

Opportunity and Risk Analysis regarding Outsourcing Contracts

CONTENT

- **Section 1:**
 - **Framework contract on 'Outsourced Domain'**
(Refers to law and deals principally with legal aspects of contract)

- **Section 2:**
 - **Description of services in 'Outsourced Domain'**
(Refers to the object of the contract, deals principally with outsourced service)

- **Section 3:**
 - **Security in the 'Outsourced Domain'**
(Deals with security aspects of the outsourced service)

- **Section 4:**
 - **Auditing of the 'Outsourced Domain' (ex post)**
(Covers co-operation on the auditing procedure between the service provider and the service recipient; refers to all parts of the contract)

*Developed and compiled by J. Krebs, CISA / IG Outsourcing ISACA Switzerland Chapter
@ ISACA Switzerland Chapter 1999*

Section 1: Framework contract for ‘Outsourced Domain’

- **Definitions**
- **Contract management**
 - Object of the contract
 - Contracting parties/contractual relationship
 - Contract duration
 - Contract termination
 - Contract modification (scope of services)
 - Contract validity (merger, take-over, bankruptcy, etc.)
- **Transfer of resources**
 - Licences
 - Human resources
 - Systems, infrastructure
- **Technological changes**
- **Liability and compensation (penalties)**
 - Damages for non-performance
 - Conflict resolution/arbitration board
 - Claims settlement
- **Rights and obligations**
 - DSG [Data Protection Law], PrHG [Product Liability Law], URG [Copyright Law]
 - Banking secrecy legislation/obligation to maintain secrecy/confidentiality
 - Exclusivity
 - Security and auditing
 - Law and place of jurisdiction

Section 1: Framework contract for 'Outsourced Domain',
continued

- **Pricing/payment procedure**
 - Price calculation basis (fair deal)
 - Calculation units
 - Special/Additional expenses
 - Method of payment/payment deadlines

- **Miscellaneous**

Section 2: Description of services in 'Outsourced Domain'

- **Definitions**

- **Description of the service**
 - Definition of service
 - Scope of service
 - Changes in the scope of service

- **Service management**
 - Delimitation of responsibility
 - Service monitoring
 - Support (user/helpdesk, hardware/software)
 - Reporting

- **Service level agreement**
 - Service standards/minimum requirements
 - Response times
 - Workload limits
 - Quality of service
 - Service availability
 - Service flexibility
 - Insurance
 - Back-Up and Archiving of Data

- **Miscellaneous**

Section 3: Security in the 'outsourced domain'

- **Definitions**
- **Contingency planning for disaster/concept for service provider**
- **Contingency planning for disaster/concept for service recipient**
- **Data of service recipient**
 - Data administration and data utilisation**
 - Data protection**
- **Logical access**
 - Security management**
 - Access security**
- **Physical security**
 - Security management**
- **Miscellaneous**

Section 4: Auditing the 'outsourced domain'

- **Definitions**

- **Auditing**
 - External auditors/Internal audit service recipient**
 - Right to audit the service provider**
 - Audit procedure and report (SAS70)**
 - Audit scope and cost compensation**

- **Miscellaneous**

Structure of Checklist

The Checklist is a generic Instrument, i.e. it is a template that has to be adapted by the user for the specific case in question. The columns are as follows:

Nr	Sequence number of questions for reference purposes
Control Objectives	The description is formulated in positive statements ("desired status")
Control Techniques	Contains examples which can be amended by the user
Compliance	Reference to working papers showing results of compliance tests
Risk Evaluation	C Control risk B Business risk L Estimation as low M Estimation as medium H Estimation as high
Comments	Examples and explanations
Report	Reference to other working papers and report