UIMC®
DR. VOSSBEIN
GMBH & CO KG

# Company Profile
## Products and Services

Telephone: 0049 202 - 265 74 - 0
Telefax: 0049 202 - 265 74 - 19
E-Mail: consultants(at)uimc.de

Nützenberger Strasse 119
42115 Wuppertal
Web: www.uimc.de

# UIMC – Our Business

The beginning of our activities is not clearly to identify: When our senior partner R. Vossbein left his leading position in a multinational corporation and joined a University as professor of economics, he stayed in close contact to industrial institutions and performed a lot of projects in co-operation with a number of well distinguished companies. Later he realised a partnership with Jörn Vossbein, who specialised in computer science and IT-security. Co-operation with other partners allowed soon to enlarge the variety of services. A third partner Heiko Haaz joined in the beginning of 1999, who worked for the senior partner since several years in his university functions.

A speciality of our business are tool supported analyses and integrated concepts. The basis is formed by a shell, which permits to be “filled” with varying contents for management investigations, security analyses, data protection audits and others. An expert system, based on the shell will be realised in 2000.

# Your Representatives:

## Reinhard Voßbein, Prof. Dr.

Dr. Reinhard Voßbein is professor of Business and Management Studies (specialising in organisation, planning and business computing) at the 'Universität Essen GH'. He is a longstanding member of the Board of the GDD (Gesellschaft für Datenschutz und Datensicherung), consultant for the ISA (International Security Academie), and member of the advisory board for the magazines 'KES' and 'IT Sicherheit'.
He has had various books and newspaper articles published including, amongst others, ones about company management controlling and industrial security management. He has many years experience as a consultant to various industrial sectors and enterprises of varying sizes.
Responsibilities include:

- management and strategic consultancy
- specialised further education
- the credit sector
- the public-service sector

## Jörn Voßbein, PhD

Jörn Voßbein wrote his dissertation for his doctorate at the University of Cologne on an empirical theme researching the construction of security concepts for computer.
He has taken an active roll in many consultancy projects dealing with company organisation and the industrial insurance security sector (banks, industry, insurance, and other businesses).
He has various books and magazine articles to his name including, amongst others, ones dealing with industrial insurance security management themes.
Responsibilities include:

- consultancy and auditing using specialist tools
- basic further education
- software projects

## Heiko Haaz, PhD

Heiko Haaz wrote his dissertation for his doctorate at the 'Universität Essen GH' about the tasks and requirements of a data protection consultant.
He has lead many consultancy projects concerning data protection in the health care services (procedural analysis, and assessment of data protection legal requirements and statements).
His various publications of books and newspaper articles include, amongst others, ones about data protection.
Responsibilities include:

- data protection consultancy and proposals
- data protection education
- the health care services sector

# Services Offered

## Individual Consultancy and Conceptualisation for:

- Business administration
- Controlling processes
- Organisation of the implementation and running phases
- Planning and budgeting
- Management of computer systems
- Marketing

## Standardised Consultancy and Conceptualisation:

- UMC – organisation and management check up
- Si-SSA – security weakness analysis for computer systems
  - general security check-ups
  - sector specific security check-ups
- DC – data protection check-up in accordance with data protection law

## Specialities

- Information Systems security
- Data protection consultation as per BDSG (the German Data Protection Act)
- Information systems revision and auditing
- Data protection and IT security in the health sector
- External data protection proposals
- Drawing up and checking of duty booklets

## On and Off Site Further and Advanced Training

- Business administration
- Company planning and budgeting
- Information system planning
- Control processes
- Information system control processes
- Conception of security concepts
- Information system work place security

## Software Solutions for Internal and External Consultancy and Auditing Projects

- Database management tool
- Template generator
- Question generator
- Connections manger
- Inquiry tool
- Evaluation tool

# UTAB – the tool for rational analysis and report generation

## Objectives of the System:

Design a tool for structured analysis

- The ability to adapt to analyse or inquiry lead interrogation
- The possibility of using inputs from various fields with similar standards
- Rational computer-aided generation of inquiry results and answers
- Automatic evaluation of analysis results
- Connection or networking of answers from different sections
- Computer-aided elimination and reappraisal of weaknesses
- The ability to assign the weaknesses exact review measures
- Rationalise the work necessary by making available intelligent text modules
- Undertake the formal revision and amendment of all answer and evaluation statements
- Inclusion of additional pre-defined modular or individually defined statements

## Implemented Task Areas

At the moment the following task areas have been implemented in the UTAB by UIMC:

- Analysis and evaluation of risk and potential
- Security target system work with help from security system scenarios
- Data protection audits and check-ups in accordance with the German Data Protection Act (BDSG)
- Auditing according to the guidelines of the FAMA
- Y2K ‘final check-up’

# Strategy Conference
# (as a company internal workshop)

## Industrial Insurance Security Strategy and Goal Setting, Development, and Adoption

## Order of Events for the Strategy Conference / Workshop

- Explanation of the purpose of the conference/workshop, presentation of the methodology
- Elaboration of the strategy scenarios
- Elaboration of the operational scenarios
- Issuing the results report
- Discussion on the security goals at a strategic level
- Establishment of the basic security goals
- Issuing the results report
- Discussion on the possibilities in detail

## The Stated Objective of the Workshop: Strategy and Goal Definition for IT Security

1. The workshop should discuss the various objectives and possibilities within the company.
2. Based on this discussion, a security strategy will be developed.
3. Based on the strategy, a required security level will be established in accordance with the company wide valid security objectives.
4. After establishing the required level of security there follows an ascertainment of graded partial levels with regard to specific security interests within the bounds of partial security regions.
5. The final result is the adoption of an accepted, company specific statement of the required security levels specifying at least two hierarchical levels – the first being of strategic character and the second having operational character.
6. From the foundation of the company specific, two-level security statement, it is possible, outside the confines of the workshop, to create a concrete task catalogue, a duty booklet, and develop other standards.

# A Si-SSA - Security Vulnerability Analysis - consists of:

- Establishing the IT security problems
- Deciding to carry out a security weakness analysis
- The adaptation of the Si-SSA to fit in with the companies existing policies
- Elaborating the security strategy and setting goals
- Specifying the extent of the Si-SSA (i.e. specifying the Si-SSA modules)
- Investigating the requisite areas requiring special analysis
- The execution of the basic analysis
- Utilising the results of the investigation
- Determination of the eventual, high risk factor programs – determination of residual risks I
- If necessary, executing a risk analysis
- The determination of residual risks II
- Working out the residual risk plan
- Drawing up a security weakness plan
- Making a list of points of weakness requiring action and/or removal
- The formulation of the plan for weakness exclusion
- Drawing up the overall plan
- Implementing the overall plan

# Areas of Special Analyses

Special areas for thorough weakness analyses (using a checklist system consisting of, at present, about 2,000 questions)
The questions cover the following areas:

- The organisation of the company
- Security measures with reference to employees
- Computer system technology and host computers
- Build in security and catastrophe recovery provisions
- Security measures
- Data storage devices
- Insurance
- Networks i.e. LANs
- Data protection in accordance with BDSG
- SAP
- Security for outsourcing
- Checking the DP system in accordance with FAMA
- OPDV (utility for testing the DP routines)
- The Internet and firewalls

# Criteria for Security Audits

## Objectives:

A security audit should produce a snapshot of the present state of an institutes IT system security and as far as possible suggest improvements and/or augmentations of security level. Because of the need to take into account company specific goals and government regulations (e.g. the data protection act, or commercial confidentiality regulations) the audit targets need to be tuned to match each individual institution.

## Conditions for a Security Audit

To achieve these objectives the following conditions need to be meet by a security audit:

1. The security audit starts by defining a target security level
2. It delivers the basis for the testing criteria
3. It delivers and verifies critical objective criteria for not passing a test
4. These ascertainments are verifiable
5. It delivers a comprehensive, objective oriented testing platform customised for the individual institution
6. It is capable of unearthing, in an organisation, existing weaknesses in order to formulate improvements
7. It permits an evaluation of the diagnosis
8. It makes available clear, comparable test results
9. The security audit serves as the foundation for a routine security certification
10. It is possible to carry out a temporal comparison over a number of years
11. The audit system is scalable, that is, the results from sections of a large firm can be concatenated to generate a overall result
12. It can't be misused as an alibi, but facilitates a use as criterion for marketing or quality assurance
13. In order to attain or hold on to a routine security certificate the security audit should be periodically reiterated