Building ISMS system & ISO 27001 certificate

How to get a secure and secure information technology (IT) system? How to prove that our system is reliable? Those are the questions that I worry about when performing my network administration task.

Dr. Trinh Ngoc Minh

How to get a secure and secure information technology (IT) system? How to prove that our system is reliable? Those are the questions that I worry about when performing my network administration task. To answer that question, I became acquainted with many different documents and documents such as ISMS, BS7799, ISO / IEC17799, ISO27001, ISO27002, .

Reading, understanding and imbuing these documents with me is really hard, but I'm not sure if I understand them properly, understand them yet. Up to now, I am responsible for implementing the ISMS system in my unit. In this "jumble", I tried to understand and "enlighten" some things, so I felt the picture became more orderly. I wrote these lines to describe my "debug" process in the hope that it might be useful for someone who is in a situation like me.

The Information Security Management System, or ISMS, can be interpreted as a set of rules (such as policies, procedures, instructions, forms, etc.) implemented in an organization (business, school) to ensure the system information of the organization is safe and secure in a way that is consistent with the business objectives of the organization. I think the above statement is accurate, but it is very abstract, there is much uncertainty about the ISMS. Dissection, explaining the above statement is the basic content of the following section.

The main reason for the existence of a business is business to develop assets (assets). So, it can be said, property is the foundation of the business. What is complicated is that the property is now very rich and exists in many different forms. One can distinguish 6 types of existence forms of different assets:
- Digital information
- Document documents
- Software
- Hardware / physics
- Human
- Additional services

With the classification of assets into 6 categories, we can more easily initiate the construction of ISMS, which lists and evaluates all the assets of the business.

List properties. This is not a difficult job because we can base on the list of hardware equipment, software, a list of documents arising in the operation of the organization, the list of people, names list of services that the organization uses. For example: computer and paper contracts, customer lists, brochures, agency staff lists . After a complete list of assets, we can limit the scope of deployment. ISMS system by eliminating assets that we think do not need to establish a protection system (at least during this period). For example, we have not considered the protection of refrigeration systems, furniture furniture systems or equipment maintenance parts for example. The remaining asset set will be the starting point of all the next steps of the ISMS system.

Asset valuation. With the list of assets to be considered for protection, we must conduct an assessment of their value. This is a difficult task if we consider asset value equal to the cost so we have it. However, this work becomes much more difficult if we take into account (and we need to consider) the value of assets through the

cost that our competitors want it, if we lose or reveal it. For example, network connection diagrams for example. We take some days with some experts to build the diagram so the cost to have it can be calculated and not large. But if we reveal the network map, what consequences will we have? How much is the damage? compromised through which we will lose credibility, lose customers, how much will business damage? If we deduce "too long" then the network map may cost more than the whole . Rolls-Royce and must buy a safe to keep it with the order to open only the director signed. If we consider simply a design with 5 public days * then it is too simple, so it is okay. The difficulty of evaluating asset value is just right. This is the first difficulty to overcome to build the ISMS. Converting from quantitative (how much) to qualitative (very expensive / expensive / cheap .) is an option that can simplify this valuation. Consultants can help us get a moderate and acceptable assessment in most other organizations for our reference.

Identification of hazards (threats). The next step is to identify threats (in English). The idea here is to list the possible threats and threats to the assets we have listed above. We need to list all, including very distant threats like the end of the world, to more specific dangers such as losing passwords, losing laptops. Because the nature enumerates all threats that do not take into account whether it can happen in practice or are only imagined by us, I choose to translate from threat as a threat or threat.

Calculation of risk. So we have two things in our hands, that is the asset list and their value and the set of dangers. We will now list the 'exhausted' form for each hazard with each asset. For each pair (property, risk) we need to make an assessment of how it actually occurs. In scientific terminology, the probability of danger is expressed in terms of how many times it occurs during the month and year. This is a difficult and very technical review. For example, we have 10 employees, each with 2 passwords. So what is the possibility of revealing passwords in the month and year? With our organization's situation, can we expose an average of 1 password in a month? Our list of customers with information about the decision maker and the phone number, their financial ability, will it be revealed once in a year? If we do these evaluations it is great because we can quantify all the risks of security insecurity. In fact, this is not simple, so people can accept qualitative, inaccurate evaluation but easier to do. For example, the loss of passwords occurs at 'high' risk, revealing the payroll for employees with 'low' capabilities.

Damage calculation. If we do well the above steps, the step of assessing the loss of security is only a good problem for arithmetic operations. We can take the value of asset value with the ability to lose them to assess the possibility of losing money in a year if we continue to maintain the organization's activities today. With great risks and high asset value (for example, exposing designs to a fashion design company, for example), there is a lot of damage that can represent the possibility of a company being closed. In this section, we do not have a ready-to-use formula, which we can, and need to, suggest how to fit the organization's needs. Another example is:

Damage = probability of occurrence of incidents + consequences of incidents + lost assets, in which the components of the formula are all characterized for simplicity as 'incident consequences' with point 3 / 2/1 with high / medium / low.

With the results of possible damage calculations, we stand before the question: what should we do now?

Risk reduction measures. Facing the risk of damage assessment, we may have several options:

- *Accept* . Do nothing and accept damage if the risk becomes a reality.

- *Minimize* . Measures should be taken to minimize the possibility of a risk to an acceptable level. This is the most popular option when we begin to build the ISMS.

- *Forward risk* . Find ways to share this risk with other partners. The most common form is to buy insurance so that the insurance organization will share the damage for us if the risk happens.

Solutions to reduce risk. If we choose the mitigation option then we have the next question which is to reduce by what measure. This is the stage where the technician has to get involved. To protect an information or information-related asset, we usually have several measures:

- Building protection system with specialized equipment such as firewall, intrusion detection, intrusion prevention, password card once .

- Increase staff in quantity and / or quality.

- Training staff.

- Develop processes, guidelines and forms for everyone to comply with.

- Determining clear personal responsibility. The fact that everyone loses responsibility when the part does not stipulate that he or she is responsible. Therefore, specifying who is responsible for each asset, each risk if occurring is a mandatory task and is emphasized in the construction of the ISMS system.

- Build a backup system so that if the biggest risks occur, we will not be "closed".

To implement this stage, the best consultant, in my opinion, is ISO27002. This is the collection of best practices, temporary translation is the best behavior, to minimize the risk of information security. This is a set of solutions, tips that have been summarized and experienced in many places in reality to improve the level of safety and security of an IT system. Therefore, we can refer to, consider and choose solutions from ISO27002 to apply for our organization.

Evaluate the cost of the solution and make a decision. Proposing risk mitigation measures, as mentioned above, is a very technical work. Therefore, the cost to implement it is something that technicians have little interest in, or inability to evaluate. Let's not forget that the above measures are to protect the property. And the property has a certain value (usually finite) of it.

We cannot invest 10 dong to protect assets worth 5 VND. If you answer 'maybe' then I think we should go back to the valuation of the property. Perhaps it is more important than what we think or we still lack something? In this step, we will have to make a pure economic problem of how much to invest to minimize losses. Answer the question 'Is this plan economically correct? After reducing the risk and the value can be lost, is the risk and damage remaining acceptable to the organization? ' For each 'no' answer, we must review all the steps performed above, review options and solutions to minimize the risk of its costs. Until all the answers are 'yes', we have completed a plan to build the ISMS system.

Implementing ISMS. After the plan for the construction of the ISMS system includes a list of assets with its value, risks and losses can, options and measures to minimize risks and losses to acceptable levels. For organizations, the next task is to put the plan into practice. The specific activities of this implementation are:

- Redesign, additional investment of technical components.

- Develop regulations, processes, guidelines and, especially, training and implementation guidance so that these regulations are captured by all employees and officials of the organization. This is a very big part because we have to change our habits of thinking, in everyone's actions. At the same time, all members, especially the

leaders of the organization, must understand and strictly implement the regulations of the agency. This is the deciding factor. Deciding that if the leader does not care enough, not spending enough time building the ISMS, the best solution is not to do ISMS until the leadership's thinking changes.

If we go here, I think we have an ISMS system. Whether this system is good or bad, perfect or not, it is difficult to affirm, and it is difficult to make our people, partners, and customers trust in this ISMS system. This is when the certification body (Certification Body) entered. They will check our ISMS system and issue a certificate that the system is 'up to standard' if it meets the requirements of the certificate. So what do you think they will do?

Evaluate and issue ISO27001 certificate. In general, the evaluation process for certification will be done by a competent organization. This organization cannot be the organization that advised us about ISMS to avoid the case of 'just kicking the ball and blowing the whistle'. The evaluation process usually consists of 2 basic stages:

- Evaluate on documents to ensure the adequacy of the document system. In other words, is the 'all but written but done' test done?

- Evaluate in practice to make sure what we intend to do is actually done. In other words, is there a test of 'doing what you wrote'?

I do not go into this testing process (because it is not known), so I only mention one idea in the method that the testing organization provides for certification. With the testing process, the Statement of Applicability (SoA), or implementation clause, plays an important role. In ISO27001, SoAs are expressed in terms of 'Control objectives and controls' and currently ISO27001 has 133 SoA.

Consider the normal learning and exam process. In order to test our knowledge of how much we grasp in the learning process, teachers often do not force us to recount the knowledge we learned described in the document, but make us answer the questions. The questions are the best way to test under a different point of knowledge we learn.

Testing for certification (ie system validation) is best done through the SoA terms. An example of a SoA that requires 'Ownership of assets' is 'All information and assets associated with information processing facilities will be owned by a designated part of the organization'. Provisional translation is required to possess property for the property. In particular, all assets must have a person / organization owned. In other words, there must be no property and no one knows who owns it, is responsible for it. With this test, it can be said that it is easy for the assessor to determine if we are satisfied. With a 133 set of test rules, the reviewer can be assured that all issues related to information security are reviewed. The evaluator is not "swept" by the logic of the ISMS system builder through the route derived from the property. If our activity is not related to a control clause, we may remove it from the scope of the assessment provided that we have to explain why we removed it.

Epilogue. Building ISMS system to get ISO27001 certificate to ensure information security, safety and security are being interested by many Vietnamese enterprises. This is a good signal, a measure of the level of development of IT applications in the socio-economic life of Vietnam. Hopefully, my presentations can help you take an approach, a way of thinking to better understand the important issues, but still quite new to us - ISMS and ISO27001.

Dr. Trinh Ngoc Minh *is currently a lecturer at Saigon Technology Institute - SaigonCTT. Any information exchanged about the article, please contact info@saigonctt.com.vn*