knowledge of the employees. The information is depended on technologies applied in the organization, therefore information and communications technology is one of the key factors in information security.

Information security includes three aspects – called by ISO/IEC27000:2014 “dimensions”, which are the following:

- confidentiality
- availability
- integrity

According to authors of ISO/IEC27000:2014, “Information security involves the application and management of appropriate security measures that involves consideration of a wide range of threats,

---

14 ISO/IEC 27000:2014
with the aim of ensuring sustained business success and continuity, and minimizing impacts of information security incidents. Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific information security and business objectives of the organization are met. Relevant information security controls are expected to be seamlessly integrated with an organization’s business processes.”

The standards guidelines the information security activities in management and process approach. Management activities include act, manner, practice and control of the management of the resources extending form one person to organized groups of individuals responsible for information security in order to protect organization's information assets while achieving organization's objectives.

“In terms of information security, a management system allows an organization to:
a) satisfy the information security requirements of customers and other stakeholders;
b) improve an organization’s plans and activities;
c) meet the organization’s information security objectives;
d) comply with regulations, legislation and industry mandates; and
e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.”

Process approach allows organizations to pursue the objectives of information security regardless of technologies and tool applied, by describing any activity via transformation of inputs into outputs by use of sets of activities. Those activities can be interrelated of interacting with each other creating a process. Then many such processes can directly interact with each other under planned and controlled conditions via inputs and outputs, creating a system of processes and allowing organization to define and apply its process approach to its own ISMS procedures.

ISMS plays an important part in the organization's information assets security and associated risks related to physical, human and technology threats. This includes all forms of information in the organization. Thus, adoption of ISMS is considered to be a strategic decision for an organization. The adoption must be integrated and prepared in accordance to organization needs, thus design and implementation of an ISMS customized to an organization must be based on organizational structure and business processes in place, and also on security requirements of all stakeholders and – if necessary – other third parties.

The idea behind ISMS is based not only on implementing the system, but on instantly monitoring, maintaining and improving an ISMS to ensure that applied ISMS is effectively protecting the organization’s information assets on-going basis. Therefore, there is instant need for identifying the information assets and their security requirements, assessment of the related risks and treats, in order to select and implement relevant controls for managing the selected risks, and then monitoring and improving the controls of the system in accordance to the business needs and information security guidelines. This process must be carried and repeated over and over again, to ensure the effectiveness of the ISMS.

The controls are specified in accordance to the guidance in the ISO/IEC 27002:2005 or could be chosen from other control sets, or even designed and developed to meet specific needs of the organization. The newest version ISO 27002:2013 contains 114 controls, as opposed to the 133 documented within the previous 2005 version. These are now presented in fourteen sections, rather than the original eleven sections.

ISO/IEC 27001 formally specifies ISMS. The ISMS ensures that the security procedures and activities are in place to keep pace with potential changes to the security risks, threats, vulnerabilities and business impacts. That is an important aspect in such a dynamic field of information security, and so a key advantage of ISO27000 family of standards' flexible risk-driven approach. The standard

ISO/IEC 27000:2014
ISO/IEC 27000:2014
covers all types of organizations, all sizes, and all industries or markets. However, the standard does not provide a clear instruction any specific information security controls, as the controls vary depending on type of an organization. The controls are that are listed in ISO/IEC 27002 are rather kind of list of available options, letting the organization to choose applicable ones. Therefore, this is only the management role to avoid, transfer, accept, or extenuate the information security risks, as a part of risk management decision making process. Furthermore, certification based on ISO/IEC 27001:2005 requires quite long list of mandatory documented information about ISMS: including its scope, information security policy, risk assessment and treatment processes, operational planing and control documentation, and even polices for suppliers or relevant laws, regulations and contractual obligations plus the associated compliance procedures. The list is quite long.

The 2005 version of the ISO/IEC 27001 standard heavily employed the Plan-Do-Check-Act (PDCA) model “to structure the processes, and reflect the principles set out in the OECG guidelines (see oecd.org). However, the latest, 2013 version, places more emphasis on measuring and evaluating how well an organization's ISMS is performing. A section on outsourcing was also added with this release, and additional attention was paid to the organizational context of information security.”

ISO/IEC 27002 is very large document that covers a very broad range of information security risks and controls. It has grown over all these years, making the latest version of 2013 quite massive content, due to so many changes related to rapid changing technologies and information security issues. It also lacks references to the current state-of-the-art technology of cloud computing and BYOD, and also is inconsistent in terms of the level of descriptions and concerns addressed. Those make the document no longer maintainable, thus difficult to predict what would happen to the standardization of this particular item.

6. INFORMATION SECURITY IN SUPPLY CHAINS

In supply chains management practice there are five basic areas of decision making that any given supply chain firm has to address on daily basis:

- Production (manufacturing) – which products are needed on a market and when? Etc.
- Reserves – management of optimal levels and of the reorder points, etc.
- Localization – where is the optimal localization for manufacturing and for storage buildings? etc.
- Transportation (shipping) – types, optimal paths, etc.
- Information – types of, optimal levels, data exchange, its security etc.

Information in supply chains is a base for decision making support for all other areas (aspects) listed above. “It is the connector between all actions and operations within the supply chain. If the connection is strong enough (meaning that the information is: completed, accurate, and on time), the supply chain’s stakeholders can make accurate business decisions in timely and cost-efficient manner. In fact, this is how the financial and stock markets operate, and the supply chains show dynamics similar to this market”. When it comes to information security, the ISO 27001 for a supply chains is only a baseline required for ensuring the appropriate processes are in place. For example, the Information Security Forum (ISF) “has developed a Supply Chain Information Risk Assurance Process (SCIRAP), designed to help companies assess tens of thousands of suppliers, with an eye toward identifying the riskiest contracts. Like any good internal review, it involves asking the right questions:

- Which products, components or raw materials are we outsourcing?
- To whom?
- What is the significance or sensitivity of those relationships?

\[^{17}\text{www.27000.org}\]
\[^{18}\text{S. Kot, M. Starostka-Patyk, D. Krzywda, „Zarządzanie łańcuchami dostaw”, Politechnika Częstochowska, 2009.}\]
\[^{19}\text{S. Kot, M. Starostka-Patyk, D. Krzywda, „Zarządzanie łańcuchami dostaw”, Politechnika Częstochowska, 2009.}\]
What's the potential fallout from a data-security breach?
What's the track record with particular suppliers?
What kind of processes and controls are in place?
Are inspections being carried out on a regular basis?
How frequently do we want to receive confirmation that our information is being protected?

With the riskiest relationships, additional information or tighter controls are often called for. A supplier might be asked to appoint an independent accounting firm to ensure that the controls specified by a given contract are firmly in place. Reports might be required annually or with even greater frequency. In cases where cloud computing is involved, companies might want more frequent assurances from suppliers, given the relative immaturity of that technology.

How a company deploys the SCIRAP depends on where it falls on the maturity scale, with respect to maintaining an effective risk-management program for data protection. Beginners need to create a basic action plan which lays out the business case, while securing senior-management backing. According to ISF, they should be focusing on building "a coalition of support" across the organization, embracing vendors and other business partners. From there, they can proceed to secure the necessary resources and craft strong information-security policies. For companies that are well aware of the problem, yet have too many suppliers to assess individually, the model can help to target contracts that pose the greatest risk, while grading relevant suppliers on their security arrangements. Finally, organizations that know which contracts require the greatest level of care need to embed their data-security processes into the procurement and vendor-management lifecycle. In this way, information protection becomes a key issue at the outset of any acquisition or contract."

Continuous flow of information on products, services, orders, product availability, transactions supports business transactions across the network of supply chains (that are typically represented by a network of suppliers, manufacturers, wholesalers, distributors, retailers, shipping providers etc. working together a central firm). It is a key factor for meeting end-user requirements for products and services standards. A good example of information flow in a supply chain is presented by A. Roy and A. Kundu [13] on an international auto-parts firm from Taiwan (2009) called Auto e-Hub. It was a supply chain network providing Software as a Service (SaaS):

“...The system provides solutions to buyers and sellers of high quality auto parts and aims to bridge the market between domestic auto-part suppliers and world-wide automobile Original Equipment Manufacturer (OEM) or the Aftermarket (AM) procurement offices. Their supply chain network, which is depicted below, has the following objectives:

- To become a seamless network
- To collect the information from N-tier suppliers
- To improve information fluency of supply chain to mitigate impact information distortion”

Auto E-Hub example shown in Figure below is a very good illustration to show how information flow extends to many suppliers and stakeholders in the network. From other hand, “pure” logistics flow of material and products extends only to some of those – direct suppliers and customers.

Auto E-Hubs example shows how many aspects of information security need to be addressed especially in modern World’s e-business (e-commerce) model, where SCM (Supply Chain Management) systems integrate the flow of data (information). Thus, it is necessary to assure the security of information across entire supply chains’ network electronically managed (e-supply chains).

The key factor in information security is the management of business risk (considered form financial, strategically, etc.) to reduce the threat to business reputation or directly to the customers.

---

Form other hand, it is important, because it ensures compliance to legislative and regulatory requirements, often enforced by business contracts and long term agreements (e.g. ISO 27001 certification).

![Diagram of Auto E-Hub Supply Chain Network example for information and logistic flow](source: [13])

7. ISO27000 CERTIFICATION

ISO 27001:2005 certification is quite complicated process. A documented ISMS scope is one of the mandatory requirements for ISO 27001 certification. Although the “Statement of Applicability” (SoA) is not explicitly defined, it is a mandatory requirement. The term SoA refers to the output from the information security risk assessments and, in particular, the decisions around treating those risks. The SoA may be in “the form of a matrix identifying various types of information security risks on one axis, and risk treatment options on the other, showing how the risks are to be treated in the body, and perhaps who is accountable for them”\(^{22}\). It usually references the relevant controls from ISO/IEC 27002, but the organization may use a different framework or a custom approach. The information security control objectives and controls from ISO/IEC 27002 are also provided.

The process of ISO 27001 certification “starts when the organization makes the decision to embark upon the exercise. Clearly, at this point, it is also important to ensure management commitment and then assign responsibilities for the project itself.

\(^{22}\) [www.iso27001Security.com](http://www.iso27001Security.com)
An organizational top level policy can then be developed and published. This can, and will normally, be supported by subordinate policies. The next stage is particularly critical: scoping. This will define which part(s) of the organization will be covered by the ISMS. Typically, it will define the location, assets and technology to be included.

At this stage a risk assessment will be undertaken, to determine the organization's risk exposure/profile, and identify the best route to address this. The document produced will be the basis for the next stage, which will be the management of those risks. A part of this process will be selection of appropriate controls with respect to those outlined in the standard (and ISO27002), with the justification for each decision recorded in a Statement of Applicability (SOA). The controls themselves should then be implemented as appropriate. The certification process itself can then be embarked upon via a suitable accredited third party.²³

The ISO/IEC 27001 certification process looks as the following diagram shows:

Figure 5. ISO 27001 certification process diagram

Source: www.27000.org

²³ www.27000.org
8. ISO/IEC 27000 INFORMATION TECHNOLOGY CERTIFICATION WORLDWIDE

In spite of quite complicated procedure of the certification, certified compliance with ISO/IEC 27001 with certified body is increasingly growing worldwide, even if it is optional. This is being driven by suppliers and business entities that are concern about their information security, demanding more an more often formal certifications.

“According to the ISO survey for 2012, there were nearly 20,000 ISO/IEC 27001 certificates worldwide, a number that had increased by more than 10% since 2011:

![Figure 6. ISO 27001 certificates survey for 2012](source: www.iso27001security.com)

Certification brings a number of benefits above and beyond mere compliance, in much the same way that an ISO 9000-series certificate says more than just “We are a quality organization”. Independent assessment necessarily brings some rigor and formality to the implementation process (implying improvements to information security and all the benefits that brings through risk reduction), and invariably requires senior management approval (which is an advantage in security awareness terms, at least!).”

“In 2006 there were less than 6000 certifications globally, and today that figure is in excess of 20 000. Consider the regional growth of ISO 27001 in 2012:

- Total growth 20 %
- Africa 60 %
- Central/ South America 25 %
- North America 27 %
- Europe 21 %
- East Asia and Pacific 7 %
- Central and South Asia 11 %
- Middle East 23 %

---

24 www.iso27001security.com
According to research conducted by the Rotterdam School of Management, Erasmus University (RSM) and BSI®, which analyzed 12 case companies in China and Europe in-depth and survey responses from 645 businesses world-wide, ISO27001 was seen as having a significant positive effect on increasing information security in an organization.

An important observation is that 64% of those surveyed that had implemented ISO/IEC 27001 stated that data breaches were the most important driving force behind adopting the information security standard.

Although this research was released in 2011, given the increase in frequency and severity of high-profile data breaches of late, the information provided can be seen as being even more relevant now. With ISO 27001:2013 now firmly in place and companies embarking on their transition journeys to the newer, more advanced standard, the benefits listed below will be within reach of a growing number of companies globally.

Of those that surveyed:
- 87% of respondents to recent survey conducted by stated that implementing ISO 27001 had a "positive" or "very positive" outcome on their information security
- 82% of those surveyed noted an increase in the quality control of information
- 39% reported a decrease in down-time of IT Systems and the same number a decrease in the number of security incidents
- 78% reported saw an increased ability to meet compliance requirements
- 44% reported an increase in sales and improvement in competitive advantage
- 56% experienced an increased ability to respond to tenders
- 51% enjoyed increased external customer satisfaction
- 62% increased their relative competitive position
- 26% of respondents said that their ROI and sales increased despite a rise in cost to develop and support IT

Key issue with information security is the limitation of risks and incidents of information (especially data) leaks and breaches. So-called “cyber security” holds the public’s attention and is understandable concern for any organization, as many of them stores huge amount of information in databases. The communication technology and open access to the Internet increases risks in the field of information security, thus organizations face instant threat of information security related incidents and breaches, causing potential serious financial penalties, reputational damages, and even business closures.

By the implementation of ISMS with accordance to ISO 27k standards those organizations are limiting such threats and risks. However, “according to the National Audit Office, the annual cost of cyber crime to the UK is between £18 billion and £27 billion, and yet 80% of the 44 million cyber attacks in the UK in 2011 could have been prevented by simple computer and network “hygiene”. Verizon’s 2012 Data Breach Investigations Report found that 85% of data breaches took weeks or more to discover, and 92% of incidents were discovered by a third party.

The Symantec Corporation and Ponemon Institute’s 2013 Cost of Data Breach report details the three main causes of data breach. In the UK last year, 29% of security incidents were caused by a system glitch, 34% by malicious attack, and 37% by human error. So, to secure your organization properly you clearly need an Information Security Management System which addresses all three of those areas in a single, holistic package. ISO27001 is the only tool which takes an integrated approach and covers those three major facets of cyber security. (…)

The rise of 3G and 4G telephony services and the increase in access to Wi-Fi has meant that mobile access to data has never been more convenient either for the worker or for the criminal. With smartphones, laptops and tablets used daily for work and for leisure, the number of people with access to data on the move presents a golden opportunity for the savvy criminal, whether

---

through the rather old-fashioned means of stealing the device itself (in London alone, the Metropolitan Police reports that 314 phones are stolen each day), or through the exploitation of one of the many documented weaknesses that Cloud computing entails in order to access information via a virtual environment.

The British government, as part of its Cyber Security Strategy, has allocated £860 million to national cyber security up to 2016. The aim of the strategy is to “derive economic and social value from a vibrant, resilient and secure cyberspace” by tackling cyber crime to help ensure the protection of organizations from online threat and promote the UK as a good place to do business online. That same document states (3.7) that “as we all benefit from the use of cyberspace, so we all have a responsibility to help protect it.”

The benefits of implementing an ISMS with accordance to the ISO27k standards will result mainly in the reduction of information security risks and incidents, but also structured framework supporting the processes across all of the organization operations and sites, assistance for the management, provision of a common language and basis for information security with business partners, especially those requiring information security certification, and many more.

9. SUMMARY

To summarize, supply chains are extended wide across any political and geographical borders, involving global enterprises, their local suppliers, as well as firms with diverse business needs, come together for optimum process of the delivery of products and services. The information security in those complex networks is essential for ensuring optimal, and yet secure, flow of products, material, services, cash, etc. Technology, formal regulations, strategy and management aspects of information security in supply chains should be discussed when deciding which way a firm should adopt and customize the solutions to ensure optimal solutions in the matter. This very important issue can be addressed by adaptation of the existing procedures or – that is preferable – customization and constant adaptation of the information security systems, applying framework based on Deming’s Plan-Do-Check-Act schedule.

The number of the ISMS critical factors for success is large, depending on the organization specifics and business objectives. Those could be, e.g. policy, objectives, framework for the ISMS consistent with the organization structure and culture, followed by commitment to all levels of management, to measurement system for the evaluation of the effectiveness and performance of the system. This could be also understanding the requirements, which are described in ISO/IEC 27005, effective information security awareness, based on proper training, educational and motivating program me, clearly setting up and informing all involved parties about the information security procedures, polices and standards in place, thus their information security obligations and rights. There could be even more key success factors, not listed in the ISO27k that could be recognized during the process of designing and implementing ISMS.

The benefits and outcomes of implementing and maintaining certified ISMS are endless, however it is important to remember that humans are major element in data leaks and security breaches, thus information security standards and procedures will not work without this key factor – the people.

Abstract

Introduction to model of security systems based on ISO 27000 family of standards. The focus on the main purpose of the information security standards, including a full listing of the ISO 27000 documentation with description of particular security standards. An official definition of Information Security Management System (ISMS) its terms and purpose. A summary of world survey from 2011-2012 showing the volume of ISO 27000 certifications and describing key factors of successful implementation of IT security standards that protect organizations against potential security threats.

Keywords: Information Security, ISO 27000, BS 7799, Information Security Management Systems (ISMS), (Electronic) Supply Chain

Zarządzanie bezpieczeństwem informacji zgodnie ze standardami ISO 27000 - charakterystyka, zastosowania, korzyści w globalnych łańcuchach dostaw

Streszczenie


Słowa kluczowe: Bezpieczeństwo informacji, ISO 27000, BS 7799, Systemy Zarządzania Bezpieczeństwem Informacji (Danych), (elektroniczne) globalne łańcuchy dostaw

BIBLIOGRAPHY:

2. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
7. ISO/IEC 27006:2011, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
10. www.iso.org
11. www.iso27001security.com
12. www.27000.org