

Case Study

Landsvirkjun produces, distributes and sells wholesale electricity to local public utilities and, under special agreements, to power-intensive industries. Its task is to promote greater utilisation of Iceland’s energy resources and ensure that electricity supply is always sufficient to meet demand.

Landsvirkjun’s mission is to provide its customers with the best energy solutions to create the basis for modern quality of life. Employees and management at Landsvirkjun strive to make it a reliable and environment-friendly company and a leader in its field, and are prepared to tackle new challenges for the benefit of its customers, staff and owners. The guiding aim is to create a flexible company which knows its customers’ needs and fulfils them in accordance with individual requirements. Landsvirkjun is a popular and diversified workplace where employees are able to develop their talents and initiative. The company aims to deploy its initiative, know-how and financial strength to enhance its value still further.

Possible threats

There are many possible threats, such as software breakdowns, resource problems, i.e. lack of electricity and lack of specialist knowledge, natural disasters, human error, organised crime and sabotage. These are some examples of the threats which can affect companies like Landsvirkjun.

$$\begin{array}{r}
 \text{Value of information assets} \\
 \times \text{ Vulnerability*} \\
 \times \text{ Annual frequency of events} \\
 \hline
 = \text{ Expected annual loss}
 \end{array}$$

*Vulnerability: The likelihood of an event causing damage



“Information systems are assets that must be protected. The operation of Landsvirkjun depends on information systems, and any failure of information systems can cause operational losses, harm the image of the company and lead to loss of income. This is why information security is the foundation for the company’s success,” says Bergur Jónsson, Head of the Information System Division of Landsvirkjun.

What is the best way to maximise security and ensure quality?

The best way to maximise security and ensure quality is to conduct the operation in accordance with standards. ISO 17799 and ISO 27001 are recognised international information security standards, as is the ISO 9001 quality standards.

Implementation of information security integrated with the quality system

When the decision was made to embark on the implementation of information security, it was decided to link it with the quality system already in place. Landsvirkjun is a quality-certified company pursuant to ISO 9001. Landsvirkjun management decided to negotiate with Stiki, which had, in the opinion of Landsvirkjun, the experience and knowledge of the implementation of information security systems that Landsvirkjun required.

Emergency plans are vital

The first issue addressed was business continuity management, which is definitely a part of information security management in accordance with international standards in this field. The goal of implementing business continuity management at Landsvirkjun is to protect important operations against major disruptions and crisis. Landsvirkjun believed that with integrated measures through prevention and error recovery, the effects of disruptions and setbacks would be reduced to an acceptable limit.

“Business continuity plans are an integral part of business continuity management. Such plans include categorising operations by importance, specifying parties with well-defined roles during emergencies, carrying out actions in order to recover operations in a timely fashion and testing on a regular basis. Business continuity plans need to be reviewed regularly to remain valid. As Landsvirkjun is engaged in activities where the discontinuation of operations can have serious consequences, we believe that an emergency plan is a priority in the implementation of information security in the company. Through the consultancy provided by Stiki, we have been able to map out our operation in detail and have, in our opinion, extremely good plans for business continuity.”

– Bergur Jónsson.

Following the implementation of the business continuity plan, a risk assessment was prepared for the Information Department of Landsvirkjun.

No matter what

Risk management involves the very basic things that keep a company operating, and business continuity plans are an important link in that chain. Through such plans, Landsvirkjun has assessed what must be done to ensure that any disruption or event has a minimum effect on the safety of employees, property and systems. Business continuity plans also shed light on the skills needed to address issues to protect the reputation of Landsvirkjun and keep it operating.

Professional and successful co-operation with Stiki

“Landsvirkjun places a great deal of emphasis on co-operating with companies and institutions that are leaders in their fields. Stiki’s work practices are in accordance with

Risk assessment using RM Studio

Risk assessment is the evaluation of threats posed to information and information processing, their effects, sensitivity to them and the probability of the risks being realised. This includes assessment of the risk of an outside party accessing information, making changes to such information or otherwise compromising its security. Risk assessment also covers the scope and results of the threat with reference to the nature of the information being used. The goal of risk assessment is to provide criteria for selecting security measures. The Landsvirkjun risk assessment was prepared using software provided by Stiki, RM Studio, which facilitated the assessment process and saved substantial time.

the high standards we set for our suppliers and partners. The fact that Stiki is itself a certified company is important to us, as we believe that it is necessary for a consultancy company in the field of information security to ‘practice what it preaches’. Landsvirkjun is very pleased with the professional work practices of Stiki. All timetables were met, and work on the project was tailored and organised. We also feel that the extensive and excellent knowledge Stiki employees have is important, and value their ambition to ensure that the customer achieves success. The fact that the implementation of information security was such a success has encouraged us to continue on this path. The Landsvirkjun Information Division now plans to obtain certification in the field of information security by the beginning of 2007,” said Bergur Jónsson.



Stiki Software Engineering and Information Technology Consultancy

Sidumuli 34, IS-108 Reykjavik, Iceland
Tel. +354 570 0600, Fax +354 570 0601
www.stiki.eu - stiki@stiki.eu

STIKI operates an Information Security Management System and a Quality Management System that fulfills the requirements of the standards BS 7799 and ISO 9001 as certified by the British Standards Institution, BSI.

