# Information Security System at Schenker Poland

## History and achievements

Quality and availability of information are key factors of effective integrated supply chain management. Logistic operator, being a connecting link within the chain, has to provide reliable and precise data for its participants. It means, first of all, reliable work of all critical IT systems. It is of fundamental importance for quality of rendered services.

Schenker Poland started the process of building an IT security system in 2002, as Spedpol during that time. The starting point were detailed analyses of the former IT attainments and projects and best practises of ISO 17799 standard. Their conclusions set the direction for an Information Security Policy (ISP) developed afterwards. From the beginning the whole undertaking has been supported by IBM consultants.

Due to the ISP, every IT system in Schenker should have defined security requirements regarding availability, confidentiality and integrity that, from the business perspective, are perceived as quality requirements of those systems. The Information Security System is mainly focused on limiting operational risk of computerized business processes. Security controls for the IT systems are designed on the basis of result of computer systems' risk analysis.

In order to ensure effective implementation of the ISP, an Information Security Officer has been appointed. He is independent of the IT team and reports directly to President of the Management Board. On the branch level, Branch System Security Coordinators have been appointed. Their main task is to actively build awareness of information security requirements at branch level.

Also there is a deep involvement of the IT team. System administrators are directly responsible for security and quality of work of their computer systems. Intensive engagement of the IT manager and his team in the process of building the Information Security System can be seen as one key factor for success of its effective performance. Strong support and continuous interest of the President of the Management Board - Janusz Górski in progress of works in the field of security is another important key success factor.
A natural consequence is undertaking actions in order to acquire the ISO-27001 certificate (a successor BS-7799-2) in the field of information security. In 2006 we plan to acquire the ISO-27001 certificate.

## Audit

In mid 2005 **Alexander Tsolkas** conducted a preliminary assessment of conformity of local achievements with information security requirements defined in the Corporate

IT Security Policy. The preliminary assessment confirmed the high level of conformity of local solutions to corporate requirements.
Recommendations were proposed for all the discrepancies and the majority of them have been implemented. Alexander Tsolkas also attended the complete De Norske Veritas certification audit in 2006 and described all central security processes and the risk management system of Schenker.

A formal DB audit started in February 2006. Auditors, apart from assessment of conformity with the Corporate IT Security Policy, focussed also on understanding really existing threats and risks to business processes supported by IT systems.

Understanding of the business context of IT systems made it easier finding such discrepancies that are closely connected with real business risks and proposing the most accurate recommendations.
It is worth stressing that an external audit has a very important advantage. It helps keep proper distance and, what is connected with it, objectivism of assessment. The auditors: Christopher Thompson and Rolf Schnarr presented openness and understanding for our specific local conditions.

Summarising, one should state that results of the external audit conducted in the above mentioned way are very helpful in improving of the information security system and the report itself confirmed the right direction of actions in this field chosen as early as in 2002.
Despite high scores of our information security system we are conscious that it has to be constantly adapted to ever appearing new threats and business risks connected with them.