Das Gesamtsystem des UTAB

Philosophie des Modells

Das **UTAB** - **U**IMC **T**ool für **A**nalyse und **B**erichterstattung - ist ein komplexes, modular aufgebautes Programmsystem, welches vornehmlich der Rationalisierung von Beratungsprozessen dient. Es setzt voraus, daß die Teilprozesse

- Analyse/Erhebung
- Auswertung
- Berichtserstellung

der Beratungsarbeit teilweise bis weitgehend automatisiert werden können und die Prozesse der

- Konzepterstellung
- Umsetzungsvorbereitung sowie
- Umsetzungsverfolgung

computergestützt ablaufen sollten, um Zeit und Ressourcen bei hoher Qualität der Ergebnisse zu sparen.

Ziel des Systems:

- eine Shell für strukturierte Analysen, speziell Unternehmens- aber auch technische Analysen zu bilden
- analyse-/erhebungsbedingte Frageprobleme den jeweiligen Erfordernissen entsprechend hochflexibel anpassen zu können
- durch die erforderliche Flexibilität Inputs verschiedener Gebiete gleichen Standards zu ermöglichen
- die Erhebungsergebnisse/Antworten rationell computergestützt erfassen zu können
- die Analyseergebnisse einer automatisierten Auswertung zuzuführen
- die Antworten verschiedener Teilgebiete zu verbinden/vernetzen
- Schwachstellen computergestützt heraus- und aufarbeiten zu können
- den Schwachstellen punktgenau Maßnahmen zur Beseitigung zuordnen zu können
- jeweils ”intelligente” Textbausteine zur Rationalisierung der Arbeit vorzuhalten, die sowohl aus Antworten/Bemerkungen als auch aus anderen Quellen zur Verfügung gestellt werden
- die formale Überarbeitung und Ergänzung aller Antwort- und Auswertungsaussagen vorzunehmen
- die Einbringung zusätzlicher Aussagen zu gestatten, die sowohl als Bausteine vorliegen können als auch als individueller Freitext eingebbar sind.

Grundsätzlich soll die qualitative und qualifizierte Bewertung und Interpretation in der Hand des geschulten, sachverständigen Beraters verbleiben, dessen Arbeit durch die Standardisierung, Rationalisierung und Computerunterstützung eine deutliche Effizienzerhöhung erfährt. Ziel dieser Rationalisierung und Effizienzerhöhung ist eine Kostenreduktion für die Erarbeitung von Analysen und Analyseauswertungsergebnissen. Die Standardisierung und Normierung erlaubt insbesondere auch, identische Analysen in unterschiedlichen Organisationseinheiten (Tochterfirmen, Filialen etc.) vorzunehmen mit dem Ziel, intraorganisationelle Vergleiche zu erhalten. Auch wenn zum Zweck der Auditierung ständig gleiche Tatbestände erhoben werden müssen, ist eine hohe Eignung der Shell für derartige Einsätze gegeben.

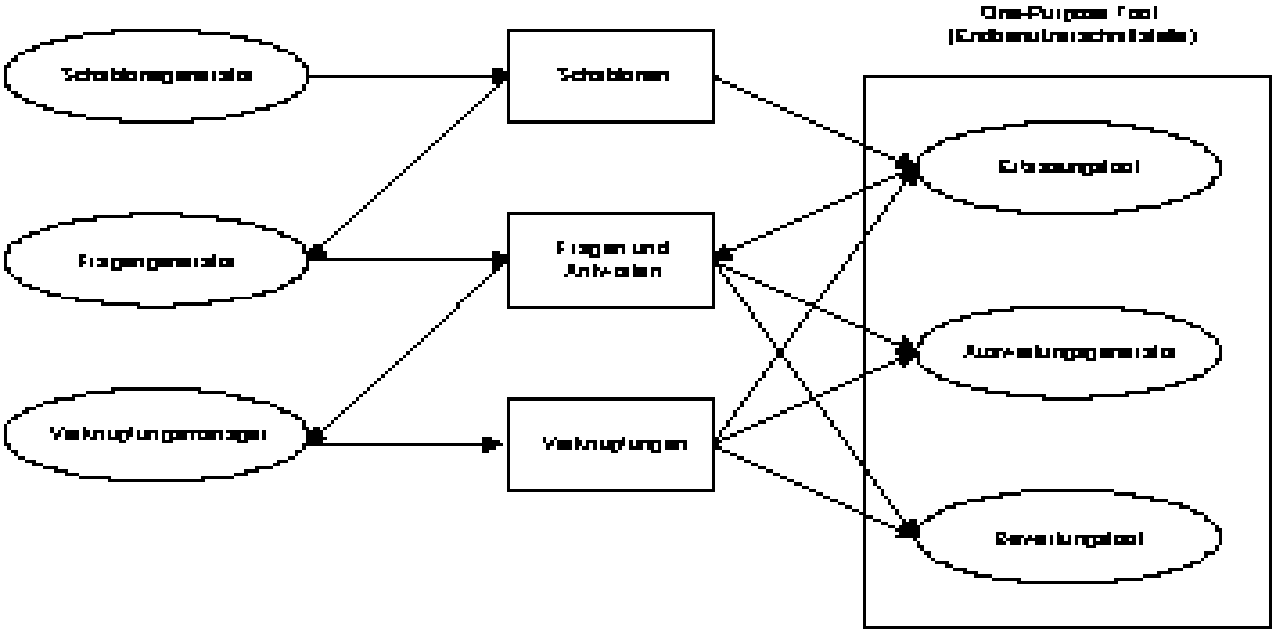
Der Aufbau des Gesamtmodells (s. Abbildung)

Das Gesamtmodell, dessen Konzeption aus der folgenden Abbildung hervorgeht, besteht nach dem derzeitigen Stand aus folgenden Modulen:

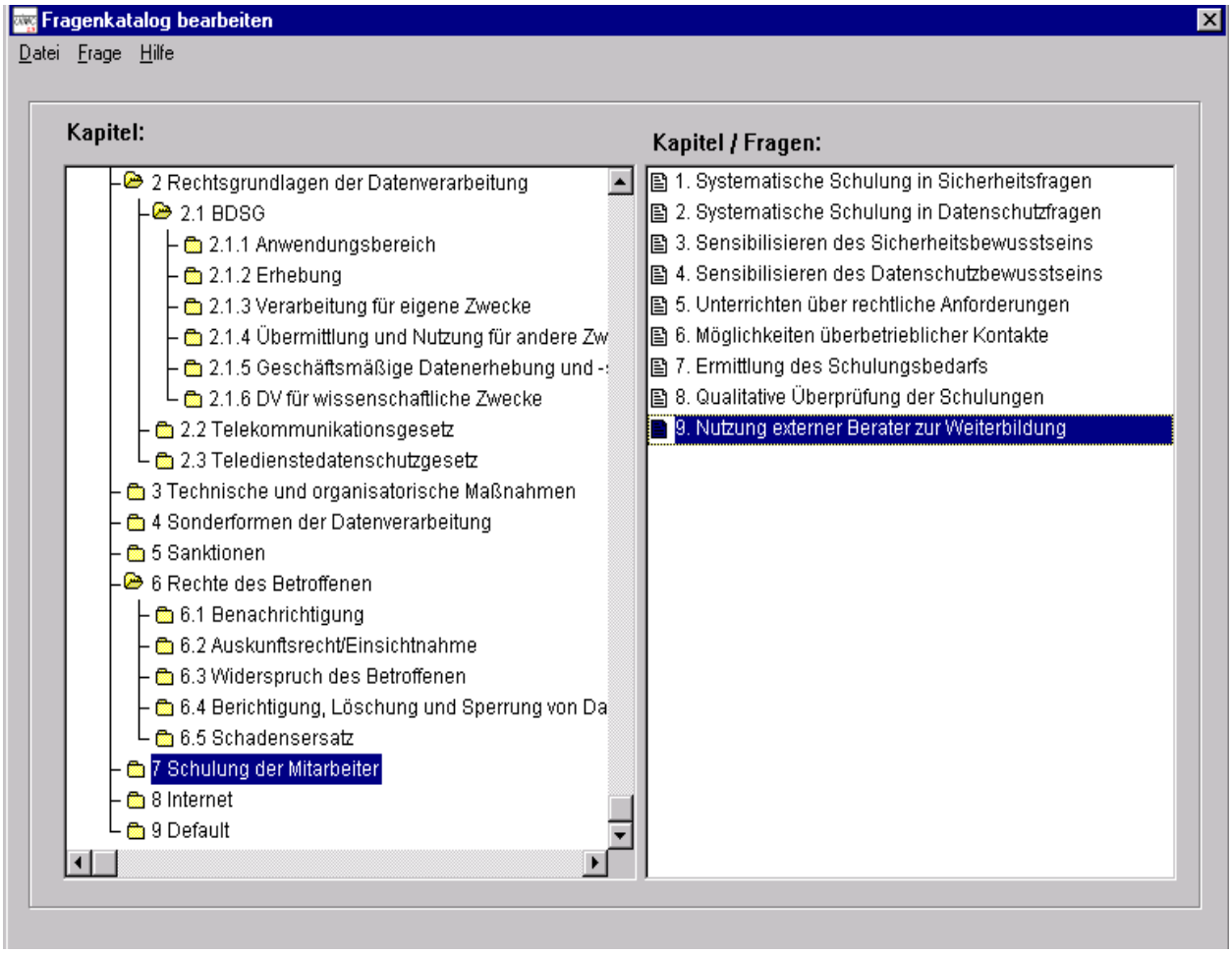
1. einem Schablonengenerator, der untersuchungsspezifische/themenspezifische Frage- und Analyseformen erzeugt,
2. einem Fragengenerator, der auf der Basis erzeugter Schablonen und gewünschter, vorstrukturierter Analysefragen die Fragen erstellt,
3. einem Antworterfassungssystem, welches die bei einer Analyse erhaltenen Antworten enthält,
4. einem Berichtserstellungssystem, welches den Status-quo-Bericht auf Basis der beantworteten Fragen erzeugt,
5. einem Verknüpfungsmanager, der
   - Verknüpfungen auf Basis der Prädikatenlogik zur Verfügung stellt,
   - Plausibilitäten berücksichtigt,
   - Redundanzen in Fragen und Antworten beseitigt bzw. offenlegt,
   - das Stellen redundant im System mehrfach benötigter Fragen verhindert,
   - Mehrfachauswertungen zu unterschiedlichen Kriterien ermöglicht (z.B. festgestellten Schwachstellen sinnvolle Maßnahmen zuordnet),
6. einer Schablonendatenbank, die sämtliche erarbeiteten Schablonen vorhält,
7. einer Fragendatenbank, die die für das jeweilige Projekt/Gebiet erzeugten Fragen vorhält,
8. einer Antwortdatenbank, die intelligente Textbausteine zur Verfügung stellt für z.B.,
   - Status-quo-Bericht,
   - Schwachstellenbericht,
   - Katalog von Umsetzungsmaßnahmen und -Aktivitätenanweisungen.

Ein Expertisesystem, welches Verkettungen und Vernetzungen von Fragen und Antworten vornimmt und damit wesentliche Grundlagen eines teilautomatisierten Konzeptes enthält, ist in Vorbereitung. Das dazugehörige Pflichtenheft ist erstellt.
Ein Auswertungssystem, welches quantitative Auswertungen und Aggregationen ermöglicht, ist in Form einer Projektstudie angedacht. Die Möglichkeit einer Realisierung wurde geprüft und ist gegeben.

Aufbau des Gesamtmodells / des Tools



Beispiel für ein Fragesystem



Realisierte Einsatzgebiete

Die UIMC hat zur Zeit folgende Einsatzgebiete für das obige System realisiert:

- Risiko- und Potentialsanalyse und -bewertung von Unternehmen und Unternehmenseinheiten
- Strategieanalysen und -szenarien
- Führungs- und Organisationsanalysen
- Unternehmens- und Management-Checkup UMC
- IV-Sicherheitsschwachstellenanalyse (Si-SSA)
- Sicherheitszielsystemerarbeitung mit Hilfe von Sicherheitsszenarien
- Datenschutz-Audit/Checkup gemäß Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze u. a. Datenschutzgesetze und -verordnungen DSC
- Risikoanalysen und -bewertungen von IT-Risiken
- Prüfungen nach den Grundsätzen der ISO-Zertifizierung (ISO/IEC 17799 und ISO/IEC 27001)
- Risiko- und Potentialsanalyse und -bewertung im Sinne des KonTraG

Angedacht wurden bisher zusätzlich folgende Einsatzgebiete:

- Sicherheitsprüfungen im Rahmen von Gebäudesicherungsvorhaben
- Zertifizierungsprüfungen (Audits) im Gesundheitswesen
- Auditierungen nach den Grundsätzen der GoBS und nach IDW-Standards

Im folgenden soll für drei Haupteinsatzgebiete

1. IV-Sicherheitsschwachstellenanalyse (Si-SSA)
2. Datenschutz-Audit/Checkup gemäß Bundesdatenschutzgesetz (BDSG) DSC
3. Unternehmens- und Management-Checkup UMC

anhand der Strukturen die Mächtigkeit der realisierten Toollösungen aufgezeigt werden.

Haupteinsatzgebiet IT-Sicherheitsschwachstellenanalyse

Inhalte des Si-SSA-Konzeptes

Stand der Sicherheit basierend auf ISO/IEC 17799
mit den Aspekten:

- Sicherheitspolitik
- Organisation der Sicherheit
- Einstufung und Kontrolle der Werte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Einhaltung der Verpflichtungen
- Ausgliederbare Risiken
- Sicherheitszielsystem
- Management der ommunikatio- nund des Betriebs
- Zugangskontrolle
- Systementwicklung und –wartung
- Management des kontinuierlichen

Spezialgebiete für tiefergehende Schwachstellenanalysen

(Checklistsystem mit z. Zt. ca. 2.100 Fragen)

- Organisation
- Mitarbeiterbezogene Sicherheitsmaßnahmen
- Systemtechnik/Host
- Bautechnische Sicherheit/Katastrophenvorsorge
- Versorgungstechnik
- Datenträger
- Versicherungen
- Netzwerke/LAN
- Datenschutz gem. DSG
- SAP
- Sicherheit beim Outsourcing
- DV-Systemprüfung gemäß FAMA
- OPDV
- Internet/Firewall
- Standardsoftware

Beispiel für die Substruktur zweier Vertiefungsmodule: Organisation und Netzwerke

Organisation

- Grundlegendes
- Sicherheitsbeauftragter und Kontrollinstanzen
- Beschaffung und Wartung von Hard-, Soft- und Netware
- Softwareentwicklung und Freigabe
- Allgemeine Benutzung des IT-Systems
- Informationsverarbeitung
- Informationseingabe
- Informationsausgabe
- Bedienerloser Betrieb

Netzwerke

- Organisation
- Personelle Sicherheit
- Physische Sicherheit
- Zuganssicherheit
- Zugriffs-/Übertragungssicherheit
- Protokollierung/Viren
- Datensicherung
- Verfügbarkeit

Gebiete des Datenschutz-Checkups

1 Grundlage
1.1 Allgemeines zum Datenschutz
1.2 Allgemeines zur IT-Sicherheit
1.3 Stellenwert des Datenschutzes
1.4 Vorabkontrolle
1.5 Kontrollorgane
1.6 Stellenbeschreibungen
1.7 Einwilligung
1.8 Datengeheimnis
1.9 DV-Systeme

2 Rechtsgrundlagen der Datenverarbeitung
2.1 BDSG
2.2 Telekommunikationsgesetz
2.3 Teledienstedatenschutzgesetz

3 Technische und organisatorische Maßnahmen
3.1 Zutrittskontrolle
3.2 Zugangskontrolle
3.3 Zugriffskontrolle
3.4 Weitergabekontrolle
3.5 Eingabekontrolle
3.6 Verfügbarkeitskontrolle
3.7 Informationsausgabe
3.8 Allgemeine Informationsverarbeitung
3.9 Dokumentationsrichtlinien
3.10 Kontrolle zum Trennungsgebot

4 Sonderformen der Datenverarbeitung
4.1 Datenverarbeitung im Auftrag
4.2 Beobachtung öffentlich zugänglicher Räume

5 Sanktionen

6 Rechte des Betroffenen
6.1 Benachrichtigung
6.2 Auskunftsrecht/Einsichtnahme
6.3 Widerspruch des Betroffenen
6.4 Berichtigung, Löschung und Sperrung von Daten
6.5 Schadensersatz

7 Schulung der Mitarbeiter

8 Internet

Einzelgebiete für Audits

- Organisationsanweisungen und Richtlinien
- Dokumentationen
- technische und organisatorische Sicherheitsmaßnahmen
- Räumlichkeiten
- Fachkenntnisse des Datenschutzbeauftragten
- Sensibilisierungsgrad auf Führungs- und Ausführungsebene
- Personelle Sicherheitsmaßnahmen/ Schulungskonzepte (auch Planung)
- Aufbewahrung von Datenträgern

Haupteinsatzgebiet
Unternehmens- und Management-Checkup

1. Unternehmenskonstitution mit den Gebieten:
   - Rechtsform
   - Unternehmensverbindungen
2. Unternehmensführung mit den Gebieten:
   - Strategisches Konzept
   - Führungsstil und -methoden
   - Zielsetzungen und Vorgabesysteme
3. Unternehmenscontrolling mit den Gebieten:
   - Controllingorganisation
   - Controllingverfahren
   - Berichtswesen- und Kontrollorganisation
   - Rechnungswesenorganisation
4. Organisation mit den Gebieten:
   - Aufbau und Strukturorganisation
   - Stellenorganisation und Funktionen
   - Wesentliche Abläufe (unternehmenskritische Prozesse)
5. Planung/Budgetierung mit den Gebieten:
   - kurz-, mittel- und langfristige Planung
   - Budgetierung
   - Planrevisionsverfahren
6. Informationssystem mit den Gebieten:
   - computerisiertes/technologie-gestütztes Informationssystem
   - Durchdringungsgrad und Prozeßunterstützung
   - IV-Sicherheitskonzept
7. Marketing mit den Gebieten:
   - Stand der Marketingkonzeption
   - Marketingorganisation
   - Marketingplanung
   - Produktentwicklung und Produktmanagement
   - Werbung und Verkaufsförderung
8. Verkauf und Distribution mit den Gebieten:
   - Verkaufsorganisation
   - Distributionsorganisation (Verfahren und Wege)
   - Kundenpflege und -betreuung
9. F+E (Entwicklungsbereich) mit den Gebieten:
   - Organisation der F+E
   - eingesetzte Methoden
   - Ergebnisse und Erfolgskontrolle
10. Beschaffung mit den Gebieten:
    - Beschaffungspolitik und -entscheidung
    - Beschaffungsmarktforschung
    - Beschaffungsverfahren
11. Logistik (Lager- und Lieferwesen) mit den Gebieten:
    - Beschaffungslogistik und innerbetriebliche Logistik
    - Absatzlogistik
    - Verfahren der Logistiksteuerung
12. Produktionsorganisation mit den Gebieten:
    - Verfahren der Produktionsplanung und -steuerung
    - Produktionsorganisation
    - Produktionsabwicklung
13. Personalwesen mit den Gebieten:
    - Personalplanung und -beschaffung
    - Personalverwaltung
    - Personalentlohnung und -anreizsy-

Vorteile der Nutzung der UIMC-SI-SSA

Die folgende Aufstellung basiert auf einem konkreten Fall. Der Einsatz wurde hier flächendekkend für ein stark dezentralisiertes und in eine Vielzahl von Organisationseinheiten gegliedertes Großunternehmen auf einem Spezial-/Teilgebiet vorgesehen. Die Argumente quantitativer und qualitativer Art lassen sich jedoch übertragen. Es erwies sich als sinnvoll, eine Unterscheidung nach rechenbaren und nichtrechenbaren Vorteilen vorzunehmen.

Es lassen sich folgende rechenbare Nutzen beim Einsatz feststellen:

	Anz. Organisationseinheiten.	Anz. Tage	Wert in EUR
Einsparung von ca. 0,5 Tage je Erhebung	100	50	20.000,00
Einsparung von ca. 1 Tag je Auswertung	100	100	40.000,00
Ergebnisdiskussion 0,5 Tage je Diskussion	100	50	20.000,00
Nebenkostenersparnis je Erhebung und Auswertung EUR 100,00 (Schreibarbeiten etc.)	100		10.000,00
Einsparungen bei der Umsetzung und Ergebnisüberwachung 3 Tage je Org.-einheit	100	300	120.000,00
Summe der Einsparungen	100		210.000,00

Diese Einsparungsarten sind nicht von der Anzahl der Erhebungen abhängig, d.h. daß bei der doppelten Anzahl von Erhebungen die doppelten Einsparungen entstehen.

Darüber hinaus lassen sich folgende nicht quantifizierte/quantifizierbare Nutzen ausmachen:

1. Standardisierung des Prüfniveaus: keine Diskussionen um die ”Zweckmäßigkeit” eines Prüfmerkmals
2. Standardisierung des Anforderungs- und Zielniveaus: Es können klare Vorgaben gemacht werden, so daß sich die Prüfungen im Verlauf der Zeit auf revisionsähnliche Zufallsprüfungen beschränken lassen
3. Es läßt sich relativ gut ein unternehmensgleiches Datenschutzniveau herstellen
4. Der Prüfkatalog läßt sich leicht anpassen, neu Prüfkriterien lassen sich ebenso leicht einfügen wie nicht mehr gewünschte herausnehmen
5. Durch die klare Dokumentation der Prüfungsergebnisse können Umsetzungsfortschritte leicht verfolgt werden.
6. Durch die Aktivitätenlisten lassen sich klare Verantwortungszuordnungen und Terminverfolgungen wahrnehmen, ohne daß hierzu zusätzliche Arbeit notwendig ist.

Die Beschaffenheit der Shell macht es weiterhin möglich, im Verlauf der Zeit gewünschte Umformulierungen von Fragen und Fragetypen sowie Antworten leicht zu verändern

Quantitatives Ergänzungsmodul (EIS) zum UTAB

Philosophie des Ergänzungsmoduls

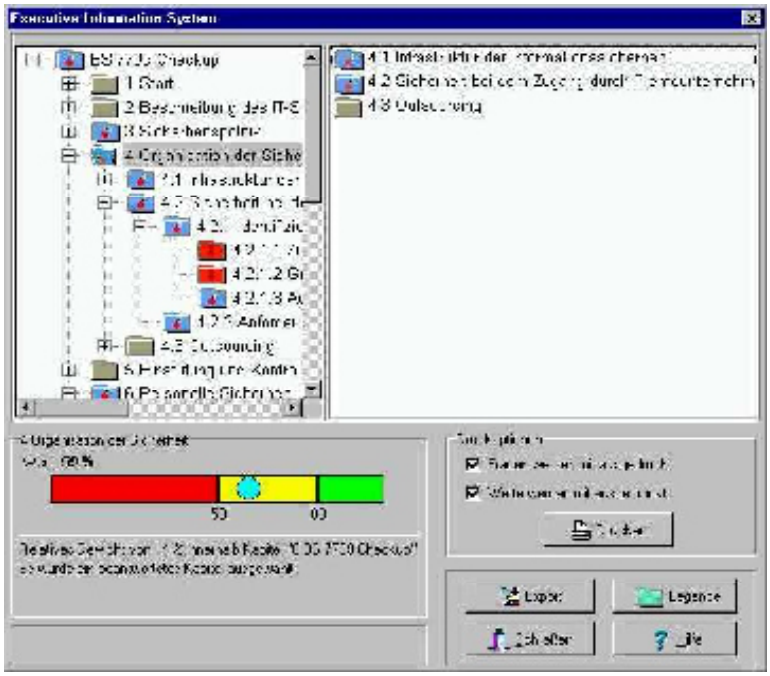
Das EIS besteht aus verschiedenen Programmodulen, die die rein qualitative Ausrichtung des UTAB um eine quantitative Komponente ergänzen. Auch hierbei werden die Teilprozesse

- Analyse/Erhebung
- Auswertung
- Berichtserstellung

in hohem Umfang computergestützt, wobei ein Mehraufwand in der Analyse-/ Erhebungsphase nicht entsteht

Ziel des Systems

- Ergänzung der qualitativen Auswertung um quantitative Inhalte,
- zusammenfassende grafische Darstellung der Erhebungsergebnisse,
- individuelle Interpretationsmöglichkeit der Ergebnisse durch angepaßte Gewichtungen,
- zusammenfassende Bewertung von Erhebungsteilgebieten und Aggregation von unterschiedlichen Erhebungen,
- Vergleich von verschiedenen durchgeführten Analysen.



Ergebnisbewertung

Die Möglichkeit der grafischen Darstellung der Erhebungsergebnisse ermöglicht es dem Fachmann einen schnellen Überblick über die in der Analyse vorgefundenen Situationen zu erhalten und bei einer Ergebnisdurchsprache eine Konzentration auf die besonders wichtigen Punkte vorzunehmen. Die Exportmöglichkeiten in Tabellenform erlaubt eine aggregierte Darstellung der Befragungsergebnisse die einerseits geeignet ist, zusammenfassende

Darstellungen von Analysen zu ermöglichen, aber auch bei entsprechender Weiterbearbeitung mit gängigen Officeprodukten Überblicke über verschiedene Analysen zu geben. Darüber hinaus gestattet die quantitative Komponente auch sowohl ein analyseinternes als auch –übergreifendes Benchmarking.
Natürlich bleiben die bewährten Ergebniskomponenten qualitativer Art

- Status-quo-Bericht mit Positivbefunden und Schwachstellen und
- Maßnahmenempfehlungen für die Schwachstellen

erhalten und können weiter genutzt werden.

Aufbau des Ergänzungsmoduls

Die quantitative Komponente ergänzt alle wichtigen Programmteile des UTAB, wobei folgende zusätzliche Funktionalitäten eingebracht werden:

1. Zu jeder Ebene der Datenbank (Frage, Subkapitel, Kapitel, Gesamtdatenbank) können Grenzen eingegeben werden, die die Ergebnisse in drei Kategorien (gut, ausreichend und ungenügend) einteilen.
2. Alle Kapitel und Fragen können durch ein individuelles Gewicht in Abhängigkeit von ihrer Bedeutung unterschiedlich stark in die Ergebnisdarstellung einfließen.
3. Jede Frage kann als kritische Frage (K.-o.-Kriterium) gekennzeichnet weden. Hierdurch kann aufgezeigt werden, wenn eine unabdingbare Forderung nicht erfüllt wird.
4. Jeder Antwortmöglichkeit kann ein spezifischer individueller Wert zugeordnet werden.
5. Eine Auswertung kann in grafischer/visueller Form durch farbige Unterstützung der Ergebnisdarstellung erfolgen.
6. Die quantitativen Ergebnisse können durch Export in ein Tabellenformat für weitere Auswertung (Aggregationen, Vergleich verschiedener Analysen) anderen Anwendungen

Realisierte Einsatzgebiete

Eine quantitative Komponente wurde von der UIMC u. a. für folgende Einsatzgebiete erarbeitet:

- Datenschutz-Audits/-Checkups gemäß Bundesdatenschutzgesetz
- Informationssystem-Sicherheitsaudits gemäß ISO/IEC 17799

Zusätzlich dazu besteht die Möglichkeit, durch den Einsatz des Tools in den Anwendungsabteilungen der Organisationseinheiten durch diese Analysen selbständig vorzunehmen zu lassen. Hierdurch können einerseits weniger bedeutende Anwendungen dezentral untersucht werden, und bei bedeutenden Anwendungen kann andererseits die durch den Datenschutzbereich durchzuführende Analyse von den Anwendungsabteilungen der Organisationseinheiten vorstrukturiert und somit noch weitere Entlastungen ermöglicht werden.

Einem ”Do-it-yourself” in bezug auf die Konstruktion eines vergleichbaren Programmes stehen folgende Argumente entgegen:

1. Unsere Erfahrungen lassen erwarten, daß die erste Lösung nicht allen Anforderungen entspricht.
2. Der Kauf der Shell ist erheblich kostengünstiger, es sei denn, man will auf Komfort und Funktionalitäten verzichten
3. Durch die UIMC wird eine Wartung, Pflege und Weiterentwicklung garantiert
4. Customizing und Ausbau (z. B. Anreicherung um ein Expertisesystem) würde in Eigenregie wegen der größeren Overheads im EDV-Bereich deutlich teurer werden

Individuelle Füllungsprojekte

Auf Grund des Shell-Charakters des UIMC-Tools ist es möglich, jeden in einem Unternehmen eingesetzten Fragebogen oder jeder Checkliste, die in erster Linie mit geschlossenen Fragen - also solchen mit vorgegebenen Antwortmöglichkeiten - in das Tool einzubringen, und somit die entsprechenden Analysen zu rationalisieren.

Hierbei ist die folgende Vorgehensweise sinnvoll:

1. Workshop mit Projektdefinition und -organisation
2. Erarbeitung der angepassten Erhebungsinhalte (inklusive der Antwortmöglichkeiten)
   Hierbei können zum einen die im Unternehmen sich schon befindenden Frage eingebracht werden, als auch Fragen aus den verschiedenen Kompetenzbereichen der UIMC, die teilweise schon in - für das Tool - aufbereiteter Form vorliegen. Natürlich kann dieser Phase auch dazu genutzt werden, einen vorhandenen Fragebogen in unterschiedlichem Umfang zu bearbeiten.
3. Erstellung der Füllung und Integration in das Tool
4. Test der Tool-Füllung durch exemplarisch vorzunehmende Analysen
5. Einarbeitung der notwendigen Korrekturen und Übergabe in den produktiven Einsatz

Ist neben der rein qualitativen Analyse eine quantitative Auswertung angestrebt, so sind entsprechend die Gewichte und die Grenzen für die verschiedenen Einstufungen festzulegen und in das Tool mit einzubringen.

Neben diesen inhaltlichen Anpassungen des Tools ist es natürlich auch möglich, in einem gewissen Umfang programmtechnische Anpassungen durchzuführen.

Insbesondere ist es möglich, durch die Einbringung eines Unternehmens-Logos die Individualität des Programmes zu dokumentieren und an eine vorgegebene Corporate Identity anzupassen.