

## Case Study

Sjóvá is the largest insurance provider in Iceland and is currently the eleventh most valuable company in the country measured by market capitalisation. Organic growth has been emphasised but opportunities for growth through mergers and acquisitions have been exploited.

Sjóvá has its headquarters in the capital of Reykjavík but service to customers far and near is provided through a net of nearly 60 tied agents around the country.

Sjóvá currently employs 180 people.

### Increased requirements for data security

With software and computers becoming ever more powerful, and with the growing number of network connections and increased Internet access, the need to secure data and equipment keeps growing. At the same time, great strides have been made in developing the security of information systems, a fact evidenced by emerging international standards in the field over recent years. Legislative requirements in this field have also increased, especially regarding the treatment of personal information.

### Data security is a key issue at Sjóvá

Sjóvá places high emphasis on security and confidentiality in the acquisition and handling of personal information. The information obtained by the company is used only when assessing insurance claims, in the settlement of claims for compensation, in information provision to customers and in the ordinary course of the company's operations. Information is never released to a third party without the consent of the customer, except as provided for by law or a court ruling.

### Encryption of electronic communications.

The SSL Standard, an approved security standard, is used when confidential information is sent over the Internet. By using the standard, all communications between the user and sjova.is are encrypted, thus ensuring that no-one can access data sent to the company.



*"As a leading insurance company, information security is of the greatest importance to us. Our goal is to provide exceptional services to the company's customers and to safeguard the information they entrust to us. Surveys among the company's beneficiaries reveal that 98% are pleased with our services, which, in our opinion, are good results." Þór Sigfússon CEO of Sjóvá.*

### Surveillance authorities lay down requirements.

Surveillance authorities establish requirements that insurance companies and other entities holding personal information must meet to ensure data security. The Financial Supervisory Authority issues guidelines to companies in the financial sector about such security, and the Data Protection Authority requires companies that use personal information to safeguard data, prepare risk assessments in the processing of information, have processes and rules of procedures written and presented in an organised manner and, finally, prepare business continuity plans, or so-called emergency plans.

## THE ROLE OF SJÓVÁ

Sjóvá's role is to insure the valuables people have in their lives. In doing so, the company wishes to participate in creating and supporting the quality of life that people seek.

### The principal goals and policies of Sjóvá are:

- Superior services
- Straightforward and economic operation
- Energetic and enterprising employees
- International operation

The management of Sjóvá decided to react immediately to the guidelines issued by the Financial Supervisory Authority and the Data Protection Authority and to implement information security in accordance with the Information Security Standard BS 7799. The company decided that it would seek co-operation with Stiki with regard to the implementation of information security.

### **The simultaneous implementation of information security and quality system**

The decision was made to implement a quality system in accordance with the ISO 9001 standard at the same time. The first step was the preparation of a web-based organisational manual that merges the quality and security manuals. Sjóvá had a substantial amount of material ready and possessed the professional knowledge, while Stiki consultants provided assistance in transforming rules of procedure and processes into practical forms and providing the specific processes relating to the requirements stipulated by the standards.

### **Plans for business continuity**

An important part of the operation of an insurance company is the availability of plans for business continuity. Sjóvá had already prepared contingency plans which were intended to revive the operation of the company in the wake of a possible operational disaster. The emphasis in contingency plans is always on the information assets of the company in question and their protection. The representatives of Sjóvá were given a presentation by Stiki employees as regards their methodology in the preparation of plans for business continuity, and an improved contingency plan was updated in accordance with the templates and documents designed by Stiki.

### **Risk assessment using RM Studio ®**

A risk assessment, moreover, was prepared for Sjóvá's information processing. An effort was made to expose all aspects affecting the security of the systems falling under the assessment's scope. The software Stiki OutGuard (now RM Studio®) was used. The software was developed by Stiki and is intended to perform risk assessments in accordance with the requirements of the Security Standard BS 7799 (now ISO 27001). The risk assessment was performed under the guidance of consultants from Stiki during work meetings. The Sjóvá safety officer recruited other Sjóvá employees as needed.

### **Proper project management is a prerequisite for success**

On the part of Stiki, the project was managed in accordance with PRINCE2 methodology and used the document templates this method provides. The risk assessment was prepared during work meetings chaired by a consultant from Stiki. Consultancy, management and procedures provided by Stiki were exemplary, as was the professionalism of its employees, as well as their attitude and services during the processing of the project. Account was taken of the special needs of the company in the analysis of procedures and in the preparation of manuals and plans. The project was on budget, although it exceeded the timetable slightly owing to the annexes to the organisational manual. Stiki deserves high praise for its part in the preparation of the organisational manual, risk assessment and the plans for business continuity at Sjóvá.

## **What is risk assessment?**

Risk assessment is the total process of risk analysis and risk weighting in accordance with standards, and the evaluation of risks to data and data 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 data, changing them or otherwise compromising their security. Risk assessment also covers the scope and results of the risk with reference to the nature of the data being used. The goal of risk assessment is to provide a basis for selecting security measures. Risk assessments are reviewed annually.



**Stiki ehf.**  
**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 ISO 27001 and ISO 9001 as certified by the British Standards Institution, BSI.

