Automating ISO 27001

Abstract

In this article, we describe the PTA threat model library for the ISO 27001 risk assessment standard. The library was found to be productive in shortening risk assessment timetables and building an effective risk mitigation program at a cost that fits the organizations pocketbook.

PTA (Practical Threat Analysis) was first introduced in a paper by Ygor Goldberg titled "Practical Threat Analysis for the Software Industry" published online at www.securitydocs.com/library/2848 in October 2005.

PTA provides a number of meaningful benefits for ISO 27001 risk assessments:

1. Quantitative: enables business decision makers to state asset values, risk profile and controls in familiar monetary values. This takes security decisions out of the realm of qualitative risk discussion and into the realm of business justification.
2. Robust: enables analysts to preserve data integrity of complex multi-dimensional risk models versus Excel spreadsheets that tend to be unwieldy, unstable and difficult to maintain.
3. Versatile: enables organizations to reuse existing threat libraries in new business situations and perform continuous risk assessment and "what-if" analysis on control scenarios without jeopardizing the integrity of the data.
4. Effective: recommends the most effective security countermeasures and their order of implementation. In our experience, PTA can help a firm mitigate 80% of the risk at 20% of the total control cost.

The PTA calculative model is implemented in a user-friendly Windows desktop application available as a freeware at www.ptatechnologies.com.

The PTA ISO 27001 library is available for free download at http://www.controlpolicy.com/PTA_ISO27001_Library.zip; and is licensed under the Creative Commons Attribution License.

The motivation for developing PTA ISO 27001

The importance of ISO security standards

The PTA ISO 27001 library is a full implementation of the ISO 27001 standard and is freely available to any ISO consultant or business wishing to certify to the standard.

ISO 27001 is the information security risk assessment standard for certification and sets the requirements that an organization must fulfill in order to establish an information security management system. The standard continues to gain a reputation for helping organizations improve their business practices and protect information assets.

ISO 27001 is increasingly popular because of compliance regulation and the growing need to reduce the operational risk of information security. In 2006, ISO Secretary-General Alan Bryden underlined the relevance of ISO 27001 for the entire industry including small to medium-sized enterprises (SME):

"SMEs may mistakenly perceive of International Standards as being only for big business and government. In fact, SMEs too can benefit from the state-of-the-art technology and management practices disseminated by International Standards which also open the door to export markets and participation in global supply chains".
http://www.iso.org/iso/en/commcentre/pressreleases/2006/Ref995.html

The role of compliance

Governance and privacy compliance regulation like SOX, GLBH and PCI are fueling demand to improve information security practices. Regulatory compliance has become a trend trickling up and down the supply chain of customers and suppliers. The big wave of customer data breach incidents over the past 3 years has pushed compliance further down the supply chain. Once an exclusive domain of large institutions; many SMEs are now performing security risk assessments as their customers call on them to manage their data better and prove it by certifying to ISO 27001.

The need for effective risk reduction

Despite the importance of privacy and governance regulation, compliance is actually a minimum but not sufficient requirement for risk management.

The question is: **What** security controls should a firm implement after a risk assessment?

An ISO 27001 certification process can be as simple or as involved as an organization wants **but** there are always far more available controls than threats. As a result, organizations, large and small, find themselves coping with a long and confusing shopping list of controls. You can implement the entire checklist of controls (if you have deep pockets), you can do nothing or you can try and achieve the most effective purchase and risk control policy (i.e. get the most for your security investment dollar) with a set of controls optimized for your business situation.

However, implementing additional controls does not necessarily reduce risk.

For example, beefing up network security (like firewalls and proxies) and installing advanced application security products is never a free lunch and tends to increase the total system risk and cost of ownership as a result of the interaction between the elements and an inflation in the number of firewall and content filtering rules.

Firms often view data asset protection as an exercise in Access Control *(Section 11 of ISO 27001)* that requires better permissions and identity management (IDM). However, further examination of IDM systems reveals that (a) IDM does not mitigate the threat of a trusted insider with appropriate privileges and (b) the majority of IDM systems are notorious for requiring large amounts of customization (as much as 90% in a large enterprise network) and may actually contribute additional vulnerabilities instead of lowering overall system risk.

The result of providing inappropriate countermeasures to threats is that the cost of attacks and security ownership goes up, instead of risk exposure going down.

Using PTA to choose cost-effective controls

The PTA ISO 27001 library enables a risk analyst to discuss risk in business terms with her client and construct an economically justified set of security controls that reduces risk in a specific customer business environment. A company can execute an implementation plan for security controls consistent with its budget instead of an all-or-nothing checklist implementation that may “massively erode the competitiveness of the business”: http://www.telberg.com/telbergblog/archives/513-IMA-Support-Much-Needed-SOX-Reform.html

How we created the PTA ISO 27001 library

Mapping ISO 27001 to the PTA threat model

The ISO 27001 contains 185 items in 11 sections, where each item has a reference number, and describes a security policy and a corresponding security control. For example Item 6.1.5 is a "Confidentiality agreements" security policy with the following control: "Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed"

We needed to map the ISO 27001 data model to the PTA threat model that is composed of threats, vulnerabilities, assets and countermeasures. Unlike PTA, the ISO 27001 model does **not** refer to particular threats or assets. We observed that the top-level items in each section mapped nicely to PTA vulnerabilities and that the sub-items were controls that translate directly to PTA countermeasures. For example the ISO item **06.1 "Internal organization; information security is lacking or not well-defined"** is a PTA "vulnerability" mitigated by the PTA "countermeasures":

- 6.1.1 Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
- 6.1.2 Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.
- 6.1.3 All information security responsibilities shall be clearly defined
- 6.1.4 a management authorization process for new information processing facilities shall be defined and implemented.
- 6.1.5 Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
- 6.1.6 appropriate contacts with relevant authorities shall be maintained.
- 6.1.7 appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
- 6.1.8 the organization's approach to managing information security and its implementation (i.e. control objectives, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

After mapping the ISO 27001 data model to the PTA threat model, we then used the import entities from text file functions in the PTA desktop application in order to load an Excel worksheet of the ISO 27001 checklist into a baseline PTA threat model of vulnerabilities and countermeasures and pack it as a PTA library.

Using the PTA ISO 27001 library in a risk assessment project

The standard specifies that the organization should use a systematic approach to risk assessment (method of risk assessment, legal requirements, policy and objectives for reducing the risks to an acceptable level). The PTA ISO 27001 library provides a systematic, and quantitative approach to risk assessment and adds value with an optimized risk mitigation program. Doing a risk audit process with the PTA ISO 27001 library is faster, easier, more robust and lot more fun than with an Excel spreadsheet.

An ISO 27001 risk assessment with PTA involves a two-stage process:

- Stage 1 is a "first cut" review of the existence and completeness of key documentation for Security Policy and Information Security Management System (ISMS). This is done by cycling through the PTA threat model, tagging top-level vulnerabilities with a status and storing appropriate documentation in the model, while linking to the appropriate entity.

- Stage 2 is a detailed, in-depth audit that tests existence and effectiveness of control policies as well as their supporting documentation. Controls that already exist would be marked as "Already Implemented" in PTA Professional Edition countermeasures detail screen. Controls needing work would be tagged with an “action-required” status (see the tagging option of the PTA tool).

PTA ISO 27001 - step by step

Here is how you would use the ISO 27001 PTA library for a risk assessment (after installing the PTA Professional Edition freeware on your Windows PC)

- Step 0 - Fire up the program
- Step 1 - Load the ISO27001.2.thl library into your own threat model or just open the ISO27001.2.thm data model in its entirety
- Step 2 - Create assets with valuations
- Step 3 - Enter the costs of countermeasures; the PTA ISO 27001 library that we provide is agnostic; we understand that each organization has their own estimates of how much a control policy should cost.
- Step 4 - Run the “Optimized Countermeasure” report. You have just built a cost-justified plan of controls compliant with ISO 27001.
- Step 5- Refine the model. Don’t stop here; return to the model periodically and test the effectiveness of your risk mitigation program. For a structured methodology of continuous security assessment see our article “Practical software security assessment” http://www.software.co.il/content/view/195/41/

The power of the PTA ISO27001 library was demonstrated by building a risk assessment model with assets and threats. The sample model is included in the download at http://www.controlpolicy.com/PTA_ISO27001_Library.zip.